9 Primitive Roots

Introduction

In this chapter, we will investigate the multiplicative structure of the set of integers modulo n, where n is a positive integer. First, we will introduce the concept of the order of an integer modulo n, which is the least power of the integer that leaves a remainder of 1 when it is divided by n. We will study the basic properties of the order of integers modulo n. A positive integer x, such that the powers of x run through all the integers modulo n, where n is a positive integer, is called a primitive root modulo n. We will determine for which integers n there is a primitive root modulo n.

Primitive roots have many uses. For example, when an integer n has a primitive root, discrete logarithms (also called indices) of integers can be defined. These discrete logarithms enjoy many properties analogous to those of logarithms of positive real numbers. Discrete logarithms can be used to simplify computations modulo n.

We will show how the results of this chapter can be used to develop primality tests that are partial converses of Fermat's little theorem. These tests, such as Proth's test, are used extensively to show that numbers of special forms are prime. We will also establish procedures that can be used to certify that an integer is prime.

Finally, we will introduce the concept of the minimal universal exponent modulo n. This is the least exponent U for which $x^U \equiv 1 \pmod{n}$ for all integers x. We will develop a formula for the minimal universal exponent of n, and use this formula to prove some useful results about Carmichael numbers.

9.1 The Order of an Integer and Primitive Roots

In this section, we begin our study of the least positive residues modulo n of powers of an integer a relatively prime to n, where n is a positive integer greater than 1. We will start by studying the *order* of a modulo n, the exponent of the least power of a congruent to 1 modulo n. Then we will study integers a such that the least positive residues of these powers run through all positive integers less than n that are relatively prime to n. Such integers, when they exist, are called *primitive roots* of n. One of our major goals in this chapter will be to determine which positive integers have primitive roots.

The Order of an Integer

By Euler's theorem, if n is a positive integer and if a is an integer relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Therefore, at least one positive integer x satisfies the congruence $a^x \equiv 1 \pmod{n}$. Consequently, by the well-ordering property, there is a least positive integer x satisfying this congruence.

Definition. Let a and n be relatively prime positive integers. Then, the least positive integer x such that $a^x \equiv 1 \pmod{n}$ is called the *order of a modulo n*.

We denote the order of a modulo n by $\text{ord}_n a$. This notation was introduced by Gauss in his *Disquisitiones Arithmeticae* in 1801.

Example 9.1. To find the order of 2 modulo 7, we compute the least positive residues modulo 7 of powers of 2. We find that

$$2^1 \equiv 2 \pmod{7},\ 2^2 \equiv 4 \pmod{7},\ 2^3 \equiv 1 \pmod{7}.$$

Therefore, $\text{ord}_7 2 = 3$.

Similarly, to find the order of 3 modulo 7 we compute

$$3^1 \equiv 3 \pmod{7},\ 3^2 \equiv 2 \pmod{7},\ 3^3 \equiv 6 \pmod{7},$$
$$3^4 \equiv 4 \pmod{7},\ 3^5 \equiv 5 \pmod{7},\ 3^6 \equiv 1 \pmod{7}.$$

We see that $\text{ord}_7 3 = 6$. ◀

To find all solutions of the congruence $a^x \equiv 1 \pmod{n}$, we need the following theorem.

Theorem 9.1. If a and n are relatively prime integers with $n > 0$, then the positive integer x is a solution of the congruence $a^x \equiv 1 \pmod{n}$ if and only if $\text{ord}_n a \mid x$.

Proof. If $\text{ord}_n a \mid x$, then $x = k \cdot \text{ord}_n a$, where k is a positive integer. Hence,

$$a^x = a^{k \cdot \text{ord}_n a} = (a^{\text{ord}_n a})^k \equiv 1 \pmod{n}.$$

Conversely, if $a^x \equiv 1 \pmod{n}$, we first use the division algorithm to write

$$x = q \cdot \text{ord}_n a + r, \quad 0 \leq r < \text{ord}_n a.$$

From this equation, we see that

$$a^x = a^{q \cdot \text{ord}_n a + r} = (a^{\text{ord}_n a})^q a^r \equiv a^r \pmod{n}.$$

Because $a^x \equiv 1 \pmod{n}$, we know that $a^r \equiv 1 \pmod{n}$. From the inequality $0 \leq r < \text{ord}_n a$, we conclude that $r = 0$ because, by definition, $y = \text{ord}_n a$ is the least positive integer such that $a^y \equiv 1 \pmod{n}$. Because $r = 0$, we have $x = q \cdot \text{ord}_n a$. Therefore, $\text{ord}_n a \mid x$. ■

Example 9.2. We can use Theorem 9.1 and Example 9.1 to determine whether $x = 10$ and $x = 15$ are solutions of $2^x \equiv 1 \pmod{7}$. By Example 9.1, we know that $\text{ord}_7 2 = 3$. Because 3 does not divide 10, but 3 divides 15, by Theorem 9.1 we see that $x = 10$ is not a solution of $2^x \equiv 1 \pmod{7}$, but $x = 15$ is a solution of this congruence. ◀

Theorem 9.1 leads to the following corollary.

Corollary 9.1.1. If a and n are relatively prime integers with $n > 0$, then $\text{ord}_n a \mid \phi(n)$.

Proof. Because $(a, n) = 1$, Euler's theorem tells us that

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Using Theorem 9.1, we conclude that $\text{ord}_n a \mid \phi(n)$. ■

We can use Corollary 9.1.1 as a shortcut when we compute orders. The following example illustrates the procedure.

Example 9.3. To find the order of 7 modulo 9, we first note that $\phi(9) = 6$. Because the only positive divisors of 6 are 1, 2, 3, and 6, by Corollary 9.1.1 these are the only possible values of $\text{ord}_9 7$. Because

$$7^1 \equiv 7 \pmod{9}, 7^2 \equiv 4 \pmod{9}, 7^3 \equiv 1 \pmod{9},$$

it follows that $\text{ord}_9 7 = 3$. ◀

Example 9.4. To find the order of 5 modulo 17, we first note that $\phi(17) = 16$. Because the only positive divisors of 16 are 1, 2, 4, 8, and 16, by Corollary 9.1.1 these are the only possible values of $\text{ord}_{17} 5$. Because

$$5^1 \equiv 5 \pmod{17}, 5^2 \equiv 8 \pmod{17}, 5^4 \equiv 13 \pmod{17},$$
$$5^8 \equiv 16 \pmod{17}, 5^{16} \equiv 1 \pmod{17},$$

we conclude that $\text{ord}_{17} 5 = 16$. ◀

The following theorem will be useful in our subsequent discussions.

Theorem 9.2. If a and n are relatively prime integers with $n > 0$, then $a^i \equiv a^j \pmod{n}$, where i and j are nonnegative integers, if and only if $i \equiv j \pmod{\text{ord}_n a}$.

Proof. Suppose that $i \equiv j \pmod{\text{ord}_n a}$ and $0 \leq j \leq i$. Then we have $i = j + k \cdot \text{ord}_n a$, where k is a positive integer. Hence

$$a^i = a^{j+k\cdot\text{ord}_n a} = a^j (a^{\text{ord}_n a})^k \equiv a^j \pmod{n},$$

because $a^{\text{ord}_n a} \equiv 1 \pmod{n}$.

Conversely, assume that $a^i \equiv a^j \pmod{n}$ with $i \geq j$. Because $(a, n) = 1$, we know that $(a^j, n) = 1$. Hence, using Corollary 4.4.1 the congruence

$$a^i \equiv a^j a^{i-j} \equiv a^j \pmod{n}$$

implies, by cancellation of a^j, that

$$a^{i-j} \equiv 1 \pmod{n}.$$

By Theorem 9.1, it follows that $\text{ord}_n a$ divides $i - j$, or equivalently, $i \equiv j \pmod{\text{ord}_n a}$. ∎

The next example illustrates the use of Theorem 9.2.

Example 9.5. Let $a = 3$ and $n = 14$. By Theorem 9.2, we see that $3^5 \equiv 3^{11} \pmod{14}$, but $3^9 \not\equiv 3^{20} \pmod{14}$, because $\phi(14) = 6$ and $5 \equiv 11 \pmod{6}$ but $9 \not\equiv 20 \pmod{6}$. ◀

Primitive Roots

Given an integer n, we are interested in integers a with order modulo n equal to $\phi(n)$, the largest possible order modulo n. As we will show, when such an integer exists, the least positive residues of its powers run through all positive integers relatively prime to n and less than n.

Definition. If r and n are relatively prime integers with $n > 0$ and if $\text{ord}_n r = \phi(n)$, then r is called a *primitive root modulo n*.

Example 9.6. We have previously shown that $\text{ord}_7 3 = 6 = \phi(7)$. Consequently, 3 is a primitive root modulo 7. Likewise, because $\text{ord}_7 5 = 6$, as can easily be verified, 5 is also a primitive root modulo 7. ◀

Euler coined the term *primitive root* in 1773. His purported proof that every prime has a primitive root was incorrect, however. In Section 9.2, we will prove that every prime has a primitive root using the first correct proof of this result by Lagrange in 1769. Gauss also studied primitive roots extensively and provided several additional proofs that every prime has a primitive root.

Not all integers have primitive roots. For instance, there are no primitive roots modulo 8. To see this, note that the only integers less than 8 and relatively prime to 8 are 1, 3, 5, and 7, and $\text{ord}_8 1 = 1$, while $\text{ord}_8 3 = \text{ord}_8 5 = \text{ord}_8 7 = 2$. Because $\phi(8) = 4$, there are no primitive roots modulo 8.

Among the first 30 positive integers, 2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19, 22, 23, 25, 26, 27, and 29 have primitive roots whereas 8, 12, 15, 16, 20, 21, 24, 28, and 30 do not. (The reader can verify this information; see Exercises 3–6 at the end of this section, for example.) What can we conjecture based on this evidence? In this range, every prime has a primitive root (as Lagrange showed), as does every power of an odd prime (since $9 = 3^2$, $25 = 5^2$, and $27 = 3^3$ have primitive roots), but the only power of 2 that has a primitive root is 4. The other integers in this range with a primitive root are 6, 10, 14, 18, 22, and 26. What do these integers have in common? Each is 2 times an odd prime or power of an odd prime. Using this evidence, we conjecture that a positive integer has a primitive root if it equals 2, 4, p^t, or $2p^t$, where p is an odd prime and t is a positive integer. Sections 9.2 and 9.3 are devoted to verifying this conjecture.

To indicate one way in which primitive roots are useful, we give the following theorem.

Theorem 9.3. If r and n are relatively prime positive integers with $n > 0$ and if r is a primitive root modulo n, then the integers

$$r^1, r^2, \ldots, r^{\phi(n)}$$

form a reduced residue set modulo n.

Proof. To demonstrate that the first $\phi(n)$ powers of the primitive root r form a reduced residue set modulo n, we need only show that they are all relatively prime to n and that no two are congruent modulo n.

Because $(r, n) = 1$, it follows from Exercise 14 of Section 3.3 that $(r^k, n) = 1$ for any positive integer k. Hence, these powers are all relatively prime to n. To show that no two of these powers are congruent modulo n, assume that

$$r^i \equiv r^j \pmod{n}.$$

By Theorem 9.2, we see that $i \equiv j \pmod{\phi(n)}$. However, for $1 \leq i \leq \phi(n)$ and $1 \leq j \leq \phi(n)$, the congruence $i \equiv j \pmod{\phi(n)}$ implies that $i = j$. Hence, no two of these powers are congruent modulo n. This shows that we do have a reduced residue system modulo n. ∎

Example 9.7. We see that 2 is a primitive root modulo 9, because $2^2 \equiv 4$, $2^3 \equiv 8$, and $2^6 \equiv 1 \pmod 9$. By Theorem 9.3, the first $\phi(9) = 6$ powers of 2 form a reduced residue system modulo 9. These are $2^1 \equiv 2 \pmod 9$, $2^2 \equiv 4 \pmod 9$, $2^3 \equiv 8 \pmod 9$, $2^4 \equiv 7 \pmod 9$, $2^5 \equiv 5 \pmod 9$, and $2^6 \equiv 1 \pmod 9$. ◀

When an integer possesses a primitive root, it usually has many primitive roots. To demonstrate this, we first prove the following theorem.

Theorem 9.4. If $\text{ord}_n a = t$ and if u is a positive integer, then

$$\text{ord}_n(a^u) = t/(t, u).$$

Proof. Let $s = \text{ord}_n(a^u)$, $v = (t, u)$, $t = t_1 v$, and $u = u_1 v$. By Theorem 3.6, we know that $(t_1, u_1) = 1$.

Because $t_1 = t/(t, u)$, we want to show that $\text{ord}_n(a^u) = t_1$. To do this, we will show that $(a^u)^{t_1} \equiv 1 \pmod{n}$ and that if $(a^u)^s \equiv 1 \pmod{n}$, then $t_1 \mid s$. First, note that

$$(a^u)^{t_1} = (a^{u_1 v})^{(t/v)} = (a^t)^{u_1} \equiv 1 \pmod{n},$$

because $\text{ord}_n a = t$. Hence, Theorem 9.1 tells us that $s \mid t_1$.

On the other hand, because

$$(a^u)^s = a^{us} \equiv 1 \pmod{n},$$

we know that $t \mid us$. Hence, $t_1 v \mid u_1 vs$ and, consequently, $t_1 \mid u_1 s$. Because $(t_1, u_1) = 1$, using Lemma 3.4, we see that $t_1 \mid s$.

Now, because $s \mid t_1$ and $t_1 \mid s$, we conclude that $s = t_1 = t/v = t/(t, u)$. This proves the result. ∎

Example 9.8. By Theorem 9.4, we see that $\text{ord}_7 3^4 = 6/(6, 4) = 6/2 = 3$, because we showed in Example 9.1 that $\text{ord}_7 3 = 6$. ◀

The following corollary of Theorem 9.4 tells us which powers of a primitive root are also primitive roots.

Corollary 9.4.1. Let r be a primitive root modulo n, where n is an integer, $n > 1$. Then r^u is a primitive root modulo n if and only if $(u, \phi(n)) = 1$.

Proof. By Theorem 9.4, we know that

$$\begin{aligned} \text{ord}_n r^u &= \text{ord}_n r/(u, \text{ord}_n r) \\ &= \phi(n)/(u, \phi(n)). \end{aligned}$$

Consequently, $\text{ord}_n r^u = \phi(n)$, and r^u is a primitive root modulo n, if and only if $(u, \phi(n)) = 1$. ∎

This leads immediately to the following theorem.

Theorem 9.5. If the positive integer n has a primitive root, then it has a total of $\phi(\phi(n))$ incongruent primitive roots.

Proof. Let r be a primitive root modulo n. Then Theorem 9.3 tells us that the integers $r, r^2, \ldots, r^{\phi(n)}$ form a reduced residue system modulo n. By Corollary 9.4.1, we know that r^u is a primitive root modulo n if and only if $(u, \phi(n)) = 1$. Because there are exactly $\phi(\phi(n))$ such integers u, there are exactly $\phi(\phi(n))$ primitive roots modulo n. ∎

Example 9.9. Let $n = 11$. Note that 2 is a primitive root modulo 11 (see Exercise 3 at the end of this section). Because 11 has a primitive root, by Theorem 9.5 we know that 11 has $\phi(\phi(11)) = 4$ incongruent primitive roots. Because $\phi(11) = 10$, by the proof of Theorem 9.5 we see that we can find these primitive roots by taking the least nonnegative

residues of $2^1, 2^3, 2^7$, and 2^9, which are 2, 8, 7, and 6, respectively. In other words, the integers 2, 6, 7, 8 form a complete set of incongruent primitive roots modulo 11. ◀

9.1 Exercises

1. Determine the following orders.

   a) $\text{ord}_5 2$ c) $\text{ord}_{13} 10$
   b) $\text{ord}_{10} 3$ d) $\text{ord}_{10} 7$

2. Determine the following orders.

   a) $\text{ord}_{11} 3$ c) $\text{ord}_{21} 10$
   b) $\text{ord}_{17} 2$ d) $\text{ord}_{25} 9$

3. a) Show that 5 is a primitive root of 6.
   b) Show that 2 is a primitive root of 11.

4. Find a primitive root modulo each of the following integers.

   a) 4 d) 13
   b) 5 e) 14
   c) 10 f) 18

5. Show that the integer 12 has no primitive roots.

6. Show that the integer 20 has no primitive roots.

7. How many incongruent primitive roots does 14 have? Find a set of this many incongruent primitive roots modulo 14.

8. How many incongruent primitive roots does 13 have? Find a set of this many incongruent primitive roots modulo 13.

9. Show that if $\overline{a}$ is an inverse of a modulo n, then $\text{ord}_n a = \text{ord}_n \overline{a}$.

10. Show that if n is a positive integer, and a and b are integers relatively prime to n such that $(\text{ord}_n a, \text{ord}_n b) = 1$, then $\text{ord}_n(ab) = \text{ord}_n a \cdot \text{ord}_n b$.

11. What can be said about $\text{ord}_n(ab)$ if a and b are integers relatively prime to n such that $\text{ord}_n a$ and $\text{ord}_n b$ are not necessarily relatively prime?

12. Decide whether it is true that if n is a positive integer and d is a divisor of $\phi(n)$, then there is an integer a with $\text{ord}_n a = d$. Give reasons for your answer.

13. Show that if a is an integer relatively prime to the positive integer m and $\text{ord}_m a = st$, then $\text{ord}_m a^t = s$.

14. Show if m is a positive integer and a is an integer relatively prime to m such that $\text{ord}_m a = m - 1$, then m is prime.

15. Show that r is a primitive root modulo the odd prime p if and only if r is an integer with $(r, p) = 1$ such that

$$r^{(p-1)/q} \not\equiv 1 \pmod{p}$$

for all prime divisors q of $p - 1$.

16. Show that if r is a primitive root modulo the positive integer m, then $\bar{r}$ is also a primitive root modulo m, if $\bar{r}$ is an inverse of r modulo m.

17. Show that $\text{ord}_{F_n} 2 \leq 2^{n+1}$, where $F_n = 2^{2^n} + 1$, is the nth Fermat number.

* 18. Let p be a prime divisor of the Fermat number $F_n = 2^{2^n} + 1$.
    a) Show that $\text{ord}_p 2 = 2^{n+1}$.
    b) From part (a), conclude that $2^{n+1} \mid (p-1)$, so that p must be of the form $2^{n+1}k + 1$.

19. Let $m = a^n - 1$, where a and n are positive integers. Show that $\text{ord}_m a = n$, and conclude that $n \mid \phi(m)$.

* 20. a) Show that if p and q are distinct odd primes, then pq is a pseudoprime to the base 2 if and only if $\text{ord}_q 2 \mid (p-1)$ and $\text{ord}_p 2 \mid (q-1)$.
    b) Use part (a) to decide which of the following integers are pseudoprimes to the base 2: $13 \cdot 67, 19 \cdot 73, 23 \cdot 89, 29 \cdot 97$.

* 21. Show that if p and q are distinct odd primes, then pq is a pseudoprime to the base 2 if and only if $M_p M_q = (2^p - 1)(2^q - 1)$ is a pseudoprime to the base 2.

There is an iterative method known as the *cycling attack* for decrypting messages that were encrypted by an RSA cipher, without knowledge of the decrypting key. Suppose that the public key (e, n) used for encrypting is known, but the decrypting key (d, n) is not. To decrypt a ciphertext block C, we form a sequence $C_1, C_2, C_3, \ldots$, setting $C_1 \equiv C^e \pmod{n}$, $0 < C_1 < n$, and $C_{j+1} \equiv C_j^e \pmod{n}$, $0 < C_{j+1} < n$ for $j = 1, 2, 3, \ldots$.

22. Show that $C_j \equiv C^{e^j} \pmod{n}$, $0 < C_j < n$.

23. Show that there is an index j such that $C_j = C$ and $C_{j-1} = P$, where P is the original plaintext message. Show that this index j is a divisor of $\text{ord}_{\phi(n)} e$.

24. Let $n = 47 \cdot 59$ and $e = 17$. Using iteration, find the plaintext corresponding to the ciphertext 1504.

(*Note:* This iterative method for attacking RSA ciphers is seldom successful in a reasonable amount of time. Moreover, the primes p and q may be chosen so that this attack is almost always futile. See Exercise 19 of Section 9.2.)

9.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find $\text{ord}_{52,579} 2$, $\text{ord}_{52,579} 3$, and $\text{ord}_{52,579} 1001$.
2. Find as many integers as you can for which 2 is a primitive root. Do you think that there are infinitely many such integers?

Programming Projects

Write projects using Maple, *Mathematica,* or a language of your choice to do the following.

1. Find the order of a modulo m, when a and m are relatively prime positive integers.

2. Find primitive roots when they exist.
3. Attempt to decrypt RSA ciphers by iteration (see the preamble to Exercise 22).

9.2 Primitive Roots for Primes

In this and the following section, our objective is to determine which integers have primitive roots. In this section, we show that every prime has a primitive root. To do this, we first need to study polynomial congruences.

Let $f(x)$ be a polynomial with integer coefficients. We say that an integer c is a *root of* $f(x)$ *modulo* m if $f(c) \equiv 0 \pmod{m}$. It is easy to see that if c is a root of $f(x)$ modulo m, then every integer congruent to c modulo m is also a root.

Example 9.10. The polynomial $f(x) = x^2 + x + 1$ has exactly two incongruent roots modulo 7, namely $x \equiv 2 \pmod{7}$ and $x \equiv 4 \pmod{7}$. ◀

Example 9.11. The polynomial $g(x) = x^2 + 2$ has no roots modulo 5. ◀

Example 9.12. Fermat's little theorem tells us that if p is prime, then the polynomial $h(x) = x^{p-1} - 1$ has exactly $p - 1$ incongruent roots modulo p, namely $x \equiv 1, 2, 3, \ldots, p - 1 \pmod{p}$. ◀

We will need the following important theorem concerning roots of polynomials modulo p where p is a prime.

Theorem 9.6. ***Lagrange's Theorem.*** Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial of degree n, $n \geq 1$, with integer coefficients and with leading coefficient a_n not divisible by p. Then $f(x)$ has at most n incongruent roots modulo p.

Proof. We use mathematical induction to prove the theorem. When $n = 1$, we have $f(x) = a_1 x + a_0$ with $p \nmid a_1$. A root of $f(x)$ modulo p is a solution of the linear congruence $a_1 x \equiv -a_0 \pmod{p}$. By Theorem 4.10, because $(a_1, p) = 1$, this linear congruence has exactly one solution, so that there is exactly one root modulo p of $f(x)$. Clearly, the theorem is true for $n = 1$.

Now, suppose that the theorem is true for polynomials of degree $n - 1$, and let $f(x)$ be a polynomial of degree n with leading coefficient not divisible by p. Assume that the polynomial $f(x)$ has $n + 1$ incongruent roots modulo p, say $c_0, c_1, \ldots, c_n$, so that $f(c_k) \equiv 0 \pmod{p}$ for $k = 0, 1, \ldots, n$. We have

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) \\ &\quad + a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + xc_0^{n-3} + c_0^{n-2}) \\ &\quad + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

where $g(x)$ is a polynomial of degree $n-1$ with leading coefficient a_n. We now show that $c_1, c_2, \ldots, c_n$ are all roots of $g(x)$ modulo p. Let k be an integer, $1 \leq k \leq n$. Because $f(c_k) \equiv f(c_0) \equiv 0 \pmod{p}$, we have

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod{p}.$$

It follows that $g(c_k) \equiv 0 \pmod{p}$, because $c_k - c_0 \not\equiv 0 \pmod{p}$. Hence, c_k is a root of $g(x)$ modulo p. This shows that the polynomial $g(x)$, which is of degree $n-1$ and has a leading coefficient not divisible by p, has n incongruent roots modulo p. This contradicts the induction hypothesis. Hence, $f(x)$ must have no more than n incongruent roots modulo p. The induction argument is complete. ∎

We use Lagrange's theorem to prove the following result.

Theorem 9.7. Let p be prime and let d be a divisor of $p-1$. Then the polynomial $x^d - 1$ has exactly d incongruent roots modulo p.

Proof. Let $p - 1 = de$. Then

$$\begin{aligned} x^{p-1} - 1 &= (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) \\ &= (x^d - 1)g(x). \end{aligned}$$

From Fermat's little theorem, we see that $x^{p-1} - 1$ has $p-1$ incongruent roots modulo p. Furthermore, any root of $x^{p-1} - 1$ modulo p is either a root of $x^d - 1$ modulo p or a root of $g(x)$ modulo p.

Lagrange's theorem tells us that $g(x)$ has at most $d(e-1) = p - d - 1$ roots modulo p. Because every root of $x^{p-1} - 1$ modulo p that is not a root of $g(x)$ modulo p must be a root of $x^d - 1$ modulo p, we know that the polynomial $x^d - 1$ has at least $(p-1) - (p-d-1) = d$ incongruent roots modulo p. On the other hand, Lagrange's theorem tells us that it has at most d incongruent roots modulo p. Consequently, $x^d - 1$ has precisely d incongruent roots modulo p. ∎

Theorem 9.7 can be used to prove a useful result that tells us how many incongruent integers have a given order modulo p. Before proving this result, we present a lemma needed for its proof.

Lemma 9.1. Let p be a prime and let d be a positive divisor of $p-1$. Then the number of positive integers less than p of order d modulo p does not exceed $\phi(d)$.

Proof. For each positive integer d dividing $p-1$, let $F(d)$ denote the number of positive integers of order d modulo p that are less than p.

If $F(d) = 0$, it is clear that $F(d) \leq \phi(d)$. Otherwise, there is an integer a of order d modulo p. Because $\operatorname{ord}_p a = d$, the integers

$$a, a^2, \ldots, a^d$$

are incongruent modulo p. Furthermore, each of these powers of a is a root of $x^d - 1$ modulo p, because $(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$ for all positive integers k. By Theorem

9.7, we know that $x^d - 1$ has exactly d incongruent roots modulo p, so every root modulo p is congruent to one of these powers of a. However, by Theorem 9.4, we know that the powers of a with order d are those of the form a^k with $(k, d) = 1$. There are exactly $\phi(d)$ such integers k with $1 \leq k \leq d$, and consequently, if there is one element of order d modulo p, there must be exactly $\phi(d)$ such positive integers less than d. Hence, $F(d) \leq \phi(d)$. ∎

We now can determine how many incongruent integers can have a given order modulo p.

Theorem 9.8. Let p be a prime and let d be a positive divisor of $p - 1$. Then the number of incongruent integers of order d modulo p is equal to $\phi(d)$.

Proof. For each positive integer d dividing $p - 1$, let $F(d)$ denote the number of positive integers of order d modulo p that are less than p. Because the order modulo p of an integer not divisible by p divides $p - 1$, it follows that

$$p - 1 = \sum_{d|p-1} F(d).$$

By Theorem 7.7, we know that

$$p - 1 = \sum_{d|p-1} \phi(d).$$

By Lemma 9.1, $F(d) \leq \phi(d)$ when $d \mid (p - 1)$. This inequality, together with the equality

$$\sum_{d|p-1} F(d) = \sum_{d|p-1} \phi(d),$$

implies that $F(d) = \phi(d)$ for each positive divisor d of $p - 1$.

Therefore, we can conclude that $F(d) = \phi(d)$, which tells us that there are precisely $\phi(d)$ incongruent integers of order d modulo p. ∎

The following corollary is derived immediately from Theorem 9.8.

Corollary 9.8.1. Every prime has a primitive root.

Proof. Let p be a prime. By Theorem 9.7, we know that there are $\phi(p - 1)$ incongruent integers of order $p - 1$ modulo p. Because each of these is, by definition, a primitive root, p has $\phi(p - 1)$ primitive roots. ∎

The smallest positive primitive root of each prime less than 1000 is given in Table 3 of Appendix E; looking at the table, we see that 2 is the least primitive root of many primes p. Is 2 a primitive root for infinitely many primes? The answer to this question is not known, and it is also unknown when we replace 2 by an integer other than ± 1 or a perfect square. Evidence suggests the truth of the following conjecture made by *Emil Artin*.

Artin's conjecture. The integer a is a primitive root of infinitely many primes if $a \neq \pm 1$ and a is not a perfect square.

Although Artin's conjecture has not been settled, there are some interesting partial results. For example, one consequence of work by Roger Heath-Brown is that there are at most two primes and three positive square-free integers a such that a is a primitive root of only finitely many primes. One implication of this work is that at least one of the integers 2, 3, and 5 is a primitive root for infinitely many primes.

Many mathematicians have studied the problem of determining bounds on g_p, the smallest primitive root for a prime p. Among the results that have been proved are that

$$g_p > C \log p$$

for some constant C and infinitely many primes p. This result, proved by Fridlender (in 1949), and independently by Salié (in 1950), shows that there are infinitely many primes where the least primitive root is larger than any particular positive integer. However, g_p does not grow very quickly. Grosswald showed (in 1981) that if p is a prime with $p > e^{e^{24}}$, then $g_p < p^{0.499}$. Another interesting result, proved in the problems section of the *American Mathematical Monthly* in 1984, is that for every positive integer M, there are infinitely many primes p such that $M < g_p < p - M$.

9.2 Exercises

1. Find the number of incongruent roots modulo 11 of each of the following polynomials.

   a) $x^2 + 2$ c) $x^3 + x^2 + 2x + 2$
   b) $x^2 + 10$ d) $x^4 + x^2 + 1$

EMIL ARTIN (1898–1962) was born in Vienna, Austria. He served in the Austrian army during World War I. In 1921, he received a Ph.D. from the University of Leipzig, which he attended both as an undergraduate and as a graduate student. He attended the University of Göttingen from 1922 until 1923. In 1923, he was appointed to a position at the University of Hamburg. Artin was forced to leave Germany in 1937 as a result of Nazi regulations because his wife was Jewish, although he was not. He emigrated to the United States, where he taught at Notre Dame University (1937–1938), Indiana University (1938–1946), and Princeton University (1946–1958). He returned to Germany, taking a position at the University of Hamburg, in 1958.

Artin made major contributions to several areas of abstract algebra, including ring theory and group theory. He also invented the concept of braids structures, defined using the concept of strings woven to form braids, now studied by topologists and algebraists. Artin made major contributions to both analytic and algebraic number theory, beginning with his research involving quadratic fields.

Artin excelled as a teacher and advisor of students. He was also a talented musician who played the harpsichord, clavichord, and flute and was a devotee of old music.

2. Find the number of incongruent roots modulo 13 of each of the following polynomials.

   a) $x^2 + 1$ c) $x^3 + 12$
   b) $x^2 + 3x + 2$ d) $x^4 + x^2 + x + 1$

3. Find the number of primitive roots of each of the following primes.

   a) 7 d) 19
   b) 13 e) 29
   c) 17 f) 47

4. Find a complete set of incongruent primitive roots of 7.

5. Find a complete set of incongruent primitive roots of 13.

6. Find a complete set of incongruent primitive roots of 17.

7. Find a complete set of incongruent primitive roots of 19.

8. Let r be a primitive root of the prime p with $p \equiv 1 \pmod 4$. Show that $-r$ is also a primitive root.

9. Show that if p is a prime and $p \equiv 1 \pmod 4$, there is an integer x such that $x^2 \equiv -1 \pmod p$. (*Hint:* Use Theorem 9.8 to show that there is an integer x of order 4 modulo p.)

10. a) Find the number of incongruent roots modulo 6 of the polynomial $x^2 - x$.
    b) Explain why the answer to part (a) does not contradict Lagrange's theorem.

11. a) Use Lagrange's theorem to show that if p is a prime and $f(x)$ is a polynomial of degree n with integer coefficients and more than n roots modulo p, then p divides every coefficient of $f(x)$.
    b) Let p be prime. Using part (a), show that every coefficient of the polynomial $f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$ is divisible by p.
    c) Using part (b), give a proof of Wilson's theorem (Theorem 6.1). (*Hint:* Consider the constant term of $f(x)$.)

12. Find the least positive residue of the product of a set of $\phi(p-1)$ incongruent primitive roots modulo a prime p.

* 13. A systematic method for constructing a primitive root modulo a prime p is outlined in this problem. Let the prime factorization of $\phi(p) = p - 1$ be $p - 1 = q_1^{t_1} q_2^{t_2} \cdots q_r^{t_r}$, where $q_1, q_2, \ldots, q_r$ are prime.
    a) Use Theorem 9.8 to show that there are integers $a_1, a_2, \ldots, a_r$ such that $\operatorname{ord}_p a_1 = q_1^{t_1}$, $\operatorname{ord}_p a_2 = q_2^{t_2}, \ldots, \operatorname{ord}_p a_r = q_r^{t_r}$.
    b) Use Exercise 10 of Section 9.1 to show that $a = a_1 a_2 \cdots a_r$ is a primitive root modulo p.
    c) Follow the procedure outlined in parts (a) and (b) to find a primitive root modulo 29.

* 14. Suppose that the composite positive integer n has prime-power factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Show that the number of incongruent bases modulo n for which n is a pseudoprime to that base is $\prod_{j=1}^{r} (n-1, p_j - 1)$.

15. Use Exercise 14 to show that every odd composite integer that is not a power of 3 is a pseudoprime to at least two bases other than ± 1.

16. Show that if p is prime and $p = 2q + 1$, where q is an odd prime and a is a positive integer with $1 < a < p - 1$, then $p - a^2$ is a primitive root modulo p.

* 17. a) Suppose that $f(x)$ is a polynomial with integer coefficients of degree $n - 1$. Let $x_1, x_2, \ldots, x_n$ be n incongruent integers modulo p. Show that for all integers x, the congruence

$$f(x) \equiv \sum_{j=1}^{n} f(x_j) \prod_{\substack{i=1 \\ i \neq j}}^{n} (x - x_i)\overline{(x_j - x_i)} \pmod{p}$$

holds, where $\overline{x_j - x_i}$ is an inverse of $x_j - x_i$ modulo p. This technique for finding $f(x)$ modulo p is called *Lagrange interpolation.*

b) Find the least positive residue of $f(5)$ modulo 11 if $f(x)$ is a polynomial of degree 3 with $f(1) \equiv 8$, $f(2) \equiv 2$, and $f(3) \equiv 4 \pmod{11}$.

18. In this exercise, we develop a threshold scheme for protection of master keys in a computer system, different from the scheme discussed in Section 8.6. Let $f(x)$ be a randomly chosen polynomial of degree $r - 1$, with the condition that K, the master key, is the constant term of the polynomial. Let p be a prime, such that $p > K$ and $p > s$. The s shadows $k_1, k_2, \ldots, k_s$ are computed by finding the least positive residue of $f(x_j)$ modulo p for $j = 1, 2, \ldots, s$, where $x_1, x_2, \ldots, x_s$ are randomly chosen integers incongruent modulo p; that is,

$$k_j \equiv f(x_j) \pmod{p}, \quad 0 \leq k_j < p,$$

for $j = 1, 2, \ldots, s$.

a) Use Lagrange interpolation, described in Exercise 17, to show that the master key K can be determined from any r shadows.

b) Show that the master key K cannot be determined from fewer than r shadows.

c) Let $K = 33$, $p = 47$, $r = 4$, and $s = 7$. Let $f(x) = 4x^3 + x^2 + 31x + 33$. Find the seven shadows corresponding to the values of $f(x)$ at 1, 2, 3, 4, 5, 6, 7.

d) Show how to find the master key from the four shadows $f(1)$, $f(2)$, $f(3)$, and $f(4)$.

19. Show that an RSA cipher with encrypting modulus $n = pq$ is resistant to the cycling attack (see the preamble to Exercise 22 of Section 9.1) if $p - 1$ and $q - 1$ have large prime factors p' and q', respectively, and $p' - 1$ and $q' - 1$ have large prime factors p'' and q'', respectively.

9.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find the least primitive root for each of the primes 10,007, 10,009, and 10,037.

2. Erdős has asked whether for each sufficiently large prime p there is a prime q for which q is a primitive root of p. What evidence can you find for this conjecture? For which small primes p is the statement in the conjecture false?

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Given a prime p, use Exercise 13 to find a primitive root of p.
2. Implement the threshold scheme given in Exercise 18.

9.3 The Existence of Primitive Roots

In the previous section, we showed that every prime has a primitive root. In this section, we will find all positive integers having primitive roots. First, we will show that every power of an odd prime possesses a primitive root.

Primitive Roots Modulo p^2, p Prime The first step in showing that every power of an odd prime has a primitive root is to show that every square of an odd prime has a primitive root.

Theorem 9.9. If p is an odd prime with primitive root r, then either r or $r + p$ is a primitive root modulo p^2.

Proof. Because r is a primitive root modulo p, we know that

$$\text{ord}_p r = \phi(p) = p - 1.$$

Let $n = \text{ord}_{p^2} r$, so that

$$r^n \equiv 1 \pmod{p^2}.$$

Because a congruence modulo p^2 obviously holds modulo p, we have

$$r^n \equiv 1 \pmod{p}.$$

By Theorem 9.1, because $p - 1 = \text{ord}_p r$, it follows that

$$p - 1 \mid n.$$

On the other hand, Corollary 9.1.1 tells us that

$$n \mid \phi(p^2).$$

Because $\phi(p^2) = p(p - 1)$, this implies that $n \mid p(p - 1)$. Because $n \mid p(p - 1)$ and $p - 1 \mid n$, either $n = p - 1$ or $n = p(p - 1)$. If $n = p(p - 1)$, then r is a primitive root modulo p^2, because $\text{ord}_{p^2} r = \phi(p^2)$. Otherwise, we have $n = p - 1$, so that

$$r^{p-1} \equiv 1 \pmod{p^2}. \tag{9.1}$$

Let $s = r + p$. Then, because $s \equiv r \pmod{p}$, s is also a primitive root modulo p. Hence, $\text{ord}_{p^2} s$ equals either $p - 1$ or $p(p - 1)$. We will show that $\text{ord}_{p^2} s = p(p - 1)$ by eliminating the possibility that $\text{ord}_{p^2} s = p - 1$.

To show that $\text{ord}_{p^2} s \neq p-1$, first note that by the binomial theorem we have

$$s^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2} r^{p-3}p^2 + \cdots + p^{p-1}$$
$$\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \pmod{p^2}.$$

Hence, using (9.1), we see that

$$s^{p-1} \equiv 1 + (p-1)p \cdot r^{p-2} \equiv 1 - pr^{p-2} \pmod{p^2}.$$

From this last congruence, we can show that

$$s^{p-1} \not\equiv 1 \pmod{p^2}.$$

To see this, note that if $s^{p-1} \equiv 1 \pmod{p^2}$, then $pr^{p-2} \equiv 0 \pmod{p^2}$. This last congruence implies that $r^{p-2} \equiv 0 \pmod{p}$, which is impossible because $p \nmid r$ (remember that r is a primitive root of p).

Because $\text{ord}_{p^2} s \neq p-1$, we can conclude that $\text{ord}_{p^2} s = p(p-1) = \phi(p^2)$. Consequently, $s = r + p$ is a primitive root of p^2. ■

Example 9.13. The prime $p = 7$ has $r = 3$ as a primitive root. Using observations made in the proof of Theorem 9.9, either $\text{ord}_{49}3 = 6$ or $\text{ord}_{49}3 = 42$. However,

$$r^{p-1} = 3^6 \not\equiv 1 \pmod{49}.$$

It follows that $\text{ord}_{49}3 = 42$. Hence 3 is also a primitive root of $p^2 = 49$. ◄

We note that it is extremely rare for the congruence

$$r^{p-1} \equiv 1 \pmod{p^2}$$

to hold when r is a primitive root modulo the prime p. Consequently, it is very seldom that a primitive root r modulo the prime p is not also a primitive root modulo p^2. When this occurs, Theorem 9.9 tell us that $r + p$ is a primitive root modulo p^2. The following example illustrates this.

Example 9.14. Let $p = 487$. For the primitive root 10 modulo 487, we have

$$10^{486} \equiv 1 \pmod{487^2}.$$

Hence, 10 is not a primitive root modulo 487^2 but, by Theorem 9.9, we know that $497 = 10 + 487$ is a primitive root modulo 487^2. ◄

Primitive Roots Modulo p^k, p Prime and k a Positive Integer Next, we show that artibrary powers of odd primes have primitive roots.

Theorem 9.10. Let p be an odd prime. Then p^k has a primitive root for all positive integers k. Moreover, if r is a primitive root modulo p^2, then r is a primitive root modulo p^k, for all positive integers k.

Proof. By Theorem 9.9, we know that p has a primitive root r that is also a primitive root modulo p^2, so that

$$r^{p-1} \not\equiv 1 \pmod{p^2}. \tag{9.2}$$

Using mathematical induction, we will prove that for this primitive root r,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k} \tag{9.3}$$

for all positive integers k, $k \geq 2$.

Once we have established congruence, we can show that r is also a primitive root modulo p^k by the following reasoning. Let

$$n = \operatorname{ord}_{p^k} r.$$

By Theorem 8.1, we know that $n \mid \phi(p^k)$. By Theorem 7.3, we have $\phi(p^k) = p^{k-1}(p-1)$. Hence, $r \mid p^k(p-1)$. On the other hand, because

$$r^n \equiv 1 \pmod{p^k},$$

we also know that

$$r^n \equiv 1 \pmod{p}.$$

By Theorem 9.1, since $\phi(p) = p - 1$ we see that $p - 1 \mid n$. Because $p - 1 \mid n$, and $n \mid p^{k-1}(p-1)$, we know that $n = p^t(p-1)$, where t is an integer such that $0 \leq t \leq k-1$. If $n = p^t(p-1)$ with $t \leq k-2$, then

$$r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv 1 \pmod{p^k},$$

which would contradict (9.3). Hence, $\operatorname{ord}_{p^k} r = p^{k-1}(p-1) = \phi(p^k)$. Consequently, r is also a primitive root modulo p^k.

All that remains is to prove (9.3) using mathematical induction. The case of $k = 2$ follows from (9.2). Let us assume that the assertion is true for the positive integer $k \geq 2$. Then

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Because $(r, p) = 1$, we know that $(r, p^{k-1}) = 1$. Consequently, from Euler's theorem, we know that

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}.$$

Therefore, there is an integer d such that

$$r^{p^{k-2}(p-1)} = 1 + dp^{k-1},$$

where $p \nmid d$, because by hypothesis $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. We take the pth power of both sides of the above equation to obtain, via the binomial theorem and using the hypothesis that p is odd,

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (1+dp^{k-1})^p \\ &= 1 + p(dp^{k-1}) + \binom{p}{2}(dp^{k-1})^2 + \cdots + (dp^{k-1})^p \\ &\equiv 1 + dp^k \pmod{p^{k+1}}. \end{aligned}$$

Because $p \nmid d$, we can conclude that

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}.$$

This completes the proof by induction. ∎

Example 9.15. By Example 9.13, we know that $r = 3$ is a primitive root modulo 7 and 7^2. Hence, Theorem 9.10 tells us that $r = 3$ is also a primitive root modulo 7^k for all positive integers k. ◀

Primitive Roots and Powers of 2 It is now time to discuss whether there are primitive roots modulo powers of 2. We first note that both 2 and $2^2 = 4$ have primitive roots, namely 1 and 3, respectively. For higher powers of 2, the situation is different, as the following theorem shows; there are no primitive roots modulo these powers of 2.

Theorem 9.11. If a is an odd integer, and if k is an integer, $k \geq 3$, then

$$a^{\phi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Proof. We prove this result using mathematical induction. If a is an odd integer, then $a = 2b + 1$, where b is an integer. Hence,

$$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1.$$

Because either b or $b + 1$ is even, we see that $8 \mid 4b(b+1)$. By Exercise 5 of Section 4.1, it follows that

$$a^2 \equiv 1 \pmod{8}.$$

This is the congruence of interest when $k = 3$.

Now, to complete the induction argument, let us assume that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Then there is an integer d such that

$$a^{2^{k-2}} = 1 + d \cdot 2^k.$$

Squaring both sides of the above equality, we obtain

$$a^{2^{k-1}} = 1 + d2^{k+1} + d^2 2^{2k}.$$

This yields

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}},$$

which completes the induction argument. ∎

Theorem 9.11 tells us that no power of 2, other than 2 and 4, has a primitive root, because when a is an odd integer, $\text{ord}_{2^k} a \neq \phi(2^k)$, because $a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$.

Even though there are no primitive roots modulo 2^k for $k \geq 3$, there always is an element of largest possible order, namely $\phi(2^k)/2$, as the following theorem shows.

Theorem 9.12. Let $k \geq 3$ be an integer. Then

$$\text{ord}_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}.$$

Proof. Theorem 9.11 tells us that

$$5^{2^{k-2}} \equiv 1 \pmod{2^k},$$

for $k \geq 3$. By Theorem 9.1, we see that $\text{ord}_{2^k} 5 \mid 2^{k-2}$. Therefore, if we show that $\text{ord}_{2^k} 5 \nmid 2^{k-3}$, we can conclude that

$$\text{ord}_{2^k} 5 = 2^{k-2}.$$

To show that $\text{ord}_{2^k} 5 \nmid 2^{k-3}$, we will prove by mathematical induction that, for $k \geq 3$,

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \pmod{2^k}.$$

For $k = 3$, we have

$$5 \equiv 1 + 4 \pmod{8}.$$

Now, we assume that

$$5^{2^{k-3}} \equiv 1 + 2^{k-1} \pmod{2^k}.$$

This means that there is a positive integer d such that

$$5^{2^{k-3}} = (1 + 2^{k-1}) + d2^k.$$

Squaring both sides, we find that

$$5^{2^{k-2}} = (1 + 2^{k-1})^2 + 2(1 + 2^{k-1})d2^k + (d2^k)^2,$$

so that

$$5^{2^{k-2}} \equiv (1 + 2^{k-1})^2 = 1 + 2^k + 2^{2k-2} \equiv 1 + 2^k \pmod{2^{k+1}}.$$

This completes the induction argument and shows that

$$\text{ord}_{2^k} 5 = \phi(2^k)/2.$$

■

Primitive Roots Modulo Integers Not Prime Powers We have now demonstrated that all powers of odd primes possess primitive roots, while the only powers of 2 having primitive roots are 2 and 4. Next, we determine which integers not powers of primes—that is, those integers divisible by two or more primes—have primitive roots. We will demonstrate that the only positive integers not powers of primes that possess primitive roots are twice powers of odd primes.

We first narrow the set of positive integers that we must consider with the following result.

Theorem 9.13. If n is a positive integer that is not a prime power or twice a prime power, then n does not have a primitive root.

Proof. Let n be a positive integer with prime-power factorization

$$n = p_1^{t_1} p_2^{t_1} \cdots p_m^{t_m}.$$

Let us assume that the integer n has a primitive root r. This means that $(r, n) = 1$ and $\text{ord}_n r = \phi(n)$. Because $(r, n) = 1$, we know that $(r, p^t) = 1$, whenever p^t is one of the prime powers occurring in the factorization of n. By Euler's theorem, we know that

$$r^{\phi(p^t)} \equiv 1 \pmod{p^t}.$$

Now, let U be the least common multiple of $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})$, that is,

$$U = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})].$$

Because $\phi(p_i^{t_i}) \mid U$, we know that

$$r^U \equiv 1 \pmod{p_i^{t_i}}$$

for $i = 1, 2, \ldots, m$. Using the Chinese remainder theorem, it now follows that

$$r^U \equiv 1 \pmod{n},$$

which implies that

$$\text{ord}_n r = \phi(n) \leq U.$$

By Theorem 7.4, because ϕ is multiplicative, we have

$$\phi(n) = \phi(p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}) = \phi(p_1^{t_1})\phi(p_2^{t_2}) \cdots \phi(p_m^{t_m}).$$

This formula for $\phi(n)$ and the inequality $\phi(n) \leq U$ imply that

$$\phi(p_1^{t_1})\phi(p_2^{t_2}) \cdots \phi(p_m^{t_m}) \leq [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})].$$

Because the product of a set of integers is less than or equal to their least common multiple only if the integers are pairwise relatively prime (and then the "less than or equal to" relation is really just an equality), the integers $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})$ must be pairwise relatively prime.

We note that $\phi(p^t) = p^{t-1}(p-1)$, so that $\phi(p^t)$ is even if p is odd, or if $p = 2$ and $t \geq 2$. Hence, the numbers $\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})$ are not pairwise relatively prime unless $m = 1$ and n is a prime power, or $m = 2$ and $n = 2p^t$, where p is an odd prime and t is a positive integer. ∎

We have now limited our consideration to integers of the form $n = 2p^t$, where p is an odd prime and t is a positive integer. We now show that all such integers have primitive roots.

Theorem 9.14. If p is an odd prime and t is a positive integer, then $2p^t$ possesses a primitive root. In fact, if r is a primitive root modulo p^t, then if r is odd, it is also a primitive root modulo $2p^t$; whereas if r is even, $r + p^t$ is a primitive root modulo $2p^t$.

Proof. If r is a primitive root modulo p^t, then

$$r^{\phi(p^t)} \equiv 1 \pmod{p^t},$$

and no positive exponent smaller than $\phi(p^t)$ has this property. By Theorem 7.4, we note that $\phi(2p^t) = \phi(2)\phi(p^t) = \phi(p^t)$, so that $r^{\phi(2p^t)} \equiv 1 \pmod{p^t}$.

If r is odd, then

$$r^{\phi(2p^t)} \equiv 1 \pmod{2}.$$

Thus, by Corollary 4.8.1, we see that $r^{\phi(2p^t)} \equiv 1 \pmod{2p^t}$. No smaller power of r is congruent to 1 modulo $2p^t$. Such power would also be congruent to 1 modulo p^t, contradicting the assumption that r is a primitive root of p^t. It follows that r is a primitive root modulo $2p^t$.

On the other hand, if r is even, then $r + p^t$ is odd. Hence,

$$(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2}.$$

Because $r + p^t \equiv r \pmod{p^t}$, we see that

$$(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{p^t}.$$

Therefore, $(r + p^t)^{\phi(2p^t)} \equiv 1 \pmod{2p^t}$, and as no smaller power of $r + p^t$ is congruent to 1 modulo $2p^t$, we see that $r + p^t$ is a primitive root modulo $2p^t$. ∎

Example 9.16. Earlier in this section we showed that 3 is a primitive root modulo 7^t for all positive integers t. Hence, because 3 is odd, Theorem 9.14 tells us that 3 is also a primitive root modulo $2 \cdot 7^t$ for all positive integers t. For instance, 3 is a primitive root modulo 14.

Similarly, we know that 2 is a primitive root modulo 5^t for all positive integers t. Because $2 + 5^t$ is odd, Theorem 9.14 tells us that $2 + 5^t$ is a primitive root modulo $2 \cdot 5^t$ for all positive integers t. For example, 27 is a primitive root modulo 50. ◀

Putting Everything Together Combining Corollary 9.8.1 and Theorems 9.10, 9.13, and 9.14, we can now describe which positive integers have a primitive root.

Theorem 9.15. The positive integer n, $n > 1$, possesses a primitive root if and only if

$$n = 2, 4, p^t, \text{ or } 2p^t,$$

where p is an odd prime and t is a positive integer.

9.3 Exercises

1. Which of the integers 4, 10, 16, 22, and 28 have a primitive root?
2. Which of the integers 8, 9, 12, 26, 27, 31, and 33 have a primitive root?
3. Find a primitive root modulo each of the following moduli.

   a) 3^2 c) 23^2
   b) 5^2 d) 29^2

4. Find a primitive root modulo each of the following moduli.

   a) 11^2 c) 17^2
   b) 13^2 d) 19^2

5. Find a primitive root for all positive integers k modulo each of the following moduli.

   a) 3^k c) 13^k
   b) 11^k d) 17^k

6. Find a primitive root for all positive integers k modulo each of the following moduli.

   a) 23^k c) 31^k
   b) 29^k d) 37^k

7. Find a primitive root modulo each of the following moduli.

   a) 10 c) 38
   b) 34 d) 50

8. Find a primitive root modulo each of the following moduli.

   a) 6 c) 26
   b) 18 d) 338

9. Find all the primitive roots modulo 22.
10. Find all the primitive roots modulo 25.
11. Find all the primitive roots modulo 38.
12. Show that there are the same number of primitive roots modulo $2p^t$ as there are modulo p^t, where p is an odd prime and t is a positive integer.

☞ 13. Show that the integer m has a primitive root if and only if the only solutions of the congruence $x^2 \equiv 1 \pmod{m}$ are $x \equiv \pm 1 \pmod{m}$.

* 14. Let n be a positive integer possessing a primitive root. Using this primitive root, prove that the product of all positive integers less than n and relatively prime to n is congruent to -1 modulo n. (When n is prime, this result is Wilson's theorem (Theorem 6.1).)

* 15. Show that although there are no primitive roots modulo 2^k, where k is an integer, $k \geq 3$, every odd integer is congruent modulo 2^n to exactly one of the integers $(-1)^\alpha 5^\beta$, where $\alpha = 0$ or 1 and β is an integer satisfying $0 \leq \beta \leq 2^{k-2} - 1$.

16. Find the smallest odd prime p that has a primitive root r that is not also a primitive root modulo p^2.

9.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find as many examples as you can where r is a primitive root of the prime p, but r is not a primitive root of p^2. Can you make any conjectures about how often this occurs?

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Find primitive roots modulo powers of odd primes.
2. Find primitive roots modulo twice powers of odd primes.

9.4 Index Arithmetic

In this section, we demonstrate how primitive roots may be used to do modular arithmetic. Let r be a primitive root modulo the positive integer m (so that m is of the form described in Theorem 9.15). By Theorem 9.3, we know that the integers

$$r, r^2, r^3, \ldots, r^{\phi(m)}$$

form a reduced system of residues modulo m. From this fact, we see that if a is an integer relatively prime to m, then there is a unique integer x with $1 \leq x \leq \phi(m)$ such that

$$r^x \equiv a \pmod{m}.$$

This leads to the following definition.

Definition. Let m be a positive integer with primitive root r. If a is a positive integer with $(a, m) = 1$, then the unique integer x with $1 \leq x \leq \phi(m)$ and $r^x \equiv a \pmod{m}$ is called the *index* (or *discrete logarithm*) *of a to the base r modulo m*. With this definition, we have $r^{\text{ind}_r a} \equiv a \pmod{m}$.

If x is the index of a to the base r modulo m, then we write $x = \text{ind}_r a$, where we do not indicate the modulus m in the notation, as it is assumed to be fixed. From the definition, we know that if a and b are integers relatively prime to m and $a \equiv b \pmod{m}$, then $\text{ind}_r a = \text{ind}_r b$. Indices share many properties of logarithms, but with equalities replaced with congruences modulo $\phi(m)$ (that is why they are called discrete logarithms).

Example 9.17. Let $m = 7$. We have seen that 3 is a primitive root modulo 7 and that $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{5}$, and $3^6 \equiv 1 \pmod{7}$.

Hence, modulo 7, we have

$$\text{ind}_3 1 = 6, \text{ind}_3 2 = 2, \text{ind}_3 3 = 1,$$
$$\text{ind}_3 4 = 4, \text{ind}_3 5 = 5, \text{ind}_3 6 = 3.$$

With a different primitive root modulo 7, we obtain a different set of indices. For instance, calculations show that with respect to the primitive root 5,

$$\text{ind}_5 1 = 6, \text{ind}_5 2 = 4, \text{ind}_5 3 = 5,$$
$$\text{ind}_5 4 = 2, \text{ind}_5 5 = 1, \text{ind}_5 6 = 3.$$ ◀

Properties of Indices We now develop properties of indices, modulo m similar to those of logarithms, but instead of equalities, we have congruences modulo $\phi(m)$.

Theorem 9.16. Let m be a positive integer with primitive root r, and let a and b be integers relatively prime to m. Then

(i) $\text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$,

(ii) $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$,

(iii) $\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$ if k is a positive integer.

Proof of (i). From Euler's theorem, we know that $r^{\phi(m)} \equiv 1 \pmod{m}$. Because r is a primitive root modulo m, no smaller positive power of r is congruent to 1 modulo m. Hence, $\text{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$.

Proof of (ii). To prove this congruence, note that from the definition of indices,

$$r^{\text{ind}_r(ab)} \equiv ab \pmod{m}$$

and

$$r^{\text{ind}_r a + \text{ind}_r b} \equiv r^{\text{ind}_r a} \cdot r^{\text{ind}_r b} \equiv ab \pmod{m}.$$

Hence,

$$r^{\text{ind}_r(ab)} \equiv r^{\text{ind}_r a + \text{ind}_r b} \pmod{m}.$$

Using Theorem 9.2, we conclude that

$$\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}.$$

Proof of (iii). To prove the congruence of interest, first note that by definition, we have

$$r^{\text{ind}_r a^k} \equiv a^k \pmod{m}$$

and

$$r^{k \cdot \text{ind}_r a} \equiv (r^{\text{ind}_r a})^k \pmod{m}.$$

Hence,

$$r^{\text{ind}_r a^k} \equiv r^{k \cdot \text{ind}_r a} \pmod{m}.$$

Using Theorem 9.2, this leads us immediately to the congruence we want, namely

$$\text{ind}_r a^k \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}.$$

■

Example 9.18. From the previous examples, we see that, modulo 7, $\text{ind}_5 2 = 4$ and $\text{ind}_5 3 = 5$. Because $\phi(7) = 6$, part (ii) of Theorem 9.16 tells us that

$$\text{ind}_5 6 = \text{ind}_5(2 \cdot 3) = \text{ind}_5 2 + \text{ind}_5 3 = 4 + 5 = 9 \equiv 3 \pmod 6.$$

Note that this agrees with the value previously found for $\text{ind}_5 6$.

From part (iii) of Theorem 9.16, we see that

$$\text{ind}_5 3^4 \equiv 4 \cdot \text{ind}_5 3 \equiv 4 \cdot 5 = 20 \equiv 2 \pmod 6.$$

Note that direct computation gives the same result, because

$$\text{ind}_5 3^4 = \text{ind}_5 81 = \text{ind}_5 4 = 2.$$

◀

Indices are helpful in the solution of certain types of congruences. Consider the following examples.

Example 9.19. We will use indices to solve the congruence $6x^{12} \equiv 11 \pmod{17}$. We find that 3 is a primitive root of 17 (because $3^8 \equiv -1 \pmod{17}$). The indices of integers to the base 3 modulo 17 are given in Table 9.1.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Table 9.1 *Indices to the base* 3 *modulo* 17.

Taking the index of each side of the congruence to the base 3 modulo 17, we obtain a congruence modulo $\phi(17) = 16$, namely

$$\text{ind}_3(6x^{12}) \equiv \text{ind}_3 11 = 7 \pmod{16}.$$

Using parts (ii) and (iii) of Theorem 9.16, we obtain

$$\text{ind}_3(6x^{12}) \equiv \text{ind}_3 6 + \text{ind}_3(x^{12}) \equiv 15 + 12 \cdot \text{ind}_3 x \pmod{16}.$$

Hence,

$$15 + 12 \cdot \text{ind}_3 x \equiv 7 \pmod{16}$$

or

$$12 \cdot \text{ind}_3 x \equiv 8 \pmod{16}.$$

From this congruence it follows (as the reader should show) that

$$\text{ind}_3 x \equiv 2 \pmod 4.$$

Hence,

$$\text{ind}_3 x \equiv 2, 6, 10, \text{ or } 14 \pmod{16}.$$

Consequently, from the definition of indices, we find that

$$x \equiv 3^2, 3^6, 3^{10}, \text{ or } 3^{14} \pmod{17}.$$

(Note that this congruence holds modulo 17). Because $3^2 \equiv 9, 3^6 \equiv 15, 3^{10} \equiv 8$, and $3^{14} \equiv 2 \pmod{17}$, we conclude that

$$x \equiv 9, 15, 8, \text{ or } 2 \pmod{17}.$$

Because each step in the computations is reversible, there are four incongruent solutions of the original congruence modulo 17. ◀

Example 9.20. We wish to find all solutions of the congruence $7^x \equiv 6 \pmod{17}$. When we take indices to the base 3 modulo 17 of both sides of this congruence, we find that

$$\text{ind}_3(7^x) \equiv \text{ind}_3 6 = 15 \pmod{16}.$$

By part (iii) of Theorem 9.16, we obtain

$$\text{ind}_3(7^x) \equiv x \cdot \text{ind}_3 7 \equiv 11x \pmod{16}.$$

Hence,

$$11x \equiv 15 \pmod{16}.$$

Because 3 is an inverse of 11 modulo 16, we multiply both sides of the linear congruence above by 3, to find that

$$x \equiv 3 \cdot 15 = 45 \equiv 13 \pmod{16}.$$

All steps in this computation are reversible. Therefore, the solutions of

$$7^x \equiv 6 \pmod{17}$$

are given by

$$x \equiv 13 \pmod{16}.$$ ◀

The Difficulty of Finding Discrete Logarithms

Given a prime p and a primitive root r, the problem of finding the index (discrete logarithm) of an integer a to the base r modulo m is called the *discrete logarithm problem*. This problem is believed to be as computationally difficult as that of factoring integers. For this reason, it has been used as the basis for several public key cryptosystems, such as the ElGamal cryptosystem discussed in Section 10.2, and protocols, such as the Diffie-Hellman key agreement scheme discussed in Section 8.3. With the growing importance of the discrete logarithm problem in cryptography, a great deal of research has been devoted to constructing efficient algorithms for computing discrete logarithms. The most efficient algorithm known for computing discrete logarithms is the number-field sieve

method, which requires approximately the same number of bit operations to find discrete logarithms modulo a prime p as it would to factor a composite number of about the same size as p. To determine how long it takes to solve the discrete logarithm problem modulo a prime p, consult Table 3.2, which shows how long it takes to factor an integer n of the same number of decimal digits as p. For more information about the discrete logarithm problem, and algorithms for solving it, consult [MevaVa97] and the many references cited there.

Power Residues

Indices are also helpful for studying congruences of the form $x^k \equiv a \pmod{m}$, where m is a positive integer with a primitive root and $(a, m) = 1$. Before we study such congruences, we present a definition.

Definition. If m and k are positive integers and a is an integer relatively prime to m, then we say that a is a *kth power residue of* m if the congruence $x^k \equiv a \pmod{m}$ has a solution.

When m is an integer possessing a primitive root, the following theorem gives a useful criterion for an integer a relatively prime to m to be a kth power residue of m.

Theorem 9.17. Let m be a positive integer with a primitive root. If k is a positive integer and a is an integer relatively prime to m, then the congruence $x^k \equiv a \pmod{m}$ has a solution if and only if

$$a^{\phi(m)/d} \equiv 1 \pmod{m},$$

where $d = (k, \phi(m))$. Furthermore, if there are solutions of $x^k \equiv a \pmod{m}$, then there are exactly d incongruent solutions modulo m.

Proof. Let r be a primitive root modulo the positive integer m. We note that the congruence

$$x^k \equiv a \pmod{m}$$

holds if and only if

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(m)}. \tag{9.4}$$

Now let $d = (k, \phi(m))$ and $y = \operatorname{ind}_r x$, so that $x \equiv r^y \pmod{m}$. By Theorem 4.10, we note that if $d \nmid \operatorname{ind}_r a$, then the linear congruence

$$ky \equiv \operatorname{ind}_r a \pmod{\phi(m)} \tag{9.5}$$

has no solutions and, hence, there are no integers x satisfying (9.4). If $d \mid \operatorname{ind}_r a$, then there are exactly d integers y incongruent modulo $\phi(m)$ such that (9.5) holds and, hence, exactly d integers x incongruent modulo m such that (9.4) holds. Because $d \mid \operatorname{ind}_r a$ if and only if

$$(\phi(m)/d)\operatorname{ind}_r a \equiv 0 \pmod{\phi(m)},$$

and this congruence holds if and only if

$$a^{\phi(m)/d} \equiv 1 \pmod{m},$$

the theorem is true. ■

We note that Theorem 9.17 tells us that if p is a prime, k is a positive integer, and a is an integer relatively prime to p, then a is a kth power residue of p if and only if

$$a^{(p-1)/d} \equiv 1 \pmod{p},$$

where $d = (k, p-1)$. We illustrate this observation with an example.

Example 9.21. To determine whether 5 is a sixth power residue of 17, that is, whether the congruence

$$x^6 \equiv 5 \pmod{17}$$

has a solution, we determine that

$$5^{16/(6,16)} = 5^8 \equiv -1 \pmod{17}.$$

Hence, 5 is not a sixth power residue of 17. ◀

A table of indices with respect to the least primitive root modulo each prime less than 100 is given in Table 4 of Appendix E.

Proving Theorem 6.10 This proof of Theorem 6.10 is quite long and complicated, but is based only on results already established. We present this proof to give the reader an indication that even elementary proofs can be difficult to create and hard to follow. As you read this proof, follow each part carefully and check each separate case. We restate Theorem 6.10 for convenience.

Theorem 6.10. If n is an odd composite positive integer, then n passes Miller's test for at most $(n-1)/4$ bases b with $1 \leq b < n-1$.

We need the following lemma in the proof.

Lemma 9.2. Let p be an odd prime and let e and q be positive integers. Then the number of incongruent solutions of the congruence $x^q \equiv 1 \pmod{p^e}$ is $(q, p^{e-1}(p-1))$.

Proof. Let r be a primitive root of p^e. By taking indices with respect to r, we see that $x^q \equiv 1 \pmod{p^e}$ if and only if $qy \equiv 0 \pmod{\phi(p^e)}$, where $y = \operatorname{ind}_r x$. Using Theorem 4.10, we see that there are exactly $(q, \phi(p^e))$ incongruent solutions of $qy = 0 \pmod{\phi(p^e)}$. Consequently, there are $(q, \phi(p^e)) = (q, p^{e-1}(p-1))$ incongruent solutions of $x^q \equiv 1 \pmod{p^e}$. ■

We now proceed with a proof of Theorem 6.10.

Proof. Let $n-1=2^s t$, where s is a positive integer and t is an odd positive integer. For n of Theorem 6.10 to be a strong pseudoprime to the base b, either

$$b^t \equiv 1 \pmod{n}$$

or

$$b^{2^j t} \equiv -1 \pmod{n}$$

for some integer j with $0 \le j \le s-1$. In either case, we have

$$b^{n-1} \equiv 1 \pmod{n}.$$

Let the prime-power factorization of n be $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. By Lemma 9.2, we know that there are $(n-1, p_j^{e_j}(p_j-1)) = (n-1, p_j-1)$ incongruent solutions of $x^{n-1} \equiv 1 \pmod{p_j^{e_j}}$, $j = 1, 2, \ldots, r$. Consequently, the Chinese remainder theorem tells us that there are exactly $\prod_{j=1}^{r}(n-1, p_j-1)$ incongruent solutions of $x^{n-1} \equiv 1 \pmod{n}$. ∎

We consider two cases.

Case (i). We first consider the case where the prime-power factorization of n contains a prime power $p_k^{e_k}$ with exponent $e_k \ge 2$. Because

$$(p_k-1)/p_k^{e_k} = \left(1/p_k^{e_k-1}\right) - \left(1/p_k^{e_k}\right) \le 2/9$$

(the largest possible value occurs when $p_j = 3$ and $e_j = 2$), we see that

$$\begin{aligned}\prod_{j=1}^{r}(n-1, p_j-1) &\le \prod_{j=1}^{r}(p_j-1) \\ &\le \left(\prod_{\substack{j=1 \\ j\neq k}}^{r} p_j\right)\left(\frac{2}{9}p_k^{e_k}\right) \\ &\le \frac{2}{9}n.\end{aligned}$$

Because $\frac{2}{9}n \le \frac{1}{4}(n-1)$ for $n \ge 9$, it follows that

$$\prod_{j=1}^{r}(n-1, p_j-1) \le (n-1)/4.$$

Consequently, there are at most $(n-1)/4$ integers b, $1 \le b \le n$, for which n is a strong pseudoprime to the base b.

Case (ii). Now, we consider the case where $n = p_1 p_2 \cdots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct odd primes. Let

$$p_i - 1 = 2^{s_i} t_i, \quad i = 1, 2, \ldots, r,$$

where s_i is a positive integer and t_i is an odd positive integer. We reorder the primes $p_1, p_2, \ldots, p_r$ (if necessary) so that $s_1 \le s_2 \le \cdots \le s_r$. We note that

$$(n-1, p_i - 1) = 2^{\min(s, s_i)}(t, t_i).$$

The number of incongruent solutions of $x^t \equiv 1 \pmod{p_i}$ is $T_i = (t, t_i)$. From Exercise 22 at the end of this section, there are $2^j T_i$ incongruent solutions of $x^{2^j t} \equiv -1 \pmod{p_i}$ when $0 \le s_i - 1$, and no solutions otherwise. Hence, using the Chinese remainder theorem, there are $T_1 T_2 \cdots T_r$ incongruent solutions of $x^t \equiv 1 \pmod{n}$, and $2^{jr} T_1 T_2 \cdots T_r$ incongruent solutions of $x^{2^j t} \equiv -1 \pmod{n}$ when $0 \le j \le s_1 - 1$. Therefore, there are a total of

$$T_1 T_2 \cdots T_r \left(1 + \sum_{j=0}^{s_1 - 1} 2^{jr}\right) = T_1 T_2 \cdots T_r \left(1 + \frac{2^{rs_1} - 1}{2^{r-1}}\right)$$

integers b, with $1 \le b \le n-1$, for which n is a strong pseudoprime to the base b.

Now, we note that

$$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) = t_1 t_2 \cdots t_r 2^{s_1 + s_2 + \cdots + s_r}.$$

We will show that

$$T_1 T_2 \cdots T_r \left(1 + \frac{2^{rs_1} - 1}{2^{r-1}}\right) \le \phi(n)/4,$$

which proves the desired result. Because $T_1 T_2 \cdots T_r \le t_1 t_2 \cdots t_r$, we can achieve our goal by showing that

$$\left(1 + \frac{2^{rs_j} - 1}{2^r - 1}\right) / 2^{s_1 + s_2 + \cdots + s_r} \le \frac{1}{4}. \tag{9.6}$$

Because $s_1 \le \cdots \le s_r$, we see that

$$\begin{aligned}
\left(1 + \frac{2^{rs_j} - 1}{2^r - 1}\right) / 2^{s_1 + s_2 + \cdots + s_r} &\le \left(1 + \frac{2^{rs_j} - 1}{2^r - 1}\right) / 2^{rs_1} \\
&= \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{2^{rs_1}(2^r - 1)} \\
&= \frac{1}{2^{rs_1}} + \frac{1}{2^{r-1}} - \frac{1}{2^{rs_1}(2^r - 1)} \\
&= \frac{1}{2^r - 1} + \frac{2^r - 2}{2^{rs_1}(2^r - 1)} \\
&\le \frac{1}{2^{r-1}}.
\end{aligned}$$

From this inequality, we conclude that (9.6) is valid when $r \ge 3$.

When $r = 2$, we have $n = p_1 p_2$, with $p_1 - 1 = 2^{s_1} t_1$ and $p_2 - 1 = 2^{s_2} t_2$, with $s_1 \le s_2$. If $s_1 < s_2$, then (9.6) is again valid, because

$$\left(1+\frac{2^{2s_1}-1}{3}\right)/2^{s_1+s_2} = \left(1+\frac{2^{2s_1}-1}{3}\right)/\left(2^{2s_1}\cdot 2^{s_2-s_1}\right)$$
$$= \left(\frac{1}{3}+\frac{1}{3\cdot 2^{s_1-1}}\right)/2^{s_2-s_1}$$
$$\leq \frac{1}{4}.$$

When $s_1 = s_2$, we have $(n-1, p_1-1) = 2^s T_1$ and $(n-1, p_2-1) = 2^s T_2$. Let us assume that $p_1 > p_2$. Note that $T_1 \neq t_1$, for if $T_1 = t_1$, then $(p_1-1) \mid (n-1)$, so that

$$n = p_1 p_2 \equiv p_2 \equiv 1 \pmod{p_1 - 1},$$

which implies that $p_2 > p_1$, a contradiction. Because $T_1 \neq t_1$, we know that $T_1 \leq t_1/3$. Similarly, if $p_1 < p_2$, then $T_2 \neq t_2$, so that $T_2 \leq t_2/3$. Hence, $T_1 T_2 \leq t_1 t_2/3$, and because $\left(1+\frac{2^{2s_1}-1}{3}\right)/2^{2s_1} \leq \frac{1}{2}$, we have

$$T_1 T_2 \left(1+\frac{2^{2s_1}-1}{3}\right) \leq t_1 t_2 2^{2s_1}/6 = \phi(n)/6,$$

proving the theorem for this final case, since $\phi(n)/6 \leq (n-1)/6 < (n-1)/4$.

By analyzing the inequalities in the proof of Theorem 6.10, we can see that the probability that n is a strong pseudoprime to the randomly chosen base b, $1 \leq b \leq n-1$, is close to 1/4 only for integers n with prime factorizations of the form $n = p_1 p_2$, with $p_1 = 1 + 2q_1$ and $p_2 = 1 + 4q_2$, where q_1 and q_2 are odd primes, or $n = q_1 q_2 q_3$, with $p_1 = 1 + 2q_1$, $p_2 = 1 + 2q_2$, and $p_3 = 1 + 2q_3$, where q_1, q_2, and q_3 are distinct odd primes (see Exercise 23).

9.4 Exercises

1. Write out a table of indices modulo 23 with respect to the primitive root 5.
2. Find all the solutions of the following congruences.

   a) $3x^5 \equiv 1 \pmod{23}$ b) $3x^{14} \equiv 2 \pmod{23}$

3. Find all the solutions of the following congruences.

   a) $3^x \equiv 2 \pmod{23}$ b) $13^x \equiv 5 \pmod{23}$

4. For which positive integers a is the congruence $ax^4 \equiv 2 \pmod{13}$ solvable?
5. For which positive integers b is the congruence $8x^7 \equiv b \pmod{29}$ solvable?
6. Find the solutions of $2^x \equiv x \pmod{13}$, using indices to the base 2 modulo 13.
7. Find all the solutions of $x^x \equiv x \pmod{23}$.
8. Show that if p is an odd prime and r is a primitive root of p, then $\text{ind}_r(p-1) = (p-1)/2$.
9. Let p be an odd prime. Show that the congruence $x^4 \equiv -1 \pmod{p}$ has a solution if and only if p is of the form $8k+1$.

10. Prove that there are infinitely many primes of the form $8k + 1$. (*Hint:* Assume that $p_1, p_2, \ldots, p_n$ are the only primes of this form. Let $Q = (2p_1, p_2 \cdots p_n)^k + 1$. Show that Q must have an odd prime factor different than $p_1, p_2, \ldots, p_n$ and, by Exercise 9, necessarily of the form $8k + 1$.)

By Exercise 15 of Section 9.3, we know that if a is an odd positive integer, then there are unique integers α and β with $\alpha = 0$ or 1 and $0 \leq \beta \leq 2^{k-2} - 1$ such that $a \equiv (-1)^\alpha 5^\beta \pmod{2^k}$. Define the *index system of a modulo* 2^k to be equal to the pair (α, β).

11. Find the index system of 7 and 9 modulo 16.

12. Develop rules for the index systems modulo 2^k of products and powers, analogous to the rules for indices.

13. Use the index system modulo 32 to find all solutions of $7x^9 \equiv 11 \pmod{32}$ and $3^x \equiv 17 \pmod{32}$.

Let $n = 2^{t_0} p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$ be the prime-power factorization of n. Let a be an integer relatively prime to n. Let $r_1, r_2, \ldots, r_m$ be primitive roots of $p_1^{t_1}, p_2^{t_2}, \ldots, p_m^{t_m}$, respectively, and let $\gamma_1 = \operatorname{ind}_{r_1} a \pmod{\phi(p_1^{t_1})}$, $\gamma_2 = \operatorname{ind}_{r_2} a \pmod{\phi(p_2^{t_2})}, \ldots, \gamma_m = \operatorname{ind}_{r_m} a \pmod{\phi(p_m^{t_m})}$. If $t_0 \leq 2$, let r_0 be a primitive root of 2^{t_0}, and let $\gamma_0 = \operatorname{ind}_{r_0} a \pmod{\phi(2^{t_0})}$. If $t_0 \geq 3$, let (α, β) be the index system of a modulo 2^k, so that $a \equiv (-1)^\alpha 5^\beta \pmod{2^k}$. Define the *index system of a modulo n* to be $(\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_m)$ if $t_0 \leq 2$ and $(\alpha, \beta, \gamma_1, \gamma_2, \ldots, \gamma_m)$ if $t_0 \geq 3$.

14. Show that if n is a positive integer, then every integer has a unique index system modulo n.

15. Find the index systems of 17 and 41 (mod 120) (in your computations, use 2 as a primitive root of the prime factor 5 of 120).

16. Develop rules for the index systems modulo n of products and powers, analogous to those for indices.

17. Use an index system modulo 60 to find the solutions of $11x^7 \equiv 43 \pmod{60}$.

18. Let p be a prime, $p > 3$. Show that if $p \equiv 2 \pmod 3$, then every integer not divisible by 3 is a third-power, or *cubic*, residue of p, whereas if $p \equiv 1 \pmod 3$, an integer a is a cubic residue of p if and only if $a^{(p-1)/3} \equiv 1 \pmod p$.

19. Let e be a positive integer with $e \geq 2$. Show that if k is an odd positive integer, then every odd integer a is a kth power residue of 2^e.

* **20.** Let e be a positive integer with $e \geq 2$. Show that if k is even, then an integer a is a kth power residue of 2^e if and only if $a \equiv 1 \pmod{(4k, 2^e)}$.

* **21.** Let e be a positive integer with $e \geq 2$. Show that if k is a positive integer, then the number of incongruent kth power residues of 2^e is

$$\frac{2^{e-1}}{(k, 2)(k, 2^{e-2})}.$$

☞ **22.** Let $N = 2^j u$ be a positive integer, with j a nonnegative integer and u an odd positive integer, and let $p - 1 = 2^s t$, where s and t are positive integers with t odd. Show that

there are $2^j(t, u)$ incongruent solutions of $x^N \equiv -1 \pmod{p}$ if $0 \leq j \leq s-1$, and no solutions otherwise.

* **23.** a) Show that the probability that n is a strong pseudoprime for a base b randomly chosen with $1 \leq b \leq n-1$ is near 1/4 only when n has a prime factorization of the form $n = p_1p_2$, where $p_1 = 1 + 2q_1$ and $p_2 = 1 + 4q_2$, with q_1 and q_2 prime, or $n = p_1p_2p_3$, where $p_1 = 1 + 2q_1$, $p_2 = 1 + 2q_2$, and $p_3 = 1 + 2q_3$, with q_1, q_2, q_3 distinct odd primes.

b) Find the probability that $n = 49{,}939 \cdot 99{,}877$ is a strong pseudoprime to the base b randomly chosen with $1 \leq b \leq n-1$.

9.4 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find integers n for which the probability that n is a strong pseudoprime to the randomly chosen base b, $1 \leq b \leq n-1$, is close to 1/4.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Construct a table of indices modulo a particular primitive root of an integer.
2. Using indices solve congruences of the form $ax^b \equiv c \pmod{m}$, where a, b, c, and m are integers with $c > 0, m > 0$, and where m has a primitive root.
3. Find kth power residues of a positive integer m having a primitive root, where k is a positive integer.
4. Find index systems modulo powers of 2 (see the preamble to Exercise 11).
5. Find index systems modulo arbitrary positive integers (see the preamble to Exercise 14).

9.5 Primality Tests Using Orders of Integers and Primitive Roots

In Chapter 6, we saw that the converse of Fermat's little theorem is not true. Fermat's little theorem tells us that if p is prime and a is an integer with $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. Even if $a^{n-1} \equiv 1 \pmod{n}$, where a is a positive integer, n may still be composite. Although the converse of Fermat's little theorem is not true, can we establish partial converses? That is, can we add hypotheses to the converse to make it true?

In this section, we will use the concepts developed in this chapter to prove some partial converses of Fermat's little theorem. We begin with a result known as *Lucas's converse of Fermat's little theorem*. This result was proved by French mathematician Edouard Lucas in 1876.

Theorem 9.18. *Lucas's Converse of Fermat's Little Theorem.* If n is a positive integer and if an integer x exists such that

$$x^{n-1} \equiv 1 \pmod{n}$$

and

$$x^{(n-1)/q} \not\equiv 1 \pmod{n}$$

for all prime divisors q of $n-1$, then n is prime.

Proof. Because $x^{n-1} \equiv 1 \pmod{n}$, Theorem 9.1 tells us that $\text{ord}_n x \mid (n-1)$. We will show that $\text{ord}_n x = n-1$. Suppose that $\text{ord}_n x \neq n-1$. Because $\text{ord}_n x \mid (n-1)$, there is an integer k with $n-1 = k \cdot \text{ord}_n x$, and because $\text{ord}_n x \neq n-1$, we know that $k > 1$. Let q be a prime divisor of k. Then

$$x^{(n-1)/q} = x^{k/(\text{ord}_n x \cdot q)} = (x^{\text{ord}_n x})^{(k/q)} \equiv 1 \pmod{n}.$$

However, this contradicts the hypotheses of the theorem, so we must have $\text{ord}_n x = n-1$. Now because $\text{ord}_n x \leq \phi(n)$ and $\phi(n) \leq n-1$, it follows that $\phi(n) = n-1$. By Theorem 7.2, we know that n must be prime. ∎

Note that Theorem 9.18 is equivalent to the fact that if there is an integer with order modulo n equal to $n-1$, then n must be prime. We illustrate the use of Theorem 9.18 with an example.

Example 9.22. Let $n = 1009$. Then $11^{1008} \equiv 1 \pmod{1009}$. The prime divisors of 1008 are 2, 3, and 7. We see that $11^{1008/2} = 11^{504} \equiv -1 \pmod{1009}$, $11^{1008/3} = 11^{336} \equiv 374 \pmod{1009}$, and $11^{1008/7} = 11^{144} \equiv 935 \pmod{1009}$. Hence, by Theorem 9.18, we know that 1009 is prime. ◀

The following corollary of Theorem 9.18 gives a slightly more efficient primality test.

Corollary 9.18.1. If n is an odd positive integer and if x is a positive integer such that

$$x^{(n-1)/2} \equiv -1 \pmod{n}$$

and

$$x^{(n-1)/q} \not\equiv 1 \pmod{n}$$

for all odd prime divisors q of $n-1$, then n is prime.

Proof. Because $x^{(n-1)/2} \equiv -1 \pmod{n}$, we see that

$$x^{n-1} = (x^{(n-1)/2})^2 \equiv (-1)^2 \equiv 1 \pmod{n}.$$

Because the hypotheses of Theorem 9.18 are met, we know that n is prime. ∎

Example 9.23. Let $n = 2003$. The odd prime divisors of $n-1 = 2002$ are 7, 11, and 13. Because $5^{2002/2} = 5^{1001} \equiv -1 \pmod{2003}$, $5^{2002/7} = 5^{286} \equiv 874 \pmod{2003}$,

$5^{2002/11} = 5^{183} \equiv 886 \pmod{2003}$, and $5^{2002/13} = 5^{154} \equiv 633 \pmod{2003}$, we see from Corollary 9.18.1 that 2003 is prime. ◀

To determine whether an integer n is prime using either Theorem 9.18 or Corollary 9.18.1, it is necessary to know the prime factorization of $n - 1$. As we have remarked before, finding the prime factorization of an integer is a time-consuming process. Only when we have some a priori information about the factorization of $n - 1$ are the primality tests given by these results practical. Indeed, with such information these tests can be useful. Such a situation occurs with the Fermat numbers; in Chapter 11 we give a primality test for these numbers based on the ideas of this section.

In Chapter 3, we discussed the recent discovery of an algorithm that can prove that an integer n is prime in polynomial time (in the number of digits in the prime). We can prove a weaker result using Corollary 9.18.1, which shows that we can prove that an integer is prime in polynomial time once particular information is known.

Theorem 9.19. If n is prime, this can be proved when sufficient information is available using $O((\log_2 n)^4)$ bit operations.

Proof. We use the second principle of mathematical induction. The induction hypothesis is an estimate for $f(n)$, where $f(n)$ is the total number of multiplications and modular exponentiations needed to verify that the integer n is prime.

We demonstrate that

$$f(n) \leq 3(\log n/\log 2) - 2.$$

First, we note that $f(2) = 1$. We assume that for all primes q, with $q < n$, the inequality

$$f(q) \leq 3(\log n/\log 2) - 2$$

holds.

To prove that n is prime, we use Corollary 9.18.1. Once we have the numbers $2^a, q_1, \ldots, q_t$, and x that supposedly satisfy

(i) $n - 1 = 2^a q_1 q_2 \cdots q_t$,

(ii) q_i is prime for $i = 1, 2, \ldots, t$,

(iii) $x^{(n-1)/2} \equiv -1 \pmod{n}$,

and

(iv) $x^{(n-1)/q_j} \equiv 1 \pmod{n}$, for $i = 1, 2, \ldots, t$,

we need to do t multiplications to check (i), $t + 1$ modular exponentiations to check (iii) and (iv), and $f(q_i)$ multiplications and modular exponentiations to check (ii), that q_i is prime for $i = 1, 2, \ldots, t$. Hence,

$$f(n) = t + (t+1) + \sum_{i=1}^{t} f(q_i)$$
$$\leq 2t + 1 + \sum_{i=1}^{t}((3 \log q_i / \log 2) - 2).$$

Now, each multiplication requires $O((\log_2 n)^2)$ bit operations and each modular exponentiation requires $O((\log_2 n)^3)$ bit operations. Because the total number of multiplications and modular exponentiations needed is $f(n) = O(\log_2 n)$, the total number of bit operations needed is $O((\log_2 n)(\log_2 n)^3) = O((\log_2 n)^4)$. ∎

Another limited converse of Fermat's little theorem was established by Henry Pocklington in 1914. He showed that the primality of n can be established using a partial factorization of $n-1$. We use the usual notation $n - 1 = FR$, where F represents the part of $n-1$ *factored* into primes and R the *remaining* part not factored into primes.

Theorem 9.20. ***Pocklington's Primality Test.*** Suppose that n is a positive integer with $n - 1 = FR$, where $(F, R) = 1$ and $F > R$. The integer n is prime if there exists an integer a such that $(a^{(n-1)/q} - 1, n) = 1$ whenever q is a prime with $q \mid F$ and $a^{n-1} \equiv 1 \pmod{n}$.

Proof. Suppose that p is a prime divisor of n with $p \leq \sqrt{n}$. Because $a^{n-1} \equiv 1 \pmod{n}$ (where a is the integer assumed to have the properties specified in the hypotheses), if $p \mid n$, we see that $a^{n-1} \equiv 1 \pmod{p}$. It follows that $\operatorname{ord}_p a \mid n - 1$. Consequently, there exists an integer t such that $n - 1 = t \cdot \operatorname{ord}_p a$.

Now, suppose that q is a prime with $q \mid F$ and that q^e is the power of q appearing in the prime-power factorization of F. We will show that $q \nmid t$. To see this, note that if $q \mid t$, then

$$a^{(n-1)/q} = a^{\operatorname{ord}_p a \cdot (t/q)} \equiv 1 \pmod{p}.$$

This implies that $p \mid (a^{(n-1)/q} - 1, n)$ because $p \mid a^{(n-1)/q} - 1$ and $p \mid n$. This contradicts the hypothesis that $(a^{(n-1)/q} - 1, n) = 1$. Consequently, $q \nmid t$. It follows that $q^e \mid \operatorname{ord}_p a$. Because for every prime dividing F the power of this prime in the prime-power factorization of F divides $\operatorname{ord}_p a$, it follows that $F \mid \operatorname{ord}_p a$. Because $\operatorname{ord}_p a \mid p - 1$, it follows that $F \mid p - 1$, implying that $F < p$.

Because $F > R$ and $n - 1 = FR$, it follows that $n - 1 < F^2$. Because both $n - 1$ and F^2 are integers, we have $n \leq F^2$, so $p > F \geq \sqrt{n}$. We can conclude that n is prime. ∎

The following example illustrates the use of Pocklington's primality test, where only a partial factorization of $n - 1$ is used to show that n is prime.

Example 9.24. We will use Pocklington's primality test to show that 23801 is prime. With $n = 23801$, we can use the partial factorization of $n - 1 = 23800 = FR$, where $F = 200 = 2^3 5^2$ and $R = 119$, so that $F > R$. Taking $a = 3$, we find (with the help of

computation software) that

$$3^{23800} \equiv 1 \pmod{23801}$$
$$3^{23800/2} \equiv -1 \pmod{23801}$$
$$3^{23800/5} \equiv 19672 \pmod{23801}.$$

From this we find (using the Euclidean algorithm) that $(3^{23800/2} - 1, 23801) = (-2, 23801) = 1$ and $(3^{23800/5} - 1, 23801) = (19671, 23801) = 1$. This shows that $n = 23801$ is prime, even though we did not use the complete factorization of $n - 1 = 23800$ (namely, $23800 = 2^3 \cdot 5^2 \cdot 7 \cdot 17$). ◀

We can use Pocklington's primality test to develop another test, which is useful for testing the primality of numbers of special form. This test (which actually predates Pocklington's) was proved by E. Proth in 1878.

Theorem 9.21. ***Proth's Primality Test.*** Let n be a positive integer with $n = k2^m + 1$, where k is an odd integer and m is an integer with $k < 2^m$. If there is an integer a such that

$$a^{(n-1)/2} \equiv -1 \pmod{n},$$

then n is prime.

Proof. Let $s = 2^m$ and $t = k$, so that $s > t$ by the hypotheses. If

(9.7) $$a^{(n-1)/2} \equiv -1 \pmod{n},$$

we can easily show that $(a^{(n-1)/2} - 1, n) = 1$. To see this, note that if $d \mid (a^{(n-1)/2} - 1)$ and $d \mid n$, then by (9.7), $d \mid (a^{(n-1)/2} + 1)$. It follows that d divides $(a^{(n-1)/2} - 1) + (a^{(n-1)/2} + 1) = 2$. Because n is odd, it follows that $d = 1$. Consequently, all the hypotheses of Pocklington's primality test are satisfied, so n is prime. ■

Example 9.25. We will use Proth's primality test to show that $n = 13 \cdot 2^8 + 1 = 3329$ is prime. First, note that $13 < 2^8 = 256$. Take $a = 3$. We find (with the help of computation software) that

$$3^{(n-1)/2} = 3^{3328/2} = 3^{1664} \equiv -1 \pmod{3329}.$$

It follows by Proth's primality test that 3329 is prime. ◀

Proth's primality test has been used extensively to prove the primality of many large numbers of the form $k2^m + 1$. Three of the ten largest primes currently known have been found using Proth's primality test; the rest are Mersenne primes. For a few years, the largest known prime was not a Mersenne prime, but one of the form $k2^m + 1$. You can download PC-based software from the Web for running Proth's primality test, and look for new primes of the form $k2^m + 1$ yourself! If you find one you will receive some small amount of fame, but it will not make you as famous as if you found a new Mersenne prime.

9.5 Exercises

1. Show that 101 is prime using Lucas's converse of Fermat's little theorem with $x = 2$.
2. Show that 211 is prime using Lucas's converse of Fermat's little theorem with $x = 2$.
3. Show that 233 is prime using Corollary 9.18.1 with $x = 3$.
4. Show that 257 is prime using Corollary 9.18.1 with $x = 3$.
5. Show that if an integer x exists such that

$$x^{2^{2^n}} \equiv 1 \pmod{F_n}$$

and

$$x^{2^{(2^n-1)}} \not\equiv 1 \pmod{F_n},$$

then the Fermat number $F_n = 2^{2^n} + 1$ is prime.

* 6. Let n be a positive integer. Show that if the prime-power factorization of $n - 1$ is $n - 1 = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$, and for $j = 1, 2, \ldots, t$, there exists an integer x_j such that

$$x_j^{(n-1)/p_j} \not\equiv 1 \pmod{n}$$

and

$$x_j^{n-1} \equiv 1 \pmod{n},$$

then n is prime.

* 7. Let n be a positive integer such that

$$n - 1 = m \prod_{j=1}^{r} q_j^{a_j},$$

where m is a positive integer, $a_1, a_2, \ldots, a_r$ are positive integers, and $q_1, q_2, \ldots, q_r$ are relatively prime integers greater than one. Furthermore, let $b_1, b_2, \ldots, b_r$ be positive integers such that there exist integers $x_1, x_2, \ldots, x_r$ with

$$x_j^{n-1} \equiv 1 \pmod{n}$$

and

$$(x_j^{(n-1)/q_j} - 1, n) = 1$$

for $j = 1, 2, \ldots, r$, where every prime factor of q_j is greater than or equal to b_j for $j = 1, 2, \ldots, r$, and

$$n < \left(1 + \prod_{j=1}^{r} b_j^{a_j}\right)^2.$$

Show that n is prime.

8. Use Pocklington's primality test to show that 7057 is prime. (*Hint:* Take $F = 2^4 \cdot 3^2 = 144$ and $R = 49$ in $7057 - 1 = 7056 = FR$.)
9. Use Pocklington's primality test to show that 9929 is prime. (*Hint:* Take $F = 136 = 2^3 \cdot 17$ and $R = 73$ in $9929 - 1 = 9928 = FR$.)

10. Use Proth's primality test to show that 449 is prime.

11. Use Proth's primality test to show that 3329 is prime.

* 12. Show that the integer n is prime if $n - 1 = FR$, where $(F, R) = 1$, B is an integer with $FB > \sqrt{n}$, and R has no prime factors less than B; for each prime q dividing F, there exists an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{(n-1)/q} - 1, n) = 1$; and there exists an integer b greater than 1 such that $b^{n-1} \equiv 1 \pmod{n}$ and $(b^F - 1, n) = 1$.

* 13. Suppose that $n = hq^k + 1$, where q is prime and $q^k > h$. Show that n is prime if there exists an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{(n-1)/q} - 1, n) = 1$.

* 14. A *Sierpinski number* is a positive odd integer k for which the integers $k2^n + 1$, where n is an integer with $n > 1$, are all composite. Show 78557 is a Sierpinski number.

9.5 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Use Pocklington's primality test to show that 10,998,989 is prime, with $n - 1 = FR$, where $s = 4004$, $t = 2747$, and $a = 3$.

2. Use Pocklington's primality test to show that 111,649,121 is prime.

3. Use Proth's primality test to find as many primes of the form $3 \cdot 2^n + 1$ as you can.

4. Use Proth's primality test to find as many primes of the form $5 \cdot 2^n + 1$ as possible.

5. It has been conjectured that 78557 is the smallest Sierpinski number (see Exercise 14). (Sierpinski showed in 1960 that there are infinitely many Sierpinski numbers.) Can you help verify this conjecture (if it is true) by eliminating any of the integers 4847, 5359, 10223, 19249, 21811, 22699, 24737, 27653, 28433, 33661, 55459, and 67607 from contention? To do so, you will have to find an integer n such that $k2^n + 1$ is prime, where k is an integer on this list. (You can monitor progress on this conjecture at www.seventeenorbust.com.)

6. Give a succinct certification of primality of $F_4 = 2^{2^4} + 1 = 65537$.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to show that a positive integer n is prime using the following.

1. Lucas's converse of Fermat's little theorem

2. Corollary 9.18.1

3. Pocklington's primality test

4. Proth's primality test

9.6 Universal Exponents

Let n be a positive integer with prime-power factorization

$$n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}.$$

If a is an integer relatively prime to n, then Euler's theorem tells us that

$$a^{\phi(p^t)} \equiv 1 \pmod{p^t},$$

whenever p^t is one of the prime powers occurring in the factorization of n. As in the proof of Theorem 9.13, let

$$U = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})],$$

the least common multiple of the integers $\phi(p_i^{t_i})$, $i = 1, 2, \ldots, m$. Because

$$\phi(p_i^{t_i}) \mid U,$$

for $i = 1, 2, \ldots, m$, using Theorem 9.1 we see that

$$a^U \equiv 1 \pmod{p_i^{t_i}},$$

for $i = 1, 2, \ldots, m$. Hence, by Corollary 4.8.1, it follows that

$$a^U \equiv 1 \pmod{n}.$$

This leads to the following definition.

Definition. A *universal exponent* of the positive integer n is a positive integer U suc that

$$a^U \equiv 1 \pmod{n},$$

for all integers a relatively prime to n.

Example 9.26. Because the prime-power factorization of 600 is $2^3 \cdot 3 \cdot 5^2$, it follow that $U = [\phi(2^3), \phi(3), \phi(5^2)] = [4, 2, 20] = 20$ is a universal exponent of 600.

From Euler's theorem, we know that $\phi(n)$ is a universal exponent. As we hav already demonstrated, the integer $U = [\phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})]$ is also a univers exponent of $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$. We are interested in finding the *smallest* positive univers exponent of n.

Definition. The least universal exponent of the positive integer n is called the *minim universal exponent of* n, and is denoted by $\lambda(n)$.

We now find a formula for the minimal universal exponent $\lambda(n)$, based on the prim power factorization of n.

First, note that if n has a primitive root, then $\lambda(n) = \phi(n)$. Because powers of odd primes possess primitive roots, we know that

$$\lambda(p^t) = \phi(p^t),$$

whenever p is an odd prime and t is a positive integer. Similarly, we have $\lambda(2) = \phi(2) = 1$ and $\lambda(4) = \phi(4) = 2$, because both 2 and 4 have primitive roots. On the other hand, if $t \geq 3$, then we know by Theorem 9.11 that

$$a^{2^{t-2}} \equiv 1 \pmod{2^t}$$

and $\text{ord}_{2^t} 5 = 2^{t-2}$, so that we can conclude that $\lambda(2^t) = 2^{t-2}$ if $t \geq 3$.

We have found $\lambda(n)$ when n is a power of a prime. Next, we turn our attention to arbitrary positive integers n.

Theorem 9.22. Let n be a positive integer with prime-power factorization

$$n = 2^{t_0} p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}.$$

Then $\lambda(n)$, the minimal universal exponent of n, is given by

$$\lambda(n) = [\lambda(2^{t_0}), \phi(p_1^{t_1}), \ldots, \phi(p_m^{t_m})].$$

Moreover, there exists an integer a such that $\text{ord}_n a = \lambda(n)$, the largest possible order of an integer modulo n.

Proof. Let a be an integer with $(a, n) = 1$. For convenience, let

$$M = [\lambda(2_0^2), \phi(p_1^{t_1}), \phi(p_2^{t_2}), \ldots, \phi(p_m^{t_m})].$$

Because M is divisible by all of the integers $\lambda(2^{t_0}), \phi(p_1^{t_1}) = \lambda(p_1^{t_1}), \phi(p_2^{t_2}) = \lambda(p_2^{t_2}), \ldots, \phi(p_m^{t_m}) = \lambda(p_m^{t_m})$, and because $a^{\lambda(p^t)} \equiv 1 \pmod{p^t}$ for all prime powers in the factorization of n, we see that

$$a^M \equiv 1 \pmod{p^t},$$

whenever p^t is a prime power occurring in the factorization of n.

Consequently, by Corollary 4.8.1 we can conclude that

$$a^M \equiv 1 \pmod{n}.$$

The last congruence established the fact that M is a universal exponent. We must now show that M is the *least* universal exponent. To do this, we find an integer a such that no positive power smaller than the Mth power of a is congruent to 1 modulo n. With this in mind, let r_i be a primitive root of $p_i^{t_i}$.

We consider the system of simultaneous congruences

$$\begin{aligned} x &\equiv 5 \pmod{2^{t_0}} \\ x &\equiv r_1 \pmod{p_1^{t_1}} \\ x &\equiv r_2 \pmod{p_2^{t_2}} \\ &\vdots \\ x &\equiv r_m \pmod{p_m^{t_m}}. \end{aligned}$$

By the Chinese remainder theorem, there is a simultaneous solution a of this system that is unique modulo $n = 2^{t_0} p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$; we will show that $\text{ord}_n a = M$. To prove this claim, assume that N is a positive integer such that

$$a^N \equiv 1 \pmod{n}.$$

Then, if p^t is a prime-power divisor of n, we have

$$a^N \equiv 1 \pmod{p^t},$$

so that

$$\text{ord}_{p^t} a \mid N.$$

But, because a satisfies each of the $m + 1$ congruences of the system, we have

$$\text{ord}_{p^t} a = \lambda(p^t),$$

for each prime power in the factorization. Hence, by Theorem 9.1, we have

$$\lambda(p^t) \mid N,$$

for all prime powers p^t in the factorization of n. Therefore, by Corollary 4.8.1, we know that $M = [\lambda(2^{t_0}), \lambda(p_1^{t_1}), \lambda(p_2^{t_2}), \ldots, \lambda(p_m^{t_m})] \mid N$.

Because $a^M \equiv 1 \pmod{n}$ and $M \mid N$ whenever $a^N \equiv 1 \pmod{n}$, we can conclude that

$$\text{ord}_n a = M.$$

This shows that $M = \lambda(n)$ and simultaneously produces a positive integer a with $\text{ord}_n a = \lambda(n)$. ∎

Example 9.27. Because the prime-power factorization of 180 is $2^2 \cdot 3^2 \cdot 5$, from Theorem 9.22 it follows that

$$\lambda(180) = [\phi(2^2), \phi(3^2), \phi(5)] = 12.$$

To find an integer a with $\text{ord}_{180} a = 12$, first we find primitive roots modulo 3^2 and 5. For instance, we take 2 and 3 as primitive roots modulo 3^2 and 5, respectively. Then, using

the Chinese remainder theorem, we find a solution of the system of congruences

$$a \equiv 3 \pmod 4$$
$$a \equiv 2 \pmod 9$$
$$a \equiv 3 \pmod 5,$$

obtaining $a \equiv 83 \pmod{180}$. From the proof of Theorem 9.22, we see that $\text{ord}_{180}83 = 12$. ◀

Example 9.28. Let $n = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 73$. Then, we have

$$\begin{aligned}\lambda(n) &= [\lambda(2^6), \phi(3^2), \phi(5), \phi(17), \phi(13), \phi(17), \phi(19), \phi(37), \phi(73)] \\ &= [2^4, 2 \cdot 3, 2^2, 2 \cdot 3, 2^2 \cdot 3, 2^4, 2 \cdot 3^2, 2^2 3^2, 2^3 3^2] \\ &= 2^4 \cdot 3^2 \\ &= 144.\end{aligned}$$

Hence, whenever a is a positive integer relatively prime to $2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 17 \cdot 19 \cdot 37 \cdot 73$, we know that $a^{144} \equiv 1 \pmod{2^6 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 37 \cdot 37 \cdot 73}$. ◀

Results About Carmichael Numbers We now return to the Carmichael numbers, which we discussed in Section 6.2. Recall that a Carmichael number is a composite integer that satisfies $b^{n-1} \equiv 1 \pmod n$ for all positive integers b with $(b, n) = 1$. We proved that if $n = q_1 q_2 \cdots q_k$, where $q_1 q_2, \ldots, q_k$ are distinct primes satisfying $(q_j - 1) \mid (n - 1)$ for $j = 1, 2, \ldots, k$, then n is a Carmichael number. Here, we prove the converse of this result.

Theorem 9.23. If $n > 2$ is a Carmichael number, then $n = q_1 q_2 \cdots q_k$, where the q_j are distinct primes such that $(q_j - 1) \mid (n - 1)$ for $j = 1, 2, \ldots, k$.

Proof. If n is a Carmichael number, then

$$b^{n-1} \equiv 1 \pmod n,$$

for all positive integers b with $(b, n) = 1$. Theorem 9.22 tells us that there is an integer a with $\text{ord}_n a = \lambda(n)$, where $\lambda(n)$ is the minimal universal exponent; and because $a^{n-1} \equiv 1 \pmod n$, Theorem 9.1 tells us that

$$\lambda(n) \mid (n - 1).$$

Now n must be odd, for if n were even, then $n - 1$ would be odd, but $\lambda(n)$ is even (because $n > 2$), contradicting the fact that $\lambda(n) \mid (n - 1)$.

We now show that n must be the product of distinct primes. Suppose that n has a prime-power factor p^t with $t \geq 2$. Then

$$\lambda(p^t) = \phi(p^t) = p^{t-1}(p - 1) \mid \lambda(n) = n - 1.$$

This implies that $p \mid (n - 1)$, which is impossible because $p \mid n$. Consequently, n must be the product of distinct odd primes, say

$$n = q_1 q_2 \cdots q_k.$$

We conclude the proof by noting that

$$\lambda(q_i) = \phi(q_i) = (q_j - 1) \mid \lambda(n) = n - 1. \qquad \blacksquare$$

We can easily prove more about the prime factorizations of Carmichael numbers.

Theorem 9.24. A Carmichael number must have at least three different odd prime factors.

Proof. Let n be a Carmichael number. Then n cannot have just one prime factor, because it is composite, and is the product of distinct primes. So assume that $n = pq$, where p and q are odd primes with $p > q$. Then

$$n - 1 = pq - 1 = (p - 1)q + (q - 1) \equiv q - 1 \not\equiv 0 \pmod{p - 1},$$

which shows that $(p - 1) \nmid (n - 1)$. Hence, n cannot be a Carmichael number if it has just two different prime factors. $\blacksquare$

9.6 Exercises

1. Find $\lambda(n)$, the minimal universal exponent of n, for the following values of n.

   a) 100
   b) 144
   c) 222
   d) 884
   e) $2^4 \cdot 3^3 \cdot 5^2 \cdot 7$
   f) $2^5 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19$
   g) 10!
   h) 20!

2. Find all positive integers n such that $\lambda(n)$ is equal to each of the following integers.

   a) 1
   b) 2
   c) 3
   d) 4
   e) 5
   f) 6

3. Find the largest integer n with $\lambda(n) = 12$.

4. Find an integer with the largest possible order for the following moduli.

   a) 12
   b) 15
   c) 20
   d) 36
   e) 40
   f) 63

5. Show that if m is a positive integer, then $\lambda(m)$ divides $\phi(m)$.

6. Show that if m and n are relatively prime positive integers, then $\lambda(mn) = [\lambda(m), \lambda(n)]$.

7. Let n be the largest positive integer satisfying the equation $\lambda(n) = a$, where a is a fixed positive integer. Show that if m is another solution of $\lambda(m) = a$, then m divides n.

8. Suppose that n is a positive integer. How many incongruent integers are there with maximal order modulo n?

9. Show that if a and m are relatively prime integers, then the solutions of the congruence $ax \equiv b \pmod{m}$ are the integers x such that $x \equiv a^{\lambda(m)-1}b \pmod{m}$.

10. Show that if c is a positive integer greater than 1, then the integers $1^c, 2^c, \ldots, (m-1)^c$ form a complete system of residues modulo m if and only if m is square-free and $(c, \lambda(m)) = 1$.

*** 11.** a) Show that if c and m are positive integers and m is odd, then the congruence $x^c \equiv x \pmod{m}$ has exactly

$$\prod_{j=1}^{r}(1 + (c-1, \phi(p_j^{a_j})))$$

incongruent solutions, where m has prime-power factorization $m = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$.

b) Show that $x^c \equiv x \pmod{m}$ has exactly r^r solutions if $(c-1, \phi(m)) = 2$.

12. Use Exercise 11 to show that there are always at least nine plaintext messages that are not changed when encrypted using an RSA cipher.

*** 13.** Show that 561 is the only Carmichael number of the form $3pq$, where p and q are primes.

*** 14.** Find all Carmichael numbers of the form $5pq$, where pq are primes.

*** 15.** Show that there are only a finite number of Carmichael numbers of the form $n = pqr$, where p is a fixed prime, and q and r are also primes.

16. Show that the decrypting exponent d for an RSA cipher with encrypting key (e, n) can be taken to be an inverse of e modulo $\lambda(n)$.

Let n be a positive integer. When $(a, n) = 1$, we define the *generalized Fermat quotient* $q_n(a)$ by $q_n(a) \equiv (a^{\lambda(n)} - 1)/n \pmod{n}$ and $0 \leq q_n(a) < n$.

17. Show that if $(a, n) = (b, n) = 1$, then $q_n(ab) \equiv q_n(a) + q_n(b) \pmod{n}$.

18. Show that if $(a, n) = 1$, then $q_n(a + nc) \equiv q_n(a)_\lambda(n)c\overline{a} \pmod{n}$, where $\overline{a}$ is the inverse of a modulo n.

9.6 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find the universal exponent of all integers less than 1000.

2. Find Carmichael numbers with at least four different prime factors.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Find the minimal universal exponent of a positive integer.

2. Find an integer with the minimal universal exponent of n as its order modulo n.

3. Given a positive integer M, find all positive integers n with minimal universal exponent equal to M.

4. Solve linear congruences using the method of Exercise 9.

10

Applications of Primitive Roots and the Order of an Integer

Introduction

In this chapter, we will introduce applications that rely on the concepts of orders and primitive roots. First, we consider the problem of generating random numbers. Computers can produce random numbers using data generated by hardware or software, but they cannot create long sequences of random numbers this way. To meet the need for long sequences of random numbers in computer programs, procedures have been developed to generate numbers that pass many statistical tests that numbers selected truly at random pass. The numbers that such procedures generate are called pseudorandom numbers. We will introduce several techniques to generate pseudorandom numbers based on modular arithmetic and the concepts of the order of integers and primitive roots.

We will also introduce a public key cryptosystem, known as the ElGamal cryptosystem, defined using the concept of a primitive root of a prime. The security of this cryptosystem is based on the difficulty of the problem of finding discrete logarithms modulo a prime. We will explain how to encrypt and decrypt messages using ElGamal encryption, and how to sign messages in this cryptosystem.

Finally, we will discuss an application of the concepts of the order of an integer and of primitive roots to the splicing of telephone cables.

10.1 Pseudorandom Numbers

Numbers chosen at random are useful in many applications. Random numbers are needed for computer simulations used to study phenomena in areas such as nuclear physics, operations research, and data networking. They can be used to construct random samples so that the behavior of a system can be studied when it is impossible to test all possible cases. Random numbers are used to test the performance of computer algorithms, and to run randomized algorithms that make random choices during their execution. Random

numbers are also extensively used in numerical analysis. For instance, random numbers can be used to estimate integrals using Riemann sums, a topic studied in calculus. In number theory, random numbers are used in probabilistic primality tests. In cryptography, random number have many applications, such as in generation of cryptokeys and in the execution of cryptographic protocols.

When we talk about *random numbers,* we mean the terms of a sequence of numbers in which each term is selected by chance without any dependence on the other terms of the sequence, and with a specified probability of lying in a particular interval. (It really makes no sense to say that a particular number, such as 47, is random, although it can be a term of a sequence of random numbers.) Before 1940, scientists requiring random numbers produced them by rolling dice, spinning roulette wheels, picking balls out of an urn, dealing cards, or taking random digits from tabulated data, such as census reports. In the 1940s, machines were invented to produce random numbers, and in the 1950s, computers were used to generate random numbers using random noise generators. However, random numbers produced by a mechanical process often became skewed from malfunctions in computer hardware. Another important problem was that random numbers generated using physical phenomena could not be reproduced to check the results of a computer program.

The idea of generating random numbers using computer programs instead of via mechanical method was first proposed in 1946 by *John von Neumann.* The method he suggested, called the *middle-square method,* works as follows. To generate four-digit random numbers, we start with an arbitrary four-digit number, say 6139. We square this number to obtain 37687321, and we take the middle four digits, 6873, as the second random number. We iterate this procedure to obtain a sequence of random numbers, always squaring and removing the middle four digits to obtain a new random number from the preceding one. (The square of a four-digit number has eight or fewer digits. Those with fewer than eight digits are considered eight-digit numbers by adding initial digits of 0.)

Sequences produced by the middle-square method are, in reality, not randomly chosen. When the initial four-digit number is known, the entire sequence is determined. However, the sequence of numbers produced appears to be random, and the numbers

JOHN VON NEUMANN (1903–1957) was born in Budapest, Hungary. In 1930, after holding several positions at universities in Germany, he came to the United States. In 1933, von Neumann became, along with Albert Einstein, one of the first members of the famous Institute for Advanced Study in Princeton, New Jersey. Von Neumann was one of the most versatile mathematical talents of the twentieth century. He invented the mathematical discipline known as game theory; using game theory, he made many important discoveries in mathematical economics. Von Neumann made fundamental contributions to the development of the first computers, and participated in the early development of atomic weapons.

produced are useful for computer simulations. The integers in sequences that have been chosen in some methodical manner, but appear to be random, are called *pseudorandom numbers.*

It turns out that the middle-square method has some unfortunate weaknesses. The most undesirable feature of this method is that, for many choices of the initial integer, the method produces the same small set of numbers over and over. For instance, starting with the four-digit integer 4100 and using the middle-square method, we obtain the sequence 8100, 6100, 2100, 4100, 8100, 6100, 2100, . . . , which only gives four different numbers before repeating.

The Linear Congruential Generation

The most commonly used method for generating pseudorandom numbers, called the *linear congruential method*, was introduced by D. H. Lehmer in 1949. It works as follows: Integers m, a, c, and x_0 are chosen so that $2 \leq a < m, 0 \leq c < m$, and $0 \leq x_0 \leq m$. The sequence of pseudorandom numbers is defined recursively by

$$x_{n+1} \equiv ax_n + c \pmod{m}, \quad 0 \leq x_{n+1} < m,$$

for $n = 0, 1, 2, 3, \ldots$. We call m the *modulus, a* the *multiplier, c* the *increment,* and x_0 the *seed* of the pseudorandom numbers generator. The following examples illustrate the linear congruential method.

Example 10.1. When we take $m = 12, a = 3, c = 4$, and $x_0 = 5$ in the linear congruential generator, we have $x_1 \equiv 3 \cdot 5 + 4 \equiv 7 \pmod{12}$, so that $x_1 = 7$. Similarly, we find that $x_2 = 1$, because $x_2 \equiv 3 \cdot 7 + r \equiv 1 \pmod{12}$, $x_3 = 7$, because $x_3 \equiv 3 \cdot 1 + r \equiv 7 \pmod{12}$, and so on. Hence, the generator produces just three different integers before repeating. The sequence of pseudorandom numbers obtained is 5, 7, 1, 7, 1, 7, 1, ... ◀

Example 10.2. When we take $m = 9, a = 7, c = 4$, and $x_0 = 3$ in the linear congruential generator, we obtain the sequence 3,7,8,6,1,2,0,4,5,3, . . . (as should be verified by the reader). This sequence contains nine different numbers before repeating. ◀

Remark. For computer simulations it is often necessary to generate pseudorandom numbers between 0 and 1. We can obtain such numbers by using a linear congruential generator to produce pseudorandom numbers $x_i, i = 1, 2, 3, \ldots$ between 0 and m, and then dividing each number by m, obtaining the sequence $x_i/m, i = 1, 2, 3, \ldots$.

The following theorem tells us how to find the terms of a sequence of pseudorandom numbers generated by the linear congruential method directly from the multiplier, the increment, and the seed.

Theorem 10.1. The terms of the sequence generated by the linear congruential method previously described are given by

$$x_k \equiv a^k x_0 + c(a^k - 1)/(a - 1) \pmod{m}, \quad 0 \leq x_k < m.$$

Proof. We prove this result using mathematical induction. For $k = 1$, the formula is obviously true, because $x_1 \equiv ax_0 + c \pmod{m}$, $0 \le x_1 < m$. Assume that the formula is valid for the kth term, so that

$$x_k \equiv a^k x_0 + c(a^k - 1)/(a - 1) \pmod{m}, \quad 0 \le x_k < m.$$

Because

$$x_{k+1} \equiv ax_k + c \pmod{m}, \quad 0 \le x_{k+1} < m,$$

we have

$$\begin{aligned} x_{k+1} &\equiv a(a^k x_0 + c(a^k - 1)/(a - 1)) + c \\ &\equiv a^{k+1} x_0 + c(a(a^k - 1)/(a - 1) + 1) \\ &\equiv a^{k+1} x_0 + c(a^{k+1} - 1)/(a - 1) \pmod{m}, \end{aligned}$$

which is the correct formula for the $(k + 1)$st term. This demonstrates that the formula is correct for all positive integers k. ∎

The *period length* of a linear congruential pseudorandom number generator is the maximum length of the sequence obtained without repetition. We note that the longest possible period length for a linear congruential generator is the modulus m. The following theorem tells us when this maximum length is obtained.

Theorem 10.2. The linear congruential generator produces a sequence of period length m if and only if $(c, m) = 1$, $a \equiv 1 \pmod{p}$ for all primes p dividing m, and $a \equiv 1 \pmod{4}$ if $4 \mid m$.

Because the proof of Theorem 10.2 is complicated and quite lengthy, we omit it. The reader is referred to [Kn97] for a proof.

The Pure Multiplicative Congruential Method

The case of the linear congruential generator with $c = 0$ is of special interest because of its simplicity. In this case, the method is called the *pure multiplicative congruential method.* We specify the modulus m, multiplier a, and seed x_0. The sequence of pseudorandom numbers is defined recursively by

$$x_{n+1} \equiv ax_n \pmod{m}, \quad 0 < x_{n+1} < m.$$

In general, we can express the pseudorandom numbers generated in terms of the multiplier and seed:

$$x_n \equiv a^n x_0 \pmod{m}, \quad 0 < x_{n+1} < m.$$

If l is the period length of the sequence obtained using this pure multiplicative generator, then l is the smallest positive integer such that

$$x_0 \equiv a^l x_0 \pmod{m}.$$

If $(x_0, m) = 1$, using Corollary 4.4.1 we have

$$a^l \equiv 1 \pmod{m}.$$

From this congruence, we know that the largest possible period length is $\lambda(m)$, where $\lambda(m)$ is the minimal universal exponent modulo m.

For many applications, the pure multiplicative generator is used with the modulus m equal to the Mersenne prime $M_{31} = 2^{31} - 1$. When the modulus m is a prime, the maximum period length is $m - 1$, and this is obtained when a is a primitive root of m. To find a primitive root of M_{31} that can be used with good results, we first demonstrate that 7 is a primitive root of M_{31}.

Theorem 10.3. The integer 7 is a primitive root of $M_{31} = 2^{31} - 1$.

Proof. To show that 7 is a primitive root of $M_{31} = 2^{31} - 1$, it is sufficient to show that

$$7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}},$$

for all prime divisors q of $M_{31} - 1$. With this information, we can conclude that $\operatorname{ord}_{M_{31}} 7 = M_{31} - 1$. To find the factorization of $M_{31} - 1$, we note that

$$\begin{aligned} M_{31} - 1 = 2^{31} - 2 &= 2(2^{30} - 1) = 2(2^{15} - 1)(2^{15} + 1) \\ &= 2(2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

If we show that

$$7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}},$$

for $q = 2, 3, 7, 11, 31, 151$, and 331, then we know that 7 is a primitive root of $M_{31} =$ 2,147,483,647. Because

$$\begin{aligned} 7^{(M_{31}-1)/2} &\equiv 2{,}147{,}483{,}646 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/3} &\equiv 1{,}513{,}477{,}735 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/7} &\equiv \quad 120{,}536{,}285 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/11} &\equiv 1{,}969{,}212{,}174 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/31} &\equiv \qquad 512 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/151} &\equiv \quad 535{,}044{,}134 \not\equiv 1 \pmod{M_{31}} \\ 7^{(M_{31}-1)/331} &\equiv 1{,}761{,}885{,}083 \not\equiv 1 \pmod{M_{31}}, \end{aligned}$$

we see that 7 is a primitive root of M_{31}. ∎

In practice, we do not want to use the primitive root 7 as the generator, because the first few integers generated are small. Instead, we find a larger primitive root using Corollary 9.4.1. We use 7^k, where $(k, M_{31} - 1) = 1$. For instance, because $(5, M_{31} - 1) = 1$, we know that $7^5 = 16{,}807$ is a primitive root. Because $(13, M_{31} - 1) = 1$, another possibility is to use $7^{13} \equiv 252{,}246{,}292 \pmod{M_{31}}$ as the multiplier.

The Square Pseudorandom Number Generator

Another example of a pseudorandom number generator is the *square pseudorandom number generator*. Given a positive integer n (the *modulus*) and an initial term x_0 (the *seed*), this generator produces a sequence of pseudorandom numbers using the congruence

$$x_{i+1} \equiv x_i^2 \pmod{n}, \quad 0 \le x_{i+1} < n.$$

From this definition, we can easily see that

$$x_i \equiv x_0^{2^i} \pmod{n}, \quad 0 \le x_i < n.$$

Example 10.3. Let $n = 209$ be the modulus and $x_0 = 6$ the seed of the square pseudorandom number generator. The sequence produced by this generator is

$$6, 36, 42, 92, 104, 157, 196, 169, 137, 168, 9, 81, 82, 36, 42, \ldots.$$

We see that this sequence has a a period of length 12. The first term is not part of the period. ◀

We can determine the length of the period of a square pseudorandom number generator using the concept of order modulo n, as the following theorem shows.

Theorem 10.4. The length of the period of the square pseudorandom number with seed x_0 and modulus n is $\text{ord}_s 2$, where the integer s is the odd positive integer such that $\text{ord}_n x_0 = 2^t s$, where t is a nonnegative integer.

Proof. We will show that $\text{ord}_s 2$ divides ℓ, the length of the period of this generator. Suppose that $x_j = x_{j+\ell}$ for some integer j. Then

$$x_0^{2^j} \equiv x_0^{2^{j+\ell}} \pmod{n},$$

which implies that

$$x_0^{2^{j+\ell}-2^j} \equiv 1 \pmod{n}.$$

Using the definition of the order of an integer modulo n, we see that

$$\text{ord}_n x_0 \mid (2^{j+\ell} - 2^j),$$

or, equivalently, that

$$2^{j+\ell} \equiv 2^j \pmod{2^t s}. \tag{10.1}$$

Because $2^t \mid (2^{j+\ell} - 2^j)$ and $2^{j+\ell} - 2^j = 2^j(2^\ell - 1)$, we see that $j \ge t$. By congruence (10.1) and Theorem 4.4, it follows that

$$2^{j+\ell-t} \equiv 2^{j-t} \pmod{s}.$$

Using Theorem 9.2, we see that $j + \ell - t \equiv j - t \pmod{\text{ord}_2 s}$. Hence, $\ell \equiv 0 \pmod{\text{ord}_2 s}$, which means that $\text{ord}_2 s$ divides ℓ, the period length.

We will now show that the period ℓ divides $\text{ord}_s 2$. To show that $\text{ord}_s 2$ is a multiple of ℓ, we need only show that there are two terms x_j and $x_j = x_k$ such that $j \equiv k \pmod{\text{ord}_s 2}$. To accomplish this, we suppose that $j \equiv k \pmod{\text{ord}_s 2}$ and that $k \geq j \geq t$. By Theorem 9.2, we see that

$$2^j \equiv 2^k \pmod{s}.$$

Furthermore, we have

$$2^k \equiv 2^j \pmod{2^t},$$

because $2^k - 2^j = 2^j(2^{k-j} - 1)$ and $j \geq t$. By Corollary 4.8.1 and the fact that $(2^t, s) = 1$, we can conclude that

$$2^j \equiv 2^k \pmod{2^t s}.$$

Because $\text{ord}_n x_0 = 2^t s$, we know that

$$\text{ord}_n x_0 \mid (2^k - 2^j),$$

which means that

$$x^{2^k - 2^j} \equiv 1 \pmod{n},$$

which in turn tells us that

$$x^{2^k} \equiv x^{2^j} \pmod{n}.$$

This implies that $x_k = x_j$. We conclude that $\text{ord}_s 2$ must be a multiple of ℓ, completing the proof. ■

Example 10.4. In Example 10.3, we used the modulus $n = 209$ and the seed $x_0 = 6$ in the square pseudorandom generator. We note that $\text{ord}_{209} 6 = 90$ (as the reader should verify). Because $90 = 2 \cdot 45$, Theorem 10.4 tells us that the period length of this generator is $\text{ord}_{45} 2 = 12$ (as the reader should verify). This is the length we observed when we listed the terms generated. ◀

How can we tell whether the terms of a sequence of pseudorandom numbers are useful for computer simulations and other applications? One method is to see whether these numbers pass statistical tests designed to determine whether a sequence has particular characteristics that a truly random sequence would most likely have. A battery of such tests can be used to evaluate pseudorandom number generators. For example, the frequencies of numbers can be tested, as can the frequencies of pairs of numbers. The frequencies of the appearance of subsequences can be checked, as can the frequency of runs of the same number of various lengths. An autocorrelation test that checks whether there are correlations of the sequence and shifted versions of it may also be helpful. These and other tests are discussed in [Kn97] and [MevaVa97].

For cryptographic applications, pseudorandom number generators must not be predictable. For example, a linear congruential pseudorandom number generator cannot be used for cryptographic applications because, in sequences generated this way, knowledge of several consecutive terms can be used to find other terms. Instead, *cryptographically*

secure pseudorandom number generators must be used. These produce sequences such that the terms of the sequence are unpredictable to an adversary with limited computational resources. These notions are made more precise in [MevaVa97], and in [La90].

We have only briefly touched upon the subject of pseudorandom numbers. For a thorough discussion of pseudorandom numbers, see [Kn97], and for a survey of the relationships between pseudorandom number generators and cryptography, see the chapter by Lagarias in [Po90].

10.1 Exercises

1. Find the sequence of two-digit pseudorandom numbers generated using the middle-square method, taking 69 as the seed.
2. Find the first ten terms of the sequence of pseudorandom numbers generated by the linear congruential method with $x_0 = 6$ and $x_{n+1} \equiv 5x_n + 2 \pmod{19}$. What is the period length of this generator?
3. Find the period length of the sequence of pseudorandom numbers generated by the linear congruential method with $x_0 = 2$ and $x_{n+1} \equiv 4x_n + 7 \pmod{25}$.
4. Show that if either $a = 0$ or $a = 1$ is used for the multiplier in the linear congruential method, the result would not be a good choice for a sequence of pseudorandom numbers.
5. Using Theorem 10.2, find those integers a that give period length m, where $(c, m) = 1$, for the linear congruential generator $x_{n+1} \equiv ax_n + c \pmod{m}$, for each of the following moduli.

   a) $m = 1000$ c) $m = 10^6 - 1$
   b) $m = 30030$ d) $m = 2^{25} - 1$

* 6. Show that every linear congruential pseudorandom number generator can be simply expressed in terms of a linear congruential generator with increment $c = 1$ and seed 0, by showing that the terms generated by the linear congruential generator $x_{n+1} \equiv ax_n + c \pmod{m}$, with seed x_0, can be expressed as $x_n \equiv b \cdot y_n + x_0 \pmod{m}$, where $b \equiv (a-1)x_0 + c \pmod{m}$, $y_0 = 0$, and $y_{n+1} \equiv ay_n + 1 \pmod{m}$.

7. Find the period length of the pure multiplicative pseudorandom number generator $x_n \equiv cx_{n-1} \pmod{2^{31} - 1}$ for each of the following multipliers c.

   a) 2 c) 4 e) 13
   b) 3 d) 5 f) 17

8. Show that the maximal possible period length for a pure multiplicative generator of the form $x_{n+1} \equiv ax_n \pmod{2^e}$, $e \geq 3$, is 2^{e-2}. Show that this is obtained when $a \equiv \pm 3 \pmod{8}$.
9. Find the sequence of numbers generated by the square pseudorandom number generator with modulus 77 and seed 8.
10. Find the sequence of numbers generated by the square pseudorandom number generator with modulus 1001 and seed 5.
11. Use Theorem 10.4 to find the period length of the pseudorandom sequence in Exercise 9.

12. Use Theorem 10.4 to find the period length of the pseudorandom sequence in Exercise 10.

13. Show that longest possible period of any sequence of pseudorandom numbers generated by the square pseudorandom number generator with modulus 77, regardless of the seed chosen, is 4.

14. What is the longest possible period of any sequence of pseudorandom numbers generated by the square pseudorandom number generator with modulus 989, regardless of the seed chosen?

Another way to generate pseudorandom numbers is to use the *Fibonacci generator.* Let m be a positive integer. Two initial integers x_0 and x_1, both less than m, are specified, and the rest of the sequence is generated recursively by the congruence $x_{n+1} \equiv x_n + x_{n-1} \pmod{m}$, $0 \leq x_{n+1} < m$.

15. Find the first eight pseudorandom numbers generated by the Fibonacci generator with modulus $m = 31$ and initial values $x_0 = 1$ and $x_1 = 24$.

16. Find a good choice for the multiplier a in the pure multiplicative pseudorandom number generator $x_{n+1} \equiv ax_n \pmod{101}$. (*Hint:* Find a primitive root of 101 that is not too small.)

17. Find a good choice for the multiplier a in the pure multiplicative pseudorandom number generator $x_n \equiv ax_{n-1} \pmod{2^{25} - 1}$. (*Hint:* Find a primitive root of $2^{25} - 1$ and then take an appropriate power of this root.)

18. Find the multiplier a and increment c of the linear congruential pseudorandom number generator $x_{n+1} \equiv ax_n + c \pmod{1003}$, $0 \leq x_{n+1} < 1003$, if $x_0 = 1, x_2 = 402$, and $x_3 = 361$.

19. Find the multiplier a of the pure multiplicative pseudorandom number generator $x_{n+1} \equiv ax_n \pmod{1000}$, $0 \leq x_{n+1} < 1000$, if 313 and 145 are consecutive terms generated.

20. The *discrete exponential generator* takes a positive integer x_0 as its seed and generates pseudorandom numbers $x_1, x_2, x_3, \ldots$ using the recursive definition $x_{n+1} \equiv g^{x_n} \pmod{p}$, $0 < x_{n+1} < p$, for $n = 0, 1, 2, \ldots$, where p is an odd prime and g is a primitive root modulo p.
    a) Find the sequence of pseudorandom numbers generated by the discrete exponential generator with $p = 17, g = 3$, and $x_0 = 2$.
    b) Find the sequence of pseudorandom numbers generated by the discrete exponential generator with $p = 47, g = 5$, and $x_0 = 3$.
    c) Given a term of a sequence of pseudorandom numbers generated by using a discrete exponential generator, can the previous term be found easily when the prime p and primitive root g are known?

21. Another method of generating pseudorandom numbers is to use the *power generator* with parameters m, d. Here, m is a positive integer and d is a positive integer relatively prime to $\phi(m)$. The generator starts with a positive integer x_0 as its seed and generates pseudorandom numbers $x_1, x_2, x_3, \ldots$ using the recursive definition $x_{n+1} \equiv x_n^d \pmod{m}$, $0 < x_{n+1} < m$.
    a) Find the sequence of pseudorandom numbers generated by a power generator with $m = 15, d = 3$, and seed $x_0 = 2$.
    b) Find the sequence of pseudorandom numbers generated by a power generator with $m = 23, d = 3$, and seed $x_0 = 3$.

10.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Examine the behavior of the sequence of five-digit pseudorandom numbers produced by the middle-square method, starting with different choices of the initial term.
2. Find the period length of different linear congruential pseudorandom generators of your choice.
3. How long is the period of the linear congruential pseudorandom number generator with $a = 65{,}539$, $c = 0$, and $m = 2^{31}$?
4. How long is the period of the linear congruential pseudorandom number generator with $a = 69{,}069$, $c = 1$, and $m = 2^{32}$?
5. Find a seed that produces the longest possible period length for the square pseudorandom number generator with modulus 2867.
6. Show that the square pseudorandom number generator with modulus 9,992,503 and seed 564 has a period length of 924.
7. Find the period length of different *quadratic congruential* pseudorandom number generators; that is, generators of the form $x_{n+1} \equiv (ax_n^2 + bx_n + c) \pmod{m}$, $0 \leq x_{n+1} < m$, where a, b, and c are integers. Can you find conditions that guarantee that the period of this generator is m?
8. Determine the length of the period of the Fibonacci generator described in the preamble to Exercise 15 for various choices of the modulus m. Do you think this is a good generator of pseudorandom numbers?
9. There are a variety of empirical tests to measure the randomness of pseudorandom number generators. Ten such tests are described in Knuth [Kn97]. Look up these tests and apply some of them to different pseudorandom number generators.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to generate pseudorandom numbers using the following generators.

1. The middle-square generator
2. The linear congruential generator
3. The pure multiplicative generator
4. The square generator
5. The Fibonacci generator (see the preamble to Exercise 15)
6. The discrete exponential generator (see Exercise 20)
7. The power generator (see Exercise 21)

10.2 The ElGamal Cryptosystem

In Chapter 8, we introduced the RSA public key cryptosystem. The security of the RSA cryptosystem is based on the difficulty of factoring integers. In this section, we introduce another public key cryptosystem known as the ElGamal cryptosystem, invented by T. ElGamal in 1985. Its security is based on the difficulty of finding discrete logarithms modulo a large prime. (Recall that if p is a prime and r is a primitive root of p, the discrete logarithm of an integer a is the exponent x for which $r^x \equiv a \pmod{p}$.)

In the ElGamal cryptosystem, each person selects a prime p, a primitive root r of p, and an integer a with $0 \leq a \leq p-1$. This exponent is the private key, that is, it is the information kept secret by that person. The corresponding public key is (p, r, b), where b is the integer with

$$b \equiv r^a \pmod{p}, 0 \leq a \leq p-1.$$

In the following example, we illustrate how keys for the ElGamal cryptosystem are selected.

Example 10.5. To generate a public and private key for the ElGamal cryptosystem, we first select a prime p. Here we will take $p = 2539$. (This four-digit prime is selected to illustrate how the cryptosystem works; in practice, a prime with several hundred digits should be used.) Next, we need a primitive root of this prime p. We select the primitive root $r = 2$ of 2539 (as the reader should verify). Next, we choose an integer a with $0 \leq a \leq 2538$. We choose $a = 14$. This exponent a is the private key. The corresponding public key is the triple $(p, r, b) = (2539, 2, 1150)$, because $b \equiv 2^{14} \equiv 1150 \pmod{2539}$. ◀

Before we encrypt a message using the ElGamal cryptosystem, we will translate letters into their numerical equivalents and then form blocks of the largest possible size (with an even number of digits), as we did when we encrypted messages in Section 8.4 using the RSA cryptosystem. (This is just one of many ways to translate messages made up of characters into integers.) To encrypt a message to be sent to the person with public key (p, r, b), we first select a random number k with $1 \leq k \leq p-2$. For each plaintext block P, we compute the integers γ and δ with

$$\gamma \equiv r^k \pmod{p}, \quad 0 \leq \gamma \leq p-1$$

and

$$\delta \equiv P \cdot b^k \pmod{p}, \quad 0 \leq \delta \leq p-1.$$

The ciphertext corresponding to the plaintext block P is the ordered pair $E(P) = (\gamma, \delta)$. The plaintext message P has been hidden by multiplying it by b^k to produce δ. This hidden message is transmitted together with γ. Only the person with the secret key a can compute b^k and γ, and use this to recover the original message.

When messages are encrypted using the ElGamal cryptosystem, the ciphertext corresponding to a plaintext block is twice as long as the original plaintext block. We say that this encryption method has a *message expansion factor* of 2. The random number k

is included in the encryption procedure to increase security in several ways that we will describe later in this section.

Decrypting a message encrypted using ElGamal encryption depends on knowledge of a, the private key. The first step of the decryption of a ciphertext pair (γ, δ) is to compute $\overline{\gamma^a}$. This is done by computing γ^{p-1-a} modulo p. Then, the pair $C = (\gamma, \delta)$ is decrypted by computing

$$D(C) = \overline{\gamma^a}\delta.$$

To see that this recovers the plaintext message note that

$$\begin{aligned} D(C) &\equiv \overline{\gamma^a}\delta \pmod{p} \\ &\equiv \overline{r^{ka}} \cdot Pb^k \pmod{p} \\ &\equiv \overline{(r^a)}^k Pb^k \pmod{p} \\ &\equiv \overline{b^k} Pb^k \pmod{p} \\ &\equiv \overline{b^k} b^k P \pmod{p} \\ &\equiv P \pmod{p}. \end{aligned}$$

Example 10.6 illustrates encryption and decryption using the ElGamal cryptosystem.

Example 10.6. We will encrypt the message

PUBLIC KEY CRYPTOGRAPHY

using the ElGamal cryptosystem with the public key we constructed in Example 10. In Example 8.16, we encrypted this same message using the RSA cryptosystem. We translated the letters into their numerical equivalents and then grouped numbers into blocks of four decimal digits. We can use this same grouping here because the largest possible block is 2525. The blocks we obtained were

1520 0111 0802 1004
2402 1724 1519 1406
1700 1507 2423,

where the dummy letter X is translated into 23 at the end of the passage to fill out the final block. ◀

To encrypt these blocks, we first select a random number k with $1 \leq k \leq 2537$ (we will use the same k for each block here; in practice, a different number k is chosen for each block to ensure a higher level of security). Picking $k = 1443$, we encrypt each plaintext block P in a ciphertext block, using the relationship $E(C) = (\gamma, \delta)$, with

$$\gamma \equiv 2^{1443} \equiv 2141 \pmod{2539}$$

and

$$\delta \equiv P \cdot 1150^{1443} \pmod{2539}, \quad 0 \leq \delta \leq 2538.$$

For example, the first block is encrypted to (2141, 216), because

$$\gamma \equiv 2^{1443} \equiv 2141 \pmod{2539}$$

and

$$\delta \equiv 1520 \cdot 1150^{1443} \equiv 216 \pmod{2539}.$$

When we encrypt each block, we obtain the following ciphertext message:

$$(2141, 0216)\ (2141, 1312)\ (2141, 1771)\ (2141, 1185)$$
$$(2141, 2132)\ (2141, 1177)\ (2141, 1938)\ (2141, 2231)$$
$$(2141, 1177)\ (2141, 1938)\ (2141, 1694).$$

To decrypt a ciphertext block, we compute

$$D(C) \equiv \overline{\gamma^{14}}\delta \pmod{2539}.$$

For example, to decrypt the second ciphertext block (2141, 1312), we compute

$$\begin{aligned} D((2141, 1312)) &\equiv \overline{2141^{14}} \cdot 1312 \\ &\equiv \overline{1430} \cdot 1312 \\ &\equiv 2452 \cdot 1312 \\ &\equiv 111 \pmod{2539}. \end{aligned}$$

We have used the fact that 2452 is an inverse of 1430 modulo 2539. This inverse can be found using the extended Euclidean algorithm, as the reader should verify. (We have also used the fact that $2141^{14} \equiv 1430 \pmod{2539}$.)

As mentioned, the security of the ElGamal cryptosystem is based on the difficulty of determining the private key a from the public key (p, r, b), an instance of the discrete logarithm problem, a computationally difficult problem described in Section 9.4. Breaking the ElGamal encryption method requires the recovery of a message P given the public key (p, r, b) together with the encrypted message (γ, δ) without knowledge of the private key a. Although there may be another way to do this other than solving a discrete logarithm problem, it is widely thought that this is a computationally difficult problem.

Signing Messages in the ElGamal Cryptosystem

We will describe a procedure invented by T. ElGamal in 1985 for signing messages using the ElGamal cryptosystem. Suppose that a person's public key is (p, r, b) and his private key is a, so that $b \equiv r^a \pmod{p}$. To sign a message P, the person with private key a does the following: First, he selects an integer k with $(k, p-1) = 1$. Next, he computes γ, where

$$\gamma \equiv r^k \pmod{p}, \quad 0 \le \gamma \le p-1$$

and

$$s \equiv (P - a\gamma)\bar{k} \pmod{p-1}, \quad 0 \le s \le p-2.$$

The signature on the message P is the pair (γ, s). Note that this signature depends on the value of the random integer k and can only be computed with knowledge of the private key a.

To see that this is a valid signature scheme, note that we know the public key (p, r, b), hence we can verify that the message came from the person who supposedly sent it. To do this, we compute

$$V_1 \equiv \gamma^s b^\gamma \pmod{p}, \quad 0 \le V_1 \le p-1$$

and

$$V_2 \equiv r^P \pmod{p}, \quad 0 \le V_2 \le p-1.$$

For this signature to be valid, we must have $V_1 = V_2$. If the signature is valid, then

$$\begin{aligned} V_1 &\equiv \gamma^s b^\gamma \pmod{p} \\ &\equiv \gamma^{(P-a\gamma)\overline{k}} b^\gamma \pmod{p} \\ &\equiv (\gamma^{\overline{k}})^{P-a\gamma} b^\gamma \pmod{p} \\ &\equiv r^{(P-a\gamma)} b^\gamma \pmod{p} \\ &\equiv r^P \overline{r^{a\gamma}} b^\gamma \pmod{p} \\ &\equiv r^P \overline{b^\gamma} b^\gamma \pmod{p} \\ &\equiv r^P \pmod{p} \\ &= V_2. \end{aligned}$$

A different integer k should be chosen to sign each message in the ElGamal signature scheme. If the same integer k is chosen for two signatures, it can be found from these signatures, making it possible to find the private key a (see Exercise 8). Another concern is whether someone could forge a signature on a message P by selecting an integer k and computing $\gamma \equiv r^k \pmod{p}$ using the public key (p, r, b). To complete the signature, this person also would have to compute $s = (P - a\gamma)\overline{k} \pmod{p-1}$. She cannot easily find a, because computing a from b requires that a discrete logarithm be found, namely the discrete logarithm of b with respect to r modulo p. Not knowing a, a person could select a value of s at random. The probability that this would work is only $1/p$, which is close to zero when p is large.

Example 10.7 illustrates how a message is signed using the ElGamal signature scheme.

Example 10.7. Suppose that a person has a public ElGamal key of $(p, r, b) = (2539, 2, 1150)$ with corresponding private ElGamal key $a = 14$. To sign the plaintext message $P = 111$, they first choose the integer $k = 457$, selected at random with $1 \le k \le 2538$ and $(k, 2538) = 1$. Note that $\overline{457} = 2227 \pmod{2538}$. ◀

The signature of this plaintext message 111 is found by computing

$$\gamma \equiv 2^{457} \equiv 1079 \pmod{2539}$$

and

$$s \equiv (111 - 14 \cdot 1079) \cdot 2227 \equiv 1139 \pmod{2538}.$$

Anyone who has this signature (1079, 1139) and the message 111 can verify that the signature is valid by computing

$$1150^{1079}1079^{1139} \equiv 1158 \pmod{2539}$$

and

$$2^{111} \equiv 1158 \pmod{2539}.$$

The ElGamal signature scheme has been modified to create another signature scheme that is widely used, known as the *Digital Signature Algorithm (DSA)*. The DSA was incorporated in 1994 as a U.S. government standard, Federal Information Processing Standard (FIPS) 186, commonly known as the *Digital Signature Standard*. To learn how the ElGamal signature scheme was modified to produce the DSA, consult [St95] and [MevaVa97].

10.2 Exercises

1. Encrypt the message HAPPY BIRTHDAY using the ElGamal cryptosystem with the public key $(p, r, b) = (2551, 6, 33)$. Show how the resulting ciphertext can be decrypted using the private key $a = 13$.
2. Encrypt the message DO NOT PASS GO using the ElGamal cryptosystem with the public key (2591, 7, 591). Show how the resulting ciphertext can be decrypted using the private key $a = 99$.
3. Decrypt the message (2161, 660), (2161, 1284), (2161, 1467) encrypted using the ElGamal cryptosystem with public key (2713, 5, 193) corresponding to the private key 17.
4. Decrypt the message (1061, 2185), (1061, 733), (1061, 1096) encrypted using the ElGamal cryptosystem with public key (2677, 2, 1410) corresponding to the private key 133.
5. Find the signature produced by the ElGamal signature scheme for the plaintext message $P = 823$ with public key $(p, r, b) = (2657, 3, 801)$, private key $a = 211$, and where the integer $k = 101$ is selected to construct the signature. Show how this signature is verified.
6. Find the signature produced by the ElGamal signature scheme for the plaintext message $P = 2525$ with public key $(p, r, b) = (2543, 5, 1615)$, private key $a = 99$, and where the integer $k = 257$ is selected to construct the signature. Show how this signature is verified.

7. Show that if the same random number k is used to encrypt two plaintext messages P_1 and P_2 using ElGamal encryption, then P_2 can be found once the plaintext message P_1 is known.
8. Show that if the same integer k is used to sign two different messages using the ElGamal signature scheme, producing signatures (γ_1, s_1) and (γ_2, s_2), the integer k can be found from these signatures as long as $s_1 \not\equiv s_2 \pmod{p-1}$. Show that once k has been found, the private key a is easily found.

10.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Construct a private key, public key pair for the ElGamal cryptosystem for each member of your class. Put together a directory of the public keys.
2. For each member of your class, encrypt a message using the ElGamal cryptosystem using the public keys published in the directory.
3. Decrypt the messages sent to you by your classmates that were encrypted using your ElGamal public key.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following things.

1. Encrypt messages using an ElGamal cryptosystem.
2. Decrypt messages that were encrypted using an ElGamal cryptosystem.
3. Sign messages using the ElGamal cryptosystem.

10.3 An Application to the Splicing of Telephone Cables

An interesting application of the preceding material involves the splicing of telephone cables. We base our discussion on the explosion in [Or88], relating the contents of an original article by Lawther [La35], reporting on work done for the Southwestern Bell Telephone Company.

To develop the application, we first make the following definition.

Definition. Let m be a positive integer and let a be an integer relatively prime to m. The *± 1-exponent of a modulo m* is the smallest positive integer x such that

$$a^x \equiv \pm 1 \pmod{m}.$$

We are interested in determining the largest possible ± 1-exponent of an integer modulo m; we denote this by $\lambda_0(m)$. The following two theorems relate the value of the maximal ± 1-exponent $\lambda_0(m)$ to $\lambda(m)$, the minimal universal exponent modulo m.

First, we consider positive integers that possess primitive roots.

Theorem 10.5. If m is a positive integer, $m > 2$, with a primitive root, then the maximal ± 1-exponent $\lambda_0(m)$ equals $\phi(m)/2 = \lambda(m)/2$.

Proof. We first note that if m has a primitive root, then $\lambda(m) = \phi(m)$. By Theorem 7.6, we know that $\phi(m)$ is even, so that $\phi(m)/2$ is an integer, if $m > 2$. Euler's theorem tells us that

$$a^{\phi(m)} = (a^{\phi(m)/2})^2 \equiv 1 \pmod{m},$$

for all integers a with $(a, m) = 1$. By Exercise 13 of Section 9.3, we know that when m has a primitive root, the only solutions of $x^2 \equiv 1 \pmod{m}$ are $x \equiv \pm 1 \pmod{m}$. Hence,

$$a^{\phi(m)/2} \equiv \pm 1 \pmod{m}.$$

This implies that

$$\lambda_0(m) \leq \phi(m)/2.$$

Now, let r be a primitive root of modulo m with ± 1-exponent e. Then

$$r^e \equiv \pm 1 \pmod{m},$$

so that

$$r^{2e} \equiv 1 \pmod{m}.$$

Because $\text{ord}_m r = \phi(m)$, Theorem 9.1 tells us that $\phi(m) \mid 2e$, or equivalently, that $(\phi(m)/2) \mid e$. Hence, the maximum ± 1-exponent $\lambda_0(m)$ is at least $\phi(m)/2$. However, we know that $\lambda(m) \leq \phi(m)/2$. Consequently, $\lambda_0(m) = \phi(m)/2 = \lambda(m)/2$. ∎

We now will find the maximal ± 1-exponent of integers without primitive roots.

Theorem 10.6. If m is a positive integer without a primitive root, then the maximal ± 1-exponent $\lambda_0(m)$ equals $\lambda(m)$, the minimal universal exponent of m.

Proof. We first show that if a is an integer of order $\lambda(m)$ modulo m with ± 1-exponent e such that

$$a^{\lambda(m)/2} \not\equiv -1 \pmod{m},$$

then $e = \lambda(m)$. Consequently, once we have found such an integer a, we will have shown that $\lambda_0(m) = \lambda(m)$.

Assume that a is an integer of order $\lambda(m)$ modulo m with ± 1-exponent e such that

$$a^{\lambda(m)/2} \not\equiv -1 \pmod{m}.$$

Because $a^e \equiv \pm 1 \pmod{m}$, it follows that $a^{2e} \equiv 1 \pmod{m}$. By Theorem 9.1, we know that $\lambda(m) \mid 2e$. Because $\lambda(m) \mid 2e$ and $e \leq \lambda(m)$, either $e = \lambda(m)/2$ or $e = \lambda(m)$. To see that $e \neq \lambda(m)/2$, note that $a^e \equiv \pm 1 \pmod{m}$, but $a^{\lambda(m)/2} \not\equiv 1 \pmod{m}$, because $\text{ord}_m a = \lambda(m)$, and $a^{\lambda(m)/2} \not\equiv -1 \pmod{m}$, by hypothesis. Therefore, we can conclude tht if $\text{ord}_m a = \lambda(m)$, a has ± 1-exponent e, and $a^e \equiv -1 \pmod{m}$, then $e = \lambda(m)$.

We now find an integer a with the desired properties. Let the prime-power factorization of m be $m = 2^{t_0}p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s}$. We consider several cases.

We first consider those m with at least two different odd prime factors. Among the prime powers $p_i^{t_i}$ dividing m, let $p_j^{t_j}$ be one with the smallest power of 2 dividing $\phi(p_j^{t_j})$. Let r_i be a primitive root of $p_i^{t_i}$ for $i = 1, 2, \ldots, s$. Let a be an integer satisfying the simultaneous congruences

$$\begin{aligned} a &\equiv 3 \pmod{2^{t_0}}, \\ a &\equiv r_i \pmod{p_i^{t_i}} \quad \text{for all } i \text{ with } i \neq j, \\ a &\equiv r_j^2 \pmod{p_j^{t_j}}. \end{aligned}$$

Such an integer a is guaranteed to exist by the Chinese remainder theorem. Note that

$$\operatorname{ord}_m a = [\lambda(2^{t_0}), \phi(p_i^{t_2}), \ldots, \phi(p_j^{t_j})/2, \ldots, \phi(p_s^{t_s})],$$

and, by our choice of $p_j^{t_j}$, we know that this least common multiple equals $\lambda(m)$. Because $a \equiv r_j^2 \pmod{p_j^{t_j}}$, it follows that $a^{\phi(p_j^{t_j})/2} \equiv r_j^{\phi(p_j^{t_j})} \equiv 1 \pmod{p_j^{t_j}}$. Because $\phi(p_j^{t_j})/2 \mid \lambda(m)/2$, we know that

$$a^{\lambda(m)/2} \equiv 1 \pmod{p_j^{t_j}},$$

so that

$$a^{\lambda(m)/2} \not\equiv -1 \pmod{m}.$$

Consequently, the ± 1-exponent of a is $\lambda(m)$.

The next case that we consider deals with integers of the form $m = 2^{t_0}p^{t_1}$, where p is an odd prime, $t_1 \geq 1$ and $t_0 \geq 2$, because m has no primitive roots. When $t_0 = 2$ or 3, we have

$$\lambda(m) = [2, \phi(p_1^{t_1})] = \phi(p_1^{t_1}).$$

Let a be a solution of the simultaneous congruences

$$\begin{aligned} a &\equiv 1 \pmod 4 \\ a &\equiv r \pmod{p_t^{t_1}}, \end{aligned}$$

where r is a primitive root of $(p_1^{t_1})$. We see that $\operatorname{ord}_m a = \lambda(m)$. Because

$$a^{\lambda(m)/2} \equiv 1 \pmod 4,$$

we know that

$$a^{\lambda(m)/2} \not\equiv -1 \pmod{m}.$$

Consequently, the ± 1-exponent of a is $\lambda(m)$.

When $t_0 \leq 4$, let a be a solution of the simultaneous congruences

$$a \equiv 3 \pmod{2^{t_0}}$$
$$a \equiv r \pmod{p_t^{t_1}};$$

the Chinese remainder theorem tells us that such an integer exists. We see that $\operatorname{ord}_m a = \lambda(m)$. Because $4 \mid \lambda(2^{t_0})$, we know that $4 \mid \lambda(m)$. Hence,

$$a^{\lambda(m)/2} \equiv 3^{\lambda(m)/2} \equiv (3^2)^{\lambda(m)/4} \equiv 1 \pmod{8}.$$

Thus,

$$a^{\lambda(m)/2} \not\equiv -1 \pmod{m},$$

so that the ± 1-exponent of a is $\lambda(m)$.

Finally, when $m = 2^{t_0}$ with $t_0 \geq 3$, we know from Theorem 9.12 that $\operatorname{ord}_m 5 = \lambda(m)$, but

$$5^{\lambda(m)/2} \equiv (5^2)^{\lambda(m)/4} \equiv 1 \pmod{8}.$$

Therefore, we see that

$$5^{\lambda(m)/2} \not\equiv -1 \pmod{m};$$

we conclude that the ± 1-exponent of 5 is $\lambda(m)$.

This finishes the argument, because we have dealt with all cases where m does not have a primitive root. ∎

We now develop a system for splicing telephone cables. Telephone cables are made up of concentric layers of insulated copper wire, as illustrated in Figure 10.1, and are produced in sections of specified length.

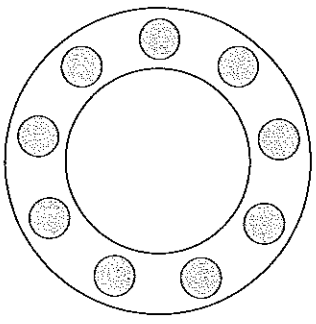


Figure 10.1 *A cross-section of one layer of a telephone cable.*

Telephone lines are constructed by splicing together sections of cable. When two wires are adjacent in the same layer in multiple sections of the cable, there are often problems with interference and crosstalk. Consequently, two wires adjacent in the same layer in one section should not be adjacent in the same layer in any nearby sections. For practical purposes, the splicing system should be simple. We use the following rules to

describe the system: Wires in concentric layers are spliced to wires in the corresponding layers of the next section, following the identical splicing direction at each connection. In a layer with m wires, we connect the wire in position j in one section, where $l \leq j \leq m$, to the wire in position $S(j)$ in the next section, where $S(j)$ is the least positive residue of $1 + (j - 1)s$ modulo m. Here, s is called the *spread* of the splicing system. We see that when a wire in one section is spliced to a wire in the next section, the adjacent wire in the first section is spliced to the wire in the next section in the position obtained by counting forward s modulo m from the position of the last wire spliced in this section. To have a one-to-one correspondence between wires of adjacent sections, we require that the spread s be relatively prime to the number of wires m. This shows that if wires in positions j and k are sent to the same wire in the next section, then $S(j) = S(k)$ and

$$1 + (j - 1)s \equiv 1 + (k - 1)s \pmod{m},$$

so that $js \equiv ks \pmod{m}$. Because $(m, s) = 1$, from Corollary 4.4.1 we see that $j \equiv k \pmod{m}$, which is impossible.

Example 10.8. Let us connect nine wires with a spread of 2. We have the correspondence

$$\begin{array}{lll} 1 \to 1 & 2 \to 3 & 3 \to 5 \\ 4 \to 7 & 5 \to 9 & 6 \to 2 \\ 7 \to 4 & 8 \to 6 & 9 \to 8, \end{array}$$

as illustrated in Figure 10.2. ◀

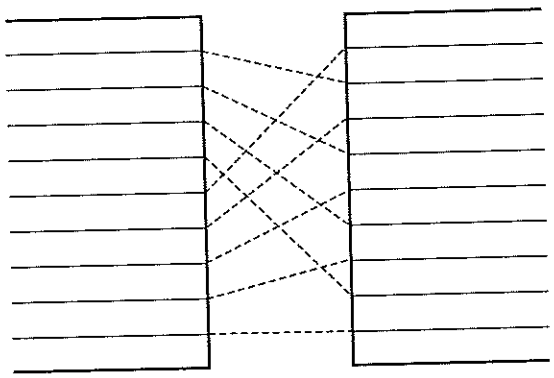


Figure 10.2 *Splicing of nine wires with a spread of* 2.

The following result tells us the correspondence of wires in the first section of cable to the wires in the nth section.

Theorem 10.7. Let $S_n(j)$ denote the position of the wire in the nth section spliced to the jth wire of the first section. Then

$$S_n(j) \equiv 1 + (j - 1)s^{n-1} \pmod{m}.$$

Proof. For $n = 2$, by the rules for the splicing system, we have

$$S_2(j) \equiv 1 + (j-1)s \pmod{m},$$

so the proposition is true for $n = 2$. Now assume that

$$S_n(j) \equiv 1 + (j-1)s^{n-1} \pmod{m}.$$

Then, in the next section, we have the wire in position $S_n(j)$ spliced to the wire in position.

$$\begin{aligned} S_{n+1}(j) &\equiv 1 + (S_n(j) - 1)s \\ &\equiv 1 + ((j-1)s^{n-1})s \\ &\equiv 1 + (j-1)s^n \pmod{m}. \end{aligned}$$

This shows that the proposition is true. ∎

In the splicing system, we want to have wires adjacent in one section separated as long as possible in the following sections. Theorem 10.7 tells us that after n splices, the adjacent wires in the jth and $(j+1)$th positions are connected to wires in positions $S_n(j) \equiv 1 + (j-1)s^n \pmod{m}$ and $S_n(j+1) = 1 + js^n \pmod{m}$, respectively. These wires are adjacent in the nth section if, and only if,

$$S_n(j) - S_n(j+1) \equiv \pm 1 \pmod{m},$$

or, equivalently,

$$(1 + (j-1)s^n) - (1 + js^n) \equiv \pm 1 \pmod{m},$$

which holds if and only if

$$s^n \equiv \pm 1 \pmod{m}.$$

We can now apply the material at the beginning of this section. To keep wires that are adjacent in the first section separated as long as possible thereafter, we should pick for the spread s an integer with maximal ± 1-exponent $\lambda_0(m)$.

Example 10.9. With 100 wires, we should choose a spread s so that the ± 1-exponent of s is $\lambda_0(100) = \lambda(100) = 20$. The appropriate computations show that $s = 3$ is such a spread. ◀

10.3 Exercises

1. Find the maximal ± 1-exponent of each of the following positive integers.

a) 17	c) 24	e) 99
b) 22	d) 36	f) 100

be used in computations and to prove useful results, such as Pepin's test, which can be used to determine whether Fermat numbers are prime.

The Legendre symbol, which tells us whether an integer is a quadratic residue modulo p, can be generalized to the Jacobi symbol. We will establish the basic properties of Jacobi symbols and show that they satisfy a reciprocity law that is a consequence of the law of quadratic reciprocity. We show how Jacobi symbols can be used to simplify computations of Legendre symbols. We also use Jacobi symbols to introduce a particular type of pseudoprime, known as an Euler pseudoprime, which is an integer that masquerades as a prime by satisfying Euler's criteria for quadratic residues. We will use this concept to develop a probabilistic primality test.

11.1 Quadratic Residues and Nonresidues

Let p be an odd prime and a an integer relatively prime to p. In this chapter, we devote our attention to the question: Is a a perfect square modulo p? We begin with a definition.

Definition. If m is a positive integer, we say that the integer a is a *quadratic residue of* m if $(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. If the congruence $x^2 \equiv a \pmod{m}$ has no solution, we say that a is a *quadratic nonresidue of* m.

Example 11.1. To determine which integers are quadratic residues of 11, we compute the squares of the integers $1, 2, 3, \ldots, 10$. We find that $1^2 \equiv 10^2 \equiv 1 \pmod{11}$, $2^2 \equiv 9^2 \equiv 4 \pmod{11}$, $3^2 \equiv 8^2 \equiv 9 \pmod{11}$, $4^2 \equiv 7^2 \equiv 5 \pmod{11}$, and $5^2 \equiv 6^2 \equiv 3 \pmod{11}$. Hence, the quadratic residues of 11 are $1, 3, 4, 5, 9$; the integers $2, 6, 7, 8, 10$ are quadratic nonresidues of 11. ◀

Note that the quadratic residues of the positive integer m are just the kth power residues of m with $k = 2$, as defined in Section 9.4. We will show that if p is an odd prime, then there are exactly as many quadratic residues as quadratic nonresidues of p among the integers $1, 2, \ldots, p - 1$. To demonstrate this fact, we use the following lemma.

Lemma 11.1. Let p be an odd prime and a an integer not divisible by p. Then, the congruence

$$x^2 \equiv a \pmod{p}$$

has either no solutions or exactly two incongruent solutions modulo p.

Proof. If $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_0$, then we can easily demonstrate that $x = -x_0$ is a second incongruent solution. Because $(-x_0)^2 = x_0^2 \equiv a \pmod{p}$, we see that $-x_0$ is a solution. We note that $x_0 \not\equiv -x_0 \pmod{p}$, for if $x_0 \equiv -x_0 \pmod{p}$, then we have $2x_0 \equiv 0 \pmod{p}$. This is impossible because p is odd and $p \nmid x_0$ because $x_0^2 \equiv a \pmod{p}$ and $p \nmid a$.

To show that there are no more than two incongruent solutions, assume that $x = x_0$ and $x = x_1$ are both solutions of $x^2 \equiv a \pmod{p}$. Then we have $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$, so that $x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0 \pmod{p}$. Hence, $p \mid (x_0 + x_1)$ or $p \mid (x_0 - x_1)$, so that $x_1 \equiv -x_0 \pmod{p}$ or $x_1 \equiv x_0 \pmod{p}$. Therefore, if there is a solution of $x^2 \equiv a \pmod{p}$, there are exactly two incongruent solutions. ∎

This leads us to the following theorem.

Theorem 11.1. If p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p and $(p-1)/2$ quadratic nonresidues of p among the integers $1, 2, \ldots, p-1$.

Proof. To find all the quadratic residues of p among the integers $1, 2, \ldots, p-1$, we compute the least positive residues modulo p of the squares of the integers $1, 2, \ldots, p-1$. Because there are $p-1$ squares to consider, and because each congruence $x^2 \equiv a \pmod{p}$ has either zero or two solutions, there must be exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, \ldots, p-1$. The remaining $p - 1 - (p-1)/2 = (p-1)/2$ positive integers less than $p-1$ are quadratic nonresidues of p. ∎

Primitive roots and indices, studied in Chapter 9, provide an alternative method for proving results about quadratic residues.

Theorem 11.2. Let p be a prime and let r be a primitive root of p. If a is an integer not divisible by p, then a is a quadratic residue of p if $\text{ind}_r a$ is even, and a is a quadratic nonresidue of p if $\text{ind}_r a$ is odd.

Proof. Suppose that $\text{ind}_r a$ is even. Then $(r^{\text{ind}_r a/2})^2 \equiv a \pmod{p}$, which shows that a is a quadratic residue of p. Now suppose that a is a quadratic residue of p. Then there exists an integer x such that $x^2 \equiv a \pmod{p}$. It follows that $\text{ind}_r x^2 = \text{ind}_r a$. By Part (iii) of Theorem 9.16, it follows that $2 \cdot \text{ind}_r x \equiv \text{ind}_r a \pmod{\phi(p)}$, so $\text{ind}_r a$ is even. We have shown that a is a quadratic residue of p if and only if $\text{ind}_r a$ is even. It follows that a is a quadratic nonresidue of p if and only if $\text{ind}_r a$ is odd. ∎

Note that by Theorem 11.2, every primitive root of an odd prime p is a quadratic nonresidue of p.

We illustrate how the relationship between primitive roots and indices and quadratic residues can be used to prove results about quadratic residues by giving an alternative proof of Theorem 11.1.

Proof. Let p be an odd prime with primitive root r. By Theorem 11.2, the quadratic residues of p among the integers $1, 2, \ldots, p-1$ are those with even index to the base r. It follows that the quadratic residues of a in this set are the least positive residues of r^k, where k is an even integer with $1 \le k \le p-1$. The result follows because there are exactly $(p-1)/2$ such integers. ∎

The special notation associated with quadratic residues is described in the following definition.

Definition. Let p be an odd prime and a be an integer not divisible by p. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p; \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

This symbol is named after the French mathematician *Adrien-Marie Legendre*, who introduced the use of this notation.

Example 11.2. The previous example shows that the Legendre symbols $\left(\frac{a}{11}\right)$, $a = 1, 2, \ldots, 10$, have the following values:

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1,$$
$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1. \quad \blacktriangleleft$$

We now present a criterion for deciding whether an integer is a quadratic residue of a prime. This criterion is useful in demonstrating properties of the Legendre symbol.

Theorem 11.3. ***Euler's Criterion.*** Let p be an odd prime and let a be a positive integer not divisible by p. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Proof. First, assume that $\left(\frac{a}{p}\right) = 1$. Then, the congruence $x^2 \equiv a \pmod{p}$ has a solution, say $x = x_0$. Using Fermat's little theorem, we see that

$$a^{(p-1)/2} = \left(x_0^2\right)^{(p-1/2)} = x_0^{p-1} \equiv 1 \pmod{p}.$$

Hence, if $\left(\frac{a}{p}\right) = 1$, we know that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

ADRIEN-MARIE LEGENDRE (1752–1833) was born into a well-to-do family. He was a professor at the École Militaire in Paris from 1775 to 1780. In 1795, he was appointed professor at the École Normale. His memoir *Recherches d'Analyse Indeterminеé*, published in 1785, contains a discussion of the law of quadratic reciprocity, a statement of Dirichlet's theorem on primes in arithmetic progressions, and a discussion of the representation of positive integers as the sum of three squares. He established the $n = 5$ case of Fermat's last theorem. Legendre wrote a textbook on geometry, *Eléments de géométrie*, that was used for more than 100 years, and served as a model for other textbooks. Legendre made fundamental discoveries in mathematical astronomy and geodesy, and gave the first treatment of the law of least squares.

Now consider the case where $\left(\frac{a}{p}\right) = -1$. Then, the congruence $x^2 \equiv a \pmod{p}$ has no solutions. By Theorem 4.10, for each integer i with $(i, p) = 1$ there is an integer j such that $ij \equiv a \pmod{p}$. Furthermore, because the congruence $x^2 \equiv a \pmod{p}$ has no solutions, we know that $i \neq j$. Thus, we can group the integers $1, 2, \ldots, p-1$ into $(p-1)/2$ pairs, each with product a. Multiplying these pairs together, we find that

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

Because Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$, we see that

$$-1 \equiv a^{(p-1)/2} \pmod{p}.$$

In this case, we also have $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. ■

Example 11.3. Let $p = 23$ and $a = 5$. Because $5^{11} \equiv -1 \pmod{23}$, Euler's criterion tells us that $\left(\frac{5}{23}\right) = -1$. Hence, 5 is a quadratic nonresidue of 23. ◀

We now prove some properties of the Legendre symbol.

Theorem 11.4. Let p be an odd prime and a and b be integers not divisible by p. Then

(i) if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(iii) $\left(\frac{a^2}{p}\right) = 1$.

Proof of (i). If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ has a solution if and only if $x^2 \equiv b \pmod{p}$ has a solution. Hence $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof of (ii). By Euler's criterion, we know that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}, \quad \left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod{p},$$

and

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \pmod{p}.$$

Hence,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Because the only possible values of a Legendre symbol are ± 1, we conclude that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Proof of (iii). Because $\left(\frac{a}{p}\right) = \pm 1$, from part (ii) it follows that

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1.$$ ∎

Part (ii) of Theorem 11.4 has the following interesting consequence. The product of two quadratic residues, or of two quadratic nonresidues, of a prime is a quadratic residue of that prime, whereas the product of a quadratic residue and a quadratic nonresidue of a prime is a quadratic nonresidue.

Relatively simple proofs of Theorems 11.3 and 11.4 can be constructed using the concepts of primitive roots and indices, together with Theorem 11.2. (See Exercises 30 and 31 at the end of this section.)

When is −1 a Quadratic Residue of the Prime p?

For which odd primes not exceeding 20 is -1 a quadratic residue? Since $2^2 \equiv -1 \pmod 5$, $5^2 \equiv -1 \pmod{13}$ and $4^2 \equiv -1 \pmod{17}$, we see that -1 is a quadratic residue of 5, 13, and 17. However it is easy to see (as the reader should verify) that the congruence $x^2 \equiv -1 \pmod p$ has no solution when $p = 3, 7, 11$, and 19. This evidence leads to the conjecture that -1 is a quadratic residue of the prime p if and only if $p \equiv 1 \pmod 4$.

Using Euler's criterion, we can prove this conjecture.

Theorem 11.5. If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Proof. By Euler's criterion, we know that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p.$$

If $p \equiv 1 \pmod 4$, then $p = 4k + 1$ for some integer k. Thus,

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1,$$

so that $\left(\frac{-1}{p}\right) = 1$. If $p \equiv 3 \pmod 4$, then $p = 4k + 3$ for some integer k. Thus,

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1,$$

so that $\left(\frac{-1}{p}\right) = -1$. ∎

Gauss's Lemma

The following elegant result of Gauss provides another criterion to determine whether an integer a relatively prime to the prime p is a quadratic residue of p.

Lemma 11.2. *Gauss's Lemma.* Let p be an odd prime and a an integer with $(a, p) = 1$. If s is the number of least positive residues of the integers $a, 2a, 3a, \ldots, ((p-1)/2)a$ that are greater than $p/2$, then $\left(\frac{a}{p}\right) = (-1)^s$.

Proof. Consider the integers $a, 2a, \ldots, ((p-1)/2)a$. Let $u_1, u_2, \ldots, u_s$ be the least positive residues of those that are greater than $p/2$, and let $v_1, v_2, \ldots, v_t$ be the least positive residues of those integers that are less than $p/2$. Because $(ja, p) = 1$ for all j with $1 \leq j \leq (p-1)/2$, these least positive residues are in the set $1, 2, \ldots, p-1$.

We will show that $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ comprise the set of integers $1, 2, \ldots, (p-1)/2$, in some order. To see this, we need only show that no two of these integers are congruent modulo p, because there are exactly $(p-1)/2$ numbers in the set, and all are positive integers not exceeding $(p-1)/2$.

Clearly, no two of the u_i are congruent modulo p and no two of the v_j are congruent modulo p; if a congruence of either of these two sorts held, we would have $ma \equiv na \pmod{p}$, where m and n are both positive integers not exceeding $(p-1)/2$. Because $p \nmid a$, this would imply that $m \equiv n \pmod{p}$, which is impossible.

In addition, one of the integers $p - u_i$ cannot be congruent to a v_j, for if such a congruence held, we would have $ma \equiv p - na \pmod{p}$, so that $ma \equiv -na \pmod{p}$. Because $p \nmid a$, this would imply that $m \equiv -n \pmod{p}$, which is impossible because both m and n are in the set $1, 2, \ldots, (p-1)/2$.

Now that we know that $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ are the integers $1, 2, \ldots, (p-1)/2$, in some order, we conclude that

$$(p - u_1)(p - u_2) \cdots (p - u_s)v_1v_2 \cdots v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p},$$

which implies that

$$(-1)^s u_1u_2 \cdots u_s v_1v_2 \cdots v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p}. \tag{11.1}$$

But, because $u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_t$ are the least positive residues of $a, 2a, \ldots, ((p-1)/2)a$ we also know that

$$\begin{aligned} u_1u_2 \cdots u_s v_1v_2 \cdots v_t &\equiv a \cdot 2a \cdots ((p-1)/2))a \\ &= a^{\frac{p-1}{2}} ((p-1)/2)! \pmod{p}. \end{aligned} \tag{11.2}$$

Hence, from (11.1) and (11.2), we see that

$$(-1)^s a^{\frac{p-1}{2}} ((p-1)/2)! \equiv ((p-1)/2)! \pmod{p}$$

Because $(p, ((p-1)/2)!) = 1$, this congruence implies that

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By multiplying both sides by $(-1)^s$, we obtain

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}.$$

Because Euler's criterion tells us that $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, it follows that

$$\left(\frac{a}{p}\right) \equiv (-1)^s \pmod{p},$$

establishing Gauss's lemma. ■

Example 11.4. Let $a = 5$ and $p = 11$. To find $\left(\frac{5}{11}\right)$ by Gauss's lemma, we compute the least positive residues of $1 \cdot 5, 2 \cdot 5, 3 \cdot 5, 4 \cdot 5$, and $5 \cdot 5$. These are 5, 10, 4, 9, and 3, respectively. Because exactly two of these are greater than 11/2, Gauss's lemma tells us that $\left(\frac{5}{11}\right) = (-1)^2 = 1$. ◄

When is 2 a Quadratic Residue of a Prime p?

For which odd primes not exceeding 50 is 2 a quadratic residue? Since $3^2 \equiv 2 \pmod{7}$, $6^2 \equiv 2 \pmod{17}$, $5^2 \equiv 2 \pmod{23}$, $8^2 \equiv 2 \pmod{31}$, $17^2 \equiv 2 \pmod{41}$, and $7^2 \equiv 2 \pmod{47}$, we see that 2 is a quadratic residue of 7, 17, 23, 31, 41, and 47. However (as the reader should verify) $x^2 \equiv 2 \pmod{p}$ has no solution when $p = 3, 5, 11, 13, 19, 29, 37$, and 43. Is there a pattern to the primes p for which 2 is a quadratic residue modulo p? Examining these primes and noting that whether 2 is a quadratic residue of p seems to depend on the congruence of p modulo 8, we conjecture that 2 is a quadratic residue of the odd prime p if and only if $p \equiv \pm 1 \pmod{8}$. Using Gauss's lemma, we can prove this conjecture.

Theorem 11.6. If p is an odd prime, then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Hence, 2 is a quadratic residue of all primes $p \equiv \pm 1 \pmod{8}$ and a quadratic nonresidue of all primes $p \equiv \pm 3 \pmod{8}$.

Proof. By Gauss's lemma, we know that if s is the number of least positive residues of the integers

$$1 \cdot 2,\ 2 \cdot 2,\ 3 \cdot 2,\ \ldots,\ ((p-1)/2) \cdot 2$$

that are greater than $p/2$, then $\left(\frac{2}{p}\right) = (-1)^s$. Because all of these integers are less than p, we need only count those greater than $p/2$ to find how many have least positive residues greater than $p/2$.

The integer $2j$, where $1 \le j \le (p-1)/2$, is less than $p/2$ when $j \le p/4$. Hence, there are $[p/4]$ integers in the set less than $p/2$. Consequently, there are

$s = (p-1)/2 - [p/4]$ greater than $p/2$. Therefore, by Gauss's lemma, we see that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}-[p/4]}.$$

To prove the theorem, it is enough to show that for every odd integer p,

$$\frac{p-1}{2} - [p/4] \equiv \frac{p^2-1}{8} \pmod 2. \tag{11.3}$$

Note that (11.3) holds for a positive integer p if and only if it holds for $p+8$. This follows because

$$\frac{(p+8)-1}{2} - [(p+8)/4] = \left(\frac{p-1}{2} + 4\right) - ([p/4]+2) \equiv \frac{p-1}{2} - [p/4] \pmod 2$$

and

$$\frac{(p+8)^2-1}{8} = \frac{p^2-1}{8} + 2p + 8 \equiv \frac{p^2-1}{8} \pmod 2.$$

Thus we can conclude that (11.3) holds for every odd integer n if it holds for $p = \pm 1$ and ± 3. We leave it to the reader to verify that (11.3) holds for these four values of p.

It follows that for every prime p we have $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

From the computations of the congruence class of $(p^2-1)/8 \pmod 2$, we see that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 \pmod 8$, while $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 \pmod 8$. ∎

Example 11.5. By Theorem 11.6, we see that

$$\left(\frac{2}{7}\right) = \left(\frac{2}{17}\right) = \left(\frac{2}{23}\right) = \left(\frac{2}{31}\right) = 1,$$

whereas

$$\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = \left(\frac{2}{11}\right) = \left(\frac{2}{13}\right) = \left(\frac{2}{19}\right) = \left(\frac{2}{29}\right) = -1. \quad ◀$$

We now present an example to show how to evaluate some Legendre symbols.

Example 11.6. To evaluate $\left(\frac{317}{11}\right)$, we use part (i) of Theorem 11.4 to obtain

$$\left(\frac{317}{11}\right) = \left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)^2 = 1,$$

because $317 \equiv 9 \pmod{11}$.

To evaluate $\left(\frac{89}{13}\right)$, because $89 \equiv -2 \pmod{13}$, we have

$$\left(\frac{89}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right).$$

Because $13 \equiv 1 \pmod 4$, Theorem 11.5 tells us that $\left(\frac{-1}{13}\right) = 1$. Because $13 \equiv -3 \pmod 8$, we see from Theorem 11.6 that $\left(\frac{2}{13}\right) = -1$. Consequently, $\left(\frac{89}{13}\right) = -1$. ◀

In the next section we will state and prove one of the most intriguing and challenging results of elementary number theory, the *law of quadratic reciprocity*. This theorem relates the values of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$, where p and q are odd primes. The law of quadratic reciprocity has many implications, both theoretical and practical, as we will see throughout this chapter. From a computational standpoint, we will see that it can help us evaluate Legendre symbols.

Modular Square Roots

Suppose that $n = pq$, where p and q are distinct odd primes, and suppose that the congruence $x^2 \equiv a \pmod n$, where $0 < a < n$ and $(a, n) = 1$, has a solution $x = x_0$. We will show that there are exactly four incongruent solutions modulo n. In other words, we will show that a has four incongruent *square roots modulo n*. To see this, let $x_0 \equiv x_1 \pmod p$, $0 < x_1 < p$, and let $x_0 \equiv x_2 \pmod q$, $0 < x_2 < q$. Then the congruence $x^2 \equiv a \pmod p$ has exactly two incongruent solutions modulo p, namely $x \equiv x_1 \pmod p$ and $x \equiv p - x_1 \pmod p$. Similarly, the congruence $x_2 \equiv a \pmod q$ has exactly two incongruent solutions modulo q, namely $x \equiv x_2 \pmod q$ and $x \equiv q - x_2 \pmod q$.

From the Chinese remainder theorem, there are exactly four incongruent solutions of the congruence $x^2 \equiv a \pmod n$; these four incongruent solutions are the unique solutions modulo pq of the four sets of simultaneous congruences:

(i) $x \equiv x_1 \pmod p$, $x \equiv x_2 \pmod q$,

(ii) $x \equiv x_1 \pmod p$, $x \equiv q - x_2 \pmod q$,

(iii) $x \equiv p - x_1 \pmod p$, $x \equiv x_2 \pmod q$,

(iv) $x \equiv p - x_1 \pmod p$, $x \equiv q - x_2 \pmod q$.

We denote solutions of (i) and (ii) by x and y, respectively. Solutions of (iii) and (iv) are easily seen to be $n - y$ and $n - x$, respectively.

We also note that when $p \equiv q \equiv 3 \pmod 4$, the solutions of $x^2 \equiv a \pmod p$ and of $x^2 \equiv a \pmod q$ are $x \equiv \pm a^{(p+1)/4} \pmod p$ and $x \equiv \pm a^{(q+1)/4} \pmod q$, respectively. By Euler's criterion, we know that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) = 1 \pmod p$ and $a^{(q-1)/2} \equiv \left(\frac{a}{q}\right) = 1 \pmod q$ (recall that we are assuming that $x^2 \equiv a \pmod{pq}$ has a solution, so that a is a quadratic residue of both p and q). Hence,

$$(a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2} \cdot a \equiv a \pmod p$$

and

$$(a^{(q+1)/4})^2 = a^{(q+1)/2} = a^{(q-1)/2} \cdot a \equiv a \pmod q.$$

Using the Chinese remainder theorem, together with the explicit solutions just constructed, we can easily find the four incongruent solutions of $x^2 \equiv a \pmod{n}$. The following example illustrates this procedure.

Example 11.7. Suppose that we know à priori that the congruence

$$x^2 \equiv 860 \pmod{11{,}021}$$

has a solution. Because $11{,}021 = 103 \cdot 107$, to find the four incongruent solutions we solve the congruences

$$x^2 \equiv 860 \equiv 36 \pmod{103}$$

and

$$x^2 \equiv 860 \equiv 4 \pmod{107}.$$

The solutions of these congruences are

$$x \equiv \pm 36^{(103+1)/4} \equiv \pm 36^{26} \equiv \pm 6 \pmod{103}$$

and

$$x \equiv \pm 4^{(107+1)/4} \equiv \pm 4^{27} \equiv \pm 2 \pmod{107},$$

respectively. Using the Chinese remainder theorem, we obtain $x \equiv \pm 212, \pm 109 \pmod{11{,}021}$ as the solutions of the four systems of congruences described by the four possible choices of signs in the system of congruences $x \equiv \pm 6 \pmod{103}$, $x \equiv \pm 2 \pmod{107}$. ◀

Flipping Coins Electronically

An interesting and useful application of the properties of quadratic residues is a method to "flip coins" electronically, invented by Blum [Bl82]. This method takes advantage of the difference in the length of time needed to find primes and needed to factor integers that are the products of two primes, also the basis of the RSA cipher discussed in Chapter 8.

We now describe a method for electronically flipping coins. Suppose that Bob and Alice are communicating electronically. Alice picks two distinct large primes p and q, with $p \equiv q \equiv 3 \pmod{4}$. Alice sends Bob the integer $n = pq$. Bob picks, at random, a positive integer x less than n and sends to Alice the integer a with $x^2 \equiv a \pmod{n}$, $0 < a < n$. Alice finds the four solutions of $x^2 \equiv a \pmod{n}$, namely $x, y, n - x$, and $n - y$. Alice picks one of these four solutions and sends it to Bob. Note that since $x + y \equiv 2x_1 \not\equiv 0 \pmod{p}$ and $x + y \equiv 0 \pmod{q}$, we have $(x + y, n) = q$, and similarly $(x + (n - y), n) = p$. Thus, if Bob receives either y or $n - y$, he can rapidly factor n by using the Euclidean algorithm to find one of the two prime factors of n. On the other hand, if Bob receives either x or $n - x$, he has no way to factor n in a reasonable length of time.

Consequently, Bob wins the coin flip if he can factor n, whereas Alice wins if Bob cannot factor n. From previous comments, we know that there is an equal chance for

Bob to receive a solution of $x^2 \equiv a \pmod{n}$ that helps him rapidly factor n, or a solution of $x^2 \equiv a \pmod{n}$ that does not help him factor n. Hence, the coin flip is fair.

11.1 Exercises

1. Find all of the quadratic residues of each of the following integers.

   a) 3 b) 5 c) 13 d) 19

2. Find all of the quadratic residues of each of the following integers.

   a) 7 b) 8 c) 15 d) 18

3. Find the value of the Legendre symbols $\left(\frac{j}{5}\right)$ for $j = 1, 2, 3, 4$.

4. Find the value of the Legendre symbols $\left(\frac{j}{7}\right)$ for $j = 1, 2, 3, 4, 5, 6$.

5. Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$

   a) using Euler's criterion.

   b) using Gauss's lemma.

6. Let a and b be integers not divisible by the prime p. Show that either one or all three of the integers a, b, and ab are quadratic residues of p.

7. Show that if p is an odd prime, then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 3 \pmod{8}; \\ -1 & \text{if } p \equiv -1 \text{ or } -3 \pmod{8}. \end{cases}$$

8. Show that if the prime-power factorization of n is

$$n = p_1^{2t_1+1} p_2^{2t_2+1} \cdots p_k^{2t_k+1} p_{k+1}^{2t_{k+1}} \cdots p_m^{2t_m}$$

   and q is a prime not dividing n, then

$$\left(\frac{n}{q}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) \cdots \left(\frac{p_k}{q}\right).$$

9. Show that if p is prime and $p \equiv 3 \pmod{4}$, then $[(p-1)/2]! \equiv (-1)^t \pmod{p}$, where t is the number of positive integers less than $p/2$ that are nonquadratic residues of p.

10. Show that if b is a positive integer not divisible by the prime p, then

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) = 0.$$

11. Let p be prime and a be a quadratic residue of p. Show that if $p \equiv 1 \pmod{4}$, then $-a$ is also a quadratic residue of p, whereas if $p \equiv 3 \pmod{4}$, then $-a$ is a quadratic nonresidue of p.

12. Consider the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$, where p is prime and a, b, and c are integers with $p \nmid a$.

    a) Let $p = 2$. Determine which quadratic congruences (mod 2) have solutions.

b) Let p be an odd prime and let $d = b^2 - 4ac$. Show that the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is equivalent to the congruence $y^2 \equiv d \pmod{p}$, where $y = 2ax + b$. Conclude that if $d \equiv 0 \pmod{p}$, then there is exactly one solution x modulo p; if d is a quadratic residue of p, then there are two incongruent solutions; and if d is a quadratic nonresidue of p, then there are no solutions.

13. Find all solutions of the following quadratic congruences.
a) $x^2 + x + 1 \equiv 0 \pmod{7}$
b) $x^2 + 5x + 1 \equiv 0 \pmod{7}$
c) $x^2 + 3x + 1 \equiv 0 \pmod{7}$

14. Show that if p is prime and $p \geq 7$, then there are always two consecutive quadratic residues of p. (*Hint:* First show that at least one of 2, 5, and 10 is a quadratic residue of p.)

* **15.** Show that if p is prime and $p \geq 7$, then there are always two quadratic residues of p that differ by 2.

16. Show that if p is prime and $p \geq 7$, then there are always two quadratic residues of p that differ by 3.

17. Show that if a is a quadratic residue of the prime p, then the solutions of $x^2 \equiv a \pmod{p}$ are
a) $x \equiv \pm a^{n+1} \pmod{p}$, if $p = 4n + 3$.
b) $x \equiv \pm a^{n+1}$ or $\pm 2^{2n+1} a^{n+1} \pmod{p}$, if $p = 8n + 5$.

* **18.** Show that if p is a prime and $p = 8n + 1$, and r is a primitive root modulo p, then the solutions of $x^2 \equiv \pm 2 \pmod{p}$ are given by

$$x \equiv \pm(r^{7n} \pm r^n) \pmod{p},$$

where the $\pm$ sign in the first congruence corresponds to the $\pm$ sign inside the parentheses in the second congruence.

19. Find all solutions of the congruence $x^2 \equiv 1 \pmod{15}$.

20. Find all solutions of the congruence $x^2 \equiv 58 \pmod{77}$.

21. Find all solutions of the congruence $x^2 \equiv 207 \pmod{1001}$.

22. Let p be an odd prime, e a positive integer, and a an integer relatively prime to p. Show that the congruence $x^2 \equiv a \pmod{p^e}$ has either no solutions or exactly two incongruent solutions.

* **23.** Let p be an odd prime, e a positive integer, and a an integer relatively prime to p. Show that there is a solution to the congruence $x^2 \equiv a \pmod{p^{e+1}}$ if and only if there is a solution to the congruence $x^2 \equiv a \pmod{p^e}$. Use Exercise 22 to conclude that the congruence $x^2 \equiv a \pmod{p^e}$ has no solutions if a is a quadratic nonresidue of p, and exactly two incongruent solutions modulo p if a is a quadratic residue of p.

24. Let n be an odd integer. Find the number of incongruent solutions modulo n of the congruence $x^2 \equiv a \pmod{n}$, where n has prime-power factorization $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$, in terms of the Legendre symbols $\left(\frac{a}{p_1}\right), \ldots, \left(\frac{a}{p_m}\right)$. (*Hint:* Use Exercise 23.)

25. Find the number of incongruent solutions of each of the following congruences.
a) $x^2 \equiv 31 \pmod{75}$

b) $x^2 \equiv 16 \pmod{105}$

c) $x^2 \equiv 46 \pmod{231}$

d) $x^2 \equiv 1156 \pmod{3^2 5^3 7^5 11^6}$

* **26.** Show that the congruence $x^2 \equiv a \pmod{2^e}$, where e is an integer, $e \geq 3$, has either no solutions or exactly four incongruent solutions. (*Hint:* Use the fact that $(\pm x)^2 \equiv (2^{e-1} \pm x)^2 \pmod{2^e}$.)

27. Show that there are infinitely many primes of the form $4k + 1$. (*Hint:* Assume that $p_1, p_2, \ldots, p_n$ are the only such primes. Form $N = 4(p_1 p_2 \cdots p_n)^2 + 1$, and show, using Theorem 11.5, that N has a prime factor of the form $4k + 1$ that is not one of $p_1, p_2, \ldots, p_n$.)

* **28.** Show that there are infinitely many primes of each of the following forms.

a) $8k + 3$ b) $8k + 5$ c) $8k + 7$

(*Hint:* For each part, assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$ of the particular form. For part (a), look at $(p_1 p_2 \cdots p_n)^2 + 2$; for part (b), look at $(p_1 p_2 \cdots p_n)^2 + 4$; and for part (c), look at $(4p_1 p_2 \cdots p_n)^2 - 2$. In each part, show that there is a prime factor of this integer of the required form not among the primes $p_1, p_2, \ldots, p_n$. Use Theorems 11.5 and 11.6.)

29. Let p and q be odd primes with $p \equiv q \equiv 3 \pmod 4$ and let a be a quadratic residue of $n = pq$. Show that exactly one of the four incongruent square roots of a modulo pq is a quadratic residue of n.

30. Prove Theorem 11.3 using the concept of primitive roots and indices.

31. Prove Theorem 11.4 using the concept of primitive roots and indices.

32. Let p be an odd prime. Show that there are $(p-1)/2 - \phi(p-1)$ quadratic nonresidues of p that are not primitive roots of p.

* **33.** Let p and $q = 2p + 1$ both be odd primes. Show that the $p - 1$ primitive roots of q are the quadratic nonresidues of q, other than the nonresidue $2p$ of q.

* **34.** Show that if p and $q = 4p + 1$ are both primes and if a is a quadratic nonresidue of q with $\text{ord}_q a \neq 4$, then a is a primitive root of q.

* **35.** Show that a prime p is a Fermat prime if and only if every quadratic nonresidue of p is also a primitive root of p.

* **36.** Show that a prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$ must be of the form $2^{n+2}k + 1$. (*Hint:* Show that $\text{ord}_p 2 = 2^{n+1}$. Then show that $2^{(p-1)/2} \equiv 1 \pmod p$ using Theorem 11.6. Conclude that $2^{n+1} \mid (p-1)/2$.)

* **37.** a) Show that if p is a prime of the form $4k + 3$ and $q = 2p + 1$ is prime, then q divides the Mersenne number $M_p = 2^p - 1$. (*Hint:* Consider the Legendre symbol $\left(\frac{2}{q}\right)$.)

b) From part (a), show that $23 \mid M_{11}$, $47 \mid M_{23}$, and $503 \mid M_{251}$.

* **38.** Show that if n is a positive integer and $2n + 1$ is prime, and if $n \equiv 0$ or $3 \pmod 4$, then $2n + 1$ divides the Mersenne number $M_n = 2^n - 1$, whereas if $n \equiv 1$ or $2 \pmod 4$, then $2n + 1$ divides $M_n + 2 = 2^n + 1$. (*Hint:* Consider the Legendre symbol $\left(\frac{2}{2n+1}\right)$ and use Theorem 11.5.)

39. Show that if p is an odd prime, then every prime divisor q of the Mersenne number M_p must be of the form $q = 8k \pm 1$, where k is a positive integer. (*Hint:* Use Exercise 38.)

40. Show how Exercise 39, together with Theorem 7.12, can be used to help show that M_{17} is prime.

*** 41.** Show that if p is an odd prime, then

$$\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p} \right) = -1.$$

(*Hint:* First show that $\left(\frac{j(j+1)}{p}\right) = \left(\frac{\overline{j}+1}{p}\right)$, where $\overline{j}$ is an inverse j of modulo p.)

*** 42.** Let p be an odd prime. Among pairs of consecutive positive integers less than p, let **(RR)**, **(RN)**, **(NR)**, and **(NN)** denote the number of pairs of two quadratic residues, of a quadratic residue followed by a quadratic nonresidue, of a quadratic nonresidue followed by a quadratic residue, and of two quadratic nonresidues, respectively.

a) Show that

$$\textbf{(RR)} + \textbf{(RN)} = \frac{1}{2}(p - 2 - (-1)^{(p-1)/2})$$

$$\textbf{(NR)} + \textbf{(NN)} = \frac{1}{2}(p - 2 + (-1)^{(p-1)/2})$$

$$\textbf{(RR)} + \textbf{(NR)} = \frac{1}{2}(p - 1) - 1$$

$$\textbf{(RN)} + \textbf{(NN)} = \frac{1}{2}(p - 1).$$

b) Using Exercise 41, show that

$$\sum_{j=1}^{p-2} \left(\frac{j(j+1)}{p} \right) = \textbf{(RR)} + \textbf{(NN)} - \textbf{(RN)} - \textbf{(NR)} = -1.$$

c) From parts (a) and (b), find **(RR)**, **(RN)**, **(NR)**, and **(NN)**.

43. Use Theorem 9.16 to prove Theorem 11.1.

*** 44.** Let p and q be odd primes. Show that 2 is a primitive root of q, if $q = 4p + 1$.

*** 45.** Let p and q be odd primes. Show that 2 is a primitive root of q, if p is of the form $4k + 1$ and $q = 2p + 1$.

*** 46.** Let p and q be odd primes. Show that -2 is a primitive root of q, if p is of the form $4k - 1$ and $q = 2p + 1$.

*** 47.** Let p and q be odd primes. Show that -4 is a primitive root of q, if $q = 2p + 1$.

48. Find the solutions of $x^2 \equiv 482 \pmod{2773}$ (note that $2773 = 47 \cdot 59$).

*** 49.** In this exercise, we develop a method for decrypting messages encrypted using a Rabin cipher. Recall that the relationship between a ciphertext block C and the corresponding plaintext block P in a Rabin cipher is $C \equiv P(P + \overline{2}b) \pmod{n}$, where $n = pq$, p and q are distinct odd primes, and b is a positive integer less than n.

a) Show that $C + a \equiv (P + \overline{2}b)^2 \pmod{n}$, where $a \equiv (\overline{2}b)^2 \pmod{n}$, and $\overline{2}$ is an inverse of 2 modulo n.

b) Using the algorithm in the text for solving congruences of the type $x^2 \equiv a \pmod{n}$, together with part (a), show how to find a plaintext block P from the corresponding ciphertext block C. Explain why there are four possible plaintext messages. (This ambiguity is a disadvantage of Rabin ciphers.)

c) Decrypt the ciphertext message 1819 0459 0803 that was encrypted using the Rabin cryptosytem with $b = 3$ and $n = 47 \cdot 59 = 2773$.

50. Let p be an odd prime, and let C be the ciphertext obtained in modular exponentiation, with exponent e and modulus p, from the plaintext P, that is, $C \equiv P^e \pmod{p}$, $0 < C < n$, where $(e, p-1) = 1$. Show that C is a quadratic residue of p if and only if P is a quadratic residue of p.

* **51.** a) Show that the second player in a game of electronic poker (see Section 8.6) can obtain an advantage by noting which cards have numerical equivalents that are quadratic residues modulo p. (*Hint:* Use Exercise 50.)

b) Show that the advantage of the second player noted in part (a) can be eliminated if the numerical equivalents of cards that are quadratic nonresidues are all multiplied by a fixed quadratic nonresidue.

* **52.** Show that if the probing sequence for resolving collisions in a hashing scheme is $h_j(K) \equiv h(K) + aj + bj^2 \pmod{m}$, where $h(K)$ is a hashing function, m is a positive integer, and a and b are integers with $(b, m) = 1$, then only half the possible file locations are probed. This is called the *quadratic search*.

We say that x and y form a *chain of quadratic residues* modulo p if x, y, and $x + y$ are all quadratic residues modulo p.

53. Find a chain $x, y, x + y$ of quadratic residues modulo 11.

54. Is there a chain of quadratic residues modulo 7?

11.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the value of each of the following Legendre symbols: $\left(\frac{1521}{451,879}\right)$, $\left(\frac{222,344}{21,155,500,207}\right)$, $\left(\frac{6,818,811}{15,454,356,666,611}\right)$.

2. Show that the prime $p = 30,059,924,764,123$ has $\left(\frac{q}{p}\right) = -1$ for all primes q with $2 \leq q \leq 181$.

3. A set of integers $x_1, x_2, \ldots, x_n$, where n is a positive integer, is called *chain of quadratic residues* if all sums of consecutive subsets of these numbers are quadratic residues. Show that the integers 1, 4, 45, 94, 261, 310, 344, 387, 393, 394, and 456 form a chain of quadratic residues modulo 631. (*Note:* There are 66 values to check.)

4. Find the smallest quadratic nonresidue of each prime less than 1000.

5. Find the smallest quadratic nonresidue of 100 randomly selected primes between 100,000 and 1,000,000, and 100 randomly selected primes between 100,000,000 and 1,000,000,000. Can you make any conjectures based on your evidence?
6. Use numerical evidence to determine for which odd primes p there are more quadratic residues a of p with $1 \le a \le (p-1)/2$ than there are with $(p+1)/2 \le a \le p-1$.
7. Let p be a prime with $p \equiv 3 \pmod 4$. It has been proved that if R is the largest number of consecutive quadratic residues of p and N is the largest number of consecutive quadratic nonresidues of p, then $R = N < \sqrt{p}$. Verify this result for all primes of this type less than 1000.
8. Let p be a prime with $p \equiv 1 \pmod 4$. It has been conjectured that if N is the largest number of consecutive quadratic nonresidues of p, then $N < \sqrt{p}$ when p is sufficiently large. Find evidence for this conjecture. For which small primes does this inequality fail?
9. Find the four modular square roots of 4,609,126 modulo $14{,}438{,}821 = 4003 \cdot 3607$.
10. Find the square roots of 11,535 modulo 142,661. Which one is a quadratic residue of 142,661?

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Evaluate Legendre symbols using Euler's criterion.
2. Evaluate Legendre symbols using Gauss's lemma.
3. Given a positive integer n that is the product of two distinct primes both congruent to 3 modulo 4, find the four square roots of the least positive residue of x^2, where x is an integer relatively prime to n.

* 4. Flip coins electronically using the procedure described in this section.

** 5. Decrypt messages that were encrypted using a Rabin cryptosystem (see Exercise 49).

11.2 The Law of Quadratic Reciprocity

Suppose that p and q are distinct odd primes. Suppose further that we know whether q is a quadratic residue of p. Do we also know whether p is a quadratic residue of q? The answer to this question was found by Euler in the mid-1700s. He found the answer by examining numerical evidence, but he did not prove that his answer was correct. Later, in 1785, Legendre reformulated Euler's answer, in its modern, elegant form, in a theorem known as the *law of quadratic reciprocity.* This theorem tells us whether the congruence $x^2 \equiv q \pmod p$ has solutions, once we know whether there are solutions of $x^2 \equiv p \pmod q$.

Theorem 11.7. ***The Law of Quadratic Reciprocity.*** Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Legendre published several proposed proofs of this theorem, but each of his proofs contained a serious gap. The first correct proof was provided by Gauss, who claimed to have rediscovered this result when he was 18 years old. Gauss devoted considerable attention to his search for a proof. In fact, he wrote that "for an entire year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof."

Once Gauss found his first proof in 1796, he continued searching for different proofs. He found at least six different proofs of the law of quadratic reciprocity. His goal in looking for more proofs was to find an approach that could be generalized to higher powers. In particular, he was interested in cubic and biquadratic residues of primes; that is, he was interested in determining when, given a prime p and an integer a not divisible by p, the congruences $x^3 \equiv a \pmod{p}$ and $x^4 \equiv a \pmod{p}$ are solvable. With his sixth proof, Gauss finally succeeded in his goal, as this proof could be generalized to higher powers. (See [IrRo91], [Go98], and [Le00] for more information about Gauss's proofs and the generalization to higher power residues.)

Finding new and different approaches did not stop with Gauss. Some of the well-known mathematicians who have published original proofs of the law of quadratic reciprocity are Cauchy, Dedekind, Dirichlet, Kronecker, and Eisenstein. One count in 1921 stated that there were 56 different proofs of the law of quadratic reciprocity, and in 1963 an article published by M. Gerstenhaber [Ge63] offered the 152nd proof of the law of quadratic reciprocity. In 2000, Franz Lemmermeyer [Le00] compiled a comprehensive list of 192 proofs of quadratic reciprocity, noting for each proof the year, the prover, and the method of proof. Lemmermeyer maintains a current version of this on the Web; as of early 2004, 207 different proofs were listed. According to his count, Gerstenhaber's proof is number 153 and eight of the proofs were completed since 2000. It will be interesting to see if new proofs continue to be found at the rate of one per year. (See Exercise 17 for an outline of the 207th proof.)

Although many of the different proofs of the law of quadratic reciprocity are similar, they encompass an amazing variety of approaches. The ideas in different approaches can have useful consequences. For example, the ideas behind Gauss's first proof, which is a complicated argument using mathematical induction, were of little interest to mathematicians for more than 175 years, until they were used in the 1970s in computations in an advanced area of algebra known as K-theory.

The version of the law of quadratic reciprocity that we have stated and proved is different from the version originally conjectured by Euler. This version, which we now state, turns out to be equivalent to the version we have stated as Theorem 11.7. Euler formulated this version based on the evidence of many computations of special cases.

Theorem 11.8. Suppose that p is an odd prime and a is an integer not divisible by p. If q is a prime with $p \equiv \pm q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

This version of the law of quadratic reciprocity shows that the value of the Legendre symbol $\left(\frac{a}{p}\right)$ depends only on the residue class of p modulo $4a$, and that the value of $\left(\frac{a}{p}\right)$ takes the same value for all primes p with remainder r or $4a - r$ when divided by $4a$.

We leave it to the reader as Exercises 10 and 11 to show that this form of the law of quadratic reciprocity is equivalent to the form given in Theorem 11.7. We also ask the reader to prove, in Exercise 12, this form of quadratic reciprocity directly, using Gauss's lemma.

Before we prove the law of quadratic reciprocity, we will discuss its consequences and how it is used to evaluate Legendre symbols. We first note that the quantity $(p-1)/2$ is even when $p \equiv 1 \pmod 4$ and odd when $p \equiv 3 \pmod 4$. Consequently, we see that $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even if $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, whereas $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is odd if $p \equiv q \equiv 3 \pmod 4$. Hence, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \text{ (or both);} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Because the only possible values of $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are ± 1, we see that

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \text{ (or both);} \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

This means that if p and q are odd primes, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, unless both p and q are congruent to 3 modulo 4, and in that case, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Example 11.8. Let $p = 13$ and $q = 17$. Because $p \equiv q \equiv 1 \pmod 4$, the law of quadratic reciprocity tells us that $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. By part (i) of Theorem 11.4, we know that $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right)$, and from part (iii) of Theorem 11.4, it follows that $\left(\frac{4}{13}\right) = \left(\frac{2^2}{13}\right) = 1$. Combining these equalities, we conclude that $\left(\frac{13}{17}\right) = 1$. ◀

Example 11.9. Let $p = 7$ and $q = 19$. Because $p \equiv q \equiv 3 \pmod 4$, by the law of quadratic reciprocity, we know that $\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right)$. From part (i) of Theorem 11.4, we see that $\left(\frac{19}{7}\right) = \left(\frac{5}{7}\right)$. Again, using the law of quadratic reciprocity, because $5 \equiv 1 \pmod 4$ and $7 \equiv 3 \pmod 4$, we have $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)$. By part (i) of Theorem 11.4 and Theorem 11.6, we know that $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1$. Hence, $\left(\frac{7}{19}\right) = 1$. ◀

We can use the law of quadratic reciprocity and Theorems 11.4 and 11.6 to evaluate Legendre symbols. Unfortunately, prime factorizations must be computed to evaluate Legendre symbols in this way.

Example 11.10. We will calculate $\left(\frac{713}{1009}\right)$ (note that 1009 is prime). We factor $713 = 23 \cdot 31$, so that by part (ii) of Theorem 11.4, we have

$$\left(\frac{713}{1009}\right) = \left(\frac{23 \cdot 31}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right).$$

To evaluate the two Legendre symbols on the right side of this equality, we use the law of quadratic reciprocity. Because $1009 \equiv 1 \pmod 4$, we see that

$$\left(\frac{23}{1009}\right) = \left(\frac{1009}{23}\right), \quad \left(\frac{31}{1009}\right) = \left(\frac{1009}{31}\right).$$

Using Theorem 11.4, part (i), we have

$$\left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right), \quad \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right).$$

By parts (ii) and (iii) of Theorem 11.4, it follows that

$$\left(\frac{20}{23}\right) = \left(\frac{2^2 \cdot 5}{23}\right) = \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{5}{23}\right).$$

The law of quadratic reciprocity, part (i) of Theorem 11.4, and Theorem 11.6 tell us that

$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Thus, $\left(\frac{23}{1009}\right) = -1$.

Likewise, using the law of quadratic reciprocity, Theorem 11.4, and Theorem 11.6, we find that

$$\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right)$$
$$= -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -\left(\frac{2^2}{3}\right) = -1.$$

Consequently, $\left(\frac{31}{1009}\right) = -1$.

Therefore, $\left(\frac{713}{1009}\right) = (-1)(-1) = 1$. ◀

A Proof of the Law of Quadratic Reciprocity

We now present a proof of the law of quadratic reciprocity originally given by *Max Eisenstein*. This proof is a simplification of the third proof given by Gauss. This simplification was made possible by the following lemma of Eisenstein, which will help us reduce the proof of the law of quadratic reciprocity to counting lattice points in triangles.

Lemma 11.3. If p is an odd prime and a is an odd integer not divisible by p, then

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

where

$$T(a, p) = \sum_{j=1}^{(p-1)/2} [ja/p].$$

Proof. Consider the least positive residues of the integers $a, 2a, \ldots, ((p-1)/2)a$; let $u_1, u_2, \ldots, u_s$ be those greater than $p/2$ and let $v_1, v_2, \ldots, v_t$ be those less than $p/2$. The division algorithm tells us that

$$ja = p[ja/p] + \text{ remainder},$$

where the remainder is one of the u_j or v_j. By adding the $(p-1)/2$ equations of this sort, we obtain

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p[ja/p] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{11.4}$$

As we showed in the proof of Gauss's lemma, the integers $p-u_1, \ldots, p-u_s, v_1, \ldots, v_t$ are precisely the integers $1, 2, \ldots, (p-1)/2$, in some order. Hence, summing all these integers, we obtain

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{11.5}$$

Subtracting (11.5) from (11.4), we find that

$$\sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p[ja/p] - ps + 2\sum_{j=1}^{s} u_j$$

FERDINAND GOTTHOLD MAX EISENSTEIN (1823–1852) suffered from poor health his entire life. He moved with his family to England, Ireland, and Wales before returning to Germany. In Ireland, Eisenstein met Sir William Rowan Hamilton, who stimulated his interest in mathematics by giving him a paper that discussed the impossibility of solving quintic equations in radicals. On his return to Germany in 1843, at the age of 20, Eisenstein entered the University of Berlin.

Eisenstein amazed the mathematical community when he quickly began producing new results soon after entering the university. In 1844, Eisenstein met Gauss in Göttingen where they discussed reciprocity for cubic residues. Gauss was extremely impressed by Eisenstein, and tried to obtain financial support for him. Gauss wrote to the explorer and scientist Alexander von Humboldt that the talent Eisenstein had was "that nature bestows upon only a few in each century." Eisenstein was amazingly prolific. In 1844, he published 16 papers in Volume 27 of *Crelle's Journal* alone. In the third semester of his studies, he received an honorary doctorate from the University of Breslau. Eisenstein was appointed to an unsalaried position as a Privatdozent at the University of Berlin; however, after 1847, Eisenstein's health worsened so much that he was mostly confined to bed. Nevertheless, his mathematical output continued unabated. After spending a year in Sicily in a futile attempt to improve his health, he returned to Germany where he died from tuberculosis at the age of 29. His early death was considered a tremendous loss by mathematicians.

or, equivalently, because $T(a, p) = \sum_{j=1}^{(p-1)/2}[ja/p]$,

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) - ps + 2\sum_{j=1}^{s} u_j.$$

Reducing this last equation modulo 2, because a and p are odd, yields

$$0 \equiv T(a,p) - s \pmod 2.$$

Hence,

$$T(a,p) \equiv s \pmod 2.$$

To finish the proof, we note that from Gauss's lemma,

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Consequently, because $(-1)^s = (-1)^{T(a,p)}$, it follows that

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}.$$ ■

Although Lemma 11.3 is used primarily as a tool in the proof of the law of quadratic reciprocity, it can also be used to evaluate Legendre symbols.

Example 11.11. To find $\left(\frac{7}{11}\right)$ using Lemma 11.3, we evaluate the sum

$$\sum_{j=1}^{5}[7j/11] = [7/11] + [14/11] + [21/11] + [28/11] + [35/11]$$
$$= 0 + 1 + 1 + 2 + 3 = 7.$$

Hence, $\left(\frac{7}{11}\right) = (-1)^7 = -1$.

Likewise, to find $\left(\frac{11}{7}\right)$, we note that

$$\sum_{j=1}^{3}[11j/7] = [11/7] + [22/7] + [33/7] = 1 + 3 + 4 = 8,$$

so that $\left(\frac{11}{7}\right) = (-1)^8 = 1$. ◀

Before we present a proof of the law of quadratic reciprocity, we use an example to illustrate the method of proof.

Let $p = 7$ and $q = 11$. We consider pairs of integers (x, y) with $1 \le x \le (7-1)/2 = 3$ and $1 \le y \le (11-1)/2 = 5$. There are 15 such pairs. We note that none of these pairs satisfies $11x = 7y$, because the equality $11x = 7y$ implies that $11 \mid 7y$, so that either $11 \mid 7$, which is absurd, or $11 \mid y$, which is impossible because $1 \le y \le 5$.

We divide these 15 pairs into two groups, depending on the relative sizes of $11x$ and $7y$, as shown in Figure 11.1.

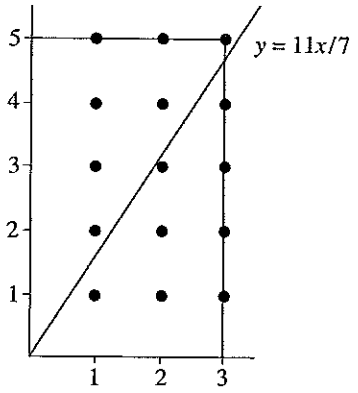


Figure 11.1 *Counting lattice points to determine* $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right)$.

The pairs of integers (x, y) with $1 \le x \le 3$, $1 \le y \le 5$, and $11x > 7y$ are precisely those pairs satisfying $1 \le x \le 3$ and $1 \le y \le 11x/7$. For a fixed integer x with $1 \le x \le 3$, there are $[11x/7]$ allowable values of y. Hence, the total number of pairs satisfying $1 \le x \le 3$, $1 \le y \le 5$, and $11x > 7y$ is

$$\sum_{j=1}^{3}[11j/7] = [11/7] + [22/7] + [33/7] = 1 + 3 + 4 = 8;$$

these eight pairs are (1, 1), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), and (3, 4).

The pairs of integers (x, y) with $1 \le x \le 3$, $1 \le y \le 5$, and $11x < 7y$ are precisely those pairs satisfying $1 \le y \le 5$ and $1 \le x \le 7y/11$. For a fixed integer y with $1 \le y \le 5$, there are $[7y/11]$ allowable values of x. Hence, the total number of pairs satisfying $1 \le x \le 3$, $1 \le y \le 5$, and $11x < 7y$ is

$$\begin{aligned}\sum_{j=1}^{5}[7j/11] &= [7/11] + [14/11] + [21/11] + [28/11] + [35/11] \\ &= 0 + 1 + 1 = 2 = 3 = 7.\end{aligned}$$

These seven pairs are (1, 2), (1, 3), (1, 4), (1, 5), (2, 4), (2, 5), and (3, 5).

Consequently, we see that

$$\frac{11-1}{2} \cdot \frac{7-1}{2} = 5 \cdot 3 = 15 = \sum_{j=1}^{3}[11j/7] + \sum_{j=1}^{5}[7j/11] = 8 + 7.$$

Hence,

$$\begin{aligned}(-1)^{\frac{11-1}{2}\cdot\frac{7-1}{2}} &= (-1)^{\sum_{j=1}^{3}[11j/7]+\sum_{j=1}^{5}[7j/11]} \\ &= (-1)^{\sum_{j=1}^{3}[11j/7]}(-1)^{\sum_{j=1}^{5}[7j/11]}.\end{aligned}$$

Because Lemma 11.3 tells us that $\left(\frac{11}{7}\right) = (-1)^{\sum_{j=1}^{3}[11j/7]}$ and $\left(\frac{7}{11}\right) = (-1)^{\sum_{j=1}^{5}[7j/11]}$, we see that $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{11-1}{2}}$.

This establishes the special case of the law of quadratic reciprocity when $p = 7$ and $q = 11$.

We now prove the law of quadratic reciprocity, using the idea illustrated in the example.

Proof. We consider pairs of integers (x, y) with $1 \le x \le (p-1)/2$ and $1 \le y \le (q-1)/2$. There are $\frac{p-1}{2} \cdot \frac{q-1}{2}$ such pairs. We divide these pairs into two groups, depending on the relative sizes of qx and py, as shown in Figure 11.2

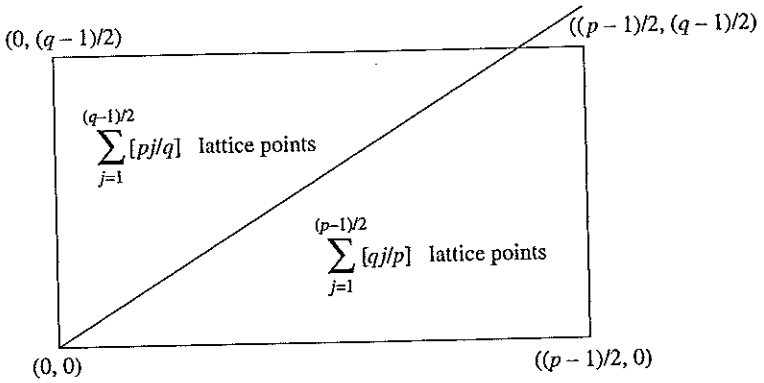


Figure 11.2 *Counting lattice points to determine* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$.

First, we note that $qx \neq py$ for all these pairs. For if $qx = py$, then $q \mid py$, which implies that $q \mid p$ or $q \mid y$. However, because q and p are distinct primes, we know that $q \nmid p$, and because $1 \le y \le (q-1)/2$, we know that $q \nmid y$.

To enumerate the pairs of integers (x, y) with $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$, and $qx > py$, we note that these pairs are precisely those where $1 \le x \le (p-1)/2$ and $1 \le y \le qx/p$. For each fixed value of the integer x, with $1 \le x \le (p-1)/2$, there are $[qx/p]$ integers satisfying $1 \le y \le qx/p$. Consequently, the total number of pairs of integers (x, y) with $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$, and $qx > py$ is $\sum_{j=1}^{(p-1)/2}[qj/p]$.

We now consider the pairs of integers (x, y) with $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$, and $qx < py$. These pairs are precisely the pairs of integers (x, y) with $1 \le y \le (q-1)/2$ and $1 \le x \le py/q$. Hence, for each fixed value of the integer y, where $1 \le y \le (q-1)/2$, there are exactly $[py/q]$ integers x satisfying $1 \le x \le py/q$. This shows that the total number of pairs of integers (x, y) with $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$, and $qx < py$ is $\sum_{j=1}^{(q-1)/2}[pj/q]$.

Adding the numbers of pairs in these classes, and recalling that the total number of such pairs is $\frac{p-1}{2} \cdot \frac{q-1}{2}$, we see that

$$\sum_{j=1}^{(p-1)/2} [qj/p] + \sum_{j=1}^{(q-1)/2} [pj/q] = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

or, using the notation of Lemma 11.3,

$$T(q, p) + T(p, q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Hence,

$$(-1)^{T(q,p)+T(p,q)} = (-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Lemma 11.2 tells us that $(-1)^{T(q,p)} = \left(\frac{q}{p}\right)$ and $(-1)^{T(p,q)} = \left(\frac{p}{q}\right)$. Hence

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

This concludes the proof of the law of quadratic reciprocity. ∎

The law of quadratic reciprocity has many applications. One use is to prove the validity of the following primality test for Fermat numbers.

Theorem 11.9. ***Pepin's Test.*** The Fermat number $F_m = 2^{2^m} + 1$ is prime if and only if

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Proof. We will first show that F_m is prime if the congruence in the statement of the theorem holds. Assume that

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

Then, by squaring both sides, we obtain

$$3^{F_m-1} \equiv -1 \pmod{F_m}.$$

From this congruence, we see that if p is a prime dividing F_m, then

$$3^{F_m-1} \equiv -1 \pmod{p},$$

and hence,

$$\operatorname{ord}_p 3 \mid (F_m - 1) = 2^{2^m}.$$

Consequently, $\operatorname{ord}_p 3$ must be a power of 2. However,

$$\operatorname{ord}_p 3 \nmid 2^{2^m-1} = (F_m - 1)/2,$$

because $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. Hence, the only possibility is that $\operatorname{ord}_p 3 = 2^{2^m} = F_m - 1$. Because $\operatorname{ord}_p 3 = F_m - 1 \leq p - 1$ and $p \mid F_m$, we see that $p = F_m$ and, consequently, F_m must be prime.

Conversely, if $F_m = 2^{2^m} + 1$ is prime for $m \geq 1$, then the law of quadratic reciprocity tells us that

$$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{2}{3}\right) = -1, \tag{11.6}$$

because $F_m \equiv 1 \pmod 4$ and $F_m \equiv 2 \pmod 3$.

Now, using Euler's criterion, we know that

$$\left(\frac{3}{F_m}\right) \equiv 3^{(F_m-1)/2} \pmod{F_m}. \tag{11.7}$$

By the two equations involving $\left(\frac{3}{F_m}\right)$, (11.6) and (11.7), we conclude that

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

This finishes the proof. ■

Example 11.12. Let $m = 2$. Then $F_2 = 2^{2^2} + 1 = 17$ and

$$3^{(F_2-1)/2} = 3^8 \equiv -1 \pmod{17}.$$

By Pepin's test, we see that $F_2 = 17$ is prime.

Let $m = 5$. Then $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4{,}294{,}967{,}297$. We note that

$$3^{(F_5-1)/2} = 3^{2^{31}} = 3^{2{,}146{,}483{,}648} \equiv 10{,}324{,}303 \not\equiv -1 \pmod{4{,}294{,}967{,}297}.$$

Hence, by Pepin's test, we see that F_5 is composite. ◀

11.2 Exercises

1. Evaluate each of the following Legendre symbols.

   a) $\left(\frac{3}{53}\right)$ c) $\left(\frac{15}{101}\right)$ e) $\left(\frac{111}{991}\right)$

   b) $\left(\frac{7}{79}\right)$ d) $\left(\frac{31}{641}\right)$ f) $\left(\frac{105}{1009}\right)$

2. Using the law of quadratic reciprocity, show that if p is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

3. Show that if p is an odd prime, then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6; \\ -1 & \text{if } p \equiv -1 \pmod 6. \end{cases}$$

4. Find a congruence describing all primes for which 5 is a quadratic residue.

5. Find a congruence describing all primes for which 7 is a quadratic residue.

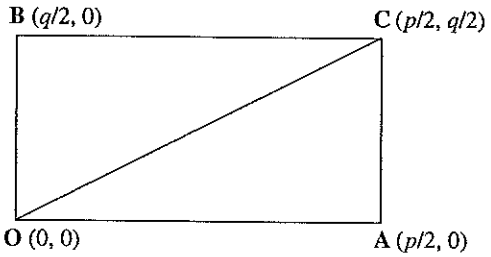
6. Show that there are infinitely many primes of the form $5k + 4$. (*Hint:* Let n be a positive integer and form $Q = 5(n!)^2 - 1$. Show that Q has a prime divisor of the form $5k + 4$ greater than n. To do this, use the law of quadratic reciprocity to show that if a prime p divides Q, then $\left(\frac{p}{5}\right) = 1$.)

7. Use Pepin's test to show that the following Fermat numbers are primes.

   a) $F_1 = 5$ b) $F_3 = 257$ c) $F_4 = 65{,}537$

* 8. Use Pepin's test to conclude that 3 is a primitive root of every Fermat prime.

* 9. In this exercise, we give another proof of the law of quadratic reciprocity. Let p and q be distinct odd primes. Let **R** be the interior of the rectangle with vertices $\mathbf{Q} = (0, 0)$, $\mathbf{A} = (p/2, 0)$, $\mathbf{B} = (q/2, 0)$, and $\mathbf{C} = (p/2, q/2)$, as shown.



   a) Show that the number of lattice points (points with integer coordinates) in **R** is $\frac{p-1}{2} \cdot \frac{q-1}{2}$.

   b) Show that there are no lattice points on the diagonal connecting **O** and **C**.

   c) Show that the number of lattice points in the triangle with vertices **O**, **A**, and **C** is $\sum_{j=1}^{(p-1)/2} [jq/p]$.

   d) Show that the number of lattice points in the triangle with vertices **O**, **B**, and **C** is $\sum_{j=1}^{(q-1)/2} [jp/q]$.

   e) Conclude from parts (a), (b), (c), and (d) that

$$\sum_{j=1}^{(p-1)/2} [jq/p] + \sum_{j=1}^{(q-1)/2} [jp/q] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

   Derive the law of quadratic reciprocity using this equation and Lemma 11.2.

Exercises 10 and 11 ask that you show that Euler's form of the law of quadratic reciprocity (Theorem 11.8) and the form given in Theorem 11.7 are equivalent.

10. Show that Euler's form of the law of quadratic reciprocity, Theorem 11.8, implies the law of quadratic reciprocity as stated in Theorem 11.7. (*Hint:* Consider separately the cases when $p \equiv q \pmod 4$ and $p \not\equiv q \pmod 4$.)

11. Show that the law of quadratic reciprocity as stated in Theorem 11.7 implies Euler's form of the law of quadratic reciprocity, Theorem 11.8. (*Hint:* First consider the cases when $a = 2$ and when a is an odd prime. Then consider the case when a is composite.)

12. Prove Euler's form of the law of quadratic reciprocity, Theorem 11.8, using Gauss's lemma. (*Hint:* Show that to find $\left(\frac{a}{p}\right)$, we need only find the parity of the number

of integers k satisfying one of the inequalities $(2t-1)(p/2a) \le k \le t(p/a)$ for $t = 1, 2, \ldots, 2u-1$, where $u = a/2$ if a is even and $u = (a-1)/2$ if a is odd. Then, take $p = 4am + r$ with $0 < r < 4a$, and show that finding the parity of the number of integers k satisfying one of the inequalities listed is the same as finding the parity of the number of integers satisfying one of the inequalities $(2t-1)r/2a \le k \le tr/a$ for $t = 1, 2, \ldots, 2u-1$. Show that this number depends only on r. Then, repeat the last step of the argument with r replaced by $4a - r$).

Exercise 13 asks that you fill in the details of a proof of the law of quadratic reciprocity originally developed by Eisenstein. This proof requires familiarity with the complex numbers.

13. A complex number ζ is an *nth root of unity*, where n is a positive integer, if $\zeta^n = 1$. If n is the least integer for which $\zeta^n = 1$, then ζ is called a *primitive nth root of unity*. Recall that $e^{2\pi i} = 1$.

a) Show that $e^{(2\pi i/n)k}$ is a root of unity if k is an integer with $0 \le k \le n-1$, which is primitive if and only if $(k, n) = 1$.

b) Show that if ζ is an nth root of unity and $m \equiv \ell \pmod{n}$, then $\zeta^m = \zeta^\ell$. Furthermore, show that if ζ is a primitive nth root of unity and $\zeta^m = \zeta^\ell$, then $m \equiv \ell \pmod{n}$.

c) Define $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin(2\pi z)$. Show that $f(z+1) = f(z)$ and $f(-z) = -f(z)$, and that the only real zeros of $f(z)$ are the numbers $n/2$, where n is an integer.

d) Show that if n is a positive integer, then $x^n - y^n = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y)$, where $\zeta = e^{2\pi i/n}$.

e) Show that if n is an odd positive integer and $f(z)$ is as defined in part (c), then

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

f) Show that if p is an odd prime and a is an integer not divisible by p, then

$$\prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell a}{p}\right) = \left(\frac{a}{p}\right) \prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell}{p}\right).$$

g) Prove the law of quadratic reciprocity using parts (e) and (f), starting with

$$\prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell q}{p}\right) = \left(\frac{q}{p}\right) \prod_{\ell=1}^{(p-1)/2} f\left(\frac{\ell}{p}\right).$$

(*Hint:* Use part (e) to obtain a formula for $f\left(\frac{\ell q}{p}\right) / f\left(\frac{\ell}{p}\right)$.)

14. Suppose that p is an odd prime with $\left(\frac{n}{p}\right) = -1$, where $n = k2^m + 1$ with $k < 2^m$ for some integers k and m. Show that n is prime if and only if $p^{(n-1)/2} \equiv -1 \pmod{n}$. (*Hint:* Use Proth's theorem from Section 9.5 for the "only if" part and Euler's criterion and the law of quadratic reciprocity for the "if" part.)

15. The integer $p = 1 + 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 892{,}371{,}481$ is prime (as the reader can verify using computational software). Show that for all primes q with $q \le 23$, $\left(\frac{q}{p}\right) = 1$. Conclude that there is no quadratic nonresidue of p less than 29 and that p has

no primitive root less than 29. (This fact is a particular case of the result established in the following exercise.)

16. In this exercise, we will show that given any integer M, there exist infinitely many primes p such that $M < r_p < p - M$, where r_p is the least primitive root modulo p.

a) Let $q_1 = 2, q_2 = 3, q_3 = 5, \ldots, q_n$ be all the primes not exceeding M. Using Dirichlet's theorem on primes in arithmetic progressions, there is a prime $p = 1 + 8q_1q_2 \cdots q_nr$, where r is a positive integer. Show that $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$, and that $\left(\frac{q_i}{p}\right) = 1$ for $i = 2, 3, \ldots, n$.

b) Deduce that all integers $t + kp$ with $-M \leq t + kp \leq M$, where t is an arbitrarily chosen integer, are quadratic residues modulo p and hence not primitive roots modulo p. Show that this implies the result of interest.

* **17.** New proofs of the law of quadratic reciprocity are found surprisingly often. In this exercise we fill in the steps of a proof discovered by Kim [Ki04], the 207th proof of quadratic reciprocity according to the count by Lemmermeyer. To set up the proof, let R be the set of integers a such that $1 \leq a \leq \frac{pq-1}{2}$ and $(a, pq) = 1$, let S be the set of integers a with $1 \leq a \leq \frac{pq-1}{2}$ and $(a, p) = 1$, and let T be the set of integers a with $q \cdot 1, q \cdot 2, \ldots, q \cdot \frac{p-1}{2}$. Finally, let $A = \prod_{a \in R} a$.

a) Show that T is a subset of S and that $R = S - T$.

b) Use part (a) and Euler's criterion to show that $A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$.

c) Show that $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$ by switching the roles of p and q in parts (a) and (b).

d) Use parts (b) and (c) to show that $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ if and only if $A \equiv \pm 1 \pmod{pq}$.

e) Show that $A \equiv 1$ or $-1 \pmod{pq}$ if and only if $p \equiv q \equiv 1 \pmod{4}$.

(*Hint:* First show that $A \equiv \pm \prod_{a \in U} a \pmod{pq}$, where $U = \{a \in R \mid a^2 \equiv \pm 1 \pmod{pq}\}$ by pairing together elements of R that have either 1 or -1 as their product. Then consider the solutions of each of the congruences $a^2 \equiv 1 \pmod{pq}$ and $a^2 \equiv -1 \pmod{pq}$.)

f) Conclude from parts (d) and (e) that $(-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right)$ if and only if $p \equiv q \equiv 1 \pmod{4}$. Deduce the law of quadratic reciprocity from this congruence.

11.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Use Pepin's test to show that the Fermat numbers F_6, F_7, and F_8 are all composite. Can you go further?

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Evaluate Legendre symbols, using the law of quadratic reciprocity.
2. Given a positive integer n, determine whether the nth Fermat number F_n is prime, using Pepin's test.

11.3 The Jacobi Symbol

In this section, we define the Jacobi symbol, named after German mathematician *Carl Jacobi* who introduced it. The Jacobi symbol is a generalization of the Legendre symbol studied in the previous two sections. Jacobi symbols are useful in the evaluation of Legendre symbols and in the definition of a type of pseudoprime.

Definition. Let n be an odd positive integer with prime factorization $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$ and let a be an integer relatively prime to n. Then, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}}\right) = \left(\frac{a}{p_1}\right)^{t_1} \left(\frac{a}{p_2}\right)^{t_2} \cdots \left(\frac{a}{p_m}\right)^{t_m},$$

where the symbols on the right-hand side of the equality are Legendre symbols.

Example 11.13. From the definition of the Jacobi symbol, we see that

$$\left(\frac{2}{45}\right) = \left(\frac{2}{3^2 \cdot 5}\right) = \left(\frac{2}{3}\right)^2 \left(\frac{2}{5}\right) = (-1)^2(-1) = -1$$

and

$$\left(\frac{109}{385}\right) = \left(\frac{109}{5 \cdot 7 \cdot 11}\right) = \left(\frac{109}{5}\right)\left(\frac{109}{7}\right)\left(\frac{109}{11}\right) = \left(\frac{4}{5}\right)\left(\frac{4}{7}\right)\left(\frac{10}{11}\right)$$
$$= \left(\frac{2}{5}\right)^2 \left(\frac{2}{7}\right)^2 \left(\frac{-1}{11}\right) = (-1)^2 1^2 (-1) = -1. \quad \blacktriangleleft$$

CARL GUSTAV JACOB JACOBI (1804–1851) was born into a well-to-do German banking family. Jacobi received an excellent early education at home. He studied at the University of Berlin, mastered mathematics through the texts of Euler, and obtained his doctorate in 1825. In 1826, he became a lecturer at the University of Königsberg; he was appointed a professor there in 1831. Besides his work in number theory, Jacobi made important contributions to analysis, geometry, and mechanics. He was also interested in the history of mathematics and was a catalyst in the publication of the collected works of Euler, a job not yet completed although it was begun more than 125 years ago!

When n is prime, the Jacobi symbol is the same as the Legendre symbol. However, when n is composite, the value of the Jacobi symbol $\left(\frac{a}{n}\right)$ does *not* tell us whether the congruence $x^2 \equiv a \pmod{n}$ has solutions. We do know that if the congruence $x^2 \equiv a \pmod{n}$ has solutions, then $\left(\frac{a}{n}\right) = 1$. To see this, note that if p is a prime divisor of n and if $x^2 \equiv a \pmod{n}$ has solutions, then the congruence $x^2 \equiv a \pmod{p}$ also has solutions. Thus, $\left(\frac{a}{p}\right) = 1$. Consequently, $\left(\frac{a}{n}\right) = \prod_{j=1}^{m} \left(\frac{a}{p_j}\right)^{t_j} = 1$, where the prime factorization of n is $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$. To see that it is possible that $\left(\frac{a}{n}\right) = 1$ when there are no solutions to $x^2 \equiv a \pmod{n}$, let $a = 2$ and $n = 15$. Note that $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. However, there are no solutions to $x^2 \equiv 2 \pmod{15}$, because the congruences $x^2 \equiv 2 \pmod{3}$ and $x^2 \equiv 2 \pmod{5}$ have no solutions.

We now show that the Jacobi symbol enjoys some properties similar to those of the Legendre symbol.

Theorem 11.10. Let n be an odd positive integer and let a and b be integers relatively prime to n. Then

(i) if $a \equiv b \pmod{n}$, then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
(iii) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
(iv) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Proof. In the proof of this theorem, we use the prime factorization $n = p_1^{t_1} p_2^{t_2} \cdots p_m^{t_m}$.

Proof of (i). We know that if p is a prime dividing n, then $a \equiv b \pmod{p}$. Hence, from Theorem 11.4 (i), we have $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Consequently, we see that

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2} \cdots \left(\frac{a}{p_m}\right)^{t_m} = \left(\frac{b}{p_1}\right)^{t_1}\left(\frac{b}{p_2}\right)^{t_2} \cdots \left(\frac{b}{p_m}\right)^{t_m} = \left(\frac{b}{n}\right).$$

Proof of (ii). From Theorem 11.4 (ii), we know that $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ for $i = 1, 2, 3, \ldots, m$. Hence,

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)^{t_1}\left(\frac{ab}{p_2}\right)^{t_2} \cdots \left(\frac{ab}{p_m}\right)^{t_m} \\ &= \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{b}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\left(\frac{b}{p_2}\right)^{t_2} \cdots \left(\frac{a}{p_m}\right)^{t_m}\left(\frac{b}{p_m}\right)^{t_m} \\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

Proof of (iii). Theorem 11.5 tells us that if p is prime, then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Consequently,

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{t_1}\left(\frac{-1}{p_2}\right)^{t_2}\cdots\left(\frac{-1}{p_m}\right)^{t_m}$$
$$= (-1)^{t_1(p_1-1)/2+t_2(p_2-1)/2+\cdots+t_m(p_m-1)/2}.$$

From the prime factorization of n, we have

$$n = (1+(p_1-1))^{t_1}(1+(p_2-1))^{t_2}\cdots(1+(p_m-1))^{t_m}.$$

Because $p_i - 1$ is even, it follows that

$$(1+(p_i-1))^{t_i} \equiv 1 + t_i(p_i-1) \pmod 4$$

and

$$(1+t_i(p_i-1))(1+t_j(p_j-1)) \equiv 1 + t_i(p_i-1) + t_j(p_j-1) \pmod 4.$$

Therefore,

$$n \equiv 1 + t_1(p_1-1) + t_2(p_2-1) + \cdots + t_m(p_m-1) \pmod 4,$$

which imples that

$$(n-1)/2 \equiv t_1(p_1-1)/2 + t_2(p_2-1)/2 + \cdots + t_m(p_m-1)/2 \pmod 2.$$

Combining this congruence for $(n-1)/2$ with the expression for $\left(\frac{-1}{n}\right)$ shows that $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

Proof of (iv). If p is prime, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Hence,

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)^{t_1}\left(\frac{2}{p_2}\right)^{t_2}\cdots\left(\frac{2}{p_m}\right)^{t_m} = (-1)^{t_1(p_1^2-1)/8+t_2(p_2^2-1)/8+\cdots+t_m(p_m^2-1)/8}.$$

As in the proof of (iii), we note that

$$n^2 = (1+(p_1^2-1)^{t_1}(1+(p_2^2-1))^{t_2}\cdots(1+(p_m^2-1))^{t_m}.$$

Because $p_i^2 - 1 \equiv 0 \pmod 8$ for $i = 1, 2, \ldots, m$, we see that

$$(1+(p_i^2-1))^{t_i} \equiv 1 + t_i(p_i^2-1) \pmod{64}$$

and

$$(1+t_i(p_i^2-1))(1+t_j(p_j^2-1)) \equiv 1 + t_i(p_i^2-1) + t_j(p_j^2-1) \pmod{64}.$$

Hence,

$$n^2 \equiv 1 + t_1(p_1^2-1) + t_2(p_2^2-1) + \cdots + t_m(p_m^2-1) \pmod{64},$$

which implies that

$$(n^2-1)/8 = t_1(p_1^2-1)/8 + t_2(p_2^2-1)/8 + \cdots + t_m(p_m^2-1)/8 \pmod 8.$$

Combining this congruence for $(n^2-1)/8$ with the expression for $\left(\frac{2}{n}\right)$ tells us that $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. ∎

We now demonstrate that the reciprocity law holds for the Jacobi symbol as well as the Legendre symbol.

Theorem 11.11. ***The Reciprocity Law for Jacobi Symbols.*** Let n and m be relatively prime odd positive integers. Then

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Proof. Let the prime factorizations of m and n be $m = p_1^{a_1}p_2^{a_s}\cdots p_s^{a_s}$ and $n = q_1^{b_1}q_2^{b_2}\cdots q_r^{b_r}$. We see that

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{m}{q_i}\right)^{b_i} = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_j}{q_j}\right)^{b_i a_j}$$

and

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{s}\left(\frac{n}{p_j}\right)^{a_j} = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{a_j b_i}.$$

Thus,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right]^{a_j b_i}.$$

By the law of quadratic reciprocity, we know that

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right) = (-1)^{\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)}.$$

Hence,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{a_j\left(\frac{p_j-1}{2}\right)b_i\left(\frac{q_i-1}{2}\right)} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\left(\frac{p_j-1}{2}\right)b_i\left(\frac{q_i-1}{2}\right)}. \tag{11.8}$$

We note that

$$\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\left(\frac{p_j-1}{2}\right)b_i\left(\frac{q_i-1}{2}\right) = \sum_{j=1}^{s}a_j\left(\frac{p_j-1}{2}\right)\sum_{i=1}^{r}b_i\left(\frac{q_i-1}{2}\right).$$

As we demonstrated in the proof of Theorem 11.10 (iii),

$$\sum_{j=1}^{s} a_j\left(\frac{p_j-1}{2}\right) \equiv \frac{m-1}{2} \pmod 2$$

and

$$\sum_{i=1}^{r} b_i\left(\frac{q_i-1}{2}\right) \equiv \frac{n-1}{2} \pmod 2.$$

Thus,

$$\sum_{i=1}^{r}\sum_{j=1}^{s} a_j\left(\frac{p_j-1}{2}\right) b_i\left(\frac{q_i-1}{2}\right) \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2. \tag{11.9}$$

Therefore, by equations (11.8) and (11.9), we can conclude that

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

■

An Algorithm for Computing Jacobi Symbols We now develop an efficient algorithm for evaluating Jacobi symbols. Let a and b be relatively prime positive integers with $a > b$. Let $R_0 = a$ and $R_1 = b$. Using the division algorithm and factoring out the highest power of two dividing the remainder, we obtain

$$R_0 = R_1 q_1 + 2^{s_1} R_2,$$

where s_1 is a nonnegative integer and R_2 is an odd positive integer less than R_1. When we successively use the division algorithm, and factor out the highest power of two that divides remainders, we obtain

$$\begin{aligned}
R_1 &= R_2 q_2 + 2^{s_2} R_3 \\
R_2 &= R_3 q_3 + 2^{s_3} R_4 \\
&\vdots \\
R_{n-3} &= R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1} \\
R_{n-2} &= R_{n-1} q_{n-1} + 2^{s_{n-1}} \cdot 1,
\end{aligned}$$

where s_j is a nonnegative integer and R_j is an odd positive integer less than R_{j-1} for $j = 2, 3, \ldots, n-1$. Note that the number of divisions required to reach the final equation does not exceed the number of divisions required to find the greatest common divisor of a and b using the Euclidean algorithm.

We illustrate this sequence of equations with the following example.

Example 11.14. Let $a = 401$ and $b = 111$. Then

$$\begin{aligned}
401 &= 111 \cdot 3 + 2^2 \cdot 17 \\
111 &= 17 \cdot 6 + 2^0 \cdot 9 \\
17 &= 9 \cdot 1 + 2^3 \cdot 1.
\end{aligned}$$

◀

Using the sequence of equations that we have described, together with the properties of the Jacobi symbol, we prove the following theorem, which gives an algorithm for evaluating Jacobi symbols.

Theorem 11.12. Let a and b be positive integers with $a > b$. Then

$$\left(\frac{a}{b}\right) = (-1)^{s_1\frac{R_1^2-1}{8}+\cdots+s_{n-1}\frac{R_{n-1}^2-1}{8}+\frac{R_1-1}{2}\cdot\frac{R_2-1}{2}+\cdots+\frac{R_{n-2}-1}{2}\cdot\frac{R_{n-1}-1}{2}},$$

where the integers R_j and s_j, $j = 1, 2, \ldots, n-1$, are as previously described.

Proof. From the first equation with (i), (ii), and (iv) of Theorem 11.10, we have

$$\left(\frac{a}{b}\right) = \left(\frac{R_0}{R_1}\right) = \left(\frac{2^{S_1}R_2}{R_1}\right) = \left(\frac{2}{R_1}\right)^{s_1}\left(\frac{R_2}{R_1}\right) = (-1)^{s_1\frac{R_1^2-1}{8}}\left(\frac{R_2}{R_1}\right).$$

Using Theorem 11.11, the reciprocity law for Jacobi symbols, we have

$$\left(\frac{R_2}{R_1}\right) = (-1)^{\frac{R_1-1}{2}\cdot\frac{R_2-1}{2}}\left(\frac{R_1}{R_2}\right),$$

so that

$$\left(\frac{a}{b}\right) = (-1)^{\frac{R_1-1}{2}\cdot\frac{R_2-1}{2}+s_1\frac{R_1^2-1}{8}}\left(\frac{R_1}{R_2}\right).$$

Similarly, using the subsequent divisions, we find that

$$\left(\frac{R_{j-1}}{R_j}\right) = (-1)^{\frac{R_j-1}{2}\cdot\frac{R_{j+1}-1}{2}+s_1\cdot\frac{R_j^2-1}{8}}\left(\frac{R_j}{R_{j+1}}\right)$$

for $j = 2, 3, \ldots, n-1$. When we combine all the equalities, we obtain the desired expression for $\left(\frac{a}{b}\right)$. ∎

The following example illustrates the use of Theorem 11.12.

Example 11.15. To evaluate $\left(\frac{401}{111}\right)$, we use the sequence of divisions in Example 11.14 and Theorem 11.12. This tells us that

$$\left(\frac{401}{111}\right) = (-1)^{2\cdot\frac{111^2-1}{8}+0\cdot\frac{17^2-1}{8}+3\cdot\frac{9^2-1}{8}+\frac{111-1}{2}\cdot\frac{17-1}{2}+\frac{17-1}{2}\cdot\frac{9-1}{2}} = 1. \quad ◀$$

The following corollary describes the computational complexity of the algorithm for evaluating Jacobi symbols given in Theorem 11.12.

Corollary 11.12.1. Let a and b be relatively prime positive integers with $a > b$. Then the Jacobi symbol $\left(\frac{a}{b}\right)$ can be evaluated using $O((\log_2 b)^3)$ bit operations.

Proof. To find $\left(\frac{a}{b}\right)$ using Theorem 11.12, we perform a sequence of $O(\log_2 b)$ divisions. To see this, note that the number of divisions does not exceed the number of divisions needed to find (a, b) using the Euclidean algorithm. Thus, by Lamé's theorem, we know that $O(\log_2 b)$ divisions are needed. Each division can be done using $O((\log_2 b)^2)$ bit

operations. Each pair of integers R_j and s_j can be found using $O(\log_2 b)$ bit operations once the appropriate division has been carried out.

Consequently, $O((\log_2 b)^3)$ bit operations are required to find the integers R_j, s_j, $j = 1, 2, \ldots, n-1$ from a and b. Finally, to evaluate the exponent of -1 in the expression for $\left(\frac{a}{b}\right)$ in Theorem 11.12, we use the last three bits in the binary expansions of R_j, $j = 1, 2, \ldots, n-1$ and the last bit in the binary expansions of s_j, $j = 1, 2, \ldots, n-1$. Therefore, we use $O(\log_2 b)$ additional bit operations to find $\left(\frac{a}{b}\right)$. Because $O((\log_2 b)^3) + O(\log_2 b) = O((\log_2 b)^3)$, the corollary holds. ∎

We can improve this corollary if we use more care when estimating the number of bit operations used by divisions. In particular, we can show that $O((\log_2 b)^2)$ bit operations suffice for evaluating $\left(\frac{a}{b}\right)$. We leave this as an exercise.

11.3 Exercises

1. Evaluate each of the following Jacobi symbols.

   a) $\left(\frac{5}{21}\right)$ c) $\left(\frac{111}{1001}\right)$ e) $\left(\frac{2663}{3299}\right)$

   b) $\left(\frac{27}{101}\right)$ d) $\left(\frac{1009}{2307}\right)$ f) $\left(\frac{10001}{20003}\right)$

2. For which positive integers n that are relatively prime to 15 does the Jacobi symbol $\left(\frac{15}{n}\right)$ equal 1?

3. For which positive integers n that are relatively prime to 30 does the Jacobi symbol $\left(\frac{30}{n}\right)$ equal 1?

Suppose that $n = pq$, where p and q are primes. We say that the integer a is a *pseudo-square* modulo n if a is a quadratic nonresidue of n, but $\left(\frac{a}{n}\right) = 1$.

4. Show that if a is a pseudo-square modulo n, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$.

5. Find all the pseudo-squares modulo 21.

6. Find all the pseudo-squares modulo 35.

7. Find all the pseudo-squares modulo 143.

8. Let a and b be relatively prime integers such that b is odd and positive and $a = (-1)^s 2^t q$, where q is odd. Show that

$$\left(\frac{a}{b}\right) = (-1)^{\frac{b-1}{2}\cdot s + \frac{b^2-1}{8}\cdot t}\left(\frac{q}{b}\right).$$

9. Let n be an odd square-free positive integer. Show that there is an integer a such that $(a, n) = 1$ and $\left(\frac{a}{n}\right) = -1$.

10. Let n be an odd square-free positive integer.

    a) Show that $\sum \left(\frac{k}{n}\right) = 0$, where the sum is taken over all k in a reduced set of residues modulo n. (*Hint:* Use Exercise 9.)

b) From part (a), show that the number of integers in a reduced set of residues modulo n such that $\left(\frac{k}{n}\right) = 1$ is equal to the number with $\left(\frac{k}{n}\right) = -1$.

* **11.** Let a and $b = r_0$ be relatively prime odd positive integers such that

$$\begin{aligned} a &= r_0 q_1 + \varepsilon_1 r_1 \\ r_0 &= r_1 q_2 + \varepsilon_2 r_2 \\ &\vdots \\ r_{n-1} &= r_{n-1} q_{n-1} + \varepsilon_n r_n, \end{aligned}$$

where q_i is a nonnegative even integer, $\varepsilon_i = \pm 1$, r_i is a positive integer with $r_i < r_{i-1}$, for $i = 1, 2, \ldots, n_j$, and $r_n = 1$. These equations are obtained by successively using the modified division algorithm given in Exercise 18 of Section 1.5.

a) Show that Jacobi symbol $\left(\frac{a}{b}\right)$ is given by

$$\left(\frac{a}{b}\right) = (-1)^{\left(\frac{r_0-1}{2}\cdot\frac{\varepsilon_1 r_1 - 1}{2} + \frac{r_1-1}{2}\cdot\frac{\varepsilon_2 r_2 - 1}{2} + \cdots + \frac{r_{n-1}-1}{2}\cdot\frac{\varepsilon_n r_n - 1}{2}\right)}.$$

b) Show that the Jacobi symbol $\left(\frac{a}{b}\right)$ is given by

$$\left(\frac{a}{b}\right) = (-1)^T,$$

where T is the number of integers i, $1 \le i \le n$, with $r_{i-1} \equiv \varepsilon_i r_i \equiv 3 \pmod 4$.

* **12.** Show that if a and b are odd integers and $(a, b) = 1$, then the following reciprocity law holds for the Jacobi symbol:

$$\left(\frac{a}{|b|}\right)\left(\frac{b}{|a|}\right) = \begin{cases} -(-1)^{\frac{a-1}{2}\frac{b-1}{2}} & \text{if } a < 0 \text{ and } b < 0; \\ (-1)^{\frac{a-1}{2}\frac{b-1}{2}} & \text{otherwise.} \end{cases}$$

In Exercises 13–19, we deal with the *Kronecker symbol* (named after Leopold Kronecker), which is defined as follows. Let a be a positive integer that is not a perfect square such that $a \equiv 0$ or $1 \pmod 4$. We define

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 8; \\ -1 & \text{if } a \equiv 5 \pmod 8. \end{cases}$$

$\left(\frac{a}{p}\right)$ = the Legendre symbol $\left(\frac{a}{p}\right)$ if p is an odd prime such that $p \nmid a$.

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{t_j} \text{ if } (a, n) = 1 \text{ and } n = \prod_{j=1}^{r} p_j^{t_j} \text{ is the prime factorization of } n.$$

13. Evaluate each of the following Kronecker symbols,

a) $\left(\frac{5}{12}\right)$ b) $\left(\frac{13}{20}\right)$ c) $\left(\frac{101}{200}\right)$

For Exercises 14–19, let a be a positive integer that is not a perfect square such that $a \equiv 0$ or $1 \pmod 4$.

14. Show that $\left(\frac{a}{2}\right) = \left(\frac{2}{|a|}\right)$ if $2 \nmid a$, where the symbol on the right is a Jacobi symbol.

15. Show that if n_1 and n_2 are positive integers and if $(a_1, n_1, n_2) = 1$, then $\left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{n_1}\right) \cdot \left(\frac{a}{n_2}\right)$.

* **16.** Show that if n is a positive integer relatively prime to a and if a is odd, then $\left(\frac{a}{n}\right) = \left(\frac{n}{|a|}\right)$, whereas if a is even and $a = 2^s t$, where t is odd, then

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^s (-1)^{\frac{t-1}{2} \cdot \frac{n-1}{2}} \left(\frac{n}{|t|}\right).$$

* **17.** Show that if n_1 and n_2 are positive integers relatively prime to a and $n_1 \equiv n_2 \pmod{|a|}$, then $\left(\frac{a}{n_1}\right) = \left(\frac{a}{n_2}\right)$.

LEOPOLD KRONECKER (1823–1891) was born in Liegnitz, Prussia, to prosperous Jewish parents. His father was a successful businessman and his mother came from a wealthy family. As a child, Kronecker was taught by private tutors. He later entered the Liegnitz Gymnasium where he was taught mathematics by the number theorist Kummer. Kronecker's mathematical talents were quickly recognized by Kummer, who encouraged Kronecker to engage in mathematics research. In 1841, Kronecker entered Berlin University where he studied mathematics, astronomy, meteorology, chemistry, and philosophy. In 1845, Kronecker wrote his doctoral thesis on algebraic number theory; his supervisor was Dirichlet.

Kronecker could have begun a promising academic career, but instead he returned to Liegnitz to help manage the banking business of an uncle. In 1848, Kronecker married a daughter of this uncle. During his time back in Liegnitz, Kronecker continued his research for his own enjoyment. In 1855, when his family obligations eased, Kronecker returned to Berlin. He was eager to participate in the mathematical life of the university. Not holding a university post, he did not teach any classes. However, he was extremely active in research and he published extensively in number theory, elliptic functions and algebra, and their interconnections. In 1860, Kronecker was elected to the Berlin Academy, giving him the right to lecture at Berlin University. He took advantage of this opportunity and lectured on number theory and other mathematical topics. Kronecker's lectures were considered very demanding but were also considered to be stimulating. Unfortunately, he was not a popular teacher with average students; most of these dropped out of his courses by the end of the semester.

Kronecker was a strong believer in constructive mathematics, thinking that mathematics should be concerned only with finite numbers and with a finite number of operations. He doubted the validity of nonconstructive existence proofs and was opposed to objects defined nonconstructively, such as irrational numbers. He did not believe that transcendental numbers could exist. He is famous for his statement: "God created the integers, all else is the work of man." Kronecker's belief in constructive mathematics was not shared by most of his colleagues, although he was not the only prominent mathematician to hold such beliefs. Many mathematicians found it difficult to get along with Kronecker, especially because he was prone to fallings out over mathematical disagreements. Also, Kronecker was self-conscious about his short height, reacting badly even to good-natured references to his short stature.

* **18.** Show that if $a \neq 0$, then there exists a positive integer n such that $\left(\frac{a}{n}\right) = -1$.

* **19.** Show that if $a \neq 0$, then $\left(\frac{a}{|a|-1}\right) = \begin{cases} 1 & \text{if } a > 0; \\ -1 & \text{if } a < 0. \end{cases}$

20. Show that if a and b are relatively prime integers with $a < b$, then Jacobi symbol $\left(\frac{a}{b}\right)$ can be evaluated using $O((\log_2 b)^2)$ bit operations.

11.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the value of each of the Legendre symbol $\left(\frac{1,656,169}{2,355,151}\right)$.

2. Find the value of the following Jacobi symbols: $\left(\frac{9343}{65,518,791}\right)$, $\left(\frac{54371}{5,400,207,333}\right)$, $\left(\frac{320001}{11,111,111,111,111}\right)$.

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Evaluate Jacobi symbols using the method of Theorem 11.12.

2. Evaluate Jacobi symbols using Exercises 8 and 11.

3. Evaluate Kronecker symbols (as defined in the preamble to Exercise 13).

11.4 Euler Pseudoprimes

Let p be an odd prime number and let b be an integer not divisible by p. By Euler's criterion, we know that

$$b^{(p-1)/2} \equiv \left(\frac{b}{p}\right) \pmod{p}.$$

Hence, if we wish to test the positive integer n for primality, we can take an integer b, with $(b, n) = 1$, and determine whether

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n},$$

where the symbol on the right-hand side of the congruence is the Jacobi symbol. If we find that this congruence fails, then n is composite.

Example 11.16. Let $n = 341$ and $b = 2$. We calculate that $2^{170} \equiv 1 \pmod{341}$. Because $341 \equiv -3 \pmod 8$, using Theorem 11.10 (iv), we see that $\left(\frac{2}{341}\right) = -1$. Consequently, $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$. This demonstrates that 341 is not prime. ◀

Thus, we can define a type of pseudoprime based on Euler's criterion.

Definition. An odd, composite, positive integer n that satisfies the congruence

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n,$$

where b is a positive integer, is called an *Euler pseudoprime to the base b.*

An Euler pseudoprime to the base b is a composite integer that masquerades as a prime by satisfying the congruence given in the definition.

Example 11.17. Let $n = 1105$ and $b = 2$. We calculate that $2^{552} \equiv 1 \pmod{1105}$. Because $1105 \equiv 1 \pmod 8$, we see that $\left(\frac{2}{1105}\right) = 1$. Hence, $2^{552} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$. Because 1105 is composite, it is an Euler pseudoprime to the base 2. ◀

The following theorem shows that every Euler pseudoprime to the base b is a pseudoprime to this base.

Theorem 11.13. If n is an Euler pseudoprime to the base b, then n is a pseudoprime to the base b.

Proof. If n is an Euler pseudoprime to the base b, then

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n.$$

Hence, by squaring both sides of this congruence, we find that

$$(b^{(n-1)/2})^2 \equiv \left(\frac{b}{n}\right)^2 \pmod n.$$

Because $\left(\frac{b}{n}\right) = \pm 1$, we see that $b^{n-1} \equiv 1 \pmod n$, which means that n is a pseudoprime to the base b. ■

Not every pseudoprime is an Euler pseudoprime. For example, the integer 341 is not an Euler pseudoprime to the base 2, as we have shown, but is a pseudoprime to this base.

We know that every Euler pseudoprime is a pseudoprime. Next, we show that every strong pseudoprime is an Euler pseudoprime.

Theorem 11.14. If n is a strong pseudoprime to the base b, then n is an Euler pseudoprime to this base.

Proof. Let n be a strong pseudoprime to the base b. Then, if $n-1=2^s t$, where t is odd, either $b^t \equiv 1 \pmod{n}$ or $b^{2^r t} \equiv -1 \pmod{n}$, where $0 \le r \le s-1$. Let $n = \prod_{i=1}^{m} p_i^{a_i}$ be the prime-power factorization of n.

First, consider the case where $b^t \equiv 1 \pmod{n}$. Let p be a prime divisor of n. Because $b^t \equiv 1 \pmod{p}$, we know that $\text{ord}_p b \mid t$. Because t is odd, we see that $\text{ord}_p b$ is also odd. Hence, $\text{ord}_p b \mid (p-1)/2$, because $\text{ord}_p b$ is an odd divisor of the even integer $\phi(p) = p-1$. Therefore,

$$b^{(p-1)/2} \equiv 1 \pmod{p}.$$

Consequently, by Euler's criterion, we have $\left(\frac{b}{p}\right) = 1$.

To compute the Jacobi symbol $\left(\frac{b}{n}\right)$, we note that $\left(\frac{b}{p}\right) = 1$ for all primes p dividing n. Hence,

$$\left(\frac{b}{n}\right) = \left(\frac{b}{\prod_{i=1}^{m} p_i^{a_i}}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{a_i} = 1.$$

Because $b^t \equiv 1 \pmod{n}$, we know that $b^{(n-1)/2} = (b^t)^{2^{s-1}} \equiv 1 \pmod{n}$. Therefore, we have

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \equiv 1 \pmod{n}.$$

We conclude that n is an Euler pseudoprime to the base b.

Next, we consider the case where

$$b^{2^r t} \equiv -1 \pmod{n}$$

for some r with $0 \le r \le s-1$. If p is a prime divisor of n, then

$$b^{2^r t} \equiv -1 \pmod{p}.$$

Squaring both sides of this congruence, we obtain

$$b^{2^{r+1} t} \equiv 1 \pmod{p},$$

which implies that $\text{ord}_p b \mid 2^{r+1} t$, but that $\text{ord}_p b \nmid 2^r t$. Hence,

$$\text{ord}_p b = 2^{r+1} c,$$

where c is an odd integer. Because $\text{ord}_p b \mid (p-1)$ and $2^{r+1} \mid \text{ord}_p b$, it follows that $2^{r+1} \mid (p-1)$. Therefore, we have $p = 2^{r+1} d + 1$, where d is an integer. Because

$$b^{(\text{ord}_p b)/2} \equiv -1 \pmod{p},$$

we have

$$\begin{aligned}\left(\frac{b}{p}\right) &\equiv b^{(p-1)/2} = b^{(\text{ord}_p b/2)((p-1)/\text{ord}_p b)} \\ &\equiv (-1)^{(p-1)/\text{ord}_p b} = (-1)^{(p-1)/2^{r+1} c} \pmod{p}.\end{aligned}$$

Because c is odd, we know that $(-1)^c = -1$. Hence,

$$\left(\frac{b}{p}\right) = (-1)^{(p-1)/2^{r+1}} = (-1)^d, \tag{11.10}$$

recalling that $d = (p-1)/2^{r+1}$. Because each prime p_i dividing n is of the form $p_i = 2^{r+1}d_i + 1$, it follows that

$$\begin{aligned} n &= \prod_{i=1}^{m} p_i^{a_i} \\ &= \prod_{i=1}^{m} (2^{r+1}d_i + 1)^{a_i} \\ &\equiv \prod_{i=1}^{m} (1 + 2^{r+1}a_i d_i) \\ &\equiv 1 + 2^{r+1} \sum_{i=1}^{m} a_i d_i \pmod{2^{2r+2}}. \end{aligned}$$

Therefore,

$$t2^{s-1} = (n-1)/2 \equiv 2^r \sum_{i=1}^{m} a_i d_i \pmod{2^{r+1}}.$$

This congruence implies that

$$t2^{s-1-r} \equiv \textstyle\sum_{i=1}^{m} a_i d_i \pmod 2$$

and

$$b^{(n-1)/2} = (b^{2^r t})^{2^{s-1-r}} \equiv (-1)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i} \pmod n. \tag{11.11}$$

On the other hand, from (11.10), we have

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{m} \left(\frac{b}{p_i}\right)^{a_i} = \prod_{i=1}^{m} ((-1)^{d_i})^{a_i} = \prod_{i=1}^{m} (-1)^{a_i d_i} = (-1)^{\sum_{i=1}^{m} a_i d_i}.$$

Therefore, combining the preceding equation with (11.11), we see that

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n.$$

Consequently, n is an Euler pseudoprime to the base b. ■

Although every strong pseudoprime to the base b is an Euler pseudoprime to this base, note that not every Euler pseudoprime to the base b is a strong pseudoprime to the base b, as the following example shows.

Example 11.18. We have previously shown that the integer 1105 is an Euler pseudoprime to the base 2. However, 1105 is not a strong pseudoprime to the base 2, because

$$2^{(1105-1)/2} = 2^{552} \equiv 1 \pmod{1105},$$

whereas

$$2^{(1105-1)/2^2} = 2^{276} \equiv 781 \not\equiv \pm 1 \pmod{1105}.$$ ◀

Although an Euler pseudoprime to the base b is not always a strong pseudoprime to this base, when certain additional conditions are met, an Euler pseudoprime to the base b is, in fact, a strong pseudoprime to this base. The following two theorems give results of this kind.

Theorem 11.15. If $n \equiv 3 \pmod 4$ and n is an Euler pseudoprime to the base b, then n is a strong pseudoprime to the base b.

Proof. From the congruence $n \equiv 3 \pmod 4$, we know that $n - 1 = 2 \cdot t$, where $t = (n-1)/2$ is odd. Because n is an Euler pseudoprime to the base b, it follows that

$$b^t = b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n.$$

Because $\left(\frac{b}{n}\right) = \pm 1$, we know that either $b^t \equiv 1 \pmod n$ or $b^t \equiv -1 \pmod n$.

Hence, one of the congruences in the definition of a strong pseudoprime to the base b must hold. Consequently, n is a strong pseudoprime to the base b. ■

Theorem 11.16. If n is an Euler pseudoprime to the base b and $\left(\frac{b}{n}\right) = -1$, then n is a strong pseudoprime to the base b.

Proof. We write $n - 1 = 2^s t$, where t is odd and s is a positive integer. Because n is an Euler pseudoprime to the base b, we have

$$b^{2^{s-1}t} = b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod n.$$

But because $\left(\frac{b}{n}\right) = -1$, we see that

$$b^{t2^{s-1}} \equiv -1 \pmod n.$$

This is one of the congruences in the definition of a strong pseudoprime to the base b. Because n is composite, it is a strong pseudoprime to the base b. ■

Using the concept of Euler pseudoprimality, we will develop a probabilistic primality test. This test was first suggested by Solovay and Strassen [SoSt 77].

Before presenting the test, we give some helpful lemmas.

Lemma 11.4. If n is an odd positive integer that is not a perfect square, then there is at least one integer b with $1 < b < n$, $(b, n) = 1$, and $\left(\frac{b}{n}\right) = -1$, where $\left(\frac{b}{n}\right)$ is the Jacobi symbol.

Proof. If n is prime, the existence of such an integer b is guaranteed by Theorem 11.1. If n is composite, because n is not a perfect square, we can write $n = rs$, where $(r, s) = 1$ and $r = p^e$, with p an odd prime and e an odd positive integer.

Now, let t be a quadratic nonresidue of the prime p; such a t exists by Theorem 11.1. We use the Chinese remainder theorem to find an integer b such that $1 < b < n$, $(b, n) = 1$, and such that b satisfies the two congruences

$$b \equiv t \pmod{r}$$
$$b \equiv 1 \pmod{s}.$$

Then

$$\left(\frac{b}{r}\right) = \left(\frac{b}{p^e}\right) = \left(\frac{b}{p}\right)^e = (-1)^e = -1$$

and $\left(\frac{b}{s}\right) = 1$. Because $\left(\frac{b}{n}\right) = \left(\frac{b}{r}\right)\left(\frac{b}{s}\right)$, it follows that $\left(\frac{b}{n}\right) = -1$. ∎

Lemma 11.5. Let n be an odd composite integer. Then there is at least one integer b with $1 < b < n$, $(b, n) = 1$, and

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Proof. Assume, for all positive integers not exceeding n and relatively prime to n, that

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}. \tag{11.12}$$

Squaring both sides of this congruence tells us that

$$b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \equiv (\pm 1)^2 = 1 \pmod{n},$$

if $(b, n) = 1$. Hence, n must be a Carmichael number. Therefore, by Theorem 9.24, we know that $n = q_1 q_2 \cdots q_r$, where $q_1, q_2, \ldots, q_r$ are distinct odd primes.

We will now show that

$$b^{(n-1)/2} \equiv 1 \pmod{n}$$

for all integers b with $1 \leq b \leq n$ and $(b, n) = 1$. Suppose that b is an integer such that

$$b^{(n-1)/2} \equiv -1 \pmod{n}.$$

We use the Chinese remainder theorem to find an integer a with $1 < a < n$, $(a, n) = 1$, and

$$a \equiv b \pmod{q_1}$$
$$a \equiv 1 \pmod{q_2 q_3 \cdots q_r}.$$

Then we observe that

(11.13) $$a^{(n-1)/2} \equiv b^{(n-1)/2} \equiv -1 \pmod{q_1}.$$

whereas

(11.14) $$a^{(n-1)/2} \equiv 1 \pmod{q_2 q_3 \cdots q_r}.$$

From congruences (11.13) and (11.14), we see that

$$a^{(n-1)/2} \not\equiv \pm 1 \pmod{n},$$

contradicting congruence (11.12). Hence, we must have

$$b^{(n-1)/2} \equiv 1 \pmod{n},$$

for all b with $1 \leq b \leq n$ and $(b, n) = 1$. Consequently, from the definition of an Euler pseudoprime, we know that

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) = 1 \pmod{n},$$

for all b with $1 \leq b \leq n$ and $(b, n) = 1$. However, Lemma 11.4 tells us that this is impossible. Hence, the original assumption is false. There must be at least one integer b with $1 < b < n$, $(b, n) = 1$, and

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$ ∎

We can now state and prove the theorem that is the basis of the probabilistic primality test.

Theorem 11.17. Let n be an odd composite integer. Then the number of positive integers less than n and relatively prime to n that are bases to which n is an Euler pseudoprime does not exceed $\phi(n)/2$.

Proof. By Lemma 11.5, we know that there is an integer b with $1 < b < n$, $(b, n) = 1$, and

(11.15) $$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}.$$

Now, let $a_1, a_2, \ldots, a_m$ denote the positive integers less than n satisfying $1 \leq a_j \leq n$, $(a_j, n) = 1$, and

(11.16) $$a_j^{(n-1)/2} \equiv \left(\frac{a_j}{n}\right) \pmod{n},$$

for $j = 1, 2, \ldots, m$.

Let $r_1, r_2, \ldots, r_m$ be the least positive residues of the integers $ba_1, ba_2, \ldots, ba_m$ modulo n. We note that the integers r_j are distinct and that $(r_j, n) = 1$ for $j = 1, 2, \ldots, m$. Furthermore,

(11.17) $$r_j^{(n-1)/2} \not\equiv \left(\frac{r_j}{n}\right) \pmod{n};$$

for, if it were true that

$$r_j^{(n-1)/2} \equiv \left(\frac{r_j}{n}\right) \pmod{n},$$

then we would have

$$(ba_j)^{(n-1)/2} \equiv \left(\frac{ba_j}{n}\right) \pmod{n},$$

which would imply that

$$b^{(n-1)/2} a_j^{(n-1)/2} \equiv \left(\frac{b}{n}\right)\left(\frac{a_j}{n}\right) \pmod{n},$$

and because (11.16) holds, we would have

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right),$$

contradicting (11.15).

Because a_j, $j = 1, 2, \ldots, m$, satisfies the congruence (11.16), whereas r_j, $j = 1, 2, \ldots, m$, does not, as (11.17) shows, we know that these two sets of integers share no common elements. Hence, looking at the two sets together, we have a total of $2m$ distinct positive integers less than n and relatively prime to n. Because there are $\phi(n)$ integers less than n that are relatively prime to n, we can conclude that $2m \leq \phi(n)$, so that $m \leq \phi(n)/2$. This proves the theorem. ■

By Theorem 11.17, we see that if n is an odd composite integer, when an integer b is selected at random from the integers $1, 2, \ldots, n-1$, the probability that n is an Euler pseudoprime to the base b is less than 1/2. This leads to the following probabilistic primality test.

Theorem 11.18. ***The Solovay-Strassen Probabilistic Primality Test.*** Let n be a positive integer. Select, at random, k integers $b_1, b_2, \ldots, b_k$ from the integers $1, 2, \ldots, n-1$. For each of these integers b_j, $j = 1, 2, \ldots, k$, determine whether

$$b_j^{(n-1)/2} \equiv \left(\frac{b_j}{n}\right) \pmod{n}.$$

If any of these congruences fails, then n is composite. If n is prime, then all these congruences hold. If n is composite, the probability that all k congruences hold is less than $1/2^k$. Therefore, if n passes this test when k is large, then n is "almost certainly prime."

Because every strong pseudoprime to the base b is an Euler pseudoprime to this base, more composite integers pass the Solovay-Strassen probabilistic primality test than the Rabin probabilistic primality test, although both require $O(k(\log_2 n)^3)$ bit operations.

11.4 Exercises

1. Show that the integer 561 is an Euler pseudoprime to the base 2.
2. Show that the integer 15,841 is an Euler pseudoprime to the base 2, a strong pseudoprime to the base 2 and a Carmichael number.
3. Show that if n is an Euler pseudoprime to the bases a and b, then n is an Euler pseudoprime to the base ab.
4. Show that if n is an Euler pseudoprime to the base b, then n is also an Euler pseudoprime to the base $n - b$.
5. Show that if $n \equiv 5 \pmod 8$ and n is an Euler pseudoprime to the base 2, then n is a strong pseudoprime to the base 2.
6. Show that if $n \equiv 5 \pmod{12}$ and n is an Euler pseudoprime to the base 3, then n is a strong pseudoprime to the base 3.
7. Find a congruence condition for an Euler pseudoprime n to the base 5 that guarantees that n is a strong pseudoprime to the base 5.

** 8. Let the composite positive integer n have prime-power factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$, where $p_j = 1 + 2^{k_j} q_j$ for $j = 1, 2, \ldots, m$, where $k_1 \le k_2 \le \cdots \le k_m$, and where $n = 1 + 2^k q$. Show that n is an Euler pseudoprime to exactly

$$\delta_n \prod_{j=1}^{m} ((n-1)/2, p_j - 1)$$

different bases b with $1 \le b < n$, where

$$\delta_n = \begin{cases} 2 & \text{if } k_1 = k; \\ 1/2 & \text{if } k_j < k \text{ and } a_j \text{ is odd for some } j; \\ 1 & \text{otherwise.} \end{cases}$$

9. For how many integers b, $1 \le b < 561$, is 561 an Euler pseudoprime to the base b?
10. For how many integers b, $1 \le b < 1729$, is 1729 an Euler pseudoprime to the base b?

11.4 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find all Euler pseudoprimes to the base 2 less than 1,000,000. Do the same thing for the bases 3, 5, 7, and 11. Devise a primality test based on your results.
2. Find 10 integers, each with between 50 and 60 decimal digits, that are "probably prime" because they pass more than 20 iterations of the Solovay-Strassen probabilistic primality test.

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Given an integer n and a positive integer b greater than 1, determine whether n passes the test for Euler pseudoprimes to the base b.
2. Given an integer n, perform the Solovay-Strassen probabilistic primality test on n.

11.5 Zero-Knowledge Proofs

Suppose that you want to convince another person that you have some important private information, without revealing this information. For example, you may want to convince someone that you know the prime factorization of a 200-digit positive integer without telling them the prime factors. Or you may have a proof of an important theorem and you want to convince the mathematical community that you have such a proof without revealing it. In this section we will discuss methods, commonly known as *zero-knowledge* or *minimum-disclosure proofs,* that can be used to convince someone that you have certain private, verifiable information, without revealing it. Zero-knowledge proofs were invented in the mid-1980s.

In a zero-knowledge proof, there are two parties, the *prover,* the person who has the secret information, and the *verifier,* who wants to be convinced that the prover has this secret information. When a zero-knowledge proof is used, the probability is extremely small that someone who does not have the information can successfully cheat the verifier by masquerading as the prover. Moreover, the verifier learns nothing, or almost nothing, about the information other than that the prover possesses it. In particular, the verifier cannot convince a third party that the verifier knows this information.

Remark: Because zero-knowledge proofs supply the verifier with a small amount of information, zero-knowledge proofs are more properly called *minimum-disclosure proofs.* Nevertheless, we will use the original terminology for such proofs.

We will illustrate the use of zero-knowledge proofs by describing several examples of such proofs, each based on the ease of finding square roots modulo products of two primes compared with the difficulty of finding square roots when the two primes are not known. (See Section 11.1 for a discussion of this topic.)

Our first example presents a proposed scheme for a zero-knowledge proof that turned out to have a flaw making it unsuitable for this use. Nevertheless, we introduce this scheme as our first example because it illustrates the concept of zero-knowledge proofs and is relatively simple. Moreover, understanding why it fails to be a valid scheme for zero-knowledge proofs adds valuable insight (see Exercise 11). In this scheme Paula, the *prover*, attempts to convince Vince, the *verifier*, that she knows the prime factors of n, where n is the product of two large primes p and q, without helping him find these two prime factors.

When this scheme was originally devised, it was thought that someone who does not know p and q would be unable to find the square root of y modulo n in a reasonable

amount of time, unlike Paula who knows these primes. This turns out not to be the case, as Exercise 11 illustrates.

The proposed scheme is based on iterating the following procedure.

(i) Vince, who knows n, but not p and q, chooses an integer x at random. He computes y, the least nonnegative residue of x^4 modulo n and sends this to Paula.

(ii) When Paula receives y, she computes its square root modulo n. (We will explain how she can do this after describing the steps of the procedure.) This square root is the least positive residue of x^2 modulo n. She sends this integer to Vince.

(iii) Vince checks Paula's answer by finding the remainder of x^2 when it is divided by n.

To see why Paula can find the least positive residue of x^2 modulo n in step (ii), note that because she knows p and q, she can easily find the four square roots of x^4 modulo n. Next, note that only one of the four square roots of x^4 modulo n is a quadratic residue modulo n (see Exercise 3). So, to find x^2, she can select the correct square root of the four square roots of x^4 modulo n by computing the value of the Legendre symbols of each of these square roots modulo p and modulo q. Note that someone who does not know p and q is unable to find the square root of y modulo n in a reasonable amount of time, unlike Paula, who knows these primes.

We illustrate this procedure in the following example.

Example 11.19. Suppose that Paula's private information is her factorization of $n = 103 \cdot 239 = 24{,}617$. She can use the procedure just described to convince Vince that she knows the primes $p = 103$ and $q = 239$ without revealing them to him. (In practice, primes p and q with hundreds of digits would be used, rather than the small primes used in this example.)

To illustrate the procedure, suppose that in step (i) Vince selects the integer 9134 at random. He computes the least positive residue of 9134^4 modulo 24,617, which equals 20,682. He sends the integer 20,682 to Paula.

In step (ii), Paula determines the integer x^2 using the congruences

$$x^2 \equiv \pm 20{,}682^{(103+1)/4} = \pm 20{,}682^{26} \equiv \pm 59 \pmod{103}$$
$$x^2 \equiv \pm 20{,}682^{(239+1)/4} = \pm 20{,}682^{60} \equiv \pm 75 \pmod{239}.$$

(Note that we have used the fact that when $p \equiv q \equiv 3 \pmod 4$, the solutions of $x^2 \equiv a \pmod p$ and $x^2 \equiv a \pmod q$ are $x^2 \equiv \pm a^{(p+1)/4} \pmod p$ and $x^2 \equiv \pm a^{(q+1)/4} \pmod q$, respectively.)

Because x^2 is a quadratic residue modulo $24{,}627 = 103 \cdot 239$, we know that it also is a quadratic residue modulo 103 and 239. Computing Legendre symbols, we find that $\left(\frac{59}{103}\right) = 1$, $\left(\frac{-59}{103}\right) = -1$, $\left(\frac{75}{239}\right) = 1$, and $\left(\frac{-75}{239}\right) = -1$. Therefore, Paula finds x^2 by solving the system $x^2 \equiv 59 \pmod{103}$ and $x^2 \equiv 75 \pmod{239}$. When she solves this system, she concludes that $x^2 \equiv 2943 \pmod{24{,}617}$.

In step (iii), Vince checks Paula's answer by noting that $x^2 = 9134^2 \equiv 2943 \pmod{24{,}617}$. ◀

We now describe a method to verify the identity of the prover, based on zero-knowledge techniques, invented by Shamir in 1985. We again suppose that $n = pq$, where p and q are two large primes both congruent to 3 modulo 4. Let I be a positive integer that represents some particular information, such as a personal identification number. The prover selects a small positive integer c, which has the property that the integer v obtained by concatenating I with c (the number obtained by writing the digits of I followed by the digits of c) is a quadratic residue modulo n. (The number c can be found by trial and error, with probability close to 1/2.) The prover can easily find u, a square root of v modulo n.

The prover convinces the verifier that she knows the primes p and q using an interactive proof. Each cycle of the proof is based on the following steps.

(i) The prover, Paula, chooses a random number r, and sends to the verifier a message containing two values: x, where $x \equiv r^2 \pmod{n}$, $0 \leq x < n$, and y, where $y \equiv v\overline{x} \pmod{n}$, $0 \leq y < n$. Here, as usual, $\overline{x}$ is an inverse of x modulo n.

(ii) The verifier, Vince, checks that $xy \equiv v \pmod{n}$ and chooses, at random, a bit b, which he sends to the prover.

(iii) If the bit b sent by Vince is 0, Paula sends r to Vince. Otherwise, if the bit b is 1, Paula sends the least positive residue of $u\,\overline{r}$ modulo n, where $\overline{r}$ is an inverse of r modulo n.

(iv) Vince computes the square of what Paula has sent. If Vince sent a 0, he checks that this square is x, that is, that $r^2 \equiv x \pmod{n}$. If he sent a 1, he checks that this square is y, that is, that $s^2 \equiv y \pmod{n}$.

This procedure is also based on the fact that the prover can find u, a square root of v modulo n, whereas someone who does not know p and q will not be able to compute a square root modulo n in a reasonable amount of time.

The four steps of this procedure form one cycle. Cycles can be repeated sufficiently often to guarantee a high degree of security, as we will subsequently describe.

We illustrate this type of zero-knowledge proof with the following example.

Example 11.20. Suppose Paula wants to verify her identity to Vince by convincing him that she knows the prime factors of $n = 31 \cdot 61 = 1891$. Her identification number is $I = 391$. Note that 391 is a quadratic residue of 1891 because, as the reader can verify, it is a quadratic residue of both 31 and 61, so she can take $v = 391$ (that is, in this case, she does not have to concatenate an integer c with I). Paula finds that $u = 239$ is a square root of 391 modulo 1891. She can easily perform this calculation, because she knows the primes 31 and 61. (Note that we have selected small primes p and q in this example to illustrate the procedure. In practice, primes with hundreds of digits should be used.)

We illustrate one cycle of this procedure. In step (i), Paula chooses a random number, say $r = 998$. She sends Vince two numbers, $x \equiv r^2 \equiv 998^2 \equiv 1338 \pmod{1891}$ and $y \equiv v\,\overline{x} \equiv 391 \cdot 1296 \equiv 1839 \pmod{1891}$.

In step (ii), Vince checks that $xy \equiv 1338 \cdot 1839 \equiv 391 \pmod{1891}$ and chooses, at random, a bit b, say $b = 1$, which he sends to Paula.

In step (iii), Paula sends $s \equiv u\,\overline{r} = 239 \cdot 1855 \equiv 851 \pmod{1891}$ to Vince. Finally, in step (iv), Vince checks that $s^2 \equiv 851^2 \equiv 1839 \equiv y \pmod{1891}$. ◀

Note that if the prover sends the verifier both r and s, the verifier will know the private information $u = rs$, which is the secret information held by the prover. By passing the test with sufficiently many cycles, the prover has shown that she can produce either r or s on request. It follows that she must know u because, in each cycle, she knows both r and s. The choice of the random bit by the verifier makes it impossible for someone to fix the procedure by using numbers that have been rigged to pass the test. For example, someone could compute the square of a known number r and send $x = r^2$, instead of choosing a random number. Similarly, someone could select a number x such that $v\overline{x}$ is a known square. However, it is impossible to do precalculations to make both x and y the squares of known numbers without knowing u.

Because the bit chosen by the verifier is chosen at random, the probability that it will be a 0 is 1/2, as is the probability that it will be a 1. If someone does not know u, the square root of v, the probability that they will pass one iteration of this test is almost exactly 1/2. Consequently, the probability that someone masquerading as the prover will pass the test with 30 cycles is approximately $1/2^{30}$, which is less than one in a billion.

A variation of this procedure, known as the Fiat-Shamir method, is the basis for verification procedures used by smart cards, such as for verifying personal identification numbers.

Next, we describe a method that can be used to prove, using a zero-knowledge proof, that someone has certain information. Suppose that the prover, Paula, has information represented by a sequence of numbers $v_1, v_2, \ldots, v_m$, where $1 \leq v_j < n$ for $j = 1, 2, \ldots, m$. Here, as before, n is the product of two primes p and q that are both congruent to 3 modulo 4. Paula makes public the sequence of integers $s_1, s_2, \ldots, s_m$, where $s_j \equiv \overline{v}_j^2 \pmod{n}$, $1 \leq s_j < n$. Paula wants to convince the verifier, Vince, that she knows the private information $v_1, v_2, \ldots, v_m$, without revealing this information to Vince. What Vince knows is her public moduli n and her public information $s_1, s_2, \ldots, s_m$.

The following procedure can be used to convince Vince she has this information. Each cycle of the procedure has the following steps.

(i) Paula chooses a random number r and computes $x = r^2$, which she sends to Vince.

(ii) Vince selects a subset S of the set $\{1, 2, \ldots, m\}$ and sends this subset to Paula.

(iii) Paula computes y, the least positive residue modulo n of the product of r and the integers v_j, with j in S, that is, $y \equiv r \prod_{j \in S} v_j \pmod{n}$, $0 \leq y < n$.

(iv) Vince verifies that $x \equiv y^2 z \pmod{n}$, where z is the product of the integers c_j, with j in S, that is, $z \equiv \prod_{j \in S} s_j \pmod{n}$, $0 \leq z < n$.

Note that the congruence in step (iv) holds, because

$$\begin{aligned} y^2 z &\equiv r^2 \prod_{j \in S} v_j^2 \prod_{j \in S} s_j \\ &\equiv r^2 \prod_{j \in S} v_j^2 \overline{v}_j^2 \\ &\equiv r^2 \pmod{n}. \end{aligned}$$

The random number r is used so that the verifier cannot determine the value of the integer v_j, part of the secret information, by selecting the set $S = \{j\}$. When this procedure is carried out, the verifier is given no new information that will help him determine the private information $c_1, \ldots, c_m$.

We illustrate one cycle of this interactive zero-knowledge proof in the following example.

Example 11.21. Suppose that Paula wants to convince Vince that she has secret information, which is represented by the integers $v_1 = 1144$, $v_2 = 877$, $v_3 = 2001$, $v_4 = 1221$, $v_5 = 101$. Her secret modulus is $n = 47 \cdot 53 = 2491$. (In practice, primes with hundreds of digits are used rather than the small primes used in this example.)

Her public information consists of the integers s_j, with $s_j \equiv \overline{v}_j^2 \pmod{2491}$, $0 < s_j < 2491$, $j = 1, 2, 3, 4, 5$. It follows, after routine calculation, that her public information consists of the integers $s_1 = 197$, $s_2 = 2453$, $s_3 = 1553$, $s_4 = 941$, and $s_5 = 494$.

Paula can convince Vince that she has the secret information using the procedure described in the text. We describe one cycle of the procedure. In step (i), Paula chooses a random number, say $r = 1253$. Next, she sends $x = 679$, the least positive residue of r^2 modulo 2491, to Vince.

In step (ii), Vince selects a subset of $\{1, 2, 3, 4, 5\}$, say $s = \{1, 3, 4, 5\}$, and informs Paula of this choice.

In step (iii), Paula computes the number y, with $0 \leq y < 2491$ and

$$\begin{aligned} y &\equiv r v_1 v_3 v_4 v_5 \\ &\equiv 1253 \cdot 1144 \cdot 2001 \cdot 1221 \cdot 101 \\ &\equiv 68 \pmod{2491}. \end{aligned}$$

Consequently, she sends $y = 68$ to Vince.

Finally, in step (iv), Vince confirms that $x \equiv y^2 s_1 s_3 s_4 s_5 \pmod{2491}$ by verifying that $x = 679 \equiv 68^2 \cdot 197 \cdot 1553 \cdot 941 \cdot 494 \pmod{2491}$.

Vince can ask Paula to run through more cycles of this procedure to verify that she does have the secret information. He stops when he feels that the probability that she is cheating is small enough to satisfy his needs. ◀

How can the prover cheat in this interactive procedure for zero-knowledge proofs of information? That is, how can the prover fool the verifier into thinking that she really knows the private information $c_1, \ldots, c_m$ when she does not? The only obvious way is for the prover to guess the set S before the verifier supplies this; in step (1), to take $x = r^2 \prod_{j \in S} v_j^2$; and in step (iii), to take $y = 4$. Because there are 2^m possible sets S (as there are that many subsets of $\{1, 2, \ldots, m\}$), the probability that someone not knowing the private information fools the verifier using this technique is $1/2^m$. Furthermore, when this cycle is iterated T times, the probability decreases to $1/2^{mT}$. For instance, if $m = 10$ and $T = 3$, the probability of the verifier being fooled is less than one in a billion.

In this section, we have only briefly touched upon zero-knowledge proofs. The reader interested in learning more about this subject should refer to the chapter by Goldwasser in [Po90], as well as to the reference supplied in that chapter.

11.5 Exercises

1. Suppose that $n = 3149 = 47 \cdot 67$ and that $x^4 \equiv 2070 \pmod{3149}$. Find the least nonnegative residue of x^2 modulo 3149.
2. Suppose that $n = 11{,}021 = 103 \cdot 107$ and that $x^4 \equiv 1686 \pmod{11{,}021}$. Find the least nonnegative residue of x^2 modulo 11,021.
3. Suppose that $n = pq$, where p and q are primes both congruent to 3 modulo 4, and that x is an integer relatively prime to n. Show that of the four square roots of x^4 modulo n, only one is the least nonnegative residue of a square of an integer.
4. Suppose that Paula has identification number 1760 and modulus $1961 = 37 \cdot 53$. Show how she verifies her identity to Vince in one cycle of the Shamir procedure, if she selects the random number 1101 and he chooses 1 as his random bit.
5. Suppose that Paula has identification number 7 and modulus $1411 = 17 \cdot 83$. Show how she verifies her identify to Vince in one cycle of the Shamir procedure, if she selects the random number 822 and he chooses 1 as his random bit.
6. Run through the steps used to verify that the prover has the secret information in Example 11.21, when the random number $r = 888$ is selected by the prover in step (i) and the verifier selects the subset $\{2, 3, 5\}$ of $\{1, 2, 3, 4, 5\}$.
7. Run through the steps used to verify that the prover has the secret information in Example 11.21, when the random number $r = 1403$ is selected by the prover in step (i) and the verifier selects the subset $\{1, 5\}$ of $\{1, 2, 3, 4, 5\}$.
8. Let $n = 2491 = 47 \cdot 53$. Suppose that Paula's identification information consists of the sequence of six numbers $v_1 = 881$, $v_2 = 1199$, $v_3 = 2144$, $v_4 = 110$, $v_5 = 557$, and $v_6 = 2200$.
   a) Find Paula's public identification information, $s_1, s_2, s_3, s_4, s_5, s_6$.
   b) Suppose that Paula selects at random the number $r = 1091$, and Vince chooses the subset $S = 2, 3, 5, 6$ and sends this to Paula. Find the number that Paula computes and sends back to Vince.
   c) What computation does Vince make to verify Paula's knowledge of her secret information?

9. Let $n = 3953 = 59 \cdot 67$. Suppose that Paula's identification information consists of the sequence of six numbers $v_1 = 1001$, $v_2 = 21$, $v_3 = 3097$, $v_4 = 989$, $v_5 = 157$, and $v_6 = 1039$.
   a) Find Paula's public identification information $s_1, s_2, s_3, s_4, s_5, s_6$.
   b) Suppose that Paula selects at random the number $r = 403$, and Vince chooses the subset $S = \{1, 2, 4, 6\}$ and sends this to Paula. Find the number that Paula computes and sends back to Vince.
   c) What computation does Vince make to verify Paula's knowledge of her secret information?

10. Suppose that $n = pq$, where p and q are large odd primes and that you are able to efficiently extract square roots modulo n without knowing p and q. Show that you can, with probability close to 1, find the prime factors p and q. (*Hint:* Base your algorithm on the following procedure. Select an integer x. Exract a square root of the least nonnegative residue of x^2 modulo n. You will need to show that there is a 1/2 chance that you found a square root not congruent to $\pm x$ modulo n.)

11. In this exercise, we expose a flaw in the proposed scheme of a zero-knowledge proof presented prior to Example 11.19. Suppose that Vince randomly chooses integers w until he finds a value of w for which the Jacobi symbol $\left(\frac{w}{n}\right)$ equals -1 and that he sends Paula z, the least nonnegative residue of w^2 modulo n. Show that Vince can factor n once Paula sends back the square root of z that she computes.

11.5 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Give one of your classmates the integer n, where $n = pq$ and p and q are primes with more than 50 decimal digits, both congruent to 3 modulo 4. Convince your classmate that you know both p and q using a zero-knowledge proof.

2. Convince one of your classmates that you know a secret in the form of a sequence of 10 positive integers each less than 10,000, using the zero-knowledge proof described in the text.

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Given n, the product of two distinct primes both congruent to 3 modulo 4, and the least positive residue of x^4 modulo n, where x is an integer relatively prime to n, find the least positive residue of x^2 modulo n.

12

Decimal Fractions and Continued Fractions

Introduction

In this chapter, we will discuss the representation of rational and irrational numbers as decimal fractions and continued fractions. We will show that every rational number can be expressed as a terminating or periodic decimal fraction, and provide some results that tell us the length of the period of the decimal fraction of a rational number. We will also construct irrational numbers using decimal fractions, and show how decimal fractions can be used to express a transcendental number and to demonstrate that the set of real numbers is uncountable.

Continued fractions provide a useful way of expressing numbers. We will show that every rational number has a finite continued fraction; that every irrational number has an infinite continued fraction and that continued fractions are the best rational approximations to numbers. We will establish a key result that will tell us that the set of quadratic irrationals can be characterized as the set of numbers with periodic continued fractions. Finally, we will show how continued fractions can be used to help factor integers.

12.1 Decimal Fractions

In this section, we discuss the representation of rational and irrational numbers as decimal fractions. We first consider base b expansions of real numbers, where b is a positive integer, $b > 1$. Let α be a positive real number, and let $a = [\alpha]$ be the integer part of α, so that $\gamma = \alpha - [\alpha]$ is the fractional part of α and $\alpha = a + \gamma$ with $0 \leq \gamma < 1$. By Theorem 2.1, the integer a has a unique base b expansion. We now show that the fractional part γ also has a unique base b expansion.

Theorem 12.1. Let γ be a real number with $0 \le \gamma < 1$, and let b be a positive integer, $b > 1$. Then γ can be uniquely written as

$$\gamma = \sum_{j=1}^{\infty} c_j / b^j,$$

where the coefficients c_j are integers with $0 \le c_j \le b - 1$ for $j = 1, 2, \ldots$, with the restriction that for every positive integer N there is an integer n with $n \ge N$ and $c_n \ne b - 1$.

In the proof of Theorem 12.1, we deal with infinite series. We will use the following formula for the sum of the terms of an infinite geometric series.

Theorem 12.2. Let a and r be real numbers with $|r| < 1$. Then

$$\sum_{j=0}^{\infty} ar^j = a/(1-r).$$

Most books on calculus or mathematical analysis contain a proof of Theorem 12.2 (see [Ru64], for instance).

We can now prove Theorem 12.1.

Proof. We first let

$$c_1 = [b\gamma],$$

so that $0 \le c_1 \le b - 1$, because $0 \le b\gamma < b$. In addition, let

$$\gamma_1 = b\gamma - c_1 = b\gamma - [b\gamma],$$

so that $0 \le \gamma_1 < 1$ and

$$\gamma = \frac{c_1}{b} + \frac{\gamma_1}{b}.$$

We recursively define c_k and γ_k for $k = 2, 3, \ldots$, by

$$c_k = [b\gamma_{k-1}]$$

and

$$\gamma_k = b\gamma_{k-1} - c_k$$

so that $0 \le c_k \le b - 1$, because $0 \le b\gamma_{k-1} < b$ and $0 \le \gamma_k < 1$. Then, it follows that

$$\gamma = \frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_n}{b^n} + \frac{\gamma_n}{b^n}.$$

Because $0 \le \gamma_n < 1$, we see that $0 \le \gamma_n / b^n < 1/b^n$. Consequently,

$$\lim_{n \to \infty} \gamma_n / b^n = 0.$$

Therefore, we can conclude that

$$\gamma = \lim_{n\to\infty}\left(\frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_n}{b_n}\right)$$
$$= \sum_{j=1}^{\infty} c_j/b^j.$$

To show that this expansion is unique, assume that

$$\gamma = \sum_{j=1}^{\infty} c_j/b^j = \sum_{j=1}^{\infty} d_j/b^j,$$

where $0 \le c_j \le b-1$ and $0 \le d_j \le b-1$ and, for every positive integer N, there are integers n and m with $c_n \ne b-1$ and $d_m \ne b-1$. Assume that k is the smallest index for which $c_k \ne d_k$, and assume that $c_k > d_k$ (the case $c_k < d_k$ is handled by switching the roles of the two expansions). Then

$$0 = \sum_{j=1}^{\infty}(c_j - d_j)/b^j = (c_k - d_k)/b^k + \sum_{j=k+1}^{\infty}(d_j - c_j)/b^j,$$

so that

$$(c_k - d_k)/b^k = \sum_{j=k+1}^{\infty}(d_j - c_j)/b^j. \tag{12.1}$$

Because $c_k > d_k$, we have

$$(c_k - d_k)/b^k \ge 1/b^k, \tag{12.2}$$

whereas

$$\sum_{j=k+1}^{\infty}(d_j - c_j)/b^j \le \sum_{j=k+1}^{\infty}(b-1)/b^j \tag{12.3}$$
$$= (b-1)\frac{1/b^{k+1}}{1-1/b}$$
$$= 1/b^k,$$

where we have used Theorem 12.2 to evaluate the sum on the right-hand side of the inequality. Note that equality holds in (12.3) if and only if $d_j - c_j = b-1$ for all j with $j \ge k+1$, and this occurs if and only if $d_j = b-1$ and $c_j = 0$ for $j \ge k+1$. However, such an instance is excluded by the hypotheses of the theorem. Hence, the inequality in (12.3) is strict, and therefore (12.2) and (12.3) contradict (12.1). This shows that the base b expansion of α is unique. ∎

The unique expansion of a real number in the form $\sum_{j=1}^{\infty} c_j/b^j$ is called the *base b expansion* of this number and is denoted by $(.c_1c_2c_3\ldots)_b$.

To find the base b expansion $(.c_1c_2c_3\ldots)_b$ of a real number γ, we can use the recursive formula for the digits given in the proof of Theorem 12.1, namely

$$c_k = [b\gamma_{k-1}], \quad \gamma_k = b\gamma_{k-1} - [b\gamma_{k-1}],$$

where $\gamma_0 = \gamma$, for $k = 1, 2, 3, \ldots$. (Note that there is also an explicit formula for these digits—see Exercise 21.)

Example 12.1. Let $(.c_1c_2c_3\ldots)_b$ be the base 8 expansion of 1/6. Then

$$c_1 = \left[8 \cdot \frac{1}{6}\right] = 1, \quad \gamma_1 = 8 \cdot \frac{1}{6} - 1 = \frac{1}{3},$$
$$c_2 = \left[8 \cdot \frac{1}{3}\right] = 2, \quad \gamma_2 = 8 \cdot \frac{1}{3} - 2 = \frac{2}{3},$$
$$c_3 = \left[8 \cdot \frac{2}{3}\right] = 5, \quad \gamma_3 = 8 \cdot \frac{2}{3} - 5 = \frac{1}{3},$$
$$c_4 = \left[8 \cdot \frac{1}{3}\right] = 2, \quad \gamma_4 = 8 \cdot \frac{1}{3} - 2 = \frac{2}{3},$$
$$c_5 = \left[8 \cdot \frac{2}{3}\right] = 5, \quad \gamma_5 = 8 \cdot \frac{2}{3} - 5 = \frac{1}{3},$$

and so on. We see that the expansion repeats; hence,

$$1/6 = (.1252525\ldots)_8. \quad \blacktriangleleft$$

We will now discuss base b expansions of rational numbers. We will show that a number is rational if and only if its base b expansion is periodic or terminates.

Definition. A base b expansion $(.c_1c_2c_3\ldots)_b$ is said to *terminate* if there is a positive integer n such that $c_n = c_{n+1} = c_{n+2} = \cdots = 0$.

Example 12.2. The decimal expansion of 1/8, $(.125000\ldots)_{10} = (.125)_{10}$, terminates. Also, the base 6 expansion of 4/9, $(.24000\ldots)_6 = (.24)_6$, terminates. $\blacktriangleleft$

To describe those real numbers with terminating base b expansion, we prove the following theorem.

Theorem 12.3. The real number α, $0 \le \alpha < 1$, has a terminating base b expansion if and only if α is rational and can be written as $\alpha = r/s$, where $0 \le r < s$ and every prime factor of s also divides b.

Proof. First, suppose that α has a terminating base b expansion,

$$\alpha = (.c_1c_2\ldots c_n)_b.$$

Then

$$\alpha = \frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_n}{b^n}$$
$$= \frac{c_1 b^{n-1} + c_2 b^{n-2} + \cdots + c_n}{b^n},$$

so that α is rational, and can be written with a denominator divisible only by primes dividing b.

Conversely, suppose that $0 \leq \alpha < 1$, and

$$\alpha = r/s,$$

where each prime dividing s also divides b. Hence, there is a power of b, say b^N, that is divisible by s (for instance, take N to be the largest exponent in the prime-power factorization of s). Then

$$b^N \alpha = b^N r/s = ar,$$

where $sa = b^N$, and a is a positive integer because $s | b^N$. Now let $(a_m a_{m-1} \ldots a_1 a_0)_b$ be the base b expansion of ar. Then

$$\alpha = ar/b^N = \frac{a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0}{b^N}$$
$$= a_m b^{m-N} + a_{m-1} b^{m-1-N} + \cdots + a_1 b^{1-N} + a_0 b^{-N}$$
$$= (.00 \ldots a_m a_{m-1} \ldots a_1 a_0)_b.$$

Hence, α has a terminating base b expansion. ■

Note that every terminating base b expansion can be written as a nonterminating base b expansion with a tail-end consisting entirely of the digit $b - 1$, because $(.c_1 c_2 \ldots c_m)_b = (.c_1 c_2 \ldots c_m - 1 \quad b - 1 \quad b - 1 \ldots)_b$. For instance, $(.12)_{10} = (.11999 \ldots)_{10}$. This is why we require in Theorem 12.1 that for every integer N there is an integer n such that $n > N$ and $c_n \neq b - 1$; without this restriction, base b expansions would not be unique.

A base b expansion that does not terminate may be *periodic*, for instance,

$$1/3 = (.333 \ldots)_{10},$$
$$1/6 = (.1666 \ldots)_{10},$$

and

$$1/7 = (.142857142857142857 \ldots)_{10}.$$

Definition. A base b expansion $(.c_1 c_2 c_3 \ldots)_b$ is called *periodic* if there are positive integers N and k such that $c_{n+k} = c_n$ for $n \geq N$.

We denote by $(.c_1c_2\ldots c_{N-1}\overline{c_N\cdots c_{N+k-1}})_b$ the periodic base b expansion $(.c_1c_2\ldots c_{N-1}c_N\ldots c_{N+k-1}c_N\ldots c_{N+k-1}c_N\ldots)_b$. For instance, we have

$$1/3 = (.\overline{3})_{10},$$

$$1/6 = (.1\overline{6})_{10},$$

and

$$1/7 = (.\overline{142857})_{10}.$$

Note that the periodic parts of the decimal expansions of 1/3 and 1/7 begin immediately, whereas in the decimal expansion of 1/6 the digit 1 precedes the periodic part of the expansion. We call the part of a periodic base b expansion preceding the periodic part the *pre-period,* and the periodic part the *period,* where we take the period to have minimal possible length.

Example 12.3. The base 3 expansion of 2/45 is $(.00\overline{1012})_3$. The pre-period is $(00)_3$ and the period is $(1012)_3$.

The next theorem tells us that the rational numbers are those real numbers with periodic or terminating base b expansions. Moreover, the theorem gives the lengths of the pre-period and periods of base b expansions of rational numbers.

Theorem 12.4. Let b be a positive integer. Then a periodic base b expansion represents a rational number. Conversely, the base b expansion of a rational number either terminates or is periodic. Further, if $0 < \alpha < 1, \alpha = r/s$, where r and s are relatively prime positive integers, and $s = TU$, where every prime factor of T divides b and $(U, b) = 1$, then the period length of the base b expansion of α is $\mathrm{ord}_U b$, and the pre-period length is N, where N is the smallest positive integer such that $T|b^N$.

Proof. First, suppose that the base b expansion of α is periodic, so that

$$\begin{aligned}\alpha &= (.c_1c_2\ldots c_N\overline{c_{N+1}\cdots c_{N+k}})_b \\ &= \frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_N}{b^N} + \left(\sum_{j=0}^{\infty}\frac{1}{b^{jk}}\right)\left(\frac{c_{N+1}}{b^{N+1}} + \cdots + \frac{c_{N+K}}{b^{N+k}}\right) \\ &= \frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_N}{b^N} + \left(\frac{b^k}{b^k-1}\right)\left(\frac{c_{N+1}}{b^{N+1}} + \cdots + \frac{c_{N+K}}{b^{N+k}}\right),\end{aligned}$$

where we have used Theorem 12.2 to see that

$$\sum_{j=0}^{\infty}\frac{1}{b^{jk}} = \frac{1}{1-\frac{1}{b^k}} = \frac{b^k}{b^k-1}.$$

Because α is the sum of rational numbers, it is rational.

Conversely, suppose that $0 < \alpha < 1, \alpha = r/s$, where r and s are relatively prime positive integers, $s = TU$, where every prime factor of T divides b, $(U, b) = 1$, and N is the smallest integer such that $T|b^N$.

Because $T|b^N$, we have $aT = b^N$, where a is a positive integer. Hence,

$$b^N\alpha = b^N \frac{r}{TU} = \frac{ar}{U}. \tag{12.4}$$

Furthermore, we can write

$$\frac{ar}{U} = A + \frac{C}{U}, \tag{12.5}$$

where A and C are integers with

$$0 \le A < b^N, \quad 0 < C < U,$$

and $(C, U) = 1$. (The inequality for A follows because $0 < b^N\alpha = \frac{ar}{U} < b^N$, which results from the inequality $0 < \alpha < 1$ when both sides are multiplied by b^N). The fact that $(C, U) = 1$ follows easily from the condition $(r, s) = 1$. By Theorem 12.1, A has a base b expansion $A = (a_n a_{n-1} \ldots a_1 a_0)_b$.

If $U = 1$, then the base b expansion of α terminates as shown. Otherwise let $v = \text{ord}_U b$. Then,

$$b^v \frac{C}{U} = \frac{(tU + 1)C}{U} = tC + \frac{C}{U}, \tag{12.6}$$

where t is an integer, because $b^v \equiv 1 \pmod{U}$. However, we also have

$$b^v \frac{C}{U} = b^v \left(\frac{c_1}{b} + \frac{c_2}{b^2} + \cdots + \frac{c_v}{b^v} + \frac{\gamma_v}{b^v} \right), \tag{12.7}$$

where $(.c_1c_2c_3\ldots)_b$ is the base b expansion of $\frac{C}{U}$, so that

$$c_k = [b\gamma_{k-1}], \quad \gamma_k = b\gamma_{k-1} - [b\gamma_{k-1}],$$

where $\gamma_0 = \frac{C}{U}$, for $k = 1, 2, 3, \ldots$. From (12.7), we see that

$$b^v \frac{C}{U} = \left(c_1 b^{v-1} + c_2 b^{v-2} + \cdots + c_v \right) + \gamma_v. \tag{12.8}$$

Equating the fractional parts of (12.6) and (12.8), noting that $0 \le \gamma_v < 1$, we find that

$$\gamma_v = \frac{C}{U}.$$

Consequently, we see that

$$\gamma_v = \gamma_0 = \frac{C}{U},$$

so that from the recursive definition of $c_1, c_2, \ldots$ we can conclude that $c_{k+v} = c_k$ for $k = 1, 2, 3, \ldots$. Hence, $\frac{C}{U}$ has a periodic base b expansion

$$\frac{C}{U} = (.\overline{c_1 c_2 \ldots c_v})_b.$$

Combining (12.4) and (10.5), and inserting the base b expansions of A and $\frac{C}{U}$, we have

$$b^N \alpha = (a_n a_{n-1} \ldots a_1 a_0 .\overline{c_1 c_2 \ldots c_v})_b. \tag{12.9}$$

Dividing both sides of (12.9) by b^N, we obtain

$$\alpha = (.00 \ldots a_n a_{n-1} \ldots a_1 a_0 \overline{c_1 c_2 \ldots c_v})_b,$$

(where we have shifted the decimal point in the base b expansion of $b^N\alpha$ N spaces to the left to obtain the base b expansion of α). In this base b expansion of α, the pre-period $(.00 \ldots a_n a_{n-1} \ldots a_1 a_0)_b$ is of length N, beginning with $N - (n+1)$ zeros, and the period length is v.

We have shown that there is a base b expansion of α with a pre-period of length N and a period of length v. To finish the proof, we must show that we cannot regroup the base b expansion of α, so that either the pre-period has length less than N, or the period has length less than v. To do this, suppose that

$$\begin{aligned}\alpha &= (.c_1 c_2 \ldots c_M \overline{c_{M+1} \ldots c_{M+k}})_b \\ &= \frac{c_1}{b} + \frac{c_2}{b_2} + \cdots + \frac{c_M}{b^M} + \left(\frac{b^k}{b^k - 1}\right)\left(\frac{c_{M+1}}{b^{M+1}} + \cdots + \frac{c_{M+k}}{b^{M+k}}\right) \\ &= \frac{(c_1 b^{M-1} + c_2 b^{M-2} + \cdots + c_M)(b^k - 1) + (c_{M+1} b^{k-1} + \cdots + c_{M+k})}{b^M (b^k - 1)}.\end{aligned}$$

Because $\alpha = r/s$, with $(r, s) = 1$, we see that $s | b^M (b^k - 1)$. Consequently, $T | b^M$ and $U | (b^k - 1)$. Hence, $M \geq N$, and $v | k$ (by Theorem 9.1, because $b^k \equiv 1 \pmod{U}$ and $v = \operatorname{ord}_U b$). Therefore, the pre-period length cannot be less than N and the period length cannot be less than v. ∎

We can use Theorem 12.4 to determine the lengths of the pre-period and period of decimal expansions. Let $\alpha = r/s$, $0 < \alpha < 1$, and $s = 2^{s_1} 5^{s_2} t$, where $(t, 10) = 1$. Then, by Theorem 12.4, the pre-period has length $\max(s_1, s_2)$ and the period has length $\operatorname{ord}_t 10$.

Example 12.4. Let $\alpha = 5/28$. Because $28 = 2^2 \cdot 7$, Theorem 12.4 tells us that the pre-period has length two and the period has length $\operatorname{ord}_7 10 = 6$. As $5/28 = (.17\overline{857142})$, we see that these lengths are correct. ◀

Note that the pre-period and period lengths of a rational number r/s, in lowest terms, depend only on the denominator s, and not on the numerator r.

We observe that by Theorem 12.4 a base b expansion that is not terminating and is not periodic represents an irrational number.

Example 12.5. The number with decimal expansion

$$\alpha = .10100100010000 \ldots,$$

consisting of a one followed by a zero, a one followed by two zeros, a one followed by three zeroes, and so on, is irrational because this decimal expansion does not terminate and is not periodic. ◀

The number α in the preceding example is concocted so that its decimal expansion is clearly not periodic. To show that naturally occurring numbers such as e and π are irrational, we cannot use Theorem 12.4, because we do not have explicit formulas for the decimal digits of these numbers. No matter how many decimal digits of their expansions we compute, we still cannot conclude that they are irrational from this evidence, because the period could be longer than the number of digits that we have computed.

Transcendental Numbers

The French mathematician Liouville was the first person to show that a particular number is transcendental. (Recall from Section 1.1 that a transcendental number is one that is not the root of a polynomial with integer coefficients.) The number that Liouville showed is transcendental is the number

$$\alpha = \sum_{i=1}^{\infty} \frac{1}{10^{i!}} = 0.11000100000000000000000100\ldots.$$

This number has a 1 in the $n!$th place for each positive integer n and a 0 elsewhere. To show that this number is transcendental, Liouville proved the following theorem, which shows that algebraic numbers cannot be approximated very well by rational numbers. In particular, this theorem provides a lower bound for how well an algebraic number of degree n can be approximated by rational numbers. Note that an *algebraic number of degree n* is a real number that is a root of a polynomial of degree n with integer coefficients which is not a root of any polynomial with integer coefficients of degree less than n.

Theorem 12.5. If α is an algebraic number of degree n, where n is a positive integer greater than 1, then there exists a positive real number C such that

$$\left|\alpha - \frac{p}{q}\right| > C/q^n$$

for every rational number p/q, where $q > 0$.

Because the proof of Theorem 12.5, although not difficult, relies on calculus, we will not supply it here. We refer the reader to [HaWr79] for a proof. We will be content to use this theorem to show that Liouville's number is transcendental.

Corollary 12.5.1. The number $\alpha = \sum_{i=1}^{\infty} 1/10^{i!}$ is transcendental.

Proof. First, note that α is not rational, because its decimal expansion does not terminate and is not periodic. To see that it is not periodic, note that there are increasingly larger numbers of 0s between successive 1s in the expansion.

Let p_k/q_k denote the sum of the first k terms in the sum defining α. Note that $q_k = 10^{k!}$. Because $10^{i!} \geq 10^{(k+1)!}$ whenever $i \geq k+1$, we have

$$\left|\alpha - \frac{p_k}{q_k}\right| = \sum_{i=k+1}^{\infty} \frac{1}{10^{i!}} < \sum_{i=k+1}^{\infty} \frac{1}{(10^{(k+1)!})^i}.$$

Because

$$\sum_{i=k+1}^{\infty} \frac{1}{10^{(k+1)!i}} = \frac{1}{10^{(k+1)!} - 1} \leq \frac{2}{10^{(k+1)!}},$$

it follows that

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{2}{10^{(k+1)!}}.$$

It therefore follows that α cannot be algebraic, for if it were algebraic of degree n, then by Theorem 12.5 there would be a positive real number C such that $|\alpha - p_k/q_k| > C/q_k^n$. This is not the case, because we have seen that $|\alpha - p_k/q_k| < 2/q_k^{k+1}$, and taking k to be sufficiently larger than n produces a contradiction. ■

The notion of the decimal expansion of real numbers can be used to show that the set of real numbers is not *countable*. A *countable set* is one that can be put into a one-to-one correspondence with the set of positive integers. Equivalently, the elements of a countable set can be listed as the terms of a sequence. The element corresponding to the integer 1 is listed first, the element corresponding to the integer 2 is listed second, and so on. We will give the proof found by German mathematician *Georg Cantor*.

Theorem 12.6. The set of real numbers is an uncountable set.

Proof. We assume that the set of real numbers is countable. Then the subset of all real numbers between 0 and 1 would also be countable, as a subset of a countable set is also

GEORG CANTOR (1845–1918) was born in St. Petersburg, Russia, where his father was a successful merchant. When he was 11, his family moved to Germany to escape the harsh weather of Russia. Cantor developed his interest in mathematics while in German high schools. He attended university at Zurich and later at the University of Berlin, studying under the famous mathematicians Kummer, Weierstrass, and Kronecker. He received his doctorate in 1867 for work in number theory. Cantor took a position at the University of Halle in 1869, a position that he held until he retired in 1913.

Cantor is considered the founder of set theory; he is also noted for his contributions to mathematical analysis. Many mathematicians had extremely high regard for Cantor's work, such as Hilbert, who said that it was "the finest product of mathematical genius and one of the supreme achievements of purely intellectual human activity." Besides mathematics, Cantor was interested in philosophy, and wrote papers connecting his theory of sets and metaphysics.

Cantor was married in 1874 and had five children. He had a melancholy temperament that was balanced by his wife's happy disposition. He received a large inheritance from his father, but since he was poorly paid as a professor at Halle, he applied for a better-paying position at the University of Berlin. His appointment there was blocked by Kronecker, who did not agree with Cantor's views on set theory. Unfortunately, Cantor suffered from mental illness throughout the later years of his life; he died of a heart attack in 1918 in a psychiatric clinic.

countable (as the reader should verify). With this assumption, the set of real numbers between 0 and 1 can be listed as terms of a sequence $r_1, r_2, r_3, \ldots$. Suppose that the decimal expansions of these real numbers are

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\ldots$$
$$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\ldots$$
$$r_3 = 0.d_{31}d_{32}d_{33}d_{34}\ldots$$
$$r_4 = 0.d_{41}d_{42}d_{43}d_{44}\ldots$$

and so on. Now form a new real number r with the decimal expansion $0.d_1d_2d_3d_4\ldots$, where the decimal digits are determined by $d_i = 4$ if $d_{ii} \neq 4$ and $d_i = 5$ if $d_{ii} = 4$.

Because every real number has a unique decimal expansion (when the possibility that the expansion has a tail end that consists entirely of 9s is excluded), the real number r that we constructed is between 0 and 1 and is not equal to any of the real numbers $r_1, r_2, r_3, \ldots$, because the decimal is a real number r between 0 and 1 not in the list, the assumption that all real numbers between 0 and 1 could be listed is false. It follows that the set of real numbers between 0 and 1, and hence the set of all real numbers, is uncountable. ■

12.1 Exercises

1. Find the decimal expansion of each of the following numbers.

   a) 2/5 c) 12/13 e) 1/111
   b) 5/12 d) 8/15 f) 1/1001

2. Find the base 8 expansions of each of the following numbers.

   a) 1/3 c) 1/5 e) 1/12
   b) 1/4 d) 1/6 f) 1/22

3. Find the fraction, in lowest terms, represented by each of the following expansions.

   a) .12 b) $.1\overline{2}$ c) $.\overline{12}$

4. Find the fraction, in lowest terms, represented by each of the following expansions.

   a) $(.123)_7$ c) $(.\overline{17})_{11}$
   b) $(.0\overline{13})_6$ d) $(.\overline{ABC})_{16}$

5. For which positive integers b does the base b expansion of 11/210 terminate?

6. Find the pre-period and period lengths of the decimal expansion of each of the following rational numbers.

   a) 7/12 c) 1/75 e) 13/56
   b) 11/30 d) 10/23 f) 1/61

7. Find the pre-period and period lengths of the base 12 expansions of each of the following rational numbers.

   a) 1/4 c) 7/10 e) 17/132
   b) 1/8 d) 5/24 f) 7/360

8. Let b be a positive integer. Show that the period length of the base b expansion of $1/m$ is $m-1$ if and only if m is prime and b is a primitive root of m.

9. For which primes p does the decimal expansion of $1/p$ have period length equal to each of the following integers?

   a) 1 c) 3 e) 5
   b) 2 d) 4 f) 6

10. Find the base b expansion of each of the following numbers.

    a) $1/(b-1)$ b) $1/(b+1)$

11. Let b be an integer with $b > 2$. Show that the base b expansion of $1/(b-1)^2$ is $(.\overline{0123\ldots b-3\ b-1})_b$.

12. Show that the real number with base b expansion

$$(.0123\ldots b-1\,101112\ldots)_b,$$

constructed by successively listing the base b expansions of the integers, is irrational.

13. Show that

$$\frac{1}{b}+\frac{1}{b^4}+\frac{1}{b^9}+\frac{1}{b^{16}}+\frac{1}{b^{25}}+\cdots$$

is irrational, whenever b is a positive integer larger than one.

14. Let $b_1, b_2, b_3, \ldots$ be an infinite sequence of positive integers greater than one. Show that every real number can be represented as

$$c_0+\frac{c_1}{b_1}+\frac{c_2}{b_1b_2}+\frac{c_3}{b_1b_2b_3}+\cdots,$$

where $c_0, c_1, c_2, c_3, \ldots$ are integers such that $0 \le c_k < k$ for $k = 1, 2, 3, \ldots$.

15. Show that every real number has an expansion

$$c_0+\frac{c_1}{1!}+\frac{c_2}{2!}+\frac{c_3}{3!}+\cdots,$$

where $c_0, c_1, c_2, c_3, \ldots$ are integers and $0 \le c_k < k$ for $k = 1, 2, 3, \ldots$.

16. Show that every rational number has a terminating expansion of the type described in Exercise 15.

* 17. Suppose that p is a prime and the base b expansion of $1/p$ is $(.\overline{c_1c_2\ldots c_{p-1}})_b$, so that the period length of the base b expansion of $1/p$ is $p-1$. Show that if m is a positive integer with $1 \le m < p$, then

$$m/p = (.\overline{c_{k+1}\ldots c_{p-1}c_1c_2\ldots c_{k-1}c_k})_b,$$

where k is the least positive residue of $\mathrm{ind}_b m$ modulo p.

* 18. Show that if p is prime and $1/p = (.\overline{c_1c_2\ldots c_k})_b$ has an even period length, $k = 2t$, then $c_j + c_{j+t} = b-1$ for $j = 1, 2, \ldots, t$.

19. For which positive integers n is the length of the period of the binary expansion of $1/n$ equal to $n-1$?

20. For which positive integers n is the length of the period of the decimal expansion of $1/n$ equal to $n-1$?

21. Suppose that b is a positive integer. Show that the coefficients in the base b expansion of the real number $\gamma = \sum_{j=1}^{\infty} c_j/b^j$ with $0 \leq \gamma < 1$ are given by the formula $c_j = [\gamma b^j] - b[\gamma b^{j-1}]$ for $j = 1, 2, \ldots$. (*Hint:* First, show that $0 \leq [\gamma b^j] - b[\gamma b^{j-1}] \leq b - 1$. Then, show that $\sum_{j=1}^{N}([\gamma b^j] - b[\gamma b^{j-1}])/b^j = \gamma - (\gamma b^N [\gamma b^N]/b^N)$ and let $N \to \infty$.)

22. Use the formula in Exercise 21 to find the base 14 expansion of 1/6.

23. Show that the number
$$\sum_{i=1}^{\infty} (-1)^{a_i}/10^{i!}$$
is transcendental for all sequences of positive integers $a_1, a_2, \ldots$.

24. Is the set of all real numbers with decimal expansions consisting of only 0s and 1s countable?

* 25. Show that the number e is irrational.

26. Pseudorandom numbers can be generated using the base m expansion of $1/P$, where P is a positive integer relatively prime to m. We set $x_n = c_{j+n}$, where j, the position of the seed, is a positive integer and $1/P = (.c_1 c_2 c_3 \ldots)_m$. This is called the $1/P$ *generator*. Find the first ten terms of the pseudorandom sequence generator with each of the following parameters.
    a) $m = 7$, $P = 19$, and $j = 6$
    b) $m = 8$, $P = 21$, and $j = 5$

12.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find the pre-period and period of the decimal expansions of 212/31597, 1053/4437189, and 81327/16666699.
2. Find as many positive integers n as you can such that the length of the period of the decimal expansion of $1/n$ is $n - 1$.
3. Find the first 10,000 terms of the decimal expansion of π. Can you find any patterns? Make some conjectures about this expansion.
4. Find the first 10,000 terms of the decimal expansion of e. Can you find any patterns? Make some conjectures about this expansion.

Programming Projects

Write computer programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Find the base b expansion of a rational number, where b is a positive integer.
2. Find the numerator and denominator of a rational number in lowest terms from its base b expansion.

3. Find the pre-period and period lengths of the base b expansion of a rational number, where b is a positive integer.
4. Generate pseudorandom numbers using the $1/P$ generator (introduced in Exercise 26) with modulus m and seed in position j, where P and m are relatively prime positive integers greater than 1 and j is a positive integer.

12.2 Finite Continued Fractions

Using the Euclidean algorithm, we can express rational numbers as *continued fractions*. For instance, the Euclidean algorithm produces the following sequence of equations:

$$\begin{aligned} 62 &= 2 \cdot 23 + 16 \\ 23 &= 1 \cdot 16 + 7 \\ 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1. \end{aligned}$$

When we divide both sides of each equation by the divisor of that equation, we obtain

$$\begin{aligned} \frac{62}{23} &= 2 + \frac{16}{23} = 2 + \frac{1}{23/16} \\ \frac{23}{16} &= 1 + \frac{7}{16} = 1 + \frac{1}{16/7} \\ \frac{16}{7} &= 2 + \frac{2}{7} = 2 + \frac{1}{7/2} \\ \frac{7}{2} &= 3 + \frac{1}{2}. \end{aligned}$$

By combining these equations, we find that

$$\begin{aligned} \frac{62}{23} &= 2 + \frac{1}{23/16} \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{16/7}} \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{7/2}}} \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}}. \end{aligned}$$

The final expression in this string of equations is a continued fraction expansion of 62/23.

We now define continued fractions.

Definition. A *finite continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}},$$

where $a_0, a_1, a_2, \ldots, a_n$ are real numbers with $a_1, a_2, a_3, \ldots, a_n$ positive. The real numbers $a_1, a_2, \ldots, a_n$ are called the *partial quotients* of the continued fraction. The continued fraction is called *simple* if the real numbers $a_0, a_1, \ldots, a_n$ are all integers.

Because it is cumbersome to fully write out continued fractions, we use the notation $[a_0; a_1, a_2, \ldots, a_n]$ to represent the continued fraction in the definition of a finite continued fraction.

We will now show that every finite simple continued fraction represents a rational number. Later we will demonstrate that every rational number can be expressed as a finite simple continued fraction.

Theorem 12.7. Every finite simple continued fraction represents a rational number.

Proof. We will prove the theorem using mathematical induction. For $n = 1$, we have

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_0},$$

which is rational. Now, we assume that for the positive integer k the simple continued fraction $[a_0; a_1, a_2, \ldots, a_k]$ is rational whenever $a_0, a_1, \ldots, a_k$ are integers with $a_1, \ldots, a_k$ positive. Let $a_0, a_1, \ldots, a_{k+1}$ be integers with $a_1, \ldots, a_{k+1}$ positive. Note that

$$[a_0; a_1, \ldots, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_k, a_{k+1}]}.$$

By the induction hypothesis, $[a_1; a_2, \ldots, a_k, a_{k+1}]$ is rational; hence, there are integers r and s, with $s \neq 0$, such that this continued fraction equals r/s. Then

$$[a_0; a_1, \ldots, a_k, a_{k+1}] = a_0 + \frac{1}{r/s} = \frac{a_0 r + s}{r},$$

which is again a rational number. ∎

We now show, using the Euclidean algorithm, that every rational number can be written as a finite simple continued fraction.

Theorem 12.8. Every rational number can be expressed by a finite simple continued fraction.

Proof. Let $x = a/b$, where a and b are integers with $b > 0$. Let $r_0 = a$ and $r_1 = b$. Then, the Euclidean algorithm produces the following sequence of equations:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 < r_3 < r_2,\\
r_2 &= r_3 q_3 + r_4 && 0 < r_4 < r_3,\\
&\vdots\\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} && 0 < r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_n.
\end{aligned}$$

In these equations, $q_2, q_3, \ldots, q_n$ are positive integers. Writing these equations in fractional form, we have

$$\begin{aligned}
\frac{a}{b} = \frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{r_1/r_2}\\
\frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{r_2/r_3}\\
\frac{r_2}{r_3} &= q_3 + \frac{r_4}{r_3} = q_3 + \frac{1}{r_3/r_4}\\
&\vdots\\
\frac{r_{n-3}}{r_{n-2}} &= q_{n-2} + \frac{r_{n-1}}{r_{n-2}} = q_{n-2} + \frac{1}{r_{n-2}/r_{n-1}}\\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n}\\
\frac{r_{n-1}}{r_n} &= q_n.
\end{aligned}$$

Substituting the value of r_1/r_2 from the second equation into the first equation, we obtain

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{r_2/r_3}}. \tag{12.10}$$

Similarly, substituting the value of r_2/r_3 from the third equation into (12.10), we obtain

$$\frac{c}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{r_3/r_4}}}.$$

Continuing in this manner, we find that

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + q_{n-1} + \cfrac{1}{q_n}}}.$$

Hence, $\frac{a}{b} = [q_1; q_2, \ldots, q_n]$. This shows that every rational number can be written as a finite simple continued fraction. ∎

We note that continued fractions for rational numbers are not unique. From the identity

$$a_n = (a_n - 1) + \frac{1}{1},$$

we see that

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1]$$

whenever $a_n > 1$.

Example 12.6. We have

$$\frac{7}{11} = [0; 1, 1, 1, 3] = [0; 1, 1, 1, 2, 1].$$ ◀

In fact, it can be shown that every rational number can be written as a finite simple continued fraction in exactly two ways, one with an odd number of terms, the other with an even number (see Exercise 12 at the end of this section).

Next, we will discuss the numbers obtained from a finite continued fraction by cutting off the expression at various stages.

Definition. The continued fraction $[a_0; a_1, a_2, \ldots, a_k]$, where k is a nonnegative integer less than or equal to n, is called the *kth convergent* of the continued fraction $[a_0; a_1, a_2, \ldots, a_n]$. The kth convergent is denoted by C_k.

In our subsequent work, we will need some properties of the convergents of a continued fraction. We now develop these properties, starting with a formula for the convergents.

Theorem 12.9. Let $a_0, a_1, a_2, \ldots, a_n$ be real numbers, with $a_1, a_2, \ldots, a_n$ positive. Let the sequences $p_0, p_1, \ldots, p_n$ and $q_0, q_1, \ldots, q_n$ be defined recursively by

$$p_0 = a_0 \qquad q_0 = 1$$
$$p_1 = a_0 a_1 + 1 \qquad q_1 = a_1$$

and

$$p_k = a_k p_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2}$$

for $k = 2, 3, \ldots, n$. Then the kth convergent $C_k = [a_0; a_1, \ldots, a_k]$ is given by

$$C_k = p_k/q_k.$$

Proof. We will prove this theorem using mathematical induction. For $k = 0$, we have

$$C_0 = [a_0] = a_0/1 = p_0/q_0.$$

For $k = 1$, we see that

$$C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Hence, the theorem is valid for $k = 0$ and $k = 1$.

Now assume that the theorem is true for the positive integer k, where $2 \leq k < n$. This means that

$$C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}. \tag{12.11}$$

Because of the way in which the p_j's and q_j's are defined, we see that the real numbers p_{k-1}, p_{k-2}, q_{k-2}, depend only on the partial quotients $a_0, a_1, \ldots, a_{k-1}$. Consequently, we can replace the real number a_k by $a_k + 1/a_{k+1}$ in (12.11), to obtain

$$\begin{aligned} C_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] &= \left[a_o; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right] \\ &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} \\ &= \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

This finishes the proof by induction. ∎

We will illustrate how to use Theorem 12.9 with the following example.

Example 12.7. We have $173/55 = [3; 6, 1, 7]$. We compute the sequences p_j and q_j for $j = 0, 1, 2, 3$, by

$$\begin{aligned} p_0 &= 3 & q_0 &= 1 \\ p_1 &= 3 \cdot 6 + 1 = 19 & q_1 &= 6 \\ p_2 &= 1 \cdot 19 + 3 = 22 & q_2 &= 1 \cdot 6 + 1 = 7 \\ p_3 &= 7 \cdot 22 + 19 = 173 & q_3 &= 7 \cdot 7 + 6 = 55. \end{aligned}$$

Hence, the convergents of the above continued fraction are

$$C_0 = p_0/q_0 = 3/1 = 3$$
$$C_1 = p_1/q_1 = 19/6$$
$$C_2 = p_2/q_2 = 22/7$$
$$C_3 = p_3/q_3 = 173/55.$$ ◀

We now state and prove another important property of the convergents of a continued fraction.

Theorem 12.10. Let $C_k = p_k/q_k$ be the kth convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$, where k is a positive integer, $1 \leq k \leq n$. If p_k are as defined in Theorem 12.9, then

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Proof. We use mathematical induction to prove the theorem. For $k = 1$, we have

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) \cdot 1 - a_0 a_1 = 1.$$

Assume that the theorem is true for an integer k, where $1 \leq k < n$, so that

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Then we have

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= p_{k-1} q_k - p_k q_{k-1} = -(-1)^{k-1} = (-1)^k, \end{aligned}$$

so that the theorem is true for $k + 1$. This finishes the proof by induction. ■

We illustrate this theorem with the example that we used to illustrate Theorem 12.9.

Example 12.8. For the continued fraction $[3; 6, 1, 7]$ we have

$$p_0 q_1 - p_1 q_0 = 3 \cdot 6 - 19 \cdot 1 = -1$$
$$p_1 q_2 - p_2 q_1 = 19 \cdot 7 - 22 \cdot 6 = 1$$
$$p_2 q_3 - p_3 q_2 = 22 \cdot 55 - 173 \cdot 7 = -1.$$

As a consequence of Theorem 12.10, we see that for $k = 1, 2, \ldots$, the convergents p_k/q_k of a simple continued fraction are in lowest terms. Corollary 12.10.1 demonstrates this. ◀

Corollary 12.10.1. Let $C_k = p_k/q_k$ be the kth convergent of the simple continued fraction $[a_0; a_1, \ldots, a_n]$, where the integers p_k and q_k are as defined in Theorem 12.9. Then the integers p_k and q_k are relatively prime.

Proof. Let $d = (p_k, q_k)$. By Theorem 12.10, we know that

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

Hence,

$$d \mid (-1)^{k-1}.$$

Therefore, $d = 1$. ∎

We also have the following useful corollary of Theorem 12.10.

Corollary 12.10.2. Let $C_k = p_k/q_k$ be the kth convergent of the simple continued fraction $[a_0; a_1, a_2, \ldots, a_k]$. Then

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

for all integers k with $1 \leq k \leq n$. Also,

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$

for all integers k with $2 \leq k \leq n$.

Proof. By Theorem 12.10, we know that $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$.

We obtain the first identity,

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}},$$

by dividing both sides by $q_k q_{k-1}$.

To obtain the second identity, note that

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}.$$

Because $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$, we see that the numerator of the fraction on the right is

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k(p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) \\ &= a_k(-1)^{k-2}, \end{aligned}$$

using Theorem 12.10 to see that $p_{k-1} q_{k-2} - p_{k-2} q_{k-1} = (-1)^{k-2}$.

Therefore, we find that

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}.$$

This is the second identity of the corollary. ∎

Using Corollary 12.10.2, we can prove the following theorem, which is useful when developing infinite continued fractions.

Theorem 12.11. Let C_k be the kth convergent of the finite simple continued fraction $[a_0; a_1, a_2, \ldots, a_n]$. Then

$$C_1 > C_3 > C_5 > \cdots,$$
$$C_0 < C_2 < C_4 < \cdots,$$

and every odd-numbered convergent C_{2j+1}, $j = 0, 1, 2, \ldots$, is greater than every even-numbered convergent C_{2j}, $j = 0, 1, 2, \ldots$.

Proof. Because Corollary 12.10.2 tells us that, for $k = 2, 3, \ldots, n$,

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$

we know that

$$C_k < C_{k-2}$$

when k is odd, and

$$C_k > C_{k-2}$$

when k is even. Hence,

$$C_1 > C_3 > C_5 > \cdots$$

and

$$C_0 < C_2 < C_4 < \cdots.$$

To show that every odd-numbered convergent is greater than every even-numbered convergent, note that from Corollary 12.10.2, we have

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m}q_{2m-1}} < 0,$$

so that $C_{2m-1} > C_{2m}$. To compare C_{2k} and C_{2j-1}, we see that

$$C_{2j-1} > C_{2j+2k-1} > C_{2j+2k} > C_{2k}.$$

so that every odd-numbered convergent is greater than every even-numbered convergent. ∎

Example 12.9. Consider the finite simple continued fraction $[2; 3, 1, 1, 2, 4]$. Then the convergents are

$$\begin{aligned} C_0 &= 2/1 = 2 \\ C_1 &= 7/3 = 2.3333\ldots \\ C_2 &= 9/4 = 2.25 \\ C_3 &= 16/7 = 2.2857\ldots \\ C_4 &= 41/18 = 2.2777\ldots \\ C_5 &= 180/79 = 2.2784\ldots. \end{aligned}$$

We see that

$$C_0 = 2 < C_2 = 2.25 < C_4 = 2.2777\ldots$$
$$< C_5 = 2.2784\ldots < C_3 = 2.2857\ldots < C_1 = 2.3333\ldots. \quad \blacktriangleleft$$

12.2 Exercises

1. Find the rational number, expressed in lowest terms, represented by each of the following simple continued fractions.

   a) [2; 7]
   b) [1; 2, 3]
   c) [0; 5, 6]
   d) [3; 7, 15, 1]
   e) [1; 1]
   f) [1; 1, 1]
   g) [1; 1, 1, 1]
   h) [1; 1, 1, 1, 1]

2. Find the rational number, expressed in lowest terms, represented by each of the following simple continued fractions.

   a) [10; 3]
   b) [3; 2, 1]
   c) [0; 1, 2, 3]
   d) [2; 1, 2, 1]
   e) [2; 1, 2, 1, 1, 4]
   f) [1; 2, 1, 2]
   g) [1; 2, 1, 2, 1]
   h) [1; 2, 1, 2, 1, 2]

3. Find the simple continued fraction expansion, not terminating with the partial quotient of 1, of each of the following rational numbers.

   a) 18/13
   b) 32/17
   c) 19/9
   d) 310/99
   e) −931/1005
   f) 831/8110

4. Find the simple continued fraction expansion, not terminating with the partial quotient of 1, of each of the following rational numbers.

   a) 6/5
   b) 22/7
   c) 19/29
   d) 5/999
   e) −943/1001
   f) 873/4867

5. Find the convergents of each of the continued fractions found in Exercise 3.

6. Find the convergents of each of the continued fractions found in Exercise 4.

7. Show that the convergents that you found in Exercise 5 satisfy Theorem 12.11.

8. Let f_k denote the kth Fibonacci number. Find the simple continued fraction, terminating with the partial quotient of 1, of f_{k+1}/f_k, where k is a positive integer.

9. Show that if the simple continued fraction expression of the rational number α, $\alpha > 1$, is $[a_0; a_1, \ldots, a_k]$, then the simple continued fraction expression of $1/\alpha$ is $[0; a_1, \ldots, a_k]$.

☞ 10. Show that if $a_0 > 0$, then

$$p_k/p_{k-1} = [a_k; a_{k-1}, \ldots, a_1, a_0]$$

and

$$q_k/q_{k-1} = [a_k; a_{k-1}, \ldots, a_2, a_1],$$

where $C_{k-1} = p_{k-1}/q_{k-1}$ and $C_k = p_k/q_k$, $k \geq 1$, are successive convergents of the continued fraction $[a_0; a_1, \ldots, a_n]$. (*Hint:* Use the relation $p_k = a_k p_{k-1} + p_{k-2}$ to show that $p_k/p_{k-1} = a_k + 1/(p_{k-1}/p_{k-2})$.)

☞ **11.** Show that $q_k \geq f_k$ for $k = 1, 2, \ldots$, where $C_k = p_k/q_k$ is the kth convergent of the simple continued fraction $[a_0; a_1, \ldots, a_n]$ and f_k denotes the kth Fibonacci number.

12. Show that every rational number has exactly two finite simple continued fraction expansions.

* **13.** Let $[a_0; a_1, a_2, \ldots, a_n]$ be the simple continued fraction expansion of r/s, where $(r, s) = 1$ and $r \geq 1$. Show that this continued fraction is symmetric, that is, $a_0 = a_n, a_1 = a_{n-1}, a_2 = a_{n-2}, \ldots$, if and only if $r|(s^2 + 1)$ if n is odd and $r|(s^2 - 1)$ if n is even. (*Hint:* Use Exercise 10 and Theorem 12.10.)

* **14.** Explain how finite continued fractions for rational numbers, with both plus and minus signs allowed, can be generated from the division algorithm given in Exercise 18 of Section 1.5.

15. Let $a_0, a_1, a_2, \ldots, a_k$ be real numbers with $a_1, a_2, \ldots$ positive, and let x be a positive real number. Show that $[a_0; a_1, \ldots, a_k] < [a_0; a_1 \ldots, a_k + x]$ if k is odd and $[a_0; a_1, \ldots, a_k] > [a_0; a_1 \ldots, a_k + x]$ if k is even.

16. Determine whether n can be expressed as the sum of positive integers a and b, where all the partial quotients of the finite simple continued fraction of a/b are either 1 or 2, for each of the following integers n.

a) 13 c) 19 e) 27
b) 17 d) 23 f) 29

12.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the simple continued fractions of 1001/3000, 10,001/30,000, and 100,001/300,000.
2. Find the finite continued fractions of x and $2x$ for 20 different rational numbers. Can you find a rule for finding the finite simple continued fraction of $2x$ from that of x?
3. Determine for each integer n, $n \leq 1000$, whether there are integers a and b with $n = a + b$ such that the partial quotients of the continued fraction of a/b are all either 1 or 2. Can you make any conjectures?

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Find the simple continued fraction expansion of a rational number.
2. Find the convergents of a finite simple continued fraction, and find the rational number that this continued fraction represents.

12.3 Infinite Continued Fractions

Suppose that we have an infinite sequence of positive integers $a_0; a_1, a_2, \ldots$. How can we define the infinite continued fraction $[a_0; a_1, a_2, \ldots]$? To make sense of infinite continued fractions, we need a result from mathematical analysis. We state the result, and refer the reader to a mathematical analysis text, such as [Ru64], for a proof.

Theorem 12.12. Let $x_0, x_1, x_2, \ldots$ be a sequence of real numbers such that $x_0 < x_1 < x_2 < \cdots$ and $x_k < U$ for $k = 0, 1, 2, \ldots$ for some real number U, or $x_0 > x_1 > x_2 > \cdots$ and $x_k > L$ for $k = 0, 1, 2, \ldots$ for some real number L. Then the terms of the sequence $x_0, x_1, x_2, \ldots$ tend to a limit x, that is, there exists a real number x such that

$$\lim_{k \to \infty} x_k = x.$$

Theorem 12.12 tells us that the terms of an infinite sequence tend to a limit in two special situations: when the terms of the sequence are increasing and all are less than an upper bound, and when the terms of the sequence are decreasing and all are greater than a lower bound.

We can now define infinite continued fractions as limits of finite continued fractions, as the following theorem shows.

Theorem 12.13. Let $a_0, a_1, a_2, \ldots$ be an infinite sequence of integers with $a_1, a_2, \ldots$ positive, and let $C_k = [a_0; a_1, a_2, \ldots, a_k]$. Then the convergents C_k tend to a limit α, that is,

$$\lim_{k \to \infty} C_k = \alpha.$$

Before proving Theorem 12.13, we note that the limit α described in the statement of the theorem is called the value of the *infinite simple continued fraction* $[a_0; a_1, a_2, \ldots]$.

To prove Theorem 12.13, we will show that the infinite sequence of even-numbered convergents is increasing and has an upper bound and that the infinite sequence of odd-numbered convergents is decreasing and has a lower bound. We then show that the limits of these two sequences, guaranteed to exist by Theorem 12.12, are in fact equal.

Proof. Let m be an even positive integer. By Theorem 12.11, we see that

$$C_1 > C_3 > C_5 > \cdots > C_{m-1},$$
$$C_0 < C_2 < C_4 < \cdots < C_m,$$

and $C_{2j} < C_{2k+1}$ whenever $2j \leq m$ and $2k + 1 < m$. By considering all possible values of m, we see that

$$C_1 > C_3 > C_5 > \cdots > C_{2n-1} > C_{2n+1} > \cdots,$$
$$C_0 < C_2 < C_4 < \cdots < C_{2n-2} < C_{2n} < \cdots,$$

and $C_{2j} > C_{2k+1}$ for all positive integers j and k. We see that the hypotheses of Theorem 12.12 are satisfied for each of the two sequences $C_1, C_3, C_2, \ldots$ and $C_0, C_2, C_4, \ldots$.

Hence, the sequence $C_1, C_3, C_5, \ldots$ tends to a limit α_1 and the sequence $C_0, C_2, C_4, \ldots$ tends to a limit α_2, that is,

$$\lim_{n\to\infty} C_{2n+1} = \alpha_1$$

and

$$\lim_{n\to\infty} C_{2n} = \alpha_2.$$

Our goal is to show that these two limits α_1 and α_2 are equal. Using Corollary 12.10.2, we have

$$C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{(2n+1)-1}}{q_{2n+1}q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Because $q_k \geq k$ for all positive integers k (see Exercise 11 of Section 12.2), we know that

$$\frac{1}{q_{2n+1}q_{2n}} < \frac{1}{(2n+1)(2n)},$$

and hence,

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}}$$

tends to zero, that is,

$$\lim_{n\to\infty} (C_{2n+1} - C_{2n}) = 0.$$

Hence, the sequences $C_1, C_3, C_5, \ldots$ and $C_0, C_2, C_4, \ldots$ have the same limit, because

$$\lim_{n\to\infty} (C_{2n+1} - C_{2n}) = \lim_{n\to\infty} C_{2n+1} - \lim_{n\to\infty} C_{2n} = 0.$$

Therefore, $\alpha_1 = \alpha_2$, and we conclude that all the convergents tend to the limit $\alpha = \alpha_1 = \alpha_2$. This finishes the proof of the theorem. ∎

Previously, we showed that rational numbers have finite simple continued fractions. Next, we will show that the value of any infinite simple continued fraction is irrational.

Theorem 12.14. Let $a_0, a_1, a_2, \ldots$ be integers with $a_1, a_2, \ldots$ positive. Then $[a_0; a_1, a_2, \ldots]$ is irrational.

Proof. Let $\alpha = [a_0; a_1, a_2, \ldots]$ and let

$$C_k = p_k/q_k = [a_0; a_1, a_2, \ldots a_k]$$

denote the kth convergent of α. When n is a positive integer, Theorem 12.13 shows that $C_{2n} < \alpha < C_{2n+1}$, so that

$$0 < \alpha - C_{2n} < C_{2n+1} - C_{2n}.$$

However, by Corollary 12.10.2, we know that

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}},$$

which means that

$$0 < \alpha - C_{2n} = \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n+1}q_{2n}},$$

and, therefore, we have

$$0 < \alpha q_{2n} - p_{2n} < \frac{1}{q_{2n+1}}.$$

Assume that α is rational, so that $\alpha = a/b$, where a and b are integers with $b \neq 0$. Then

$$0 < \frac{aq_{2n}}{b} - p_{2n} < \frac{1}{q_{2n+1}},$$

and by multiplying this inequality by b, we see that

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}}.$$

Note that $aq_{2n} - bp_{2n}$ is an integer for all positive integers n. However, because $q_{2n+1} > 2n + 1$, for each integer n there is an integer n_0 such that $q_{2n_0+1} > b$, so that $b/q_{2n_0+1} < 1$. This is a contradiction, because the integer $aq_{2n_0} - bp_{2n_0}$ cannot be between 0 and 1. We conclude that α is irrational. ∎

We have demonstrated that every infinite simple continued fraction represents an irrational number. We will now show that every irrational number can be uniquely expressed by an infinite simple continued fraction, by first constructing such a continued fraction, and then by showing that it is unique.

Theorem 12.15. Let $\alpha = \alpha_0$ be an irrational number, and define the sequence $a_0, a_1, a_2, \ldots$ recursively by

$$a_k = [\alpha_k] \quad \alpha_{k+1} = 1/(\alpha_k - a_k)$$

for $k = 0, 1, 2, \ldots$. Then α is the value of the infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$.

Proof. From the recursive definition of the integers a_k, we see that a_k is an integer for every k. Furthermore, using mathematical induction, we can show that α_k is irrational for every nonnegative integer k and that, as a consequence, α_{k+1} exists. First, note that $\alpha_0 = \alpha$ is irrational, so that $\alpha_0 \neq a_0 = [\alpha_0]$ and $\alpha_1 = 1/(\alpha_0 - a_0)$ exists.

Next, we assume that α_k is irrational. As a consequence, α_{k+1} exists. We can easily see that α_{k+1} is also irrational, because the relation

$$\alpha_{k+1} = 1/(\alpha_k - a_k)$$

implies that

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}, \tag{12.12}$$

and if α_{k+1} were rational, then α_k would also be rational. Now, because α_k is irrational and a_k is an integer, we know that $\alpha_k \neq a_k$, and

$$a_k < \alpha_k < a_k + 1,$$

so that

$$0 < \alpha_k - a_k < 1.$$

Hence,

$$\alpha_{k+1} = 1/(\alpha_k - a_k) > 1$$

and, consequently,

$$a_{k+1} = [\alpha_{k+1}] \geq 1$$

for $k = 0, 1, 2, \ldots$. This means that all the integers $a_1, a_2, \ldots$ are positive.

Note that by repeatedly using (12.12), we see that

$$\begin{aligned}
\alpha = \alpha_0 &= a_0 + \frac{1}{\alpha_1} = [a_0; \alpha_1] \\
&= a_0 + \frac{1}{a_1 + \dfrac{1}{\alpha_2}} = [a_0; a_1, a_2] \\
&\vdots \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + a_k + \cfrac{1}{\alpha_{k+1}}}} = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}].
\end{aligned}$$

What we must now show is that the value of $[a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$ tends to α as k tends to infinity, that is, as k grows without bound. By Theorem 12.9, we see that

$$\alpha = [a_0; a_1, \ldots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}},$$

where $C_j = p_j/q_j$ is the jth convergent of $[a_0; a_1, a_2, \ldots]$. Hence,

$$\begin{aligned}\alpha - C_k &= \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} \\ &= \frac{-(p_kq_{k-1} - p_{k-1}q_k)}{(\alpha_{k+1}q_k + q_{k-1})q_k} \\ &= \frac{-(-1)^{k-1}}{(\alpha_{k+1}q_k + q_{k-1})q_k},\end{aligned}$$

where we have used Theorem 12.10 to simplify the numerator on the right-hand side of the second equality. Because

$$\alpha_{k+1}q_k + q_{k-1} > a_{k+1}q_k + q_{k-1} = q_{k+1},$$

we see that

$$|\alpha - C_k| < \frac{1}{q_kq_{k+1}}.$$

Because $q_k > k$ (from Exercise 11 of Section 12.2), we note that $1/(q_kq_{k+1})$ tends to zero as k tends to infinity. Hence, C_k tends to α as k tends to infinity or, phrased differently, the value of the infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$ is α. ∎

To show that the infinte simple continued fraction that represent an irrational number is unique, we prove the following theorem.

Theorem 12.16. If the two infinite simple continued fractions $[a_0; a_1, a_2, \ldots]$ and $[b_0; b_1, b_2, \ldots]$ represent the same irrational number, then $a_k = b_k$ for $k = 0, 1, 2, \ldots$.

Proof. Suppose that $\alpha = [a_0; a_1, a_2, \ldots]$. Then, because $C_0 = a_0$ and $C_1 = a_0 + 1/a_1$, Theorem 12.11 tells us that

$$a_0 < \alpha < a_0 + 1/a_1,$$

so that $a_0 = [\alpha]$. Further, we note that

$$[a_0; a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]},$$

because

$$\begin{aligned}\alpha = [a_0; a_1, a_2, \ldots] &= \lim_{k\to\infty} [a_0; a_1, a_2, \ldots, a_k] \\ &= \lim_{k\to\infty} \left(a_0 + \frac{1}{[a_1; a_2, a_3, \ldots, a_k]}\right) \\ &= a_0 + \frac{1}{\lim\limits_{k\to\infty} [a_1; a_2, \ldots, a_k]} \\ &= a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]}.\end{aligned}$$

Suppose that

$$[a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots].$$

Our remarks show that

$$a_0 = b_0 = [\alpha]$$

and that

$$a_0 + \frac{1}{[a_1; a_2, \ldots]} = b_0 + \frac{1}{[b_1; b_2, \ldots]},$$

so that

$$[a_1; a_2, \ldots] = [b_1; b_2, \ldots].$$

Now, assume that $a_k = b_k$, and that $[a_{k+1}; a_{k+2}, \ldots] = [b_{k+1}; b_{k+2}, \ldots]$. Using the same argument, we see that $a_{k+1} = b_{k+1}$, and

$$a_{k+1} + \frac{1}{[a_{k+2}; a_{k+3}, \ldots]} = b_{k+1} + \frac{1}{[b_{k+1}; b_{k+3}, \ldots]},$$

which implies that

$$[a_{k+2}; a_{k+3} \ldots] = [b_{k+2}; b_{k+3}, \ldots].$$

Hence, by mathematical induction, we see that $a_k = b_k$ for $k = 0, 1, 2, \ldots$. ∎

To find the simple continued fraction expansion of a real number, we use the algorithm given in Theorem 12.15. We illustrate this procedure with the following example.

Example 12.10. Let $\alpha = \sqrt{6}$. We find that

$$a_0 = [\sqrt{6}] = 2, \qquad \alpha_1 = \frac{1}{\sqrt{6} - 2} = \frac{\sqrt{6} + 2}{2},$$

$$a_1 = \left[\frac{\sqrt{6} + 2}{2}\right] = 2, \quad \alpha_2 = \frac{1}{\left(\frac{\sqrt{6}+2}{2}\right) - 2} = \sqrt{6} + 2,$$

$$a_2 = [\sqrt{6} + 2] = 4, \quad \alpha_3 = \frac{1}{\left(\sqrt{6} + 2\right) - 4} = \frac{\sqrt{6} + 2}{2} = \alpha_1.$$

Because $\alpha_3 = \alpha_1$, we see that $a_3 = a_1, a_4 = a_2, \ldots$, and so on. Hence

$$\sqrt{6} = [2; 2, 4, 2, 4, 2, 4, \ldots].$$

The simple continued fraction of $\sqrt{6}$ is periodic. We will discuss periodic simple continued fractions in the next section. ◀

The convergents of the infinite simple continued fraction of an irrational number are good approximations to α. This leads to the following theorem, which we introduced in Exercise 34 of Section 1.1.

Theorem 12.17. ***Dirichlet's Theorem on Diophantine Approximation.*** If α is an irrational number, then there are infinitely many rational numbers p/q such that

$$|\alpha - p/q| < 1/q^2.$$

Proof. Let p_k/q_k be the kth convergent of the continued fraction of α. Then, by the proof of Theorem 12.15, we know that

$$|\alpha - p_k/q_k| < 1/(q_k q_{k+1}).$$

Because $q_k < q_{k+1}$, it follows that

$$|\alpha - p_k/q_k| < 1/q_k^2.$$

Consequently, the convergents of α, p_k/q_k, $k = 1, 2, \ldots$, are infinitely many rational numbers meeting the conditions of the theorem. ∎

The next theorem and corollary show that the convergents of the simple continued fraction of α are the *best rational approximations* to α, in the sense that p_k/q_k is closer to α than any other rational number with a denominator less than q_k.

Theorem 12.18. Let α be an irrational number and let p_j/q_j, $j = 1, 2, \ldots$, be the convergents of the infinite simple continued fraction of α. If r and s are integers with $s > 0$ and if k is a positive integer such that

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

then $s \geq q_{k+1}$.

Proof. Assume that $|s\alpha - r| < |q_k\alpha - p_k|$, but that $1 \leq s < q_{k+1}$. We consider the simultaneous equations

$$p_k x + p_{k+1} y = r$$
$$q_k x + q_{k+1} y = s.$$

By multiplying the first equation by q_k and the second by p_k, and then subtracting the second from the first, we find that

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k.$$

By Theorem 12.10, we know that $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$, so that

$$y = (-1)^k(rq_k - sp_k).$$

Similarly, multiplying the first equation by q_{k+1} and the second by p_{k+1}, and then subtracting the first from the second, we find that

$$x = (-1)^k(sp_{k+1} - rq_{k+1}).$$

We note that $s \neq 0$ and $y \neq 0$. If $x = 0$, then $sp_{k+1} = rq_{k+1}$. Because $(p_{k+1}, q_{k+1}) = 1$, Lemma 3.4 tells us that $q_{k+1}|s$, which implies that $q_{k+1} \leq s$, contrary to our assumption. If $y = 0$, then $r = p_k x$ and $s = q_k x$, so that

$$|s\alpha - r| = |x|\,|q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

because $|x| \geq 1$, contrary to our assumption.

We will now show that x and y have opposite signs. First, suppose that $y < 0$. Because $q_k x = s - q_{k+1}y$, we know that $x > 0$, because $q_k x > 0$ and $q_k > 0$. When $y > 0$, because $q_{k+1}y \geq q_{k+1} > s$, we see that $q_k x = s - q_{k+1}y < 0$, so that $x < 0$.

By Theorem 12.11, we know that either $p_k/q_k < \alpha < p_{k+1}/q_{k+1}$ or that $p_{k+1}/q_{k+1} < \alpha < p_k/q_k$. In either case, we easily see that $q_k\alpha - p_k$ and $q_{k+1}\alpha - p_{k+1}$ have opposite signs.

From the simultaneous equations we started with, we see that

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1}y)\alpha - (p_k x + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})|. \end{aligned}$$

Combining the conclusions of the previous two paragraphs, we see that $x(q_k\alpha - p_k)$ and $y(q_{k+1}\alpha - p_{k+1})$ have the same sign, so that

$$\begin{aligned} |s\alpha - r| &= |x|\,|q_k\alpha - p_k| + |y|\,|q_{k+1}\alpha - p_{k+1}| \\ &\geq |x|\,|q_k\alpha - p_k| \\ &\geq |q_k\alpha - p_k|, \end{aligned}$$

because $|x| \geq 1$. This contradicts our assumption.

We have shown that our assumption is false and, consequently, the proof is complete. ∎

Corollary 12.18.1. Let α be an irrational number and let p_j/q_j, $j = 1, 2, \ldots$ be the convergents of the infinite simple continued fraction of α. If r/s is a rational number, where r and s are integers with $s > 0$, and if k is a positive integer such that

$$|\alpha - r/s| < |\alpha - p_k/q_k|,$$

then $s > q_k$.

Proof. Suppose that $s \leq q_k$ and that

$$|\alpha - r/s| < |\alpha - p_k/q_k|.$$

By multiplying these two inequalities, we find that

$$s|\alpha - r/s| < q_k|\alpha - p_k/q_k|,$$

so that

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

violating the conclusion of Theorem 12.18. ∎

Example 12.11. The simple continued fraction of the real number π is $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \ldots]$. Note that there is no discernible pattern in the sequence of partial quotients. The convergents of this continued fraction are the best rational approximations to π. The first five are 3, 22/7, 333/106, 355/113, and 103,993/33,102. We conclude from Corollary 12.18.1 that 22/7 is the best rational approximation of π with denominator less than or equal to 105, and so on. ◀

Finally, we conclude this section with a result that shows that any sufficiently close rational approximation to an irrational number must be a convergent of the infinite simple continued fraction expansion of this number.

Theorem 12.19. If α is an irrational number and if r/s is a rational number in lowest terms, where r and s are integers with $s > 0$ such that

$$|\alpha - r/s| < 1/(2s^2),$$

then r/s is a convergent of the simple continued fraction expansion of α.

Proof. Assume that r/s is not a convergent of the simple continued fraction expansion of α. Then, there are successive convergents p_k/q_k and p_{k+1}/q_{k+1} such that $q_k \leq s < q_{k+1}$. By Theorem 12.18, we see that

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s|\alpha - r/s| < 1/(2s).$$

Dividing by q_k, we obtain

$$|\alpha - p_k/q_k| < 1/(2sq_k).$$

Because we know that $|sp_k - rq_k| \geq 1$ (we know that $sp_k - rq_k$ is a nonzero integer because $r/s \neq p_k/q_k$), it follows that

$$\begin{aligned}\frac{1}{sq_k} &\leq \frac{|sp_k - rq_k|}{sq_k} \\ &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \\ &\leq \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right| \\ &< \frac{1}{2sq_k} + \frac{1}{2s^2}\end{aligned}$$

(where we have used the triangle inequality to obtain the second inequality). Hence, we see that

$$1/2sq_k < 1/2s^2.$$

Consequently,

$$2sq_k > 2s^2,$$

which implies that $q_k > s$, contradicting the assumption. ∎

Applying Continued Fractions to Attack the RSA Cryptosystem We can use a version of Theorem 12.19 for rational numbers to explain why an attack on certain implementations of RSA ciphers works. We leave it as an exercise to prove that this version of Theorem 12.19 is valid.

Theorem 12.20. ***Wiener's Low Encryption Exponent Attack on RSA.*** Suppose that $n = pq$, where p and q are odd primes with $q < p < 2q$ and that $d < n^{1/4}/3$. Then,

given an RSA encryption key (e, n), the decryption key can be found using $O((\log n)^3)$ bit operations.

Proof. We will base the proof on approximation of a rational number by continued fractions. First note that because $de \equiv 1 \pmod{\phi(n)}$, there is an integer k such that $de - 1 = k\phi(n)$. Dividing both sides of this equation by $d\phi(n)$, we find that

$$\frac{e}{\phi(n)} - \frac{1}{d\phi(n)} = \frac{k}{d},$$

which implies that

$$\frac{e}{\phi(n)} - \frac{k}{d} = \frac{1}{d\phi(n)}.$$

This shows that the fraction k/d is a good approximation of $e/\phi(n)$.

Note also that $q < \sqrt{n}$, because $q < p$ and $n = pq$ by the hypotheses of the theorem. Using the hypothesis that $q < p$, it follows that

$$p + q - 1 \leq 2q + q - 1 = 3q - 1 < 3\sqrt{n}.$$

Because $\phi(n) = n - p - q + 1$, we see that $n - \phi(n) = n - (n - p - q + 1) = p + q - 1 < 3\sqrt{n}$.

We can make use of this last inequality to show that k/d is an excellent approximation of e/n. We see that

$$\begin{aligned}\left|\frac{e}{n} - \frac{k}{d}\right| &= \left|\frac{de - kn}{nd}\right| \\ &= \left|\frac{(de - k\phi(n)) - (kn + k\phi(n))}{nd}\right| \\ &= \left|\frac{1 - k(n - \phi(n))}{nd}\right| \leq \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}}.\end{aligned}$$

Because $e < \phi(n)$, we see that $ke < k\phi(n) = de - 1 < de$. This implies that $k < d$. We now use the hypothesis that $d < n^{1/4}/3$ to see that $k < n^{1/4}/3$.

It follows that

$$\left|\frac{e}{n} - \frac{k}{d}\right| \leq \frac{3k\sqrt{n}}{nd} \leq \frac{3(n^{1/4}/3)\sqrt{n}}{nd} = \frac{1}{dn^{1/4}} < \frac{1}{2d^2}.$$

We now use the version of Theorem 12.19 for rational numbers. By this theorem, we know that k/d is a convergent of the continued fraction expansion of e/n. Note also that both e and n are public information. Consequently, to find k/d we need only examine the convergents of e/n. Because k/d is a reduced fraction, to check each convergent to see whether it equals k/d, we suppose that its denominator equals k. We then use this value to compute $\phi(n)$, because $\phi(n) = (de - 1)/k$. We use this purported value of $\phi(n)$ and the value of n to factor n (see the discussion in Section 8.4 to see how this is done). Once we have found k/d, we know d because k/d is a reduced fraction and d is its denominator. To see that k/d is reduced, note that $ed - k\phi(n) = 1$, which implies, by

Theorem 3.8, that $(d, k) = 1$. Because computing all convergents of a rational number with denominator n uses $O((\log n)^3)$ bit operations, we see that d can be found using $O((\log n)^3)$ bit operations. ■

12.3 Exercises

1. Find the simple continued fractions of each of the following real numbers.

   a) $\sqrt{2}$ c) $\sqrt{5}$

   b) $\sqrt{3}$ d) $(1 + \sqrt{5})/2$

2. Find the first five partial quotients of the simple continued fractions of each of the following real numbers.

   a) $\sqrt[3]{2}$ c) $(e - 1)/(e + 1)$

   b) 2π d) $(e^2 - 1)/(e^2 + 1)$

3. Find the best rational approximation to π with a denominator less than or equal to 100,000.

4. The infinite simple continued fraction expansion of the number e is

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].$$

   a) Find the first eight convergents of the continued fraction of e.

   b) Find the best rational approximation to e having a denominator less than or equal to 536.

* 5. Let α be an irrational number with simple continued fraction expansion $\alpha = [a_0; a_1, a_2, \ldots]$. Show that the simple continued fraction of $-\alpha$ is $[-a_0 - 1; 1, a_1 - 1, a_2, a_3, \ldots]$ if $a_1 > 1$ and $[-a_0 - 1; a_2 + 1, a_3, \ldots]$ if $a_1 = 1$.

* 6. Show that if p_k/q_k and p_{k+1}/q_{k+1} are consecutive convergents of the simple continued fraction of an irrational number α, then

$$|\alpha - p_k/q_k| < 1/(2q_k^2)$$

or

$$|\alpha - p_{k+1}/q_{k+1}| < 1/(2q_{k+1}^2).$$

(*Hint:* First show that $|\alpha - p_{k+1}/q_{k+1}| + |\alpha - p_k/q_k| = |p_{k+1}/q_{k+1} - p_k/q_k| = 1/(q_k q_{k+1})$.)

☞ 7. Let α be an irrational number, $\alpha > 1$. Show that the kth convergent of the simple continued fraction of $1/\alpha$ is the reciprocal of the $(k - 1)$th convergent of the simple continued fraction of α.

* 8. Let α be an irrational number, and let p_j/q_j denote the jth convergent of the simple continued fraction expansion of α. Show that at least one of any three consecutive convergents satisfies the inequality

$$|\alpha - p_j/q_j| < 1/(\sqrt{5}q_j^2).$$

Conclude that there are infinitely many rational numbers p/q, where p and q are integers with $q \neq 0$, such that

$$|\alpha - p/q| < 1/(\sqrt{5}q^2).$$

* **9.** Show that if $\alpha = (1+\sqrt{5})/2$, and $c > \sqrt{5}$, then there are only a finite number of rational numbers p/q, where p and q are integers, $q \neq 0$, such that

$$|\alpha - p/q| < 1/(cq^2).$$

(*Hint:* Consider the convergents of the simple continued fraction expansion of $\sqrt{5}$.)

If α and β are two real numbers, we say that β is *equivalent* to α if there are integers a, b, c, and d such that $ad - bc = \pm 1$ and $\beta = \frac{a\alpha+b}{c\alpha+d}$.

10. Show that a real number α is equivalent to itself.

11. Show that if α and β are real numbers with β equivalent to α, then α is equivalent to β. Hence, we can say that two numbers α and β are equivalent.

12. Show that if α, β, and λ are real numbers such that α and β are equivalent and β and λ are equivalent, then α and λ are equivalent.

13. Show that any two rational numbers are equivalent.

* **14.** Show that two irrational numbers α and β are equivalent if and only if the tails of their simple continued fractions agree, that is, if $\alpha = [a_0; a_1, a_2, \ldots, a_j, c_1, c_2, c_3, \ldots]$, $\beta = [b_0; b_1, b_2, \ldots, b_k, c_1, c_2, c_3, \ldots]$, where $a_i, i = 0, 1, 2, \ldots, j$; $b_i, i = 0, 1, 2, \ldots, k$; and $c_i, i = 1, 2, 3, \ldots$ are integers, all positive except perhaps a_0 and b_0.

Let α be an irrational number, and let the simple continued fraction expansion of α be $\alpha = [a_0; a_1, a_2, \ldots]$. Let p_k/q_k denote, as usual, the kth convergent of this continued fraction. We define the *pseudoconvergents* of this continued fraction to be

$$p_{k,t}/q_{k,t} = (tp_{k-1} + p_{k-2})/(tq_{k-1} + q_{k-2}),$$

where k is a positive integer, $k \geq 2$, and t is an integer with $0 < t < a_k$.

15. Show that each pseudoconvergent is in lowest terms.

* **16.** Show that the sequence of rational numbers $p_{k,2}/q_{k,2}, \ldots, p_{k,a_{k-1}}/q_{k,a_{k-1}}, p_k/q_k$ is increasing if k is even, and decreasing if k is odd.

* **17.** Show that if r and s are integers with $s > 0$ such that

$$|\alpha - r/s| \leq |\alpha - p_{k,t}/q_{k,t}|,$$

where k is a positive integer and $0 < t < a_k$, then $s > q_{k,t}$ or $r/s = p_{k-1}/q_{k-1}$. This shows that the closest rational approximations to a real number are the convergents and pseudoconvergents of its simple continued fraction.

18. Find the pseudoconvergents of the simple continued fraction of π for $k = 2$.

19. Find a rational number r/s that is closer to π than 22/7 with denominator s less than 106. (*Hint:* Use Exercise 17.)

20. Find the rational number r/s that is closest to e with denominator s less than 100.

21. Show that the version of Theorem 12.19 for rational numbers is valid. That is, show that if a, b, c, and d are all integers with b and d nonzero, $(a, b) = (c, d) = 1$ and

$$\left|\frac{a}{b} - \frac{c}{d}\right| < \frac{1}{2d^2},$$

then c/d is a convergent of the continued fraction expansion of a/b.

22. Show that computing all convergents of a rational number with denominator n can be done using $O((\log n)^3)$ bit operations.

12.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Compute the first 100 partial quotients of each of the real numbers in Exercise 2.
2. Compute the first 100 partial quotients of the simple continued fraction of e^2. From this, find the rule for the partial quotients of this simple continued fraction.
3. Compute the first 1000 partial quotients of the simple continued fraction of π. What is the largest partial quotient that appears? How often does the integer 1 appear as a partial quotient?

Programming Projects

Write programs in Maple, *Mathematica,* or a language of your choice to do the following.

1. Given a real number x, find the simple continued fraction of x.
2. Given an irrational number x and a positive integer n, find the best rational approximation to x with denominator not exceeding n.

12.4 Periodic Continued Fractions

We call the infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$ *periodic* if there are positive integers N and k such that $a_n = a_{n+k}$ for all positive integers n with $n \geq N$. We use the notation

$$[a_0; a_1, a_2, \ldots, a_{N-1}, \overline{a_N, a_{N+1}, a_{N+k-1}}]$$

to express the periodic infinite simple continued fraction

$$[a_0; a_1, a_2, \ldots, a_{N-1}, a_N, a_{N+1}, \ldots, a_{N+k-1}a_N, a_{N+1}, \ldots].$$

For instance, $[1; 2, \overline{3, 4}]$ denotes the infinite simple continued fraction $[1; 2, 3, 4, 3, 4, 3, 4, \ldots]$.

In Section 12.1, we showed that the base b expansion of a number is periodic if and only if the number is rational. To characterize those irrational numbers with periodic infinite simple continued fractions, we need the following definition.

Definition. The real number α is said to be a *quadratic irrational* if α is irrational and is a root of a quadratic polynomial with integer coefficients, that is,

$$A\alpha^2 + B\alpha + C = 0,$$

where A, B, and C are integers and $A \neq 0$.

Example 12.12. Let $\alpha = 2 + \sqrt{3}$. Then α is irrational, for if α were rational, then by Exercise 3 of Section 1.1, $\alpha - 2 = \sqrt{3}$ would be rational, contradicting Theorem 3.18. Next, note that

$$\alpha^2 - 4\alpha + 1 = (7 + 4\sqrt{3}) - 4(2 + \sqrt{3}) + 1 = 0.$$

Hence, α is a quadratic irrational. ◀

We will show that the infinite simple continued fraction of an irrational number is periodic if and only if this number is a quadratic irrational. Before we do this, we first develop some useful results about quadratic irrationals.

Lemma 12.1. The real number α is a quadratic irrational if and only if there are integers a, b, and c with $b > 0$ and $c \neq 0$, such that b is not a perfect square and

$$\alpha = (a + \sqrt{b})/c.$$

Proof. If α is a quadratic irrational, then α is irrational, and there are integers A, B, and C such that $A\alpha^2 + B\alpha + C = 0$. From the quadratic formula, we know that

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Because α is a real number, we have $B^2 - 4AC > 0$, and because α is irrational, $B^2 - 4AC$ is not a perfect square and $A \neq 0$. By either taking $a = -B, b = B^2 - 4AC$, and $c = 2A$, or $a = B, b = B^2 - 4AC$, and $c = -2A$, we have our desired representation of α.

Conversely, if

$$\alpha = (a + \sqrt{b})/c,$$

where a, b, and c are integers with $b > 0, c \neq 0$, and b not a perfect square, then by Exercise 3 of Section 1.1 and Theorem 3.18, we can easily see that α is irrational. Furthermore, we note that

$$c^2\alpha^2 - 2ac\alpha + (a^2 - b) = 0,$$

so that α is a quadratic irrational. ■

The following lemma will be used when we show that periodic simple continued fractions represent quadratic irrationals.

Lemma 12.2. If α is a quadratic irrational and if r, s, t, and u are integers, then $(r\alpha + s)/(t\alpha + u)$ is either rational or a quadratic irrational.

Proof. From Lemma 12.1, there are integers a, b, and c with $b > 0$, $c \neq 0$, and b not a perfect square, such that

$$\alpha = (a + \sqrt{b})/c.$$

Thus,

$$\begin{aligned}\frac{r\alpha + s}{t\alpha + u} &= \left[\frac{r(a+\sqrt{b})}{c} + s\right] \Big/ \left[\frac{t(a+\sqrt{b})}{c} + u\right] \\ &= \frac{(ar + cs) + r\sqrt{b}}{(at + cu) + t\sqrt{b}} \\ &= \frac{[(ar + cs) + r\sqrt{b}][(at + cu) - t\sqrt{b}]}{[(at + cu) + t\sqrt{b}][(at + cu) - t\sqrt{b}]} \\ &= \frac{[(ar + cs)(at + cu) - rtb] + [r(at + cu) - t(ar + cs)]\sqrt{b}}{(at + cu)^2 - t^2 b}.\end{aligned}$$

Hence, by Lemma 12.1, $(r\alpha + s)/(t\alpha + u)$ is a quadratic irrational, unless the coefficient of $\sqrt{b}$ is zero, which would imply that this number is rational. ∎

In our subsequent discussions of simple continued fractions of quadratic irrationals, we will use the notion of the conjugate of a quadratic irrational.

Definition. Let $\alpha = (a + \sqrt{b})/c$ be a quadratic irrational. Then the *conjugate* of α, denoted by α', is defined by $\alpha' = (a - \sqrt{b})/c$.

Lemma 12.3. If the quadratic irrational α is a root of the polynomial $Ax^2 + Bx + C = 0$, then the other root of this polynomial is α', the conjugate of α.

Proof. From the quadratic formula, we see that the two roots of $Ax^2 + Bx + C = 0$ are

$$\frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

If α is one of these roots, then α' is the other root, because the sign of $\sqrt{B^2 - 4AC}$ is reversed to obtain α' from α. ∎

The following lemma tells us how to find the conjugates of arithmetic expressions involving quadratic irrationals.

Lemma 12.4. If $\alpha_1 = (a_1 + b_1\sqrt{d})/c_1$ and $\alpha_2 = (a_2 + b_2\sqrt{d})/c_2$ are rational or quadratic irrationals, then

(i) $(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$
(ii) $(\alpha_1 + \alpha_2)' = \alpha_1' - \alpha_2'$
(iii) $(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$
(iv) $(\alpha_1/\alpha_2)' = \alpha_1'/\alpha_2'$.

The proof of (iv) will be given here; the proofs of the other parts are easier, and appear at the end of this section as problems for the reader.

Proof of (iv). Note that

$$\begin{aligned}\alpha_1/\alpha_2 &= \frac{(a_1 + b_1\sqrt{d})/c_1}{(a_2 + b_2\sqrt{d})/c_2} \\ &= \frac{c_2(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d})}{c_1(a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d})} \\ &= \frac{(c_2a_1a_2 - c_2b_1b_2d) + (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1(a_2^2 - b_2^2d)},\end{aligned}$$

whereas

$$\begin{aligned}\alpha_1'/\alpha_2' &= \frac{(a_1 - b_1\sqrt{d})/c_1}{(a_2 - b_2\sqrt{d})/c_2} \\ &= \frac{c_2(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d})}{c_1(a_2 - b_2\sqrt{d})(a_2 + b_2\sqrt{d})} \\ &= \frac{(c_2a_1a_2 - c_2b_1b_2d) - (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1(a_2^2 - b_2^2d)}.\end{aligned}$$

Hence, $(\alpha_1/\alpha_2)' = \alpha_1'/\alpha_2'$. ∎

The fundamental result about periodic simple continued fractions is called Lagrange's theorem (although part of the theorem was proved by Euler). (Note that this theorem is different from Lagrange's theorem on polynomial congruences discussed in Chapter 9. In this chapter, we do not refer to that result.) Euler proved in 1737 that a periodic infinite simple continued fraction represents a quadratic irrational. Lagrange showed in 1770 that a quadratic irrationality has a periodic continued fraction.

Theorem 12.21. ***Lagrange's Theorem.*** The infinite simple continued fraction of an irrational number is periodic if and only if this number is a quadratic irrational.

We first prove that a periodic continued fraction represents a quadratic irrational. The converse, that the simple continued fraction of a quadratic irrational is periodic, will be proved after a special algorithm for obtaining the continued fraction of a quadratic irrational is developed.

Proof. Let the simple continued fraction of α be periodic, so that

$$\alpha = [a_0; a_1, a_2, \ldots a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k}}].$$

Now, let

$$\beta = [\overline{a_N; a_{N+1}, \ldots, a_{N+k}}].$$

Then

$$\beta = [a_N; a_{N+1}, \ldots, a_{N+k}, \beta],$$

and by Theorem 12.9, it follows that

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}, \tag{12.13}$$

where p_k/q_k and p_{k-1}/q_{k-1} are convergents of $[a_N; a_{N+1}, \ldots, a_{N+k}]$. Because the simple continued fraction of β is infinite, β is irrational, and by (12.13), we have

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0,$$

so that β is a quadratic irrational. Now, note that

$$\alpha = [a_0; a_1, a_2, \ldots, a_{N-1}, \beta],$$

so that, from Theorem 12.11, we have

$$\alpha = \frac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}},$$

where p_{N-1}/q_{N-1} and p_{N-2}/q_{N-2} are convergents of $[a_0; a_1, a_2, \ldots, a_{N-1}]$. Because β is a quadratic irrational, Lemma 12.2 tells us that α is also a quadratic irrational (we know that α is irrational because it has an infinite simple continued fraction expansion). ■

The following example shows how to use the proof of Theorem 12.21 to find the quadratic irrational represented by a periodic simple continued fraction.

Example 12.13. Let $x = [3; \overline{1, 2}]$. By Theorem 12.21, we know that x is a quadratic irrational. To find the value of x, we let $x = [3; y]$, where $y = [\overline{1; 2}]$, as in the proof of Theorem 12.21. We have $y = [1; 2, y]$, so that

$$y = 1 + \frac{1}{2 + \frac{1}{y}} = \frac{3y + 1}{2y + 1}.$$

It follows that $2y^2 - 2y - 1 = 0$. Because y is positive, by the quadratic formula, we have $y = \frac{1+\sqrt{3}}{2}$. Because $x = 3 + \frac{1}{y}$, we have

$$x = 3 + \frac{2}{1+\sqrt{3}} = 3 + \frac{2-\sqrt{3}}{-2} = \frac{4+\sqrt{3}}{2}.$$ ◀

To develop an algorithm for finding the simple continued fraction of a quadratic irrational, we need the following lemma.

Lemma 12.5. If α is a quadratic irrational, then α can be written as

$$\alpha = (P + \sqrt{d})/Q,$$

where P, Q, and d are integers, $Q \neq 0$, $d > 0$, d is not a perfect square, and $Q|(d - P^2)$.

Proof. Because α is a quadratic irrational, Lemma 12.1 tells us that

$$\alpha = (a + \sqrt{b})/c,$$

where a, b, and c are integers, $b > 0$, and $c \neq 0$. We multiply both the numerator and the denominator of this expression for α by $|c|$ to obtain

$$\alpha = \frac{a|c| + \sqrt{bc^2}}{c|c|}$$

(where we have used the fact that $|c| = \sqrt{c^2}$). Now, let $P = a|c|$, $Q = c|c|$, and $d = bc^2$. Then P, Q, and d are integers, $Q \neq 0$, because $c \neq 0$, $d > 0$ (because $b > 0$). d is not a perfect square because b is not a perfect square and, finally, $Q|(d - P^2)$ because $d - P^2 = bc^2 - a^2c^2 = c^2(b - a^2) = \pm Q(b - a^2)$. ∎

We now present an algorithm for finding the simple continued fractions of quadratic irrationals.

Theorem 12.22. Let α be a quadratic irrational, so that by Lemma 12.5 there are integers P_0, Q_0, and d such that

$$\alpha = (P_0 + \sqrt{d})/Q_0,$$

where $Q_0 \neq 0$, $d > 0$, d is not a perfect square, and $Q_0|(d - P_0^2)$. Recursively define

$$\begin{aligned} \alpha_k &= (P_k + \sqrt{d})/Q_k, \\ a_k &= [\alpha_k], \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= (d - P_{k+1}^2)/Q_k, \end{aligned}$$

for $k = 0, 1, 2, \ldots$. Then, $\alpha = [a_0; a_1, a_2, \ldots]$.

Proof. Using mathematical induction, we will show that P_k and Q_k are integers with $Q_k \neq 0$ and $Q_k|(d - P_k^2)$, for $k = 0, 1, 2, \ldots$. First, note that this assertion is true for $k = 0$ from the hypotheses of the theorem. Next,, assume that P_k and Q_k are integers with $Q_k \neq 0$ and $Q_k|(d - P_k^2)$. Then,

$$P_{k+1} = a_k Q_k - P_k$$

is also an integer. Further,

$$\begin{aligned} Q_{k+1} &= (d - P_{k+1}^2)/Q_k \\ &= [d - (a_k Q_k - P_k)^2]/Q_k \\ &= (d - P_k^2)/Q_k + (2a_k P_k - a_k^2 Q_k). \end{aligned}$$

Because $Q_k|(d - P_k^2)$, by the induction hypothesis, we see that Q_{k+1} is an integer, and because d is not a perfect square, we see that $d \neq P_k^2$, so that $Q_{k+1} = (d - P_{k+1}^2)/Q_k \neq 0$. Because

$$Q_k = (d - P_{k+1}^2)/Q_{k+1},$$

we can conclude that $Q_{k+1}|(d - P_{k+1}^2)$. This finishes the inductive argument.

To demonstrate that the integers $a_0, a_1, a_2, \ldots$ are the partial quotients of the simple continued fraction of α, we use Theorem 12.15. If we can show that

$$\alpha_{k+1} = 1/(\alpha_k - a_k),$$

for $k = 0, 1, 2, \ldots$, then we know that $\alpha = [a_0; a_1, a_2, \ldots]$. Note that

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k \\
&= [\sqrt{d} - (a_k Q_k - P_k)]/Q_k \\
&= (\sqrt{d} - P_{k+1})/Q_k \\
&= (\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})/Q_k(\sqrt{d} + P_{k+1}) \\
&= (d - P_{k+1}^2)/(Q_k(\sqrt{d} + P_{k+1})) \\
&= Q_k Q_{k+1}/(Q_k(\sqrt{d} + P_{k+1})) \\
&= Q_{k+1}/(\sqrt{d} + P_{k+1}) \\
&= 1/\alpha_{k+1},
\end{aligned}$$

where we have used the defining relation for Q_{k+1} to replace $d - P_{k+1}^2$ with $Q_k Q_{k+1}$. Hence, we can conclude that $\alpha = [a_0; a_1, a_2, \ldots]$. ∎

We illustrate the use of the algorithm given in Theorem 12.22 with the following example.

Example 12.14. Let $\alpha = (3 + \sqrt{7})/2$. Using Lemma 12.5, we write

$$\alpha = (6 + \sqrt{28})/4,$$

where we set $P_0 = 6$, $Q_0 = 4$, and $d = 28$. Hence, $a_0 = [\alpha] = 2$, and

$$P_1 = 2 \cdot 4 - 6 = 2, \qquad \alpha_1 = (2 + \sqrt{28})/6,$$
$$Q_1 = (28 - 2^2)/4 = 6, \qquad a_1 = [(2 + \sqrt{28})/6] = 1,$$

$$P_2 = 1 \cdot 6 - 2 = 4, \qquad \alpha_2 = (4 + \sqrt{28})/2$$
$$Q_2 = (28 - 4^2)/6 = 2, \qquad a_2 = [(4 + \sqrt{28})/2] = 4,$$

$$P_3 = 4 \cdot 2 - 4 = 4, \qquad \alpha_3 = (4 + \sqrt{28})/6,$$
$$Q_3 = (28 - 4^2)/2 = 6 \qquad a_3 = [(4 + \sqrt{28})/6] = 1,$$

$$P_4 = 1 \cdot 6 - 4 = 2, \qquad \alpha_4 = (\sqrt{28})/4,$$
$$Q_4 = (28 - 2^2)/6 = 4, \qquad a_4 = [(2 + \sqrt{28})/4] = 1,$$

$$P_5 = 1 \cdot 4 - 2 = 2, \qquad \alpha_5 = (\sqrt{28})/6,$$
$$Q_5 = (28 - 2^2)/4 = 6, \qquad a_5 = [(2 + \sqrt{28})/6] = 1,$$

and so on, with repetition, because $P_1 = P_5$ and $Q_1 = Q_5$. Hence, we see that

$$(3 + \sqrt{7})/2 = [2; 1, 4, 1, 1, 1, 4, 1, 1, \ldots]$$
$$= [2; 1, 4, 1, 1]. \quad \blacktriangleleft$$

We now finish the proof of Lagrange's theorem by showing that the simple continued fraction expansion of a quadratic irrational is periodic.

Proof of Theorem 12.21 (continued). Let α be a quadratic irrational, so that by Lemma 12.5, we can write α as

$$\alpha = (P_0 + \sqrt{d})/Q_0.$$

Furthermore, by Theorem 12.20, we have $\alpha = [a_0; a_1, a_2, \ldots]$, where

$$\alpha_k = (P_k + \sqrt{d})/Q_k,$$
$$a_k = [\alpha_k],$$
$$P_{k+1} = a_k Q_k - P_k,$$
$$Q_{k+1} = (d - P_{k+1}^2)/Q_k,$$

for $k = 0, 1, 2, \ldots$.

Because $\alpha = [a_0; a_1, a_2, \ldots, \alpha_k]$, Theorem 12.11 tells us that

$$\alpha = (p_{k-1}\alpha_k + p_{k-2})/(q_{k-1}\alpha_k + q_{k-2}).$$

Taking conjugates of both sides of this equation, and using Lemma 12.4, we see that

$$\alpha' = (p_{k-1}\alpha_k' + p_{k-2})/(q_{k-1}\alpha_k' + q_{k-2}). \tag{12.14}$$

When we solve (12.14) for α'_k, we find that

$$\alpha'_k = \frac{-q_{k-2}}{q_{k-1}} \left(\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}} \right).$$

Note that the convergents p_{k-2}/q_{k-2} and p_{k-1}/q_{k-1} tend to α as k tends to infinity, so that

$$\left(\alpha' - \frac{p_{k-2}}{q_{k-2}}\right) \Big/ \left(\alpha' - \frac{p_{k-1}}{q_{k-1}}\right)$$

tends to 1. Hence, there is an integer N such that $\alpha'_k < 0$ for $k \geq N$. Because $\alpha_k > 0$ for $k > 1$, we have

$$\alpha_k - \alpha'_k = \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k} > 0,$$

so that $Q_k > 0$ for $k \geq N$.

Because $Q_k Q_{k+1} = d - P_{k+1}^2$, we see that for $k \geq N$,

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d.$$

Also for $k \geq N$, we have

$$P_{k+1}^2 \leq d = P_{k+1}^2 - Q_k Q_{k+1},$$

so that

$$-\sqrt{d} < P_{k+1} < \sqrt{d}.$$

From the inequalities $0 \leq Q_k \leq d$ and $-\sqrt{d} < P_{k+1} < \sqrt{d}$, which hold for $k \geq N$, we see that there are only a finite number of possible values for the pair of integers P_k, Q_k for $k > N$. Because there are infinitely many integers k with $k \geq N$, there are two integers i and j such that $P_i = P_j$ and $Q_i = Q_j$ with $i < j$. Hence, from the defining relation for α_k, we see that $\alpha_i = \alpha_j$. Consequently, we can see that $a_i = a_j, a_{i+1} = a_{j+1}, a_{i+2} = a_{j+2}, \ldots$. Hence,

$$\begin{aligned} \alpha &= [a_0; a_1, a_2, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{j-1}, a_i, a_{i+1}, \ldots, a_{j-1}, \ldots] \\ &= [a_0; a_1, a_2, \ldots, a_{i-1}, \overline{a_i, a_{i+1}, \ldots, a_{j-1}}]. \end{aligned}$$

This shows that α has a periodic simple continued fraction. ∎

Purely Periodic Continued Fractions Next, we investigate those periodic simple continued fractions that are *purely periodic*, that is, those without a pre-period.

Definition. The continued fraction $[a_0; a_1, a_2, \ldots]$ is *purely periodic* if there is an integer n such that $a_k = a_{n+k}$, for $k = 0, 1, 2, \ldots$, so that

$$[a_0; a_1, a_2, \ldots] = [\overline{a_0; a_1, a_2, a_3, \ldots, a_{n-1}}].$$

Example 12.15. The continued fraction $[\overline{2;3}] = (1+\sqrt{3})/2$ is purely periodic, whereas $[2;\overline{2,4}] = \sqrt{6}$ is not. ◀

The next definition and theorem describe those quadratic irrationals with purely periodic simple continued fractions.

Definition. A quadratic irrational α is called *reduced* if $\alpha > 1$ and $-1 < \alpha' < 0$, where α' is the conjugate of α.

Theorem 12.23. The simple continued fraction of the quadratic irrational α is purely periodic if and only if α is reduced. Further, if α is reduced and $\alpha = [\overline{a_0; a_1, a_2, \ldots, a_n}]$, then the continued fraction of $-1/\alpha'$ is $[\overline{a_n; a_{n-1}, \ldots, a_0}]$.

Proof. First, assume that α is a reduced quadratic irrational. Recall from Theorem 12.18 that the partial fractions of the simple continued fraction of α are given by

$$a_k = [\alpha_k], \quad \alpha_{k+1} = 1/(\alpha_k - a_k),$$

for $k = 0, 1, 2, \ldots$, where $\alpha_0 = \alpha$. We see that

$$1/\alpha_{k+1} = \alpha_k - a_k,$$

and by taking conjugates and using Lemma 12.4, we see that

$$1/\alpha'_{k+1} = \alpha'_k - a_k. \tag{12.15}$$

We can prove, by mathematical induction, that $-1 < \alpha'_k < 0$ for $k = 0, 1, 2, \ldots$. First, note that because $\alpha_0 = \alpha$ is reduced, $-1 < \alpha'_0 < 0$. Now, assume that $-1 < \alpha'_k < 0$. Then, because $a_k \geq 1$ for $k = 0, 1, 2, \ldots$ (note that $a_0 \geq 1$ because $\alpha > 1$), we see from (12.15) that

$$1/\alpha'_{k+1} < -1,$$

so that $-1 < \alpha'_{k+1} < 0$. Hence, $-1 < \alpha'_k < 0$ for $k = 0, 1, 2, \ldots$.

Next, note that from (12.15) we have

$$\alpha'_k = a_k + 1/\alpha'_{k+1},$$

and because $-1 < \alpha'_k < 0$, it follows that

$$-1 < a_k + 1/\alpha'_{k+1} < 0.$$

Consequently,

$$-1 - 1/\alpha'_{k+1} < a_k < -1/\alpha'_{k+1},$$

so that

$$a_k = [-1/\alpha'_{k+1}].$$

Because α is a quadratic irrational, the proof of Lagrange's theorem shows that there are nonnegative integers i and j, $i < j$, such that $\alpha_i = \alpha_j$, and hence with $-1/\alpha'_i = -1/\alpha'_j$.

Because $a_{i-1} = [-1/\alpha_i']$ and $a_{j-1} = [-1/\alpha_j']$, we see that $a_{i-1} = a_{j-1}$. Furthermore, because $\alpha_{i-1} = a_{i-1} + 1/\alpha_i$ and $\alpha_{j-1} = a_{j-1} + 1/\alpha_j$, we also see that $\alpha_{i-1} = \alpha_{j-1}$. Continuing this argument, we see that $\alpha_{i-2} = \alpha_{j-2}, \alpha_{j-3} = \alpha_{j-3}, \ldots$, and, finally, that $\alpha_0 = \alpha_{j-1}$. Because

$$\begin{aligned}\alpha_0 = \alpha &= [a_0; a_1, \ldots, a_{j-i-1}, \alpha_{j-1}] \\ &= [a_0; a_1, \ldots, a_{j-i-1}, \alpha_0] \\ &= \overline{[a_0; a_1, \ldots, a_{j-i-1}]},\end{aligned}$$

we see that the simple continued fraction of α is purely periodic.

To prove the converse, assume that α is a quadratic irrational with a purely periodic continued fraction $\alpha = \overline{[a_0; a_1, a_2, \ldots, a_k]}$. Because $\alpha = [a_0; a_1, a_2, \ldots, a_k, \alpha]$, Theorem 12.11 tells that

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}, \tag{12.16}$$

where p_{k-1}/q_{k-1} and p_k/q_k are the $(k-1)$th and kth convergents of the continued fraction expansion of α. From (12.16), we see that

$$q_k\alpha^2 + (q_{k-1} - p_k)\alpha - p_{k-1} = 0. \tag{12.17}$$

Now, let β be the quadratic irrational such that $\beta = \overline{[a_k; a_{k-1}, \ldots, a_1, a_0]}$, that is, with the period of the simple continued fraction for α reversed. Then $\beta = [a_k; a_{k-1}, \ldots, a_1, a_0, \beta]$, so that by Theorem 12.11, it follows that

$$\beta = \frac{\beta p_k' + p_{k-1}'}{\beta q_k' + q_{k-1}'}, \tag{12.18}$$

where p_{k-1}'/q_{k-1}' and p_K'/q_k' are the $(k-1)$th and kth convergents of the continued fraction expansion of β. Note, however, from Exercise 10 of Section 12.2, that

$$p_k/p_{k-1} = [a_k; a_{k-1}, \ldots, a_1, a_0] = p_k'/q_k'$$

and

$$q_k/q_{k-1} = [a_k; a_{k-1}, \ldots, a_2, a_1] = p_{k-1}'/q_{k-1}'.$$

Because p_{k-1}'/q_{k-1}' and p_k'/q_k' are convergents, we know that they are in lowest terms. Also, p_k/p_{k-1} and q_k/q_{k-1} are in lowest terms, because Theorem 12.12 tells us that $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$. Hence,

$$p_k' = p_k, \quad q_k' = p_{k-1}$$

and

$$p_{k-1}' = q_k, \quad q_{k-1}' = q_{k-1}.$$

Inserting these values into (12.18), we see that

$$\beta = \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}.$$

Therefore, we know that

$$p_{k-1}\beta^2 + (q_{k-1} - p_k)\beta - q_k = 0.$$

This imples that

$$q_k(-1/\beta)^2 + (q_{k-1} - p_k)(-1/\beta) - p_{k-1} = 0. \tag{12.19}$$

By (12.17) and (12,19), we see that the two roots of the quadratic equation

$$q_k x^2 + (q_{k-1} - p_k)x - p_{k-1} = 0$$

are α and $-1/\beta$, so that by the quadratic equation, we have $\alpha' = -1/\beta$. Because $\beta = [\overline{a_n; a_{n-1}, \ldots, a_1, a_0}]$, we see that $\beta > 1$, so that $-1 < \alpha' = -1/\beta < 0$. Hence, α is a reduced quadratic irrational.

Furthermore, note that because $\beta = -1/\alpha'$, it follows that

$$-1/\alpha' = [\overline{a_n; a_{n-1}, \ldots, a_1, a_0}].$$

■

We now find the form of the periodic simple continued fraction of $\sqrt{D}$, where D is a positive integer that is not a perfect square. Although $\sqrt{D}$ is not reduced, because its conjugate, $-\sqrt{D}$, is not between -1 and 0, the quadratic irrational $[\sqrt{D}] + \sqrt{D}$ is reduced because its conjugate, $[\sqrt{D}] - \sqrt{D}$, does lie between -1 and 0. Therefore, from Theorem 12.23, we know that the continued fraction of $[\sqrt{D}] + \sqrt{D}$ is purely periodic. Because the initial partial quotient of the simple continued fraction of $[\sqrt{D}] + \sqrt{D}$ is $[[\sqrt{D}] + \sqrt{D}] = 2[\sqrt{D}] = 2a_0$, where $a_0 = [\sqrt{D}]$, we can write

$$\begin{aligned}[\sqrt{D}] + \sqrt{D} &= [\overline{2a_0; a_1, a_2, \ldots, a_n}] \\ &= [2a_0; a_1, a_2, \ldots, a_n, 2a_0, a_1, \ldots, a_n].\end{aligned}$$

Subtracting $a_0 = \sqrt{D}$ from both sides of this equality, we find that

$$\begin{aligned}\sqrt{D} &= [a_0; a_1, a_2, \ldots, 2a_0, a_1, a_2, \ldots 2a_0, \ldots] \\ &= [a_0; \overline{a_1, a_2, \ldots, a_n, 2a_0}].\end{aligned}$$

To obtain even more information about the partial quotients of the continued fraction of $\sqrt{D}$, we note that from Theorem 12.23, the simple continued fraction expansion of $-1/([\sqrt{D}] - \sqrt{D})$ can be obtained from that for $[\sqrt{D}] + \sqrt{D}$ by reversing the period, so that

$$1/(\sqrt{D} - [\sqrt{D}]) = [\overline{a_n; a_{n-1}, \ldots, a_1, 2a_0}].$$

But also note that

$$\sqrt{D} - [\sqrt{D}] = [0; \overline{a_1, a_2, \ldots, a_n, 2a_0}],$$

so that by taking reciprocals, we find that

$$1/(\sqrt{D} - [\sqrt{D}]) = [\overline{a_1; a_2, \ldots, a_n, 2a_0}].$$

Therefore, when we equate these two expressions for the simple continued fraction of $1/(\sqrt{D} - [\sqrt{D}])$, we obtain

$$a_1 = a_n, a_2 = a_{n-1}, \ldots, a_n = a_1,$$

so that the periodic part of the continued fraction for $\sqrt{D}$ is symmetric from the first to the penultimate term.

In conclusion, we see that the simple continued fraction of $\sqrt{D}$ has the form

$$\sqrt{D} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}].$$

We illustrate this with some examples.

Example 12.16. Note that

$$\sqrt{23} = [4; \overline{1, 3, 1, 8}],$$
$$\sqrt{31} = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}],$$
$$\sqrt{46} = [6; \overline{1, 2, 1, 1, 2, 6, 2, 1, 1, 2, 1, 12}],$$
$$\sqrt{76} = [8; \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}],$$

and

$$\sqrt{97} = [9; \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}],$$

where each continued fraction has a pre-period of length 1, and a period ending with twice the first partial quotient, which is symmetric from the first to the next-to-the-last term. ◀

The simple continued fraction expansions of $\sqrt{d}$ for positive integers d such that d is not a perfect square and $d < 100$ can be found in Table 5 of Appendix D.

12.4 Exercises

1. Find the simple continued fractions of each of the following numbers.

a) $\sqrt{7}$ c) $\sqrt{23}$ e) $\sqrt{59}$
b) $\sqrt{11}$ d) $\sqrt{47}$ f) $\sqrt{94}$

2. Find the simple continued fractions of each of the following numbers.

a) $\sqrt{101}$ c) $\sqrt{107}$ e) $\sqrt{203}$
b) $\sqrt{103}$ d) $\sqrt{201}$ f) $\sqrt{209}$

3. Find the simple continued fractions of each of the following numbers.

a) $1 + \sqrt{2}$ b) $\left(2 + \sqrt{5}\right)/3$ c) $\left(5 - \sqrt{7}\right)/4$

4. Find the simple continued fractions of each of the following numbers.

a) $\left(1 + \sqrt{3}\right)/2$ b) $\left(14 + \sqrt{37}\right)/3$ c) $\left(13 - \sqrt{2}\right)/7$

5. Find the quadratic irrational with each of the following simple continued fraction expansions.

a) $[2; 1, \overline{5}]$ b) $[2; \overline{1, 5}]$ c) $[\overline{2; 1, 5}]$

6. Find the quadratic irrational with each of the following simple continued fraction expansions.

a) $[1; 2, \overline{3}]$ b) $[1; \overline{2, 3}]$ c) $[\overline{1; 2, 3}]$

7. Find the quadratic irrational with each of the following simple continued fraction expansions.

a) $[3; \overline{6}]$ b) $[4; \overline{8}]$ c) $[5; \overline{10}]$ d) $[6; \overline{12}]$

8. a) Let d be a positive integer. Show that the simple continued fraction of $\sqrt{d^2+1}$ is $[d; \overline{2d}]$.

b) Use part (a) to find the simple continued fractions of $\sqrt{101}$, $\sqrt{290}$, and $\sqrt{2210}$.

9. Let d be an integer, $d \geq 2$.

a) Show that the simple continued fraction of $\sqrt{d^2-1}$ is $[d-1; \overline{1, 2d-2}]$.

b) Show that the simple continued fraction of $\sqrt{d^2-d}$ is $[d-1; \overline{2, 2d-2}]$.

c) Use parts (a) and (b) to find the simple continued fractions of $\sqrt{99}$, $\sqrt{110}$, $\sqrt{272}$, and $\sqrt{600}$.

10. a) Show that if d is an integer, $d \geq 3$, then the simple continued fraction of $\sqrt{d^2-2}$ is $[d-1; \overline{1, d-2, 1, 2d-2}]$.

b) Show that if d is a positive integer, then the simple continued fraction of $\sqrt{d^2+2}$ is $[d; \overline{d, 2d}]$.

c) Find the simple continued fraction expansions of $\sqrt{47}$, $\sqrt{51}$, and $\sqrt{287}$.

11. Let d be an odd positive integer.

a) Show that the simple continued fraction of $\sqrt{d^2+4}$ is $[d; \overline{(d-1)/2, 1, 1, (d-1)/2, 2d}]$, if $d > 1$.

b) Show that the simple continued fraction of $\sqrt{d^2-4}$ is $[d-1; \overline{1, (d-3)/2, 2, (d-3)/2, 1, 2d-2}]$, if $d > 3$.

12. Show that the simple continued fraction of $\sqrt{d}$, where d is a positive integer, has period length one if and only if $d = a^2 + 1$, where a is a nonegative integer.

13. Show that the simple continued fraction of $\sqrt{d}$, where d is a positive integer, has period length two if and only if $d = a^2 + b$, where a and b are integers, $b > 1$, and $b|2a$.

14. Prove that if $\alpha_1 = (a_1 + b_1\sqrt{d})/c_1$ and $\alpha_2 = (a_2 + b_2\sqrt{d})/c_2$ are quadratic irrationals, then the following hold.

a) $(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$

b) $(\alpha_1 - \alpha_2)' = \alpha_1' - \alpha_2'$

c) $(\alpha_1\alpha_2)' = \alpha_1' \cdot \alpha_2'$

15. Which of the following quadratic irrationals have purely periodic continued fractions?

a) $1+\sqrt{5}$ c) $4+\sqrt{17}$ e) $(3+\sqrt{23})/2$
b) $2+\sqrt{8}$ d) $(11-\sqrt{10})/9$ f) $(17+\sqrt{188})/3$

16. Suppose that $\alpha = (a+\sqrt{b})/c$, where a, b, and c are integers, $b > 0$, and b is not a perfect square. Show that α is a reduced quadratic irrational if and only if $0 < a < \sqrt{b}$ and $\sqrt{b} - a < c < \sqrt{b} + a < 2\sqrt{b}$.

17. Show that if α is a reduced quadratic irrational, then $-1/\alpha'$ is also a reduced quadratic irrational.

* **18.** Let k be a positive integer. Show that there are not infinitely many positive integers D, such that the simple continued fraction expansion of $\sqrt{D}$ has a period of length k. (*Hint:* Let $a_1 = 2, a_2 = 5$, and for $k \geq 3$, let $a_k = 2a_{k-1} + a_{k-2}$. Show that if $D = (ta_k + 1)^2 + 2ta_{k-1} + 1$, where t is a nonnegative integer, then $\sqrt{D}$ has a period of length $k+1$.)

* **19.** Let k be a positive integer. Let $D_k = (3^k + 1)^2 + 3$. Show that the simple continued fraction of $\sqrt{D_k}$ has a period of length $6k$.

12.4 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the simple continued fraction of $\sqrt{100{,}007}$, $\sqrt{1{,}000{,}007}$, and $\sqrt{10{,}000{,}007}$.

2. Find the smallest positive integer D such that the length of the period of the simple continued fraction of $\sqrt{D}$ is 10, 100, 1000, and 10,000.

3. Find the length of the largest period of the simple continued fraction of $\sqrt{D}$, where D is a positive integer less than 1003, less than 10,000, and less than 100,000. Can you make any conjectures?

4. Look for patterns in the continued fractions of $\sqrt{D}$ for many different values of D.

Programming Projects

Write programs in Maple, *Mathematica*, or a language of your choice to do the following.

* **1.** Find the quadratic irrational that is the value of a periodic simple continued fraction.

2. Find the periodic simple continued fraction expansion of a quadratic irrational.

12.5 Factoring Using Continued Fractions

We can factor the positive integer n if we can find positive integers x and y such that $x^2 - y^2 = n$ and $x - y \neq 1$. This is the basis of the Fermat factorization method discussed in Section 3.6. However, it is possible to factor n if we can find positive integers x and y that satisfy the weaker condition

(12.20) $$x^2 \equiv y^2 \pmod{n}, \quad 0 < y < x < n, \quad \text{and} \quad x + y \neq n.$$

To see this, note that if (12.20) holds, then n divides $x^2 - y^2 = (x + y)(x - y)$, and n divides neither $x - y$ nor $x + y$. It follows that $(n, x - y)$ and $(n, x + y)$ are divisors of n that do not equal 1 or n. We can find these divisors rapidly using the Euclidean algorithm.

Example 12.17. Note that $29^2 - 17^2 = 841 - 289 = 552 \equiv 0 \pmod{69}$. Because $29^2 - 17^2 = (29 - 17)(29 + 17) \equiv 0 \pmod{69}$, both $(29 - 17, 69) = (12, 69)$ and $(29 + 17, 69) = (46, 69)$ are divisors of 69 not equal to either 1 or 69; using the Euclidean algorithm, we find that these factors are $(12, 69) = 3$ and $(46, 69) = 23$. ◀

The continued fraction expansion of $\sqrt{n}$ can be used to find solutions of the congruence $x^2 \equiv y^2 \pmod{n}$. The following theorem is the basis for this.

Theorem 12.24. Let n be a positive integer that is not a perfect square. Define $\alpha_k = (P_k + \sqrt{n})/Q_k$, $a_k = [\alpha_k]$, $P_{k+1} = a_k Q_k - P_k$, and $Q_{k+1} = (n - P_{k+1}^2)/Q_k$, for $k = 0, 1, 2, \ldots$, where $\alpha_0 = \sqrt{n}$. Furthermore, let p_k/q_k denote the kth convergent of the simple continued fraction expansion of $\sqrt{n}$. Then,

$$p_k^2 - nq_k^2 = (-1)^{k-1} Q_{k+1}.$$

The proof of Theorem 12.24 depends on the following useful lemma.

Lemma 12.6. Let $r + s\sqrt{n} = t + u\sqrt{n}$, where r, s, t, and u are rational numbers and n is a positive integer that is not a perfect square. Then, $r = t$ and $s = u$.

Proof. Because $r + s\sqrt{n} = t + u\sqrt{n}$, we see that if $s \neq u$, then

$$\sqrt{n} = \frac{r - t}{u - s}.$$

Because $(r - t)/(u - s)$ is rational and $\sqrt{n}$ is irrational, it follows that $s = u$, and consequently, that $r = t$. ∎

We can now prove Theorem 12.24.

Proof. Because $\sqrt{n} = \alpha_0 = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$, Theorem 12.9 tells us that

$$\sqrt{n} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

Because $\alpha_{k+1} = (P_{k+1} + \sqrt{n})/Q_{k+1}$, we have

$$\sqrt{n} = \frac{(P_{k+1} + \sqrt{n})\, p_k + Q_{k+1} P_{k-1}}{(P_{k+1} + \sqrt{n})\, q_k + Q_{k+1} q_{k-1}}.$$

Therefore, we see that

$$nq_k + (P_{k+1} q_k + Q_{k+1} q_{k-1})\sqrt{n} = (P_{k+1} p_k + Q_{k+1} p_{k-1}) + p_k \sqrt{n}.$$

By Lemma 12.6, we see that $nq_k = P_{k+1} p_k + Q_{k+1} p_{k-1}$ and $P_{k+1} q_k + Q_{k+1} q_{k-1} = p_k$. When we multiply the first of these two equations by q_k and the second by p_k, subtract

the first from the second, and then simplify, we obtain

$$p_k^2 - nq_k^2 = (p_k q_{k-1} - p_{k-1} q_k) Q_{k+1} = (-1)^{k-1} Q_{k+1},$$

where we have used Theorem 12.10 to complete the proof. ■

We now outline the technique known as the *continued fraction algorithm* for factoring an integer n, which was proposed by D. H. Lehmer and R. E. Powers in 1931, and further developed by J. Brillhart and M. A. Morrison in 1975 (see [LePo31] and [MoBr75] for details). Suppose that the terms p_k, q_k, Q_k, a_k, and α_k have their usual meanings in the computation of the continued fraction expansion of $\sqrt{n}$. By Theorem 12.24, it follows that for every nonnegative integer k,

$$p_k^2 \equiv (-1)^{k-1} Q_{k+1} \pmod{n},$$

where p_k and Q_{k+1} are as defined in the statement of the theorem. Now, suppose that k is odd and that Q_{k+1} is a square, that is, $Q_{k+1} = s^2$, where s is a positive integer. Then $p_k^2 \equiv s^2 \pmod{n}$, and we may be able to use this congruence of two squares modulo n to find factors of n. Summarizing, to factor n we carry out the algorithm described in Theorem 12.10 to find the continued fraction expansion of $\sqrt{n}$. We look for squares among the terms with even indices in the sequence $\{Q_k\}$. Each such occurrence may lead to a nonproper factor of n (or may just lead to the factorization $n = 1 \cdot n$). We illustrate this technique with several examples.

Example 12.18. We can factor 1037 using the continued fraction algorithm. Take $\alpha = \sqrt{1037} = (0 + \sqrt{1037})/1$ with $P_0 = 0$ and $Q_0 = 1$, and generate the terms P_k, Q_k, α_k, and a_k. We look for squares among the terms with even indices in the sequence $\{Q_k\}$. We find that $Q_1 = 13$ and $Q_2 = 49$. Because $49 = 7^2$ is a square, and the index of Q_2 is even, we examine the congruence $p_1^2 \equiv (-1)^2 Q_2 \pmod{1037}$. Computing the terms of the sequence $\{p_k\}$, we find that $p_1 = 129$. This gives the congruence $129^2 \equiv 49 \pmod{1037}$. Hence, $129^2 - 7^2 = (129 - 7)(129 + 7) \equiv 0 \pmod{1037}$. This produces the factors $(129 - 7, 1037) = (122, 1037) = 61$ and $(129 + 7, 1037) = (136, 1037) = 17$ of 1037. ◄

Example 12.19. We can use the continued fraction algorithm to find factors of 1,000,009 (we follow computations of [Ri85]). We have $Q_1 = 9$, $Q_2 = 445$, $Q_3 = 873$, and $Q_4 = 81$. Because $81 = 9^2$ is a square, we examine the congruence $p_3^2 \equiv (-1)^4 Q_4 \pmod{1{,}000{,}009}$. However, $p_3 = 2{,}000{,}009 \equiv -9 \pmod{1{,}000{,}009}$, so that $p_3 + 9$ is divisible by 1,000,009. It follows that we do not get any proper factors of 1,000,009 from this.

We continue until we reach another square in the sequence $\{Q_k\}$ with k even. This happens when $k = 18$ with $Q_{18} = 16$. Calculating p_{17} gives $p_{17} = 494{,}881$. From the congruence $p_{17}^2 \equiv (-1)^{18} Q_{18} \pmod{1{,}000{,}009}$, we have $494{,}881^2 \equiv 4^2 \pmod{1{,}000{,}009}$. It follows that $(494881 - 4, 1000009) = (494877, 1000009) = 293$ and $(494881 + 4, 1000009) = (494885, 1000009) = 3413$ are factors of 1,000,009. ◄

More powerful techniques based on continued fraction expansions are known. These are described in [Di84], [Gu75], and [WaSm87]. We describe one such generalization in the exercises.

12.5 Exercises

1. Find factors of 119 using the congruence $19^2 \equiv 2^2 \pmod{119}$.
2. Factor 1537 using the continued fraction algorithm.
3. Factor the integer 13,290,059 using the continued fraction algorithm. (*Hint:* Use a computer program to generate the integers Q_k for the continued fraction for $\sqrt{13{,}290{,}059}$. You will need more than 50 terms.)
4. Let n be a positive integer and let $p_1, p_2, \ldots,$ and p_m be primes. Suppose that there exist integers $x_1, x_2, \ldots, x_r$ such that

$$\begin{aligned} x_1^2 &\equiv (-1)^{e_{01}} p_1^{e_{11}} \cdots p_m^{e_{m1}} \pmod{n}, \\ x_2^2 &\equiv (-1)^{e_{02}} p_1^{e_{12}} \cdots p_m^{e_{m2}} \pmod{n}, \\ &\vdots \\ x_r^2 &\equiv (-1)^{e_{0r}} p_1^{e_{1r}} \cdots p_m^{e_{mr}} \pmod{n}, \end{aligned}$$

where

$$\begin{aligned} e_{01} + e_{02} + \cdots + e_{0r} &= 2e_0 \\ e_{11} + e_{12} + \cdots + e_{1r} &= 2e_1 \\ &\vdots \\ e_{m1} + e_{m2} + \cdots + e_{mr} &= 2e_m. \end{aligned}$$

Show that $x^2 \equiv y^2 \pmod{n}$, where $x = x_1 x_2 \cdots x_r$ and $y = (-1)^{e_0} p_1^{e_1} \cdots p_r^{e_r}$. Explain how to factor n using this information. Here the primes $p_1, \ldots, p_r$, together with -1, are called the *factor base.*

5. Show that 143 can be factored by setting $x_1 = 17$ and $x_2 = 19$, taking the factor base to be $\{3, 5\}$.
6. Let n be a positive integer and let $p_1, p_2, \ldots, p_r$ be primes. Suppose that $Q_{k_i} = \prod_{j=1}^{r} p_j^{k_{ij}}$ for $i = 1, \ldots, t$, where the integers Q_j have their usual meaning with respect to the continued fraction of $\sqrt{n}$. Explain how n can be factored if $\sum_{i=1}^{t} k_i$ is even and $\sum_{i=1}^{t} k_{ij}$ is even for $j = 1, 2, \ldots, r$.
7. Show that 12,007,001 can be factored using the continued fraction expansions of $\sqrt{12{,}007{,}001}$ with factor base $-1, 2, 31, 71, 97$. (*Hint:* Use the factorizations $Q_1 = 2^3 \cdot 97$, $Q_{12} = 2^4 \cdot 71$, $Q_{28} = 2^{11}$, $Q_{34} = 31 \cdot 97$, and $Q_{41} = 31 \cdot 71$, and show that $p_0 p_{11} p_{27} p_{33} p_{40} = 9{,}815{,}310$.)
8. Factor 197,209 using the continued fraction expansion of $\sqrt{197{,}209}$ and factor base 2, 3, 5.

12.5 Computational and Programming Exercises

Computations and Explorations

Using a computational program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Use the continued fraction algorithm to factor $F_7 = 2^{2^7} + 1$.

* 2. Use the continued fraction algorithm to find the prime factorization of N_{11}, where N_j is the jth term of the sequence defined by $N_1 = 2$, $N_{j+1} = p_1 p_2 \cdots p_j + 1$, where p_j is the largest prime factor of N_j. (For example, $N_2 = 3$, $N_3 = 7$, $N_4 = 43$, $N_5 = 1807$, and so on.)

Programming Projects

Write programs using Maple or *Mathematica*, or a language of your choice to do the following things.

* 1. Factor positive integers using the continued fraction algorithmn.

** 2. Factor positive integers using factor bases and continued fraction expansions (see Exercise 6).

13 Some Nonlinear Diophantine Equations

Introduction

An equation with the restriction that only integer (or sometimes rational) solutions are sought is called a diophantine equation. We have already studied a simple type of diophantine equation, namely linear diophantine equations (Section 3.6). We learned how all solutions in integers of a linear diophantine equation can be found. But what about nonlinear diophantine equations?

It is a deep theorem (beyond the scope of this text) that there is no general method for solving all nonlinear diophantine equations. However, many results have been established about particular nonlinear diophantine equations, as well as certain families of nonlinear diophantine equations. This chapter addresses several types of nonlinear diophantine equations. First, we will consider the diophantine equation $x^2 + y^2 = z^2$, satisfied by the lengths of the sides of a right triangle. We will be able to provide an explicit formula for all of its solutions in integers.

After studying the diophantine equation $x^2 + y^2 = z^2$, we will consider the famous diophantine equation $x^n + z^n = z^n$, where n is an integer greater than 2. That is, we will be interested in whether the sum of the nth powers of two integers can also be the nth power of an integer, where none of the three integers equals 0. Fermat stated that there are no solutions of this diophantine equation when $n > 2$ (a statement known as Fermat's last theorem), but for more than 350 years no one could find a proof. The first proof of this theorem was discovered by Andrew Wiles in 1995, which ended one of the greatest challenges of mathematics. The proof of Fermat's last theorem is far beyond the scope of this book, but we will be able to provide a proof for the case when $n = 4$.

Next, we will consider the problem of representing integers as the sums of squares. We will determine which integers can be written as the sum of two squares. Furthermore, we will prove that every positive integer is the sum of four squares.

Finally, we will study the diophantine equation $x^2 - dy^2 = 1$, known as Pell's equation. We will show that the solutions of this equation can be found using the simple continued fraction of $\sqrt{d}$, providing another example of the usefulness of continued fractions.

13.1 Pythagorean Triples

The Pythagorean theorem tells us that the sum of the squares of the lengths of the legs of a right triangle equals the square of the length of the hypotenuse. Conversely, any triangle for which the sum of the squares of the lengths of the two shortest sides equals the square of the third side is a right triangle. Consequently, to find all right triangles with integral side lengths, we need to find all triples of positive integers x, y, z satisfying the diophantine equation

$$x^2 + y^2 = z^2. \tag{13.1}$$

Triples of positive integers satisfying this equation are called *Pythagorean triples* after the ancient Greek mathematician *Pythagoras.*

Example 13.1. The triples 3, 4, 5; 6, 8, 10; and 5, 12, 13 are Pythagorean triples because $3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$, and $5^2 + 12^2 = 13^2$. ◀

Unlike most nonlinear diophantine equations, it is possible to explicitly describe all the integral solutions of (13.1). Before developing the result describing all Pythagorean triples, we need a definition.

Definition. A Pythagorean triple x, y, z is called *primitive* if $(x, y, z) = 1$.

PYTHAGORAS (c. 572–c. 500 B.C.E.) was born on the Greek island of Samos. After extensive travels and studies, Pythagoras founded his famous school at the Greek port of Crotona, in what is now southern Italy. Besides being an academy devoted to the study of mathematics, philosophy, and science, the school was the site of a brotherhood sharing secret rites. The Pythagoreans, as the members of this brotherhood were called, published nothing and ascribed all their discoveries to Pythagoras himself. However, it is believed that Pythagoras himself discovered what is now called the Pythagorean theorem, namely that $a^2 + b^2 = c^2$, where a, b, and c are the lengths of the two legs and of the hypotenuse of a right triangle, respectively. The Pythagoreans believed that the key to understanding the world lay with natural numbers and form. Their central tenet was "Everything is Number." Because of their fascination with the natural numbers, the Pythagoreans made many discoveries in number theory. In particular, they studied perfect numbers and amicable numbers for the mystical properties they felt these numbers possessed.

Example 13.2. The Pythagorean triples 3, 4, 5 and 5, 12, 13 are primitive, whereas the Pythagorean triple 6, 8, 10 is not. ◀

Let x, y, z be a Pythagorean triple with $(x, y, z) = d$. Then there are integers x_1, y_1, z_1 with $x = dx_1$, $y = dy_1$, $z = dz_1$, and $(x_1, y_1, z_1) = 1$. Furthermore, because

$$x^2 + y^2 = z^2$$

we have

$$(x/d)^2 + (y/d)^2 = (z/d)^2,$$

so that

$$x_1^2 + y_1^2 = z_1^2.$$

Hence, x_1, y_1, z_1 is a primitive Pythagorean triple, and the original triple x, y, z is simply an integral multiple of this primitive Pythagorean triple.

Also note that any integral multiple of a primitive (or for that matter any) Pythagorean triple is again a Pythagorean triple. If x_1, y_1, z_1 is a primitive Pythagorean triple, then we have

$$x_1^2 + y_1^2 = z_1^2,$$

and hence,

$$(dx_1)^2 + (dy_1)^2 = (dz_1)^2,$$

so that dx_1, dy_1, dz_1, is a Pythagorean triple.

Consequently, all Pythagorean triples can be found by forming integral multiples of primitive Pythagorean triples. To find all primitive Pythagorean triples, we need some lemmas. The first lemma tells us that any two integers of a primitive Pythagorean triple are relatively prime.

Lemma 13.1. If x, y, z is a primitive Pythagorean triple, then $(x, y) = (x, z) = (y, z) = 1$.

Proof. Suppose that x, y, z is a primitive Pythagorean triple and $(x, y) > 1$. Then, there is a prime p such that $p \mid (x, y)$, so that $p \mid x$ and $p \mid y$. Because $p \mid x$ and $p \mid y$, we know that $p \mid (x^2 + y^2) = z^2$. Because $p \mid z^2$, we can conclude that $p \mid z$. This is a contradiction, because $(x, y, z) = 1$. Therefore, $(x, y) = 1$. In a similar manner we can easily show that $(x, z) = (y, z) = 1$. ■

Next, we establish a lemma about the parity of the integers of a primitive Pythagorean triple.

Lemma 13.2. If x, y, z is a primitive Pythagorean triple, then x is even and y is odd or x is odd and y is even.

Proof. Let x, y, z be a primitive Pythagorean triple. By Lemma 13.1, we know that $(x, y) = 1$, so that x and y cannot both be even. Also x and y cannot both be odd. If x and y were both odd, then we would have

$$x^2 \equiv y^2 \equiv 1 \pmod 4,$$

so that

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

This is impossible. Therefore, x is even and y is odd, or vice versa. ∎

The final lemma that we need is a consequence of the fundamental theorem of arithmetic. It tells us that two relatively prime integers that multiply together to give a square must both be squares.

Lemma 13.3. If r, s, and t are positive integers such that $(r, s) = 1$ and $rs = t^2$, then there are integers m and n such that $r = m^2$ and $s = n^2$.

Proof. If $r = 1$ or $s = 1$, then the lemma is obviously true, so we may suppose that $r > 1$ and $s > 1$. Let the prime-power factorizations of r, s, and t be

$$r = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u},$$
$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v},$$

and

$$t = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}.$$

Because $(r, s) = 1$, the primes occurring in the factorizations of r and s are distinct. Because $rs = t^2$, we have

$$p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \cdots q_k^{2b_k}.$$

From the fundamental theorem of arithmetic, the prime-powers occurring on the two sides of the above equation are the same. Hence, each p_i must be equal to q_j for some j with matching exponents, so that $a_i = 2b_j$. Consequently, every exponent a_i is even, and therefore $a_i/2$ is an integer. We see that $r = m^2$ and $s = n^2$, where m and n are the integers

$$m = p_1^{a_1/2} p_2^{a_2/2} \cdots p_u^{a_u/2}$$

and

$$n = p_{u+1}^{a_{u+1}/2} p_{u+2}^{a_{u+2}/2} \cdots p_v^{a_v/2}.$$ ∎

We can now prove the desired result that describes all primitive Pythagorean triples.

Theorem 13.1. The positive integers x, y, z form a primitive Pythagorean triple, with y even, if and only if there are relatively prime positive integers m and n, $m > n$, with

m odd and n even or m even and n odd, such that

$$x = m^2 - n^2,$$
$$y = 2mn,$$
$$z = m^2 + n^2.$$

Proof. Let x, y, z be a primitive Pythagorean triple. We will show that there are integers m and n as specified in the statement of the theorem. Lemma 13.2 tells us that x is odd and y is even, or vice versa. Because we have assumed that y is even, x and z are both odd. Hence, $z + x$ and $z - x$ are both even, so that there are positive integers r and s with $r = (z + x)/2$ and $s = (z - x)/2$.

Because $x^2 + y^2 = z^2$, we have $y^2 = z^2 - x^2 = (z + x)(z - x)$. Hence,

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = rs.$$

We note that $(r, s) = 1$. To see this, let $(r, s) = d$. Because $d \mid r$ and $d \mid s$, $d \mid (r + s) = z$ and $d \mid (r - s) = x$. This means that $d \mid (x, z) = 1$, so that $d = 1$.

Using Lemma 13.3, we see that there are positive integers m and n such that $r = m^2$ and $s = n^2$. Writing x, y, and z in terms of m and n, we have

$$x = r - s = m^2 - n^2,$$
$$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn,$$
$$z = r + s = m^2 + n^2.$$

We also see that $(m, n) = 1$, because any common divisor of m and n must also divide $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$, and we know that $(x, y, z) = 1$. We also note that m and n cannot both be odd, for if they were, then x, y, and z would all be even, contradicting the condition $(x, y, z) = 1$. Because $(m, n) = 1$ and m and n cannot both be odd, we see that m is even and n is odd, or vice versa. This shows that every primitive Pythagorean triple has the appropriate form.

To complete the proof, we must show that every triple

$$x = m^2 - n^2,$$
$$y = 2mn,$$
$$z = m^2 + n^2,$$

where m and n are positive integers $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod 2$, forms a primitive Pythagorean triple. First note that $m^2 - n^2, 2mn, m^2 + n^2$ forms a Pythagorean triple since

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2 \\ &= z^2. \end{aligned}$$

To see that this triple forms a primitive Pythagorean triple, we must show that these values of x, y, and z are mutually relatively prime. Assume for the sake of contradiction that $(x, y, z) = d > 1$. Then, there is a prime $p \mid (x, y, z)$. We note that $p \neq 2$, because x is odd (because $x = m^2 - n^2$, where m^2 and n^2 have opposite parity). Also, note that because $p \mid x$ and $p \mid z$, $p \mid (z + x) = 2m^2$ and $p \mid (z - x) = 2n^2$. Hence, $p \mid m$ and $p \mid n$, contradicting the fact that $(m, n) = 1$. Therefore, $(x, y, z) = 1$, and x, y, z is a primitive Pythagorean triple, concluding the proof. ■

The following example illustrates the use of Theorem 13.1 to produce a Pythagorean triple.

Example 13.3. Let $m = 5$ and $n = 2$, so that $(m, n) = 1$, $m \not\equiv n \pmod 2$, and $m > n$. Hence, Theorem 13.1 tells us that

$$\begin{aligned} x &= m^2 - n^2 = 5^2 - 2^2 = 21, \\ y &= 2mn = 2 \cdot 5 \cdot 2 = 20, \\ z &= m^2 + n^2 = 5^2 + 2^2 = 29 \end{aligned}$$

is a primitive Pythagorean triple. ◀

We list the primitive Pythagorean triple generated using Theorem 13.1 with $m \leq 6$ in Table 13.1.

m	n	$x = m^2 - n^2$	$y = 2mn$	$z = m^2 + n^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Table 13.1 *Some primitive Pythagorean triples.*

13.1 Exercises

1. a) Find all primitive Pythagorean triples x, y, z with $z \leq 40$.
   b) Find all Pythagorean triples x, y, z with $z \leq 40$.
2. Show that if x, y, z is a primitive Pythagorean triple, then either x or y is divisible by 3.
3. Show that if x, y, z is a primitive Pythagorean triple, then exactly one of x, y, and z is divisible by 5.

4. Show that if x, y, z is a primitive Pythagorean triple, then at least one of x, y, and z is divisible by 4.

5. Show that every positive integer greater than 2 is part of at least one Pythagorean triple.

6. Let $x_1 = 3, y_1 = 4, z_1 = 5$, and let x_n, y_n, z_n, for $n = 2, 3, 4, \ldots$, be defined recursively by

$$x_{n+1} = 3x_n + 2z_n + 1,$$
$$y_{n+1} = 3x_n + 2z_n + 2,$$
$$z_{n+1} = 4x_n + 3z_n + 2.$$

Show that x_n, y_n, z_n is a Pythagorean triple.

7. Show that if x, y, z is a Pythagorean triple with $y = x + 1$, then x, y, z is one of the Pythagorean triples given in Exercise 6.

8. Find all solutions in positive integers of the diophantine equation $x^2 + 2y^2 = z^2$.

9. Find all solutions in positive integers of the diophantine equation $x^2 + 3y^2 = z^2$.

* 10. Find all solutions in positive integers of the diophantine equation $w^2 + x^2 + y^2 = z^2$.

11. Find all Pythagorean triples containing the integer 12.

12. Find formulas for the integers of all Pythagorean triples x, y, z with $z = y + 1$.

13. Find formulas for the integers of all Pythagorean triples x, y, z with $z = y + 2$.

* 14. Show that the number of Pythagorean triples x, y, z (with $x^2 + y^2 = z^2$) with a fixed integer x is $(\tau(x^2) - 1)/2$ if x is odd, and $(\tau(x^2/4) - 1)/2$ if x is even.

* 15. Find all solutions in positive integers of the diophantine equation $x^2 + py^2 = z^2$, where p is a prime.

16. Find all solutions in positive integers of the diophantine equation $1/x^2 + 1/y^2 = 1/z^2$.

17. Show that $f_n f_{n+3}$, $2f_{n+1}f_{n+2}$, and $f_{n+1}^2 + f_{n+2}^2$ form a Pythagorean triple, where f_k denotes the kth Fibonacci number.

18. Find the length of the sides of all right triangles, where the sides have integer lengths and the area equals the perimeter.

13.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Find as many Pythagorean triples x, y, z as you can, where each of x, y, and z is 1 less than the square of an integer. Do you think that there are infinitely many such triples?

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Find all Pythagorean triples x, y, z with x, y, and z less than a given bound.

2. Find all Pythagorean triples containing a given integer.

13.2 Fermat's Last Theorem

In the previous section, we showed that the diophantine equation $x^2 + y^2 = z^2$ has infinitely many solutions in nonzero integers x, y, z. What happens when we replace the exponent 2 in this equation with an integer greater than 2? Next to the discussion of the equation $x^2 + y^2 = z^2$ in his copy of the works of Diophantus, Fermat wrote in the margin:

"However, it is impossible to write a cube as the sum of two cubes, a fourth power as the sum of two fourth powers and in general any power as the sum of two similar powers. For this I have discovered a truly wonderful proof, but the margin is too small to contain it."

Fermat did have a proof of this theorem for the special case of $n = 4$. We will present a proof for this case, using his basic methods, later in this section. Although we will never know for certain whether Fermat had a proof of this result for all integers $n > 2$, mathematicians believe it is extremely unlikely that he did. By 1800, all other statements that he made in the margins of his copy of the works of Diophantus were resolved; some were proved and some were shown to be false. Nevertheless, the following theorem is called *Fermat's last theorem.*

Theorem 13.2. ***Fermat's Last Theorem.*** The diophantine equation

$$x^n + y^n = z^n$$

has no solutions in nonzero integers x, y, and z when n is an integer with $n \geq 3$.

Note that if we could show that the diophantine equation

$$x^p + y^p = z^p$$

has no solution in nonzero integers x, y, and z whenever p is an odd prime, we would know that Fermat's last theorem is true (see Exercise 2 at the end of this section).

The quest for a proof of Fermat's last theorem challenged mathematicians for more than 350 years. Many great mathematicians have worked on this problem without ultimate success. However, a long series of interesting partial results was established, and new areas of number theory were born as mathematicians attempted to solve this problem. The first major development was Euler's proof in 1770 of Fermat's last theorem for the case $n = 3$. (That is, he showed that there are no solutions of the equation $x^3 + y^3 = z^3$ in nonzero integers.) Euler's proof contained an important error, but Legendre managed to fill in the gap soon afterward.

In 1805, French mathematician *Sophie Germain* proved a general result about Fermat's last theorem, as opposed to a proof for a particular value of the exponent n. She showed that if p and $2p + 1$ are both primes, then $x^p + y^p = z^p$ has no solutions in integers x, y, and z, with $xyz \neq 0$ when $p \nmid xyz$. As a special case, she showed that if $x^5 + y^5 = z^5$, then one of the integers x, y, and z must be divisible by 5. In 1825, both Dirichlet and Legendre, in independent work, completed the proof of the case when $n = 5$, using the method of infinite descent used by Fermat to prove the $n = 4$ case (and

which we will demonstrate later in this section). Fourteen years later, the case of $n = 7$ was settled by Lamé, also using a proof by infinite descent.

In the mid-nineteenth century, mathematicians took some new approaches in attempts to prove Fermat's last theorem for all exponents n. The greatest success in this direction was made by the German mathematician *Ernst Kummer.* He realized that a potentially promising approach, based on the assumption that unique factorization into primes held for certain sets of algebraic integers, was doomed to failure. To overcome this

SOPHIE GERMAIN (1776–1831) was born in Paris and educated at home, using her father's extensive library as a resource. She decided as a young teenager to study mathematics when she discovered that Archimedes was murdered by the Romans. She started by reading the works of Euler and Newton. Although Germain did not attend classes, she learned from university course notes that she managed to obtain. After reading the notes from Lagrange's lectures, she sent him a letter under the pseudonym M. Leblanc. Lagrange, impressed with the insights displayed in this letter, decided to meet M. Leblanc; he was surprised to find that its author was a young woman. Germain corresponded under the pseudonym M. LeBlanc with many mathematicians, including Legrende who included many of her discoveries in his book *Theorie des Nombres.* She also made important contributions to the mathematical theories of elasticity and acoustics. Gauss was impressed by her work and recommended that she receive a doctorate from the University of Göttingen. Unfortunately, she died just before she was to receive this degree.

ERNST EDUARD KUMMER (1810–1893) was born in Sorau, Prussia (now Germany). His father, a physician, died in 1813. Kummer received private tutoring before entering the Gymnasium in Sorau in 1819. In 1828, he entered the University of Halle to study theology; his training for philosophy included the study of mathematics. Inspired by his mathematics instructor H. F. Scherk, he switched to mathematics as his major field of study. Kummer was awarded a doctorate from the University of Halle in 1831, and began teaching at the Gymnasium in Sorau, his old school, that same year. The following year he took a similar position teaching at the Gymnasium in Liegnitz (now the Polish city of Legnica), holding the post for ten years. His research on topics in function theory, including extensions of Gauss's work on hypergeometric series, attracted the attention of leading German mathematicians. They worked to find him a university position.

In 1842, Kummer was appointed to a position at the University of Breslau (now Wroclaw, Poland) and began working on number theory. In 1843, in an attempt to prove Fermat's last theorem, he introduced the concept of "ideal numbers." Although this did not lead to a proof of Fermat's last theorem, Kummer's ideas led to the development of new areas of abstract algebra and the new subject of algebraic number theory. In 1855, he moved to the University of Berlin where he remained until his retirement in 1883.

Kummer was a popular instructor. He was noted for the clarity of his lectures as well as his sense of humor and concern for his students. He was married twice. His first wife, the cousin of Dirichlet's wife, died in 1848, eight years after she and Kummer were married.

difficulty, Kummer developed a theory that supported unique factorization into primes. His basic idea was the concept of "ideal numbers." Using this concept, Kummer could prove Fermat's last theorem for a large class of primes called regular primes. Although there are primes, and perhaps infinitely many primes, that are irregular, Kummer's work showed that Fermat's last theorem was true for many values of n. In particular, Kummer's work showed that Fermat's last theorem was true for all prime exponents less than 100 other than 37, 59, and 67, since these are the only primes less than 100 that are irregular. Kummer's introduction of "ideal numbers" gave birth to the subject of algebraic number theory, which blossomed into a major field of study, and to the part of abstract algebra known as ring theory. The exponents Kummer's work did not address—37, 59, 67, and other relatively irregular primes—fell to a variety of more powerful techniques in subsequent years.

In 1986, German mathematician Gerhard Frey made the first connection of Fermat's last theorem to the subject of elliptic curves. His work surprised mathematicians by linking two seemingly unrelated areas. Frey also managed to show (in 1983) that $x^n + y^n = z^n$ can have only a finite number of solutions in nonzero integers. Of course, if this finite number was shown to be zero for $n \geq 3$, Fermat's last theorem would be proved.

Computers were used to run several different numerical tests that could verify that Fermat's last theorem was true for particular values of n. By 1977, Sam Wagstaff used such tests (and several years of computer time) to verify that Fermat's last theorem held for all exponents n with $n \leq 125{,}000$. By 1993, such tests had been used to verify that Fermat's last theorem was true for all exponents n with $n < 4 \cdot 10^6$. However, at that time, no proof of Fermat's last theorem seemed to be in sight.

Then, in 1993, *Andrew Wiles,* a professor at Princeton University, shocked the mathematical world when he showed that he could prove Fermat's last theorem. He did this in a series of lectures in Cambridge, England. He had given no hint that the subject of his lectures was a proof of this notorious theorem. The proof he outlined was the culmination of seven years of solitary work. It used a vast array of highly sophisticated

ANDREW WILES (b. 1953) became interested in Fermat's last theorem at the age of 10 when, during a visit to his local library, he found a book stating the problem. He was struck that though it looked simple, none of the great mathematicians could solve it, and he knew that he would never let this problem go. In 1971, Wiles entered Merton College, Oxford. He graduated with his B.A. in 1974, and entered Clare College, Cambridge, where he pursued his doctorate, working on the theory of elliptic curves under John Coates. He was a Research Fellow at Clare College and a Benjamin Pierce Assistant Professor at Harvard from 1977 until 1980. In 1981, he held a post at the Institute for Advanced Study in Princeton, and in 1982 he was appointed to a professorship at Princeton University. He was awarded a Guggenheim Fellowship in 1985, and spent a year studying at the Institut des Hautes Études Scientifique and the École Normale Supérieure in Paris. Ironically, he did not realize that during his years of work in the field of elliptic curves he was learning techniques that would someday help him solve the problem that obsessed him.

Wiles's Seven-Year Quest

In 1986, Wiles learned of work by Frey and Ribet that showed that Fermat's last theorem follows from a conjecture in the theory of elliptic curves, known as the Shimura-Taniyama conjecture. Realizing that this led to a possible strategy for proving the theorem, he abandoned his ongoing research and devoted himself entirely to working on Fermat's last theorem.

During the first few years of this work he talked to colleagues about his progress. However, he decided that talking to others generated too much interest and was too distracting. During his seven years of concentrated, solitary work on Fermat's last theorem he decided that he only had time for "his problem" and his family. His best way to relax during time away from his work was to spend time with his young children.

In 1993, Wiles revealed to several colleagues that he was close to a proof of Fermat's last theorem. After filling what he thought were the remaining gaps, he presented an outline of his proof at Cambridge. Although there had been false alarms in the past about promising proofs of Fermat's last theorem, mathematicians generally believed Wiles had a valid proof. However, a subtle but serious error in reasoning was found when he wrote up his results for publication. Wiles worked diligently, with the help of a former student, for more than a year, almost giving up in frustration, before he found a way to fill the gap.

Wiles's success has brought him countless awards and accolades. It has also brought him peace of mind. He has said that "having solved this problem there's certainly a sense of loss, but at the same time there is this tremendous sense of freedom. I was so obsessed by this problem that for eight years I was thinking about it all the time—when I woke up in the morning to when I went to sleep at night. That particular odyssey is now over. My mind is at rest."

The Wolfskehl Prize

There was added incentive besides fame to prove Fermat's last theorem. In 1908, the German industrialist Paul Wolfskehl bequeathed a prize of 100,000 marks to the Göttingen Academy of Sciences, to be awarded to the first person to publish a proof of Fermat's last theorem. Unfortunately, thousands of incorrect proofs were published in a vain attempt to win the prize, with more than 1000 published, usually as privately printed pamphlets, between 1908 and 1912 alone. (Many people, often without serious mathematical training and sometimes without a clear notion of what a correct proof is, attempt to solve famous problems such as this one even if no prize is available.) Even though Wiles's proof was acclaimed to be correct, it took two years for the Göttingen Academy of Sciences to award the Wolfskehl prize to Wiles; they wanted to be certain the proof was really correct.

Contrary to rumors that the prize had been reduced by inflation to almost nothing, maybe even a pfennig (a German penny), Wiles received approximately $50,000. The prize of 100,000 marks, originally worth around $1,500,000, had been reduced to approximately $500,000 after World War I by German hyperinflation, and the introduction of the deutsche mark after World War II further reduced its value. Many people have speculated about why Wolfskehl left such a large prize for a proof of Fermat's last theorem. People with a romantic slant enjoyed the rumor that, suicidal after being jilted by his true love, he had regained his will to live when he found out about Fermat's last theorem. However, more realistic biographical research indicates that he donated the money to spite his wife, Marie, whom he was forced to marry by his family. He did not want his fortune going to her after he died, so instead it went to the first person who could prove Fermat's last theorem.

methods related to the theory of elliptic curves. Knowledgeable mathematicians were impressed with Wiles's arguments. Word began to spread that Fermat's last theorem had finally been proved. However, when Wiles's 200-page manuscript was studied carefully, a serious problem was found. Although it appeared for a time that it might not be possible to fill the gap in the proof, more than a year later, Wiles (with the help of R. Taylor) managed to fill in the remaining portions of the proof. In 1995, Wiles published his revised proof of Fermat's last theorem, now only 125 pages long. This version passed careful review. Wiles's 1995 proof marked the end of the more than 350-year search for a proof of Fermat's last theorem.

Wiles's proof of Fermat's last theorem is one of those rare mathematical discoveries covered by the popular media. An excellent NOVA episode about this discovery was produced by PBS (information on this show can be found at the PBS Web site). Another source of general information about the proof is *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem* by Simon Singh ([Si97)]. A thorough treatment of the proof, including the mathematics of elliptic curves used in it, can be found in [CoSiSt97]. The original proof by Wiles was published in the *Annals of Mathematics* in 1995 ([Wi95]).

Readers interested in learning more about the history of Fermat's last theorem, and how investigations relating to this conjecture led to the genesis of the theory of algebraic numbers, are encouraged to consult [Ed96], [Ri79], and [Va96].

The Proof for $n = 4$

The proof we will give for the case when $n = 4$ uses the *method of infinite descent* devised by Fermat. This method is an offshoot of the well-ordering property, and shows that a diophantine equation has no solutions by showing that for every solution there is a "smaller" solution, contradicting the well-ordering property.

Using the method of infinite descent, we will show that the diophantine equation $x^4 + y^4 = z^2$ has no solutions in nonzero integers x, y, and z. This is stronger than showing Fermat's last theorem is true for $n = 4$, because any $x^4 + y^4 = z^4 = (z^2)^2$ gives a solution of $x^4 + y^4 = z^2$.

Theorem 13.3. The diophantine equation

$$x^4 + y^4 = z^2$$

has no solutions in nonzero integers x, y, and z.

Proof. Assume that this equation has a solution in nonzero integers x, y, and z. Because we may replace any number of the variables with their negatives without changing the validity of the equation, we may assume that x, y, and z are positive integers.

We may also suppose that $(x, y) = 1$. To see this, let $(x, y) = d$. Then $x = dx_1$ and $y = dy_1$, with $(x_1, y_1) = 1$, where x_1 and y_1 are positive integers. Because $x^4 + y^4 = z^2$,

we have

$$(dx_1)^4 + (dy_1)^4 = z^2,$$

so that

$$d^4(x_1^4 + y_1^4) = z^2.$$

Hence, $d^4 \mid z^2$ and, by Exercise 43 of Section 3.5, we know that $d^2 \mid z$. Therefore, $z = d^2 z_1$, where z_1 is a positive integer. Thus,

$$d^4(x_1^4 + y_1^4) = (d^2 z_1)^2 = d^4 z_1^2,$$

so that

$$x_1^4 + y_1^4 = z_1^4.$$

This gives a solution of $x^4 + y^4 = z^2$ in positive integers $x = x_1$, $y = y_1$, and $z = z_1$ with $(x_1, y_1) = 1$.

So suppose that $x = x_0$, $y = y_0$, and $z = z_0$ is a solution of $x^4 + y^4 = z^2$, where x_0, y_0, and z_0 are positive integers with $(x_0, y_0) = 1$. We will show that there is another solution in positive integers $x = x_1$, $y = y_1$, and $z = z_1$ with $(x_1, y_1) = 1$, such that $z_1 < z_0$.

Because $x_0^4 + y_0^4 = z_0^2$, we have

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2,$$

so that x_0^2, y_0^2, z_0 is a Pythagorean triple. Furthermore, we have $(x_0^2, y_0^2) = 1$, for if p is a prime such that $p \mid x_0^2$ and $p \mid y_0^2$, then $p \mid x_0$ and $p \mid y_0$, contradicting the fact that $(x_0, y_0) = 1$. Hence, x_0^2, y_0^2, z_0 is a primitive Pythagorean triple, and by Theorem 13.1, we know that there are positive integers m and n with $(m, n) = 1$, $m \not\equiv n \pmod 2$, and

$$x_0^2 = m^2 - n^2,$$
$$y_0^2 = 2mn,$$
$$z_0 = m^2 + n^2,$$

where we have interchanged x_0^2 and y_0^2, if necessary, to make y_0^2 the even integer of this part.

From the equation for x_0^2, we see that

$$x_0^2 + n^2 = m^2.$$

Because $(m, n) = 1$, it follows that x_0, n, m is a primitive Pythagorean triple, m is odd, and n is even. Again, using Theorem 13.1, we see that there are positive integers r and s with $(r, s) = 1$, $r \not\equiv s \pmod 2$, and

$$x_0 = r^2 - s^2,$$
$$n = 2rs,$$
$$m = r^2 + s^2.$$

Because m is odd and $(m, n) = 1$, we know that $(m, 2n) = 1$. We note that because $y_0^2 = (2n)m$, Lemma 13.3 tells us that there are positive integers z_1 and w with $m = z_1^2$ and $2n = w^2$. Because w is even, $w = 2v$, where v is a positive integer, so that

$$v^2 = n/2 = rs.$$

Because $(r, s) = 1$, Lemma 13.3 tells us that there are positive integers x_1 and y_1 such that $r = x_1^2$ and $s = y_1^2$. Note that because $(r, s) = 1$, it easily follows that $(x_1, y_1) = 1$. Hence,

$$x_1^4 + y_1^4 = r^2 + s^2 = m = z_1^2,$$

where x_1, y_1, z_1 are positive integers with $(x_1, y_1) = 1$. Moreover, we have $z_1 < z_0$, because

$$z_1 \leq z_1^4 = m^2 < m^2 + n^2 = z_0.$$

To complete the proof, assume that $x^4 + y^4 = z^2$ has at least one integral solution. By the well-ordering property, we know that among the solutions in positive integers, there is a solution with the smallest value z_0 of the variable z. However, we have shown that from this solution we can find another solution with a smaller value of the variable z, leading to a contradiction. This completes the proof by the method of infinite descent. ■

Conjectures About Some Diophantine Equations

The resolution of a longstanding conjecture in mathematics often leads to new conjectures, and this certainly is the case for Fermat's last theorem. For example, Andrew Beal, a banker and amateur mathematician, conjectured that a generalized version of Fermat's last theorem is true, where the exponents on the three terms in the equation $x^n + y^n = z^n$ are allowed to be different.

Beal's Conjecture The equation $x^a + y^b = z^c$ has no solutions in positive integers x, y, z, a, b, c, where $a \geq 3$, $b \geq 3$, and $c \geq 3$ and $(x, y) = (y, z) = (x, z) = 1$.

Beal's conjecture has not been solved. To generate interest in his conjecture, Andrew Beal has offered a prize of $100,000 for a proof or a counterexample.

The proof of Fermat's last theorem in the 1990s settled what was the best-known conjecture related to diophantine equations. Surprisingly, in 2002, another well-known, longstanding conjecture about diophantine equations was also settled. In 1844, the Belgian mathematician Eugene Catalan conjectured that the only consecutive positive integers that are both powers (squares, cubes, or higher powers) of integers are $8 = 2^3$ and $9 = 3^2$. In other words, he made the following conjecture.

The Catalan Conjecture The diophantine equation

$$x^m - y^n = 1$$

has no solutions in positive integers x, y, m, and n, where $m \geq 2$ and $n \geq 2$, other than $x = 3$, $y = 2$, and $m = 2$, and $n = 3$.

Certain cases of the Catalan conjecture have been settled since the fourteenth century when Levi ben Gerson proved that 8 and 9 were the only consecutive integers that are powers of 2 and 3. That is, he showed that if $3^n - 2^m \neq \pm 1$, where m and n are positive integers with $m \geq 2$ and $n \geq 2$, then $m = 3$ and $n = 2$. In the eighteenth century, Euler used the method of infinite descent to prove that the only consecutive cube and square are 8 and 9. That is, he proved that the only solution of the diophantine equation $x^3 - y^2 = \pm 1$ is $x = 2$ and $y = 3$. Additional progress was made during the nineteenth and early twentieth centuries, and in 1976, R. Tijdeman showed that the Catalan equation had at most a finite number of solutions. It was not until 2002 that the Catalan conjecture was settled, when Preda Mihailescu finally proved that this conjecture is correct.

A new conjecture has been formulated which attempts to unify Fermat's last theorem and Mihailescu's theorem proving the Catalan conjecture.

Fermat-Catalan Conjecture The equation $x^a + y^b = z^c$ has at most finitely many solutions if $(x, y) = (y, z) = (x, z) = 1$ and $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$.

The Fermat-Catalan conjecture remains open. At the present time, ten solutions of this diophantine equation are known that satisfy the hypotheses. They are:

$$1 + 2^3 = 3^2,$$
$$2^5 + 7^2 = 3^4,$$
$$7^3 + 13^2 = 2^9,$$
$$2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2,$$
$$17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2,$$
$$33^8 + 1549034^2 = 15613^3.$$

The abc Conjecture

In 1985, Joseph Oesterlé and David Masser formulated a conjecture that intrigues many mathematicians. If true, their conjecture could be used to resolve questions about many well-known diophantine equations. Before stating the conjecture we need to introduce some notation.

Definition. If n is a positive integer, then $\text{rad}(n)$ is the product of the distinct prime factors of n. Note that $\text{rad}(n)$ is also called the *squarefree* part of n because it can be obtained by eliminating all the factors that produce squares from the prime factorization of n.

Example 13.4. If $n = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 11$, then $\text{rad}(n) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. ◀

We can now state the conjecture.

abc Conjecture For every real number $\epsilon > 0$ there exists a constant $K(\epsilon)$ such that if a, b, and c are integers such that $a + b = c$ and $(a, b) = 1$, then

$$\max(|a|, |b|, |c|) < K(\epsilon)(\text{rad}(abc))^{1+\epsilon}.$$

Many deep results have been shown to be consequences of this conjecture. It would take us too far afield to develop the background and motivation for the abc conjecture. To learn about the origins of the conjecture and its consequences, see [GrTu02] and [Ma00]. In the following example we will show how the abc conjecture can be used to prove a result related to Fermat's last theorem.

Example 13.5. We can apply the abc conjecture to obtain a partial solution of Fermat's last theorem. We follow an argument of Granville and Tucker [GrTu02]. Suppose that

$$x^n + y^n = z^n,$$

where x, y, and z are pairwise relatively prime integers. Let $a = x^n$, $b = y^n$, and $c = z^n$. We can estimate $\text{rad}(abc) = \text{rad}(x^n y^n z^n)$ by noting that

$$\text{rad}(x^n y^n z^n) = \text{rad}(xyz) \leq xyz < z^3.$$

The equality $\text{rad}(x^n y^n z^n) = \text{rad}(xyz)$ holds because the primes dividing $x^n y^n z^n$ are the same as the primes dividing xyz. The first inequality follows because $\text{rad}(m) \leq m$ for

LEVI BEN GERSON (1288–1344), born at Bagnols in southern France, was a man of many talents. He was a Jewish philosopher and biblical scholar, a mathematician, an astronomer, and a physician. Most likely he made his living by practicing medicine, especially since he never held a rabbinical post. Little is known about the particulars of his life other than that he lived in Orange and later in Avignon. In 1321, Levi wrote *The Book of Numbers* dealing with arithmetical operations, including the extraction of roots. Later in life, he wrote *On Sines, Chords and Arcs*, a book dealing with trigonometry, which gives sine tables that were long noted for their accuracy. In 1343, the bishop of Meaux asked Levi to write a commentary on the first five books of Euclid, which he called *The Harmony of Numbers*. Levi also invented an instrument to measure the angular distance between celestial objects called Jacob's staff. He observed both lunar and solar eclipses and proposed new astronomical models based on the data he collected. His philosophical writings are extensive. They are considered to be major contributions to medieval philosophy.

Levi maintained contacts with prominent Christians, and was noted for the universality of his thinking. Pope Clement VI even translated some of Levi's astronomical writings into Latin, and the astronomer Kepler made use of this translation. Levi was fortunate to live in Provence, where popes provided some protection to Jews, rather than another part of France. However, at times persecution made it difficult for Levi to work, even preventing him from obtaining important volumes of Jewish scholarship.

every positive integer m and the last inequality holds because x and y are positive, so that $x < z$ and $y < z$.

Now applying the abc conjecture and noting that $\max(|a|, |b|, |c|) = z^n$, for every $\epsilon > 0$, there exists a constant $K(\epsilon) > 0$ such that

$$z^n \leq K(\epsilon)(z^3)^{1+\epsilon}.$$

If we can take $\epsilon = 1/6$ and $n \geq 4$, it is easy to see that $n - 3(1 + \epsilon) \geq n/8$. This implies that

$$z^n \leq K(1/6)^8,$$

where $K(1/6)$ is the value of the constant $K(\epsilon)$ for $\epsilon = 1/6$. It follows that $z \leq K(1/6)^{8/n}$. Consequently, in a solution of $x^n + y^n = z^n$ with $n \geq 4$, the numbers x, y, and z are all less than a fixed bound, which implies that there are only finitely many such solutions. ◀

13.2 Exercises

1. Show that if x, y, z is a Pythagorean triple and n is an integer with $n > 2$, then $x^n + y^n \neq z^n$.
2. Show that Fermat's last theorem is a consequence of Theorem 13.3, and of the assertion that $x^p + y^p = z^p$ has no solutions in nonzero integers when p is an odd prime.
3. Using Fermat's little theorem, show that if p is prime, and
   a) if $x^{p-1} + y^{p-1} = z^{p-1}$, then $p \mid xyz$.
   b) if $x^p + y^p = z^p$, then $p \mid (x + y - z)$.
4. Show that the diophantine equation $x^4 - y^4 = z^2$ has no solutions in nonzero integers using the method of infinite descent.
5. Using Exercise 4, show that the area of a right triangle with integer sides is never a perfect square.

EUGÈNE CATALAN (1814–1894) was born in Bruges, Belgium. He graduated from the École Polytechnique in 1835. He then was appointed to a teaching post at Châlons sur Marne. Catalan obtained a lectureship in descriptive geometry at the École Polytechnique in 1838, with the help of his schoolmate Joseph Liouville who was impressed by Catalan's mathematical talents. Unfortunately, Catalan's career was aversely affected by the reaction of the authorities to his political activity in favor of the French Republic. Catalan published extensively on topics in number theory and other areas of mathematics. Perhaps he is best known for his definition of the numbers now known as Catalan numbers, which appear in so many contexts in enumeration problems. He used these numbers to solve the problem of determining the number of regions produced by the dissection of a polygon into triangles by nonintersecting diagonals. It turns out that Catalan was not the first to solve this problem, because it was solved in the eighteenth century by Segner, who presented a less elegant solution than Catalan.

* **6.** Show that the diophantine equation $x^4 + 4y^4 = z^2$ has no solutions in nonzero integers.

* **7.** Show that the diophantine equation $x^4 + 8y^4 = z^2$ has no solutions in nonzero integers.

8. Show that the diophantine equation $x^4 + 3y^4 = z^2$ has infinitely many solutions.

9. Find all solutions in the rational numbers of the diophantine equation $y^2 = x^4 + 1$.

A diophantine equation of the form $y^2 = x^3 + k$, where k is an integer, is called a *Bachet equation* after Claude Bachet, a French mathematician of the early seventeenth century.

10. Show that the Bachet equation $y^2 = x^3 + 7$ has no solutions. (*Hint:* Consider the congruence resulting by first adding 1 to both sides of the equation and reducing modulo 4.)

* **11.** Show that the Bachet equation $y^2 = x^3 + 23$ has no solutions in integers x and y. (*Hint:* Look at the congruence obtained by reducing this equation modulo 4.)

* **12.** Show that the Bachet equation $y^2 = x^3 + 45$ has no solutions in integers x and y. (*Hint:* Look at the congruence obtained by reducing this equation modulo 8.)

13. Show that in a Pythagorean triple there is at most one perfect square.

14. Show that the diophantine equation $x^2 + y^2 = z^3$ has infinitely many integer solutions, by showing that for each positive integer k, the integers $x = 3k^2 - 1$, $y = k(k^2 - 3)$, and $z = k^2 + 1$ form a solution.

15. This exercise asks for a proof of a theorem proved by Sophie Germain in 1805. Suppose that n and p are odd primes, such that $p \mid xyz$ whenever x, y, and z are integers such that $x^n + y^n + z^n \equiv 0 \pmod{p}$. Further suppose that there are no solutions of the congruence $w^n \equiv n \pmod{p}$. Show that if x, y, and z are integers such that $x^n + y^n + z^n = 0$, then $n \mid xyz$.

CLAUDE GASPAR BACHET DE MÉZIRIAC (1581–1638) was born in Bourg-en-Bresse, France. his father was an aristocrat and was the highest judicial officer in the province. His early education took place at a house of the Jesuit order of the Duchy of Savoy. Later, he studied under the Jesuits in Lyon, Padua, and Milan. In 1601, he entered the Jesuit Order in Milan where it is presumed that he taught. Unfortunately, he became ill in 1602 and left the Jesuit Order. He resolved to live a life of leisure on his estate at Bourg-en-Bresse, which produced a considerable annual income for him. Bachet married in 1612. Bachet spent almost all of his life living on his estate, except for 1619–1620 when he lived in Paris. While in Paris, it was suggested that he become tutor to Louis XIII. This led to a hasty departure from the royal court.

Bachet's work in number theory concentrated on diophantine equations. In 1612, he presented a complete discussion on the solution of linear diophantine equations. In 1621, Bachet conjectured that every positive integer can be written as the sum of four squares; he checked his conjecture for all integers up to 325. Also, in 1621, Bachet discussed the diophantine equation that now bears his name. He is best known, however, for his Latin translation from the original Greek of Diophantus' book *Arithmetica*. It was in his copy of this book that Fermat wrote his marginal note about what we now call Fermat's last theorem. Bachet also wrote books on mathematical puzzles. His writings were the basis of most later books on mathematical recreations. Bachet discovered a method of constructing magic squares. He was elected to the French Academy in 1635.

16. Show that the diophantine equation $w^3 + x^3 + y^3 = z^3$ has infinitely many nontrivial solutions. (*Hint:* Take $w = 9zk^4$, $x = z(1 - 9k^3)$, and $y = 3zk(1 - 3k^3)$, where z and k are nonzero integers.)

17. Can you find four consecutive positive integers such that the sum of the cubes of the first three is the cube of the fourth integer?

18. Prove that the diophantine equation $w^4 + x^4 = y^4 + z^4$ has infinitely many nontrivial solutions. (*Hint:* Follow Euler by taking $w = m^7 + m^5n^2 - 2m^3n^4 + 3m^2n^5 + mn^6$, $x = m^6n - 3m^5n^2 - 2m^4n^3 + m^2n^5 + n^7$, $y = m^7 + m^5n^2 - 2m^3n^4 - 3m^2n^5 + mn^6$, and $z = m^6n + 3m^5n^2 - 2m^4n^3 + m^2n^5 + n^7$, where m and n are positive integers.)

19. Show that the only solution of the diophantine equation $3^n - 2^m = -1$ in positive integers m and n is $m = 2$ and $n = 1$.

20. Show that the only solution of the diophantine equation $3^n - 2^m = 1$ in positive integers m and n is $m = 3$ and $n = 2$.

21. The diophantine equation $x^2 + y^2 + z^2 = 3xyz$ is called *Markov's equation.*

a) Show that if $x = a$, $y = b$, and $z = c$ is a solution of Markov's equation, then $x = a$, $y = b$, and $z = 3ab - c$ is also a solution of Markov's equation.

* b) Show that every solution in integers of Markov's equation is generated starting with the solution $x = 1$, $y = 1$, and $z = 1$ and successively using part (a).

** **22.** Apply the abc conjecture to the Catalan equation $x^m - y^n = 1$, where m and n are integers with $m \geq 2$ and $n \geq 2$ to obtain a partial solution of the Catalan conjecture.

** **23.** Apply the abc conjecture to show that there are no solutions to Beal's conjecture when the exponents are sufficiently large.

The positive integer d is called a *congruent number* if there is a right triangle of area d with sides that have rational numbers as their length. (Unfortunately, the terminology for congruent numbers is easily confused with the terminology for the congruence of numbers). The problem determining which positive integers are congruent numbers is more than a millennium old (see [Gu94]).

24. a) Show that d is a congruent number if and only if there are positive rational numbers a, b, and c such that $ab = 2d$ and $a^2 + b^2 = c^2$.

b) Show that 5, 6, and 7 are congruent numbers by considering right triangles with sides of length 3/2, 20/3, and 41/6; sides of length 3, 4, and 5; and sides of length 35/12, 24/5, and 337/60, respectively. Also, show that 24 and 30 are congruent numbers.

25. a) Show that 1 is a congruent number if and only if there is a right triangle with area equal to a perfect square with sides of integer length.

b) Use part (a) and Theorem 13.1 to show that if 1 is a congruent number, then there is a solution in positive integers of the diophantine equation $x^2 + y^4 = z^4$. Deduce from this fact and Exercise 4 that 1 is not a congruent number.

In 1983, J. Tunnell characterized congruent numbers using the theory of elliptic curves (see [Ko96] for details). Suppose that d is a squarefree positive integer, $a = 1$ when d is odd and $a = 2$ when d is even, n is the number of triples of integers (x, y, z) such that $x^2 + 2ay^2 + 8z^3 = d/a$, and m is the number of triples of integers (x, y, z) such that $x^2 + 2ay^2 + 32z^2 = d/a$. Tunnell showed that if $n \neq 2m$, then d is not a congruent number.

He also showed that if $n = 2m$ and a well-known conjecture about elliptic curves is true, then d is a congruent number.

26. a) Show that $m = n = 2$, when $d = 1$ or $d = 2$.
b) Show that $m = n = 4$, when $d = 3$ or $d = 10$.
c) Show that $n = 12$ and $m = 2$, when $d = 11$.
d) Show that $n = 8$ and $m = 4$, when $d = 34$.
e) Show that $n = m = 0$, when d is of the form $8k + j$, where k is a positive integer and $j = 5, 6$, or 7.
f) Using Tunnell's theorem and parts (a), (b), and (c), show that 1, 2, 3, 10, and 11 are not congruent numbers.
g) Tunnell's conjecture implies that 34 is a congruent number. Show that 34 is a congruent number by finding a right triangle with sides of rational length with area 34.

13.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Euler conjectured that no sum of fewer than n nth powers of nonzero integers is equal to the nth power of an integer. Show that this conjecture is false (as was shown in 1966 by Lander and Parkin) by finding four fifth powers of integers whose sum is also the fifth power of an integer. Can you find other counterexamples to Euler's claim?
2. Given a positive integer n, find as many pairs of equal sums of nth powers as you can.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Given a positive integer n, search for solutions of the diophantine equation $x^n + y^n = z^n$.
2. Generate solutions of the diophantine equation $x^2 + y^2 = z^3$ (see Exercise 16).
3. Given a positive integer k, search for solutions in integers of Bachet's equation $y^2 = x^3 + k$.
4. Generate the solutions of Markov's equation, defined in Exercise 21.

13.3 Sums of Squares

Mathematicians throughout history have been interested in problems regarding the representation of integers as sums of squares. Diophantus, Fermat, Euler, and Lagrange are among the mathematicians who made important contributions to the solution of such problems. In this section, we discuss two questions of this kind: Which integers are the sum of two squares? What is the least integer n such that every positive integer is the sum of n squares?

We begin by considering the first question. Not every positive integer is the sum of two squares. In fact, n is not the sum of two squares if it is of the form $4k + 3$. To see this, note that because $a^2 \equiv 0$ or $1 \pmod 4$ for every integer a, $x^2 + y^2 \equiv 0, 1$, or $2 \pmod 4$.

To conjecture which integers are the sum of two squares, we first examine some small positive integers.

Example 13.6. Among the first 20 positive integers, note that

$1 = 0^2 + 1^2$,	11 is not the sum of two squares,
$2 = 1^2 + 1^2$,	12 is not the sum of two squares,
3 is not the sum of two squares,	$13 = 3^2 + 2^2$,
$4 = 2^2 + 0^2$,	14 is not the sum of two squares,
$5 = 1^2 + 2^2$,	15 is not the sum of two squares,
6 is not the sum of two squares,	$16 = 4^2 + 0^2$,
7 is not the sum of two squares,	$17 = 4^2 + 1^2$,
$8 = 2^2 + 2^2$,	$18 = 3^2 + 3^2$,
$9 = 3^2 + 0^2$,	19 is not the sum of two squares,
$10 = 3^2 + 1^2$,	$20 = 2^2 + 4^2$. ◀

It is not immediately obvious from the evidence in Example 13.6 which integers, in general, are the sum of two squares. (Can you see anything in common among those positive integers not representable as the sum of two squares?)

We now begin a discussion that will show that the prime factorization of an integer determines whether this integer is the sum of two squares. There are two reasons for this. The first is that the product of two integers that are sums of two squares is again the sum of two squares; the second is that a prime is representable as the sum of two squares if and only if it is not of the form $4k + 3$. We will prove both of these results. Then we will state and prove the theorem that specifies which integers are the sum of two squares.

The proof that the product of sums of two squares is again the sum of two squares relies on an important algebraic identity that we will use several times in this section.

Theorem 13.4. If m and n are both sums of two squares, then mn is also the sum of two squares.

Proof. Let $m = a^2 + b^2$ and $n = c^2 + d^2$. Then

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \tag{13.2}$$

The reader can easily verify this identity by expanding all the terms. ■

Example 13.7. Because $5 = 2^2 + 1^2$ and $13 = 3^2 + 2^2$, it follows from (13.2) that

$$\begin{aligned} 65 &= 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2) \\ &= (2 \cdot 3 + 1 \cdot 2)^2 + (2 \cdot 2 - 1 \cdot 3)^2 = 8^2 + 1^2. \end{aligned}$$ ◀

One crucial result is that every prime of the form $4k + 1$ is the sum of two squares. To prove this result we will need the following lemma.

Lemma 13.4. If p is a prime of the form $4m + 1$, where m is an integer, then there exist integers x and y such that $x^2 + y^2 = kp$ for some positive integer k with $k < p$.

Proof. By Theorem 11.4, we know that -1 is a quadratic residue of p. Hence, there is an integer $a, a < p$, such that $a^2 \equiv -1 \pmod{p}$. It follows that $a^2 + 1 = kp$ for some positive integer k. Hence, $x^2 + y^2 = kp$, where $x = a$ and $y = 1$. From the inequality $kp = x^2 + y^2 \leq (p-1)^2 + 1 < p^2$, we see that $k < p$. ∎

We can now prove the following theorem, which tells us that all primes not of the form $4k + 3$ are the sum of two squares.

Theorem 13.5. If p is a prime, not of the form $4k + 3$, then there are integers x and y such that $x^2 + y^2 = p$.

Proof. Note that 2 is the sum of two squares, because $1^2 + 1^2 = 2$. Now, suppose that p is a prime of the form $4k + 1$. Let m be the smallest positive integer such that $x^2 + y^2 = mp$ has a solution in integers x and y. By Lemma 13.4, there is such an integer less than p; by the well-ordering property, a least such integer exists. We will show that $m = 1$.

Assume that $m > 1$. Let a and b be defined by

$$a \equiv x \pmod{m}, \quad b \equiv y \pmod{m}$$

and

$$-m/2 < a \leq m/2, \quad -m/2 < b \leq m/2.$$

It follows that $a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{m}$. Hence, there is an integer k such that

$$a^2 + b^2 = km.$$

We have

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2 p.$$

By equation (13.2), we have

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2.$$

Furthermore, because $a \equiv s \pmod{m}$ and $b \equiv y \pmod{m}$, we have

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$$
$$ay - bx \equiv xy - yx \equiv 0 \pmod{m}.$$

Hence, $(ax + by)/m$ and $(ay - bx)/m$ are integers, so that

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ax - by}{m}\right)^2 = km^2 p/m^2 = kp$$

is the sum of two squares. If we show that $0 < k < m$, this will contradict the choice of m as the minimum positive integer such that $x^2 + y^2 = mp$ has a solution in integers. We know that $a^2 + b^2 = km$, $-m/2 < a \leq m/2$, and $-m/2 < b \leq m/2$. Hence, $a^2 \leq m^2/4$ and $b^2 \leq m^2/4$. We have

$$0 \leq km = a^2 + b^2 \leq 2(m^2/4) = m^2/2.$$

Consequently, $0 \leq k \leq m/2$. It follows that $k < m$. All that remains is to show that $k \neq 0$. If $k = 0$, we have $a^2 + b^2 = 0$. This implies that $a = b = 0$, so that $x \equiv y \equiv 0 \pmod{m}$, which shows that $m \mid x$ and $m \mid y$. Because $x^2 + y^2 = mp$, this implies that $m^2 \mid mp$, which implies that $m \mid p$. Because m is less than p, this implies that $m = 1$, which is what we wanted to prove. ∎

We can now put all the pieces together, and prove the fundamental result that classifies the positive integers that are representable as the sum of two squares.

Theorem 13.6. The positive integer n is the sum of two squares if and only if each prime factor of n of the form $4k + 3$ occurs to an even power in the prime factorization of n.

Proof. Suppose that in the prime factorization of n there are no primes of the form $4k + 3$ that appear to an odd power. We write $n = t^2u$, where u is the product of primes. No primes of the form $4k + 3$ appear in u. By Theorem 13.5, each prime in u can be written as the sum of two squares. Applying Theorem 13.4 one time fewer than the number of different primes in u shows that u is also the sum of two squares, say

$$u = x^2 + y^2.$$

It then follows that n is also the sum of two squares, namely

$$n = (tx)^2 + (ty)^2.$$

Now, suppose that there is a prime p, $p \equiv 3 \pmod{4}$, that occurs in the prime factorization of n to an odd power, say the $(2j + 1)$th power. Furthermore, suppose that n is the sum of two squares, that is,

$$n = x^2 + y^2.$$

Let $(x, y) = d$, $a = x/d$, $b = y/d$, and $m = n/d^2$. It follows that $(a, b) = 1$ and

$$a^2 + b^2 = m.$$

Suppose that p^k is the largest power of p that divides d. Then m is divisible by $p^{2j-2k+1}$, and $2j - 2k + 1$ is at least 1 because it is nonnegative; hence, $p \mid m$. We know that p does not divide a, for if $p \mid a$, then $p \mid b$, because $b^2 = m - a^2$ and $(a, b) = 1$.

Thus, there is an integer z such that $az \equiv b \pmod{p}$. It follows that

$$a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1 + z^2) \pmod{p}.$$

Because $a^2 + b^2 = m$ and $p \mid m$, we see that

$$a^2(1 + z^2) \equiv 0 \pmod{p}.$$

Because $(a, p) = 1$, it follows that $1 + z^2 \equiv 0 \pmod{p}$. This implies that $z^2 \equiv -1 \pmod{p}$, which is impossible because -1 is not a quadratic residue of p, because $p \equiv 3 \pmod{4}$. This contradiction shows that n could not have been the sum of two squares. ■

Because there are positive integers not representable as the sum of two squares, we can ask whether every positive integer is the sum of three squares. The answer is no, as it is impossible to write 7 as the sum of three squares (as the reader should show). Because three squares do not suffice, we ask whether four squares do. The answer to this is yes, as we will show. Fermat wrote that he had a proof of this fact, although he never published it (and most historians of mathematics believe that he actually had such a proof). Euler was unable to find a proof, although he made substantial progress toward a solution. It was in 1770 that Lagrange presented the first published solution.

The proof that every positive integer is the sum of four squares depends on the following theorem, which shows that the product of two integers both representable as the sum of four squares can also be so represented. Just as with the analogous result for two squares, there is an important algebraic identity used in the proof.

Theorem 13.7. If m and n are positive integers that are each the sum of four squares, then mn is also the sum of four squares.

Proof. Let $m = a^2 + b^2 + c^2 + d^2$ and $n = e^2 + f^2 + g^2 + h^2$. The fact that mn is also the sum of four squares follows from the following algebraic identity:

$$\begin{aligned} mn &= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \\ &= (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 \\ &\quad + (ag - bh - ce + df)^2 + (ah + bg - cf - de)^2. \end{aligned} \tag{13.3}$$

The reader can easily verify this identity by multiplying all the terms. ■

We illustrate the use of Theorem 13.7 with an example.

Example 13.8. Because $7 = 2^2 + 1^2 + 1^2 + 1^2$ and $10 = 3^2 + 1^2 + 0^2 + 0^2$, from (13.3) it follows that

$$\begin{aligned} 70 = 7 \cdot 10 &= (2^2 + 1^2 + 1^2 + 1^2)(3^2 + 1^2 + 0^2 + 0^2) \\ &= (2 \cdot 3 + 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0)^2 + (2 \cdot 1 - 1 \cdot 3 + 1 \cdot 0 - 1 \cdot 0)^2 \\ &\quad + (2 \cdot 0 - 1 \cdot 0 - 1 \cdot 3 = 1 \cdot 1)^2 + (2 \cdot 0 + 1 \cdot 0 - 1 \cdot 1 - 1 \cdot 3)^2 \\ &= 7^2 + 1^2 + 2^2 + 4^2. \end{aligned}$$

◀

We will now begin our work to show that every prime is the sum of four squares. We begin with a lemma.

Lemma 13.5. If p is an odd prime, then there exists an integer k, $k < p$, such that

$$kp = x^2 + y^2 + z^2 + w^2$$

has a solution in integers x, y, z, and w.

Proof. We will first show that there are integers x and y such that

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

with $0 \leq x < p/2$ and $0 \leq y < p/2$.

Let

$$S = \left\{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

and

$$T = \left\{-1 - 0^2, -1 - 1^2, \ldots, -1 - \left(\frac{p-1}{2}\right)^2\right\}.$$

No two elements of S are congruent modulo p (because $x^2 \equiv y^2 \pmod{p}$ implies that $x \equiv \pm y \pmod{p}$). Likewise, no two elements of T are congruent modulo p. It is easy to see that the set $S \cup T$ contains $p + 1$ distinct integers. By the pigeonhole principle, there are two integers in this union that are congruent modulo p. It follows that there are integers x and y such that $x^2 \equiv -1 - y^2 \pmod{p}$ with $0 \leq x \leq (p-1)/2$ and $0 \leq y < (p-1)/2$. We have

$$x^2 + y^2 + 1 \equiv 0 \pmod{p};$$

it follows that $x^2 + y^2 + 1 + 0^2 = kp$ for some integer k. Because $x^2 + y^2 + 1 < 2((p-1)/2)^2 + 1 < p^2$, it follows that $k < p$. ∎

We can now prove that every prime is the sum of four squares.

Theorem 13.8. Let p be a prime. Then the equation $x^2 + y^2 + z^2 + w^2 = p$ has a solution, where x, y, z, and w are integers.

Proof. The result is true when $p = 2$, because $2 = 1^2 + 1^2 + 0^2 + 0^2$. Now, assume that p is an odd prime. Let m be the smallest integer such that $x^2 + y^2 + z^2 + w^2 = mp$ has a solution, where x, y, z, and w are integers. (By Lemma 13.5, such integers exist, and by the well-ordering property, there is a minimal such integer.) The theorem will follow if we can show that $m = 1$. To do this, we assume that $m > 1$ and find a smaller such integer.

If m is even, then either all of x, y, z, and w are odd, all are even, or two are odd and two are even. In all these cases, we can rearrange these integers (if necessary) so that $x \equiv y \pmod{2}$ and $z \equiv w \pmod{2}$. It then follows that $(x - y)/2$, $(x + y)/2$, $(z - w)/2$, and $(x + w)/2$ are integers, and

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 = (m/2)p.$$

This contradicts the minimality of m.

Now suppose that m is odd and $m > 1$. Let a, b, c, and d be integers such that

$$a \equiv x \pmod{m}, \quad b \equiv y \pmod{m}, \quad c \equiv z \pmod{m}, \quad d \equiv w \pmod{m},$$

and

$$-m/2 < a < m/2, \quad -m/2 < b < m/2, \quad -m/2 < c < m/2, \quad -m/2 < d < m/2.$$

We have

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod{m};$$

hence,

$$a^2 + b^2 + c^2 + d^2 = km$$

for some integer k, and

$$0 \le a^2 + b^2 + c^2 + d^2 < 4(m/2)^2 = m^2.$$

Consequently, $0 \le k < m$. If $k = 0$, we have $a = b = c = d = 0$, so that $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$. From this, it follows that $m^2 \mid mp$, which is impossible because $1 < m < p$. It follows that $k > 0$.

We have

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = mp \cdot km = m^2kp.$$

But by the identity in the proof of Theorem 13.7, we have

$$\begin{aligned}&(ax + by + cz + dw)^2 + (bx - ay + dz - cw)^2 \\ &\quad + (cx - dy - az + bw)^2 + (dx + cy - bz - aw)^2 = m^2kp.\end{aligned}$$

Each of the four terms being squared is divisible by m, because

$$\begin{aligned}ax + by + cz + dw &\equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m},\\ bx - ay + dz - cw &\equiv yx - xy + wz - zw \equiv 0 \pmod{m},\\ cx - dy - az + bw &\equiv zx - wy - xz + yw \equiv 0 \pmod{m},\\ dx + cy - bz - aw &\equiv wx + zy - yz - xw \equiv 0 \pmod{m}.\end{aligned}$$

Let X, Y, Z, and W be the integers obtained by dividing these quantities by m, that is,

$$\begin{aligned}X &= (ax + by + cz + dw)/m,\\ Y &= (bx - ay + dz - cw)/m,\\ Z &= (cx - dy - az + bw)/m,\\ W &= (dx + cy - bz - aw)/m.\end{aligned}$$

It then follows that

$$X^2 + Y^2 + Z^2 + W^2 = m^2kp/m^2 = kp.$$

But this contradicts the choice of m; hence, m must be 1. ∎

We now can state and prove the fundamental theorem about representations of integers as sums of four squares.

Theorem 13.9. Every positive integer is the sum of the squares of four integers.

Proof. Suppose that n is a positive integer. Then, by the fundamental theorem of arithmetic, n is the product of primes. By Theorem 13.8, each of these prime factors can be written as the sum of four squares. Applying Theorem 13.7 a sufficient number of times, it follows that n is also the sum of four squares. ■

We have shown that every positive integer can be written as the sum of four squares. As mentioned, this theorem was originally proved by Lagrange in 1770. Around the same time, the English mathematician Edward Waring generalized this problem. He stated, but did not prove, that every positive integer is the sum of 9 cubes of nonnegative integers, the sum of 19 fourth powers of nonnegative integers, and so on. We can phrase this conjecture in the following way.

EDWARD WARING (1736–1798) was born in Old Heath in Shropshire, England, where his father was a farmer. As a youth, Edward attended Shrewsbury School. He entered Magdalene College, Cambridge, in 1753, winning a scholarship qualifying him for a reduced fee if he also worked as a servant. His mathematical talents quickly impressed his teachers and he was elected a fellow of the college in 1754, graduating in 1757. Noted by many as a prodigy, Waring was nominated for the Lucasian Chair of Mathematics at Cambridge in 1759; after some controversy, he was confirmed as the Lucasian professor in 1760 at the age of 23.

Waring's most important work was *Meditationes Algebraicae*, which covered topics in the theory of equations, number theory, and geometry. In this book he makes one of the first important contributions to the part of abstract algebra now known as Galois theory. It was also in this book that he stated without proof that every integer is equal to the sum of not more than 9 cubes, that every integer is the sum of not more than 19 fourth powers, and so on—the result we now call Waring's theorem. To honor his contributions in the *Meditationes Algebraicae*, Waring was elected a Fellow of the Royal Society in 1763. However, few scholars read the book because of its difficult subject matter and because Waring was a poor communicator who used a notation that made his work hard to understand.

Surprisingly, Waring also studied medicine while holding his chair in mathematics. He graduated with an M.D. in 1767 and for a brief time practiced medicine at several hospitals, before giving up medicine in 1770. His lack of success in medicine has been attributed to his shy manner and poor eyesight. Waring was able to pursue medicine while holding his chair in mathematics because he did not present lectures on mathematics. In fact, Waring was noted as a poor communicator with handwriting almost impossible to read. Regrettably, this is not such a rare trait among mathematics professors!

Waring was married to Mary Oswell in 1776. He and his wife lived in the town of Shrewsbury for a while, but his wife did not like the town. The couple later moved to Waring's country estate.

Waring was considered by his contemporaries to possess an odd combination of vanity and modesty, but with vanity predominating. He is recognized as one of the greatest English mathematicians of his time, although his poor communication skills limited his reputation while he was alive. Moreover, according to one account, near the end of his life he fell into a deep religious melancholy which approached insanity and prevented him from accepting several awards.

Waring's Problem. If k is a positive integer, is there an integer $g(k)$ such that every positive integer can be written as the sum of $g(k)$ kth powers of nonnegative integers, and no smaller number of kth powers will suffice?

Lagrange's theorem shows that we can take $g(2) = 4$ (because there are integers that are not the sum of three squares). In the nineteenth century, mathematicians showed that such an integer $g(k)$ exists for $3 \leq k \leq 8$ and $k = 10$. But it was not until 1906 that David Hilbert showed that for every positive integer k, there is a constant $g(k)$ such that every positive integer may be expressed as the sum of $g(k)$ kth powers of nonnegative integers. Hilbert's proof is extremely complicated and is not constructive, so that it gives no formula for $g(k)$. It is now known that $g(3) = 9$, $g(4) = 19$, $g(5) = 37$, and

$$g(k) = [(3/2)^k] + 2^k - 2$$

for $6 \leq k \leq 471{,}600{,}000$. Proofs of these formulas rely on nonelementary results from analytical number theory. There are still many unanswered questions about the values of $g(k)$.

Although every positive integer can be written as the sum of 9 cubes, it is known that the only positive integers not representable as the sum of 8 cubes are 23 and 239. It is also known that every sufficiently large integer can be represented as the sum of at most 7 cubes. Observations of this sort lead to the definition of the function $G(k)$, which equals the least positive integer such that all sufficiently large positive integers can be represented as the sum of at most $G(k)$ kth powers. The preceding remarks imply that $G(3) \leq 7$. It is also not hard to see that $G(3) \geq 4$, because no positive integer n with $n \equiv \pm 4 \pmod 9$ can be expressed as the sum of three cubes (see Exercise 22). This implies that $4 \leq G(3) \leq 7$. It may surprise you to learn that it is still not known whether $G(3) = 4, 5, 6,$ or 7. The value of $G(k)$ is extremely difficult to determine; the only known values of $G(k)$ are $G(2) = 4$ and $G(4) = 16$. The best currently known inequalities for $G(k)$, with $k = 5, 6, 7,$ and 8 are $6 \leq G(5) \leq 17$, $9 \leq G(6) \leq 24$, $8 \leq G(7) \leq 32$, and $32 \leq G(8) \leq 42$.

The interested reader can learn about recent results regarding Waring's problem by consulting the numerous articles on this problem described in [Le74]. The paper of Wunderlich and Kubina [WuKu90] established the upper limit of the range for which it has been verified that $g(k)$ is given by this formula.

13.3 Exercises

1. Given that $13 = 3^2 + 2^2$, $29 = 5^2 + 2^2$, and $50 = 7^2 + 1^2$, write each of the following integers as the sum of two squares.

   a) $377 = 13 \cdot 29$ c) $1450 = 29 \cdot 50$
   b) $650 = 13 \cdot 50$ d) $18{,}850 = 13 \cdot 29 \cdot 50$

2. Determine whether each of the following integers can be written as the sum of two squares.

a) 19 d) 45 g) 99
b) 25 e) 65 h) 999
c) 29 f) 80 i) 1000

3. Represent each of the following integers as the sum of two squares.

a) 34 c) 101 e) 21,658
b) 90 d) 490 f) 324,608

4. Show that a positive integer is the difference of two squares if and only if it is not of the form $4k + 2$, where k is an integer.

5. Represent each of the following integers as the sum of three squares if possible.

a) 3 c) 11 e) 23
b) 90 d) 18 f) 28

6. Show that the positive integer n is not the sum of three squares of integers if n is of the form $8k + 7$, where k is an integer.

7. Show that the positive integer n is not the sum of three squares of integers if n is of the form $4^m(8k + 7)$, where m and k are nonnegative integers.

8. Prove or disprove that the sum of two integers each representable as the sum of three squares of integers is also thus representable.

9. Given that $7 = 2^2 + 1^2 + 1^2 + 1^2$, $15 = 3^2 + 2^2 + 1^2 + 1^2$, and $34 = 4^2 + 4^2 + 1^2 + 1^2$, write each of the following integers as the sum of four squares.

a) $105 = 7 \cdot 15$ c) $238 = 7 \cdot 34$
b) $510 = 15 \cdot 34$ d) $3570 = 7 \cdot 15 \cdot 34$

10. Write each of the following positive integers as the sum of four squares.

a) 6 c) 21 e) 99
b) 12 d) 89 f) 555

11. Show that every integer n, $n \geq 170$, is the sum of the squares of five positive integers. (*Hint:* Write $m = n - 169$ as the sum of the squares of four integers, and use the fact that $169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 10^2 + 8^2 + 2^2 + 1^2$.)

12. Show that the only positive integers that are not expressible as the sum of five squares of positive integers are 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33. (*Hint:* Use Exercise 11, show that each of these integers cannot be expressed as stated, and then show all remaining positive integers less than 170 can be expressed as stated.)

* **13.** Show that there are arbitrarily large integers that are not the sums of the squares of four positive integers.

We outline a second proof for Theorem 13.5 in Exercises 14–15.

* **14.** Show that if p is prime and a is an integer not divisible by p, then there exist integers x and y such that $ax \equiv y \pmod{p}$ with $0 <| x |< \sqrt{p}$ and $0 <| y |< \sqrt{p}$. This result is called *Thue's lemma* after Norwegian mathematician *Axel Thue*. (*Hint:* Use the pigeonhole principle to show that there are two integers of the form $au - v$, with $0 \le u \le [\sqrt{p}]$ and $0 \le v \le [\sqrt{p}]$, that are congruent modulo p. Construct x and y from the two values of u and the two values of v, respectively.)

15. Use Exercise 14 to prove Theorem 13.5. (*Hint:* Show that there is an integer a with $a^2 \equiv -1 \pmod{p}$. Then apply Thue's lemma with this value of a.)

16. Show that 23 is the sum of nine cubes of nonnegative integers but not the sum of eight cubes of nonnegative integers.

Exercises 17–21 give an elementary proof that $g(4) \le 50$.

17. Show that

$$\sum_{1 \le i < j \le 4} \left((x_i + x_j)^4 + (x_i - x_j)^4 \right) = 6 \left(\sum_{k=1}^{4} x_k^2 \right)^2 .$$

(*Hint:* Start with the identity $(x_i + x_j)^4 + (x_i - x_j)^4 = 2x_i^4 + 12x_i^2 x_j^2 + 2x_j^4$.)

18. Show from Exercise 17 that every integer of the form $6n^2$, where n is a positive integer, is the sum of 12 fourth powers.

19. Use Exercise 18 and the fact that every positive integer is the sum of four squares to show that every positive integer of the form $6m$, where m is a positive integer, can be written as the sum of 48 fourth powers.

20. Show that the integers 0, 1, 2, 81, 16, 17 form a complete system of residues modulo 6, each of which is the sum of at most two fourth powers. Show from this that every integer n with $n > 81$ can be written as $6m + k$, where m is a positive integer and k comes from this complete system of residues. Conclude from this that every integer n with $n < 81$ is the sum of 50 fourth powers.

21. Show that every positive integer n with $n \le 81$ is the sum of at most 50 fourth powers. (*Hint:* For $51 \le n \le 81$, start by using three terms equal to 2^4.) Conclude from this exercise and Exercise 20 that $g(4) \le 50$.

22. Show that no positive integer n, $n \equiv \pm 4 \pmod{9}$, is the sum of three cubes.

AXEL THUE (1863–1922) was born in Tönsberg, Norway. He received his degree from the University of Oslo in 1889. He studied under the German mathematician Lie in Liepzig and in Berlin from 1891 until 1894, and he was professor of applied mechanics at the University of Oslo from 1903 until 1922. Thue was the first person to study the problem of finding an infinite sequence over a finite alphabet that does not contain any occurrences of adjacent identical blocks. His work on the approximations of algebraic numbers was seminal, and was later improved by Siegel and by Roth. Using his results, he managed to prove that certain diophantine equations such as $y^3 - 2x^3 = 1$ have a finite number of solutions. Edmund Landau characterized Thue's theorem on approximation as "the most important discovery in elementary number theory that I know."

23. Show that $G(4) \leq 15$ by showing that if n is a positive integer with $n \equiv 15 \pmod{16}$, then n cannot be represented as the sum of fewer than 15 fourth powers of integers.

24. Use the fact that 31 is not the sum of 15 fourth powers and the method of infinite descent, to show that no positive integer of the form $31 \cdot 16^m$ is the sum of 15 fourth powers. (*Hint:* Suppose that $\sum_{i=1}^{15} x_i^4 = 31 \cdot 16^m$. Show that each x_i must be even, so that $\sum_{i=1}^{15} (x_i/2)^4 = 31 \cdot 16^{m-1}$.)

13.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the number of ways that each integer less than 100 can be written as the sum of two squares. (Count the sum $(\pm x^2) + (\pm y^2)$ four times, once for each choice of signs.)

2. Using numerical evidence, make a conjecture concerning which positive integers can be expressed as the sum of three squares. (Be sure to consult Exercise 7.)

3. Explore which positive integers can be written as the sum of n cubes of nonnegative integers for $n = 2, 3, 4, 5$.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

* **1.** Determine whether a positive integer n can be represented as the sum of two squares and so represent it if possible.

* **2.** Given a positive integer n, represent n as the sum of four squares.

13.4 Pell's Equation

In this section, we study diophantine equations of the form

$$x^2 - dy^2 = n, \tag{13.4}$$

where d and n are fixed integers. When $d < 0$ and $n < 0$, there are no solutions of (13.4). When $d < 0$ and $n > 0$, there can be at most a finite number of solutions, because the equation $x^2 - dy^2 = n$ implies that $|x| \leq \sqrt{n}$ and $|y| \leq \sqrt{n/|d|}$. Also, note that when d is a perfect square, say $d = D^2$, then

$$x^2 - dy^2 = x^2 - D^2y = (x + Dy)(x - Dy) = n.$$

Hence, any solution of (13.4), when d is a perfect square, corresponds to a simultaneous solution of the equations

$$x + Dy = a,$$
$$x - Dy = b,$$

where a and b are integers such that $n = ab$. In this case, there are only a finite number of solutions, because there is at most one solution in integers of these two equations for each factorization $n = ab$.

For the rest of this section, we are interested in the diophantine equation $x^2 - dy^2 = n$, where d and n are integers and d is a positive integer that is not a perfect square. As the following theorem shows, the simple continued fraction of $\sqrt{d}$ is very useful for the study of this equation.

Theorem 13.10. Let d and n be integers such that $d > 0$, d is not a perfect square, and $|n| < \sqrt{d}$. If $x^2 - dy^2 = n$, then x/y is a convergent of the simple continued fraction of $\sqrt{d}$.

Proof. First consider the case where $n > 0$. Because $x^2 - dy^2 = n$, we see that

$$(x + y\sqrt{d})(x - y\sqrt{d}) = n. \tag{13.5}$$

From (13.5), we see that $x - y\sqrt{d} > 0$, so that $x > y\sqrt{d}$. Consequently,

$$\frac{x}{y} - \sqrt{d} > 0,$$

and, because $0 < n < \sqrt{d}$, we see that

$$\begin{aligned}\frac{x}{y} - \sqrt{d} &= \frac{(x - \sqrt{d}\,y)}{y} \\ &= \frac{x^2 - dy^2}{y(x + y\sqrt{d})} \\ &< \frac{n}{y(2y\sqrt{d})} \\ &< \frac{\sqrt{d}}{2y^2\sqrt{d}} \\ &= \frac{1}{2y^2}.\end{aligned}$$

Because $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2}$, Theorem 12.19 tells us that x/y must be a convergent of the simple continued fraction of $\sqrt{d}$.

When $n < 0$, we divide both sides of $x^2 - dy^2 = n$ by $-d$, to obtain

$$y^2 - (1/d)x^2 = -n/d.$$

By a similar argument to that given when $n > 0$, we see that y/x is a convergent of the simple continued fraction expansion of $1/\sqrt{d}$. Therefore, from Exercise 7 of Section 12.3, we know that $x/y = 1/(y/x)$ must be a convergent of the simple continued fraction of $\sqrt{d} = 1/(1/\sqrt{d})$. ∎

We have shown that solutions of the diophantine equation $x^2 - dy^2 = n$, where $|n| < \sqrt{d}$, are given by the convergents of the simple continued fraction expansion of $\sqrt{d}$. We will restate Theorem 12.24 here, replacing n by d, because it will help us to use these convergents to find solutions of this diophantine equation.

Theorem 12.24. Let d be a positive integer that is not a perfect square. Define $\alpha_k = (P_k + \sqrt{d})/Q_k$, $a_k = [\alpha_k]$, $P_{k+1} = a_k Q_k - P_k$, and $Q_{k+1} = (d - P_{k+1}^2)/Q_k$, for $k = 0, 1, 2, \ldots$, where $\alpha_0 = \sqrt{d}$. Furthermore, let p_k/q_k denote the kth convergent of the simple continued fraction expansion of $\sqrt{d}$. Then

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}.$$

The special case of the diophantine equation $x^2 - dy^2 = n$ with $n = 1$ is called *Pell's equation,* after *John Pell.* Although Pell played an important role in the mathematical community of his day, he played only a minor part in solving the equation named in his honor. The problem of finding the solutions of this equation has a long history. Special cases of Pell's equations are discussed in ancient works by Archimedes and Diophantus. Moreover, the twelfth-century Indian mathematician *Bhaskara* described a method for finding the solutions of Pell's equation. In more recent times, in a letter written in 1657, Fermat posed to the "mathematicians of Europe" the problem of showing that there are infinitely many integral solutions of the equation $x^2 - dy^2 = 1$, when d is a positive integer greater than 1 that is not a square. Soon afterward, the English mathematicians Wallis and Brouncker developed a method to find these solutions, but did not provide a proof that their method works. Euler provided all the theory needed for a proof in a paper published in 1767, and Lagrange published such a proof in 1768. The methods of Wallis and Brouncker, Euler, and Lagrange all are related to the use of the continued fraction of $\sqrt{d}$. We will show how this continued fraction is used to find the solutions of Pell's equation. In particular, we will use Theorems 13.9 and 12.24 to find all solutions of

JOHN PELL (1611–1683), the son of a clergyman, was born in Sussex, England, and was educated at Trinity College, Cambridge. He became a schoolmaster instead of following his father's wishes that he enter the clergy. After developing a reputation for scholarship in both mathematics and languages, he took a position at the University of Amsterdam. He remained there until, at the request of the Prince of Orange, he joined the faculty of a new college at Breda. Among Pell's writings in mathematics are a book, *Idea of Mathematics*, as well as many pamphlets and articles. He corresponded and discussed mathematics with the leading mathematicians of his day, including Leibniz and Newton, the inventors of calculus. Euler may have called $x^2 - dy^2 = 1$ "Pell's equation" because he was familiar with a book in which Pell augmented the work of other mathematicians on the solutions of the equation $x^2 - 12y^2 = n$.

Pell was involved with diplomacy; he served in Switzerland as an agent of Oliver Cromwell and he joined the English diplomatic service in 1654. He finally decided to join the clergy in 1661, when he took his holy orders and became chaplain to the Bishop of London. Unfortunately, at the time of his death, Pell was living in abject poverty.

Pell's equation and the related equation $x^2 - dy^2 = -1$. More information about Pell's equation can be found in [Ba03], a book entirely devoted to this equation.

Theorem 13.11. Let d be a positive integer that is not a perfect square. Let p_k/q_k denote the kth convergent of the simple continued fraction of $\sqrt{d}$, $k = 1, 2, 3 \ldots$, and let n be the period length of this continued fraction. Then, when n is even, the positive solutions of the diophantine equation $x^2 - dy^2 = 1$ are $x = p_{jn-1}$, $y = q_{jn-1}$, $j = 1, 2, 3 \ldots$, and the diophantine equation $x^2 - dy^2 = -1$ has no solutions. When n is odd, the positive solutions of $x^2 - dy^2 = 1$ are $x = p_{2jn-1}$, $y = q_{2jn-1}$, $j = 1, 2, 3, \ldots$, and the solutions of $x^2 - dy^2 = -1$ are $x = p_{(2j-1)n-1}$, $y = q_{(2j-1)n-1}$, $j = 1, 2, 3, \ldots$.

Proof. Theorem 13.9 tells us that if x_0, y_0 is a positive solution of $x^2 - dy^2 = \pm 1$. then $x_0 = p_k$, $y_0 = q_k$, where p_k/q_k is a convergent of the simple continued fraction of $\sqrt{d}$. On the other hand, from Theorem 12.24, we know that

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1},$$

where Q_{k+1} is as defined as in the statement of Theorem 12.24.

Because the period of the continued expansion of $\sqrt{d}$ is n, we know that $Q_{jn} = Q_0 = 1$ for $j = 1, 2, 3, \ldots$, because $\sqrt{d} = \frac{P_0 + \sqrt{d}}{Q_0}$. Hence,

$$p_{jn-1}^2 - d\, q_{jn-1}^2 = (-1)^{jn} Q_{nj} = (-1)^{jn}.$$

This equation shows that when n is even, p_{jn-1}, q_{jn-1} is a solution of $x^2 - dy^2 = 1$ for $j = 1, 2, 3 \ldots$, and when n is odd, p_{2jn-1}, q_{2jn-1} is a solution of $x^2 - dy^2 = 1$ and $p_{2(j-1)n-1}, q_{2(j-1)n-1}$ is a solution of $x^2 - dy^2 = -1$ for $j = 1, 2, 3, \ldots$.

To show that the diophantine equations $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$ have no solutions other than those already found, we will show that $Q_{k+1} = 1$ implies that $n \mid k$ and that $Q_j \neq -1$ for $j = 1, 2, 3, \ldots$.

We first note that if $Q_{k+1} = 1$, then

BHASKARA (1114–1185) was born in Biddur, in the Indian state of Mysore. Bhaskara was the head of the astronomical observatory at Ujjain, the center of mathematical studies in India for many centuries. He is the best known of all Indian mathematicians of his era. Bhaskara's works on mathematics include *Lilavati* (The Beautiful) and *Bijaganita* (Seed Counting), which are both textbooks that cover parts of algebra, arithmetic, and geometry. Bhaskara studied systems of linear equations in more unknowns than equations, and knew many combinatorial formulas. He investigated the solutions of many different diophantine equations. In particular, he solved the equation $x^2 - dy^2 = 1$ in integers for $d = 8, 11, 32, 61$, and 67, using what he called the "cycle method." One illustration of his keen computational skill is his discovery of the solution of $x^2 - 61y^2 = 1$ with $x = 1{,}766{,}319{,}049$ and $y = 226{,}153{,}980$. Bhaskara also wrote several important books on astronomy, including the *Siddhantasiromani*.

$$\alpha_{k+1} = P_{k+1} + \sqrt{d}.$$

Because $\alpha_{k+1} = [a_{k+1}; a_{k+2}, \ldots]$, the continued fraction expansion of α_{k+1} is purely periodic. Hence, Theorem 12.23 tells us that $-1 < \alpha_{k+1} = P_{k+1} - \sqrt{d} < 0$. This implies that $P_{k+1} = [\sqrt{d}]$, so that $\alpha_k - \alpha_0$, and $n \mid k$.

To see that $Q_j \neq -1$ for $j = 1, 2, 3, \ldots$, note that $Q_j = -1$ implies that $\alpha_j = -P_j - \sqrt{d}$. Because α_j has a purely periodic simple continued fraction expansion, we know that

$$-1 < \alpha_j' = -P_j + \sqrt{d} < 0$$

and

$$\alpha_j = -P_j - \sqrt{d} > 1.$$

From the first of these inequalities, we see that $P_j > -\sqrt{d}$, and from the second, we see that $P_j < -1 - \sqrt{d}$. Because these two inequalities for p_j are contradictory, we see that $Q_j \neq -1$.

Because we have found all solutions of $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$, where x and y are positive integers, we have completed the proof. ∎

We illustrate the use of Theorem 13.10 with the following examples.

Example 13.9. Because the simple continued fraction of $\sqrt{13}$ is $[3; \overline{1, 1, 1, 1, 6}]$, the positive solutions of the diophantine equation $x^2 - 13y^2 = 1$ are p_{10j-1}, q_{10j-1}, $j = 1, 2, 3, \ldots$, where p_{10j-1}/q_{10j-1} is the $(10j - 1)$th convergent of the simple continued fraction expansion of $\sqrt{13}$. The least positive solution is $p_9 = 649, q_9 = 180$. The positive solutions of the diophantine equation $x^2 - 13y^2 = -1$ are p_{10j-6}, $j = 1, 2, 3, \ldots$; the least positive solution is $p_4 = 18, q + 4 = 5$. ◀

Example 13.10. Because the continued fraction of $\sqrt{14}$ is $[3; \overline{1, 2, 1, 6}]$, the positive solutions of $x^2 - 14y^2 = 1$ are p_{4j-1}, q_{4j-1}, $j = 1, 2, 3, \ldots$, where p_{4j-1}/q_{j-1} is the jth convergent of the simple continued fraction expansion of $\sqrt{14}$. The least positive solution is $p_3 = 15, q_3 = 4$. The diophantine equation $x^2 - 14y^2 = -1$ has no solutions, because the period length of the simple continued fraction expansion of $\sqrt{14}$ is even. ◀

We conclude this section with the following theorem, which shows how to find all the positive solutions of Pell's equation, $x^2 - dy^2 = 1$, from the least positive solution, without finding subsequent convergents of the continued fraction expansion of $\sqrt{d}$.

Theorem 13.12. Let x_1, y_1 be the least positive solution of the diophantine equation $x^2 - dy^2 = 1$, where d is a positive integer that is not a perfect square. Then all positive solutions x_k, y_k are given by

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k$$

for $k = 1, 2, 3, \ldots$. (Note that x_k and y_k are determined by the use of Lemma 13.4.)

Proof. We must show that x_k, y_k is a solution for $k = 1, 2, 3, \ldots$, and that every solution is of this form.

To show that x_k, y_k is a solution, first note that by taking conjugates, it follows that $x_k - y_k\sqrt{d} = (x_1 - y_1\sqrt{d})^k$ because, from Lemma 12.4, the conjugate of a power is the power of the conjugate. Now, note that

$$\begin{aligned} x_k^2 - dy_k^2 &= (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^k(x_1 - y_1\sqrt{d})^k \\ &= (x_1^2 - dy_1^2)^k \\ &= 1. \end{aligned}$$

Hence, x_k, y_k is a solution for $k = 1, 2, 3, \ldots$.

To show that every positive solution is equal to x_k, y_k for some positive integer k, assume that X, Y is a positive solution from x_k, y_k for $k = 1, 2, 3, \ldots$. Then there is an integer n such that

$$(x_1 + y_1\sqrt{d})^n < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

When we multiply this inequality by $(x_1 + y_1\sqrt{d})^{-n}$, we obtain

$$1 < (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) < x_1 + y_1\sqrt{d},$$

because $x_1^2 - dy_1^2 = 1$ implies that $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$.

Now, let

$$s + t\sqrt{d} = (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d})$$

and note that

$$\begin{aligned} s^2 - dt^2 &= (s - t\sqrt{d})(s + t\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(X - Y\sqrt{d})(x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) \\ &= (x_1^2 - dy_1^2)^n(X^2 - dY^2) \\ &= 1. \end{aligned}$$

We see that s, t is a solution of $x^2 - dy^2 = 1$ and, furthermore, we know that $1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Moreover, because we know that $s + t\sqrt{d} > 1$, we see that $0 < (s + t\sqrt{d})^{-1} < 1$. Hence,

$$s = \frac{1}{2}\left[(s + t\sqrt{d}) + (s - t\sqrt{d})\right] > 0$$

and

$$t = \frac{1}{2\sqrt{d}}\left[(s + t\sqrt{d}) - (s - t\sqrt{d})\right] > 0.$$

This means that s, t is a positive solution, so that $s \geq x_1$, and $t \geq y_1$, by the choice of x_1, y_1 as the smallest positive solution. But this contradicts the inequality $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Therefore, X, Y must be x_k, y_k for some choice of k. ■

The following example illustrates the use of Theorem 13.11.

Example 13.11. From Example 13.9, we know that the least positive solution of the diophantine equation $x^2 - 13y^2 = 1$ is $x_1 = 649$, $y = 180$. Hence, all positive solutions are given by x_k, y_k where

$$x_k + y_k\sqrt{13} = (649 + 180\sqrt{13})^k.$$

For instance, we have

$$x_2 + y_2\sqrt{13} = 842{,}401 + 233{,}640\sqrt{13}.$$

Hence, $x_2 = 842{,}401$, $y_2 = 233{,}640$ is the least positive solution of $x^2 - 13y^2 = 1$, other than $x_1 = 649$, $y_1 = 180$. ◄

13.4 Exercises

1. Find all of the solutions, where x and y are integers, of each of the following equations.

a) $x^2 + 3y^2 = 4$ b) $x^2 + 5y^2 = 7$ c) $2x^2 + 7y^2 = 30$

2. Find all of the solutions, where x and y are integers, of each of the following equations.

a) $x^2 - y^2 = 8$ b) $x^2 + 4y^2 = 40$ c) $4x^2 + 9y^2 = 100$

3. For which of the following values of n does the diophantine equation $x^2 - 31y^2 = n$ have a solution?

a) 1 c) 2 e) 4
b) -1 d) -3 f) -45

4. Find the least positive solution in integers of each of the following diophantine equations.

a) $x^2 - 29y^2 = -1$ b) $x^2 - 29y^2 = 1$

5. Find the three smallest positive solutions of the diophantine equation $x^2 - 37y^2 = 1$.

6. For each of the following values of d, determine whether the diophantine equation $x^2 - dy^2 = -1$ has solutions in integers.

a) 2 e) 17
b) 3 f) 31
c) 6 g) 41
d) 13 h) 50

7. The least positive solution of the diophantine equation $x^2 - 61y^2 = 1$ is $x_1 = 1{,}766{,}319{,}049$, $y_1 = 226{,}153{,}980$. Find the least positive solution other than x_1, y_1.

* **8.** Show that if p_k/q_k is a convergent of the simple continued fraction expansion of $\sqrt{d}$, then $|p_k^2 - dq_k^2| < 1 + 2\sqrt{d}$.

9. Show that if d is a positive integer divisible by a prime of the form $4k + 3$, then the diophantine equation $x^2 - dy^2 = -1$ has no solutions.

10. Let d and n be positive integers.
    a) Show that if r, s is a solution of the diophantine equation $x^2 - dy^2 = 1$ and X, Y is a solution of the diophantine equation $x^2 - dy^2 = n$, then $Xr \pm dYs, Xs \pm Yr$ is also a solution of $x^2 - dy^2 = n$.
    b) Show that the diophantine equation $x^2 - dy^2 = n$ either has no solutions or has infinitely many solutions.

11. Find those right triangles having legs with lengths that are consecutive integers. (*Hint:* Use Theorem 13.1 to write the lengths of the legs as $x = s^2 - t^2$ and $y = 2st$, where s and t are positive integers such that $(s, t) = 1, s > t$ and s and t have opposite parity. Then $x - y = \pm 1$ implies that $(s - t)^2 - 2t^2 = \pm 1$.)

12. Show that the diophantine equation $x^4 - 2y^4 = 1$ has no nontrivial solutions.

13. Show that the diophantine equation $x^4 - 2y^2 = -1$ has no nontrivial solutions.

14. Show that if t_n, the nth triangular number, equals the mth square, so that $n(n + 1)/2 = m^2$, then $x = 2n + 1$ and $y = m$ are solutions of the diophantine equation $x^2 - 8y^2 = 1$. Find the first five solutions of this diophantine equation in terms of increasing values of the positive integer x and the corresponding pairs of triangular and square numbers.

13.4 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the least positive solution of the diophantine equation $x^2 - 109y^2 = 1$. (This problem was posed by Fermat to English mathematicians in the mid-1600s.)
2. Find the least positive solution of the diophantine equation $x^2 - 991y^2 = 1$.
3. Find the least positive solution of the diophantine equation $x^2 - 1{,}000{,}099y^2 = 1$.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Find those integers n with $|n| < \sqrt{d}$ such that the diophantine equation $x^2 - dy^2 = n$ has no solutions.
2. Find the least positive solutions of the diophantine equations $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$.
3. Find the solutions of Pell's equation from the least positive solution (see Theorem 13.12).

14 The Gaussian Integers

Introduction

In previous chapters we studied properties of the set of integers. A particularly appealing aspect of number theory is that many basic properties of the integers relating to divisibility, primality, and factorization can be carried over to other sets of numbers. In this chapter we study the set of Gaussian integers, numbers of the form $a + bi$, where a and b are integers and $i = \sqrt{-1}$. We will introduce the concept of divisibility for Gaussian integers and establish a version of the division algorithm for these numbers. We will describe what it means for a Gaussian integer to be prime. We will develop the notion of greatest common divisors for pairs of Gaussian integers and show that Gaussian integers can be written uniquely as the product of Gaussian primes (taking into account a few minor details). Finally, we will show how the Gaussian integers can be used to determine how many ways a positive integer can be written as the sum of two squares. The material in this chapter is a small step into the world of algebraic number theory, a major branch of number theory devoted to the study of algebraic numbers and their properties. Students continuing their study of number theory will find this fairly concrete treatment of the Gaussian integers a useful bridge to more advanced studies. Excellent references for the study of algebraic number theory include [AlWi03], [Mo96], [Mo99], [Po99], and [Ri01].

14.1 Gaussian Integers and Gaussian Primes

In this chapter we extend our study of number theory into the realm of complex numbers. We begin with a brief review of the basic properties of the complex numbers for those who have either never seen this material or need a brief refresher.

The complex numbers are the numbers of the form $x + yi$, where $i = \sqrt{-1}$. Complex numbers can be added, subtracted, multiplied, and divided, according to the following rule.

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi) - (c + di) = (a - c) + (b - d)i$$
$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$
$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{ac + bd}{c^2 + d^2} + \frac{(-ad + bc)i}{c^2 + d^2}$$

Note that addition and multiplication of complex numbers are commutative. We use the absolute value of an integer to describe the size of this integer. For complex numbers, there are several commonly used ways to describe the size of numbers.

Definition. If $z = x + iy$ is a complex number, then $|z|$, the *absolute value* of z, equals

$$|z| = \sqrt{x^2 + y^2},$$

and $N(z)$, the *norm* of z, equals

$$|z|^2 = x^2 + y^2.$$

Given a complex number, we can form another complex number with the same absolute value and norm by changing the sign of the imaginary part of the number.

Definition. The *conjugate* of the complex number $z = a + bi$, denoted by $\bar{z}$, is the complex number $x - iy$.

Note that if w and z are two complex numbers, then the conjugate of wz is the product of the conjugates of w and z. That is, $\overline{(wz)} = (\bar{w})(\bar{z})$. Also note that if $z = x + iy$ is a complex number, then

$$z\bar{z} = (x + iy)(x - iy) = x^2 + y^2 = N(z).$$

We will now prove some useful properties of norms.

Theorem 14.1. The norm function N from the set of complex numbers to the set of nonnegative real numbers satisfies the following properties.

(i) $N(z)$ is a nonnegative real number for all complex numbers z.
(ii) $N(zw) = N(z)N(w)$ for all complex numbers z and w.
(iii) $N(z) = 0$ if and only if $z = 0$.

To prove (i), suppose that z is a complex number. Then $z = x + iy$, where x and y are real numbers. It follows that $N(z) = x^2 + y^2$ is a nonnegative real number because both x^2 and y^2 are nonnegative real numbers.

To prove (ii), note that

$$N(zw) = (zw)\overline{(zw)} = (zw)(\overline{z}\,\overline{w}) = (z\overline{z})(w\overline{w}) = N(z)N(w),$$

whenever z and w are complex numbers.

To prove (iii), note that $0 = 0 + 0i$, so that $N(0) = 0^2 + 0^2 = 0$. Conversely, suppose that $N(x + iy) = 0$, where x and y are integers. Then $x^2 + y^2 = 0$, which implies that $x = 0$ and $y = 0$ because both x^2 and y^2 are nonnegative. Hence, $x + iy = 0 + i0 = 0$. ■

Gaussian Integers

In previous chapters we generally restricted ourselves to the rational numbers and integers. An important branch of number theory, called *algebraic number theory*, extends the theory we have developed for the integers to particular sets of algebraic integers. By an algebraic integer, we mean a root of a monic polynomial (that is, with leading coefficient 1) with integer coefficients. We now introduce the particular set of algebraic integers we will study in this chapter.

Definition. Complex numbers of the form $a + bi$, where a and b are integers, are called *Gaussian integers*. The set of all Gaussian integers is denoted by $\mathbf{Z}[i]$.

Note that if $\gamma = a + bi$ is a Gaussian integer, then it is an algebraic integer satisfying the equation

$$\gamma^2 - 2a\gamma + (a^2 + b^2) = 0,$$

as the reader should verify. Because γ satisfies a monic polynomial with integer coefficients of degree two, it is called a *quadratic irrational*. Conversely, note that if α is a number of the form $r + si$, where r and s are rational numbers and α is a root of a monic quadratic polynomial with integer coefficients, then α is a Gaussian integer (see Exercise 20.) The Gaussian integers are named after the great German mathematician Carl Friedrich Gauss, who was the first to extensively study their properties.

The usual convention is to use Greek letters, such as α, β, γ, and δ to denote Gaussian integers. Note that if n is an integer, then $n = n + 0i$ is also a Gaussian integer. We call an integer n a *rational integer* when we are discussing Gaussian integers.

The Gaussian integers are closed under addition, subtraction, and multiplication, as the following theorem shows.

Theorem 14.2. Suppose that $\alpha = x + iy$ and $\beta = w + iz$ are Gaussian integers, where x, y, w, and z are rational integers. Then $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ are all Gaussian integers.

Proof. We have $\alpha + \beta = (x + iy) + (w + iz) = (x + w) + i(y + z)$, $\alpha - \beta = (x + iy) - (w + iz) = (x - w) + i(y - z)$, and $\alpha\beta = (x + iy)(w + iz) = xw + iyw + ixz + i^2yz = (xw - yz) + i(yw + xz)$. Because the rational integers are closed under addition, subtraction, and multiplication, it follows that each of $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ are Gaussian integers. ■

Although the Gaussian integers are closed under addition, subtraction, and multiplication, they are not closed under division, which is also the case for the rational integers. Also, note that if $\alpha = a + bi$ is a Gaussian integer, then $N(\alpha) = a^2 + b^2$ is a nonnegative rational integer.

Divisibility of Gaussian Integers

We can study the set of Gaussian integers much as we have studied the set of rational integers. There are straightforward analogies to many of the basic properties of the integers for the Gaussian integers. To develop these properties for the Gaussian integers, we need to introduce some concepts for the Gaussian integers analogous to those for the ordinary integers. In particular, we need to define what it means for one Gaussian integer to divide another. Later, we will define Gaussian primes, greatest common divisors of pairs of Gaussian integers, and other important notions.

Definition. Suppose that α and β are Gaussian integers. We say that α *divides* β if there exists a Gaussian integer γ such that $\beta = \alpha\gamma$. If α divides β, we write $\alpha \mid \beta$, whereas if α does not divide β, we write $\alpha \nmid \beta$.

Example 14.1. We see that $2 - i \mid 13 + i$ because

$$(2 - i)(5 + 3i) = 13 + i.$$

However, $3 + 2i \nmid 6 + 5i$ because

$$\frac{6 + 5i}{3 + 2i} = \frac{(6 + 5i)(3 - 2i)}{(3 + 2i)(3 - 2i)} = \frac{28 + 3i}{13} = \frac{28}{13} + \frac{3i}{13},$$

which is not a Gaussian integer. ◀

Example 14.2. We see that $-i \mid (a + bi)$ for all Gaussian integers $a + bi$ because $a + bi = -i(-b + ai)$, whenever a and b are integers. The only other Gaussian integers that divide all other Gaussian integers are 1, -1, and i. We will see why this is true later in this section. ◀

Example 14.3. The Gaussian integers divisible by the Gaussian integer $3 + 2i$ are the numbers $(3 + 2i)(a + ib)$, where a and b are integers. Note that $(3 + 2i)(a + ib) = 3a + 2ia + 3ib + 2i^2b = (3a - 2b) + i(2a + 3b)$. We display these Gaussian integers in Figure 14.1. ◀

Divisibility in the Gaussian integers satisfies many of the same properties satisfied by divisibility of rational integers. For example, if α, β, and γ are Gaussian integers and $\alpha \mid \beta$ and $\beta \mid \gamma$, then $\alpha \mid \gamma$. Furthermore, if α, β, γ, ν, and μ are Gaussian integers and $\gamma \mid \alpha$ and $\gamma \mid \beta$, then $\gamma \mid (\mu\alpha + \nu\beta)$. We leave it to the reader to verify that these properties hold.

In the integers, there are exactly two integers that are divisors of the integer 1, namely 1 and -1. We now determine which Gaussian integers are divisors of 1. We begin with a definition.

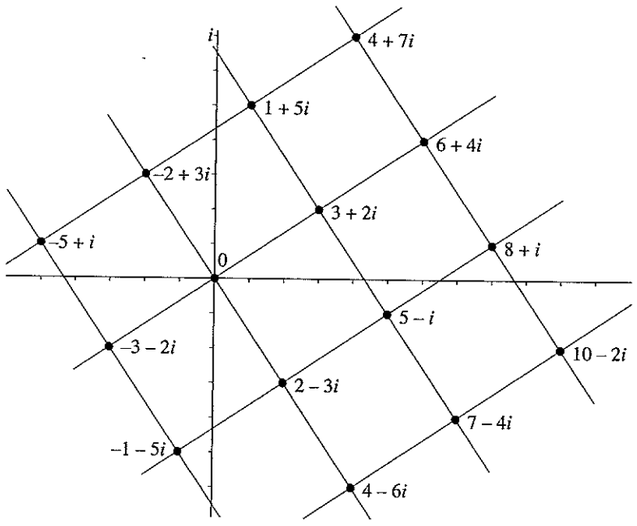


Figure 14.1 *The Gaussian integers divisible by* $3 + 2i$.

Definition. A Gaussian integer ϵ is called a *unit* if ϵ divides 1. When ϵ is a unit, $\epsilon\alpha$ is an *associate* of the Gaussian integer α

We now characterize which Gaussian integers are units in a way that will make them easy to find.

Theorem 14.3. A Gaussian integer ϵ is a unit if and only if $N(\epsilon) = 1$.

Proof. First suppose that ϵ is a unit. Then there a Gaussian integer ν such that $\epsilon\nu = 1$. By part (ii) of Theorem 14.1, it follows that $N(\epsilon\nu) = N(\epsilon)N(\nu) = 1$. Because ϵ and ν are Gaussian integers, both $N(\epsilon)$ and $N(\nu)$ are positive integers. It follows that $N(\epsilon) = N(\nu) = 1$.

Conversely, suppose that $N(\epsilon) = 1$. Then $\epsilon\overline{\epsilon} = N(\epsilon) = 1$. It follows that $\epsilon \mid 1$ and ϵ is a unit. ∎

We now determine which Gaussian integers are units.

Theorem 14.4. The Gaussian integers that are units are $1, -1, i$, and $-i$.

Proof. By Theorem 14.3, the Gaussian integer $\epsilon = a + bi$ is a unit if and only if $N(\epsilon) = 1$. Because $N(\epsilon) = N(a + bi) = a^2 + b^2$, ϵ is a unit if and only if $a^2 + b^2 = 1$. Because a and b are rational integers, we can conclude that $\epsilon = a + bi$ is a unit if and only if $(a, b) = (1, 0), (-1, 0), (0, 1)$, or $(0, -1)$. It follows that ϵ is a unit if and only if $\epsilon = 1, -1, i$, or $-i$. ∎

Now that we know which Gaussian integers are units, we see that the associates of a Gaussian integer β are the four Gaussian integers $\beta, -\beta, i\beta$, and $-i\beta$.

Example 14.4. The associates of the Gaussian integer $-2+3i$ are $-2+3i$, $-(-2+3i) = 2-3i$, $i(-2+3i) = -2i+3i^2 = -3-2i$, and $-i(-2+3i) = 2i-3i^2 = 3+2i$. ◀

Gaussian Primes

Note that a rational integer is prime if and only if it is not divisible by an integer other than $1, -1$, itself, or its negative. To define Gaussian primes, we want to ignore divisibility by units and associates.

Definition. A nonzero Gaussian integer π is a Gaussian *prime* if it is not a unit and is divisible only by units and its associates.

It follows from the definition of a Gaussian prime that a Gaussian integer π is prime if and only if it has exactly eight divisors, the four units and its four associates, namely $1, -1, i, -i, \pi, -\pi, i\pi$, and $-i\pi$. (Units in the Gaussian integers have exactly four divisors, namely the four units. Gaussian integers that are not prime and are not units have more than eight different divisors.)

An integer that is prime in the set of integers is called a *rational prime*. Later we will see that some rational primes are Gaussian primes, but some are not. Prior to providing examples of Gaussian primes, we prove a useful result which we can use to help determine whether a Gaussian integer is prime.

Theorem 14.5. If π is a Gaussian integer and $N(\pi) = p$, where p is a rational prime, then π and $\overline{\pi}$ are Gaussian primes, but p is not a Gaussian prime.

Proof. Suppose that $\pi = \alpha\beta$, where α and β are Gaussian integers. Then $N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta)$, so that $p = N(\alpha)N(\beta)$. Because $N(\alpha)$ and $N(\beta)$ are positive integers, it follows that $N(\alpha) = 1$ and $N(\beta) = p$ or $N(\alpha) = p$ and $N(\beta) = 1$. We conclude by Theorem 14.3 that either α is a unit or β is a unit. This means that π cannot be factored into two Gaussian integers neither of which is a unit, so it must be a Gaussian prime.

Note that $N(\pi) = \pi \cdot \overline{\pi}$. Because $N(\pi) = p$, it follows that $p = \pi\overline{\pi}$, which means that p is not a Gaussian prime. Note that because $N(\overline{\pi}) = p$, $\overline{\pi}$ is also a Gaussian prime. ■

We now give some examples of Gaussian primes.

Example 14.5. We can use Theorem 14.5 to show that $2 - i$ is a Gaussian prime because $N(2-i) = 2^2 + 1^2 = 5$ and 5 is a rational prime. Also, note that $5 = (2+i)(2-i)$, so that 5 is not a Gaussian prime. Similarly, $2+3i$ is a Gaussian prime because $N(2+3i) = 2^2 + 3^2 = 13$ and 13 is a rational prime. Moreover, 13 is not a Gaussian prime because $13 = (2+3i)(2-3i)$. ◀

The converse of Theorem 14.5 is not true. It is possible for a Gaussian prime to have a norm that is not a rational prime, as we will see in Example 14.6.

Example 14.6. The integer 3 is a Gaussian prime, as we will show, but $N(3) = N(3+0i) = 3^2 + 0^2 = 9$ is not a rational prime. To see that 3 is a Gaussian prime, suppose that $3 = (a+bi)(c+di)$, where $a+bi$ and $c+di$ are not units. By taking norms of both sides of this equation, we find that

$$N(3) = N((a+bi)\cdot(c+di)).$$

It follows that

$$9 = N(a+ib)N(c+id),$$

using part (ii) of Theorem 14.1. Because neither $a+ib$ nor $c+id$ is a unit, $N(a+ib) \neq 1$ and $N(c+id) \neq 1$. Consequently, $N(a+ib) = N(c+id) = 3$. This means that $N(a+ib) = a^2 + b^2 = 3$, which is impossible because 3 is not the sum of two squares. It follows that 3 is a Gaussian prime. ◀

We now determine whether the rational prime 2 is also a Gaussian prime.

Example 14.7. To determine whether 2 is a Gaussian prime, we determine whether there are Gaussian integers α and β neither a unit such that $2 = \alpha\beta$, where $\alpha = a+ib$ and $\beta = c+id$. If $2 = \alpha\beta$, by taking norms, we see that

$$N(2) = N(\alpha)N(\beta).$$

Because $N(2) = N(2+0i) = 2^2 + 0^2 = 4$, this means that

$$N(\alpha)N(\beta) = (a^2+b^2)(c^2+d^2) = 4.$$

Because neither α nor β is a unit, we know that $N(\alpha) \neq 1$ and $N(\beta) \neq 1$. It follows that $a^2 + b^2 = 2$ and $c^2 + d^2 = 2$ so that each of a, b, c, and d equals 1 or -1. Consequently, α and β must take on one of the values $1+i$, $-1+i$, $1-i$, or $-1-i$. On inspection, we find that when $\alpha = 1+i$ and $\beta = 1-i$, we have $\alpha\beta = 2$. We conclude that 2 is not a Gaussian prime and $2 = (1+i)(1-i)$.

However, $1+i$ and $1-i$ are both Gaussian primes, because $N(1+i) = N(1-i) = 2$ and 2 is prime, so that Theorem 14.5 applies. ◀

Looking at Examples 14.5, 14.6, and 14.7, we see that some rational primes are also Gaussian primes, such as 3, while other rational primes, such as $2 = (1-i)(1+i)$ and $5 = (2+i)(2-i)$ are not Gaussian primes. In Section 14.3 we will determine which rational primes are also Gaussian primes and which are not.

The Division Algorithm for Gaussian Integers

In the first chapter of this book we introduced the division algorithm for rational integers, which shows that when we divide an integer a by a positive integer divisor b, we obtain a nonnegative remainder r less than b. Furthermore, the quotient and remainder we

obtain are unique. We would like an analogous result for the Gaussian integers, but in the Gaussian integers it does not make sense to say that a remainder of a division is smaller than the divisor. We overcome this difficulty by developing a division algorithm where the remainder of a division has norm less than the norm of the divisor. However, unlike the situation for rational integers, the quotient and remainder we compute are not unique, as we will illustrate with a subsequent example.

Theorem 14.6. ***The Division Algorithm for Gaussian Integers.*** Let α and β be Gaussian integers with $\beta \neq 0$. Then there exist Gaussian integers γ and ρ such that

$$\alpha = \beta\gamma + \rho$$

and $0 \leq N(\rho) < N(\beta)$. Here γ is called the *quotient* and ρ is called the *remainder* of this division.

Proof. Suppose that $\alpha/\beta = x + iy$. Then $x + iy$ is a complex number which is a Gaussian integer if and only if β divides α. Suppose that $s = [x + \frac{1}{2}]$ and $t = [y + \frac{1}{2}]$ (these are the integers closest to x and y, respectively, rounded up if the fractional part of x or y equals 1/2; see Figure 14.2).

With these choices for s and t, we find that

$$x + iy = (s + f) + i(t + g),$$

where f and g are real numbers with $|f| \leq 1/2$ and $|g| \leq 1/2$. Now, let $\gamma = s + ti$ and $\rho = \alpha - \beta\gamma$. By Theorem 14.1, we know that $N(\rho) \geq 0$.

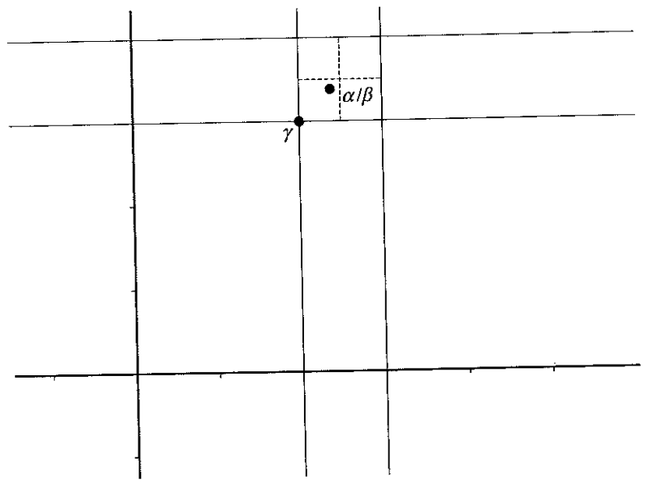


Figure 14.2 *Determining the quotient γ when α is divided by β.*

To show that $N(\rho) < N(\beta)$, recalling that $\alpha/\beta = x + iy$ and using Theorem 14.1 (ii), we see that

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\gamma) = N(((\alpha/\beta) - \gamma)\beta) = N((x + iy) - \gamma)\beta) \\ &= N((x + iy) - \gamma)N(\beta). \end{aligned}$$

Because $\gamma = s + ti$, $x - s = f$, and $y - t = g$, we find that

$$N(\rho) = N((x + iy) - (s + ti))N(\beta) = N(f + ig)N(\beta).$$

Finally, because $|f| \leq 1/2$ and $|g| \leq 1/2$, we conclude that

$$N(\rho) = N(f + ig)N(\beta) \leq ((1/2)^2 + (1/2)^2)N(\beta) \leq N(\beta)/2 < N(\beta).$$

This completes the proof. ■

Remark. In the proof of Theorem 14.6 when we divide a Gaussian integer α by a nonzero Gaussian integer β, we construct a remainder ρ such that $0 \leq N(\rho) \leq N(\beta)/2$. That is, the norm of the remainder does not exceed 1/2 of the norm of the divisor. This will be a useful fact to remember.

Example 14.8 illustrates how to find the quotient and remainder computed in the proof of Theorem 14.6. This example also illustrates that these values are not unique, in the sense that there are other possible values that satisfy the conclusions of the theorem.

Example 14.8. Let $\alpha = 13 + 20i$ and $\beta = -3 + 5i$. We can follow the steps in the proof of Theorem 14.6 to find γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$, that is, with $13 + 20i = (-3 + 5i)\gamma + \rho$ and $0 \leq N(\rho) < N(-3 + 5i) = 34$. We first divide α by β to obtain

$$\frac{13 + 20i}{-3 + 5i} = \frac{61}{34} - \frac{125}{34}i.$$

Next, we find the integers closest to $\frac{61}{34}$ and $\frac{-125}{34}$, namely 2 and -4, respectively. Consequently, we take $\gamma = 2 - 4i$ as the quotient. The corresponding remainder is $\rho = \alpha - \beta\gamma = (13 + 20i) - (-3 + 5i)\gamma = (13 + 20i) - (-3 + 5i)(2 - 4i) = -1 - 2i$. We verify that $N(\rho) < N(\beta)$ by noting that $N(-1 - 2i) = 5 < N(-3 + 5i) = 34$, as expected.

Other choices for γ and ρ besides those produced by the construction in the proof of Theorem 14.6 satisfy the consequences of the division algorithm. For example, we can take $\gamma = 2 - 3i$ and $\rho = 4 + i$, because $13 + 20i = (-3 + 5i)(2 - 3i) + (4 + i)$ and $N(4 + i) = 17 < N(-3 + 5i) = 34$. (See Exercise 19.) ◀

14.1 Exercises

1. Simplify each of the following expressions, expressing your answer in the form of a Gaussian integer $a + bi$.

a) $(2 + i)^2(3 + i)$ b) $(2 - 3i)^3$ c) $-i(-i + 3)^3$

2. Simplify each of the following expressions, expressing your answer in the form of a Gaussian integer $a + bi$.

a) $(-1+i)^3(1+i)^3$ b) $(3+2i)(3-i)^2$ c) $(2+i)^2(5-i)^3$

3. Determine whether the Gaussian integer α divides the Gaussian integer β if

a) $\alpha = 2 - i$, $\beta = 5 + 5i$.
b) $\alpha = 1 - i$, $\beta = 8$.
c) $\alpha = 5$, $\beta = 2 + 3i$.
d) $\alpha = 3 + 2i$, $\beta = 26$.

4. Determine whether the Gaussian integer α divides the Gaussian integer β, where

a) $\alpha = 3$, $\beta = 4 + 7i$.
b) $\alpha = 2 + i$, $\beta = 15$.
c) $\alpha = 5 + 3i$, $\beta = 30 + 6i$.
d) $\alpha = 11 + 4i$, $\beta = 274$.

5. Give a formula for all Gaussian integers divisible by $4 + 3i$ and display the set of all such Gaussian integers in the plane.

6. Give a formula for all Gaussian integers divisible by $4 - i$ and display the set of all such Gaussian integers in the plane.

7. Show that if α, β, and γ are Gaussian integers and $\alpha \mid \beta$ and $\beta \mid \gamma$, then $\alpha \mid \gamma$.

8. Show that if α, β, γ, μ, and ν are Gaussian integers and $\gamma \mid \alpha$ and $\gamma \mid \beta$, then $\gamma \mid (\mu\alpha + \nu\beta)$.

9. Show that if ϵ is a unit for the Gaussian integers, then $\epsilon^5 = \epsilon$.

10. Find all Gaussian integers $\alpha = a + bi$ such that $\overline{\alpha} = a - bi$, the conjugate of α, is an associate of α.

11. Show that the Gaussian integers α and β are associates if $\alpha \mid \beta$ and $\beta \mid \alpha$.

12. Show that if α and β are Gaussian integers and $\alpha \mid \beta$, then $N(\alpha) \mid N(\beta)$.

13. Suppose that $N(\alpha) \mid N(\beta)$, where α and β are Gaussian integers. Does it necessarily follow that $\alpha \mid \beta$? Supply either a proof or a counterexample.

14. Show that if α divides β, where α and β are Gaussian integers, then $\overline{\alpha}$ divides $\overline{\beta}$.

15. Show that if $\alpha = a + bi$ is a nonzero Gaussian integer, then α has exactly one associate $c + di$ (including α itself), where $c > 0$ and $d \geq 0$.

16. For each pair of values for α and β, find the quotient γ and the remainder ρ when α is divided by β computed following the construction in the proof of Theorem 14.6, and verify that $N(\rho) < N(\beta)$.

a) $\alpha = 14 + 17i$, $\beta = 2 + 3i$
b) $\alpha = 7 - 19i$, $\beta = 3 - 4i$
c) $\alpha = 33$, $\beta = 5 + i$

17. For each pair of values for α and β, find the quotient γ and the remainder ρ when α is divided by β computed following the construction in the proof of Theorem 14.6, and verify that $N(\rho) < N(\beta)$.

a) $\alpha = 24 - 9i$, $\beta = 3 + 3i$
b) $\alpha = 18 + 15i$, $\beta = 3 + 4i$
c) $\alpha = 87i$, $\beta = 11 - 2i$

18. For each pair of values for α and β in Exercise 16, find a pair of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ different from that computed following the construction in Theorem 14.6.

19. For each pair of values for α and β in Exercise 17, find a pair of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ different from that computed following the construction in Theorem 14.6.

20. Show that for every pair of Gaussian integers α and β with $\beta \neq 0$ and $\beta \nmid \alpha$, there are at least two different pairs of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$.

* **21.** Determine all possible values for the number of pairs of Gaussian integers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$ when α and β are Gaussian integers and $\beta \neq 0$. (*Hint:* Analyze this geometrically by looking at the position of α/β in the square containing it and with four lattice points as its corners.)

22. Show that if a number of the form $r + si$, where r and s are rational numbers, is an algebraic integer, then r and s are integers.

23. Show that $1 + i$ divides a Gaussian integer $a + ib$ if and only if a and b are both even or both odd.

24. Show that if π is a Gaussian prime, then $N(\pi) = 2$ or $N(\pi) \equiv 1 \pmod 4$.

25. Find all Gaussian primes of the form $\alpha^2 + 1$, where α is a Gaussian integer.

26. Show that if $a + bi$ is a Gaussian prime, then $b + ai$ is also a Gaussian prime.

27. Show that the rational prime 7 is also a Gaussian prime by adapting the argument given in Example 14.6 that shows 3 is a Gaussian prime.

28. Show that every rational prime p of the form $4k + 3$ is also a Gaussian prime.

29. Suppose that α is a nonzero Gaussian integer which is neither a unit nor a prime. Show that a Gaussian integer β exists such that $\beta \mid \alpha$ and $1 < N(\beta) \leq \sqrt{N(\alpha)}$.

30. Explain how to adapt the sieve of Eratosthenes to find all the Gaussian primes with norm less than a specified limit.

31. Find all the Gaussian primes with norm less than 100.

32. Display all the Gaussian primes with norm less than 200 as lattice points in the plane.

We can define the notion of congruence for Gaussian integers. Suppose that α, β, and γ are Gaussian integers and that $\gamma \neq 0$. We say that α is *congruent* to β modulo γ and we write $\alpha \equiv \beta \pmod \gamma$ if $\gamma \mid (\alpha - \beta)$.

33. Suppose that μ is a nonzero Gaussian integer. Show that each of the following properties holds.

a) If α is a Gaussian integer, then $\alpha \equiv \alpha \pmod \mu$.

b) If $\alpha \equiv \beta \pmod \mu$, then $\beta \equiv \alpha \pmod \mu$.

c) If $\alpha \equiv \beta \pmod \mu$ and $\beta \equiv \gamma \pmod \mu$, then $\alpha \equiv \gamma \pmod \mu$.

34. Suppose that $\alpha \equiv \beta \pmod \mu$ and $\gamma \equiv \delta \pmod \mu$, where α, β, γ, δ, and μ are Gaussian integers and $\mu \neq 0$. Show that each of these properties holds.

a) $\alpha + \gamma \equiv \beta + \delta \pmod \mu$

b) $\alpha - \gamma \equiv \beta - \delta \pmod \mu$

c) $\alpha\gamma \equiv \beta\delta \pmod \mu$

35. Show that two Gaussian integers $\alpha = a_1 + ib_1$ and $\beta = a_2 + ib_2$ can multiplied using only three multiplications of rational integers, rather than the four in the equation shown

in the text, together with five additions and subtractions. (*Hint:* One way to do this uses the product $(a_1 + b_1)(a_2 + b_2)$. A second way uses the product $b_2(a_1 + b_1)$.)

36. When a and b are real numbers, let $\{a + bi\} = \{a\} + \{b\}i$, where $\{x\}$ is the closest integer to the real number x, rounding up in the case of a tie. Show that if z is a complex number, no Gaussian integer is closer to z than $\{z\}$ and $N(z - \{z\}) \leq 1/2$.

Let k be a nonnegative integer. The *Gaussian Fibonacci number* G_k is defined in terms of the Fibonacci numbers with $G_k = f_k + if_{k+1}$. Exercises 37–39 involve Gaussian Fibonacci numbers.

37. a) List the terms of the Gaussian Fibonacci sequence for $k = 0, 1, 2, 3, 4, 5$. (Recall that $f_0 = 0$.)

b) Show that $G_k = G_{k-1} + G_{k-2}$ for $k = 2, 3, \ldots$.

38. Show that $N(G_k) = f_{2k+1}$ for all nonnegative integers k.

39. Show that $G_{n+2}G_{n+1} - G_{n+3}G_n = (-1)^n(2 + i)$, whenever n is a positive integer.

40. Show that every Gaussian integer can be written in the form $a_n(-1 + i)^n + a_{n-1}(-1 + i)^{n-1} + \cdots + a_1(-1 + i) + a_0$, where $a_j = 0$ or 1 for $j = 0, 1, \ldots, n - 1, n$.

41. Show that if α is a number of the form $r + si$, where r and s are rational numbers and α is a root of a monic quadratic polynomial with integer coefficients, then α is a Gaussian integer.

42. What can you conclude if $\pi = a + bi$ is a Gaussian prime and one of the Gaussian integers $(a + 1) + bi$, $(a - 1) + bi$, $a + (b + 1)i$, and $a + (b - 1)i$ is also a Gaussian prime?

43. Show that if $\pi_1 = a - 1 + bi, \pi_2 = a + 1 + bi, \pi_3 = a + (b - 1)i$, and $\pi_4 = a + (b + 1)i$ are all Gaussian primes and $|a| + |b| > 5$, then 5 divides both a and b and neither a nor b is zero.

44. Describe the block of Gaussian integers containing no Gaussian primes that can be constructed by first forming the product of all Gaussian integers $a + bi$ with a and b rational integers, $0 \leq a \leq m$, and $0 \leq b \leq n$.

45. Find all Gaussian integers α, β, and γ such that $\alpha\beta\gamma = \alpha + \beta + \gamma = 1$.

46. Show that if π is a Gaussian prime with $N(\pi) \neq 2$, then exactly one of the associates of π is congruent to either 1 or $3 + 2i$ modulo 4.

14.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find all pairs of Gaussian integers γ and ρ such that $180 - 181i = (12 + 13i)\gamma + \rho$ and $N(\rho) < N(12 + 13i)$.

2. Use a version of the sieve of Eratosthenes to find all Gaussian primes with norm less than 1000.

3. Find as many different pairs of Gaussian primes that differ by 2 as you can.

4. Find as many triples of Gaussian primes that form an arithmetic progression with a common difference of 2 as you can.
5. Find as many Gaussian primes of the form $\alpha^2 + \alpha + (9 + 4i)$ as you can.
6. Estimate the probability that two randomly chosen Gaussian integers are relatively prime by testing whether a large number of randomly chosen pairs of Gaussian integers are relatively prime.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Given two Gaussian integers α and β, find all pairs of Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$.
2. Implement a version of the sieve of Eratosthenes to find all Gaussian primes with norm less than a specified integer.
3. Given a positive real number k and a positive integer n, find all Gaussian primes with norm less than n that can be reached, starting with a Gaussian prime with norm not exceeding five moving from one Gaussian prime to the next in steps not exceeding k.
4. Display a graph of the Gaussian primes that can be reached as described in the preceding programming project.

** 5. Given a positive real number k, search for *Gaussian moats,* which are regions of width k in the complex plane surrounding the origin that contain no Gaussian integers. (See [GeWaWi98] for more information about Gaussian moats.)

14.2 Greatest Common Divisors and Unique Factorization

In Chapter 3 we showed that every pair of rational integers not both zero has a greatest common divisor. Using properties of the greatest common divisor, we showed that if a prime divides the product of two integers, it must divide one of these integers. We used this fact to show that every integer can be uniquely written as the product of the powers of primes when these primes are written in increasing order. In this section we will establish analogous results for the Gaussian integers. We first develop the concept of greatest common divisors for Gaussian integers. We will show that every pair of Gaussian integers, not both zero, has a greatest common divisor. Then we will show that if a Gaussian prime divides the product of two Gaussian integers, it must divide one of these integers. We will use this result to develop a unique factorization theorem for the Gaussian integers.

Greatest Common Divisors

We cannot adapt the original definition we gave for greatest common divisors of integers because it does not make sense to say that one Gaussian integer is larger than another one. However, we will be able to define the notion of a greatest common divisor for a pair of Gaussian integers by adapting the characterization of the greatest common divisor of two rational integers that does not use the ordering of the integers given in Theorem 3.10.

Definition. Let α and β be Gaussian integers. A *greatest common divisor* of α and β is a Gaussian integer γ with these two properties:

(i) $\gamma \mid \alpha$ and $\gamma \mid \beta$;

and

(ii) if $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$.

If γ is a greatest common divisor of the Gaussian integers α and β, then it is straightforward to show that all associates of γ are also greatest common divisors of α and β (see Exercise 5). Consequently, if γ is a greatest common divisor of α and β, then $-\gamma$, $i\gamma$, and $-i\gamma$ are also greatest common divisors of α and β. The converse is also true, that is, any two greatest common divisors of two Gaussian integers are associates, as we will prove later in this section. First, we will show that a greatest common divisor exists for every two Gaussian integers.

Theorem 14.7. If α and β are Gaussian integers, not both zero, then

(i) there exists a greatest common divisor γ of α and β;

and

(ii) if γ is a greatest common divisor of α and β, then there exist Gaussian integers μ and ν such that $\gamma = \mu\alpha + \nu\beta$.

Proof. Let S be the set of norms of nonzero Gaussian integers of the form

$$\mu\alpha + \nu\beta,$$

where μ and ν are Gaussian integers. Because $\mu\alpha + \nu\beta$ is a Gaussian integer when μ and ν are Gaussian integers and the norm of a nonzero Gaussian integer is a positive integer, every element of S is a positive integer. S is nonempty, which can be seen because $N(1 \cdot \alpha + 0 \cdot \beta) = N(\alpha)$ and $N(0 \cdot \alpha + 1 \cdot \beta) = N(\beta)$ both belong to S and both cannot be 0.

Because S is a nonempty set of positive integers, by the well-ordering property, it contains a least element. Consequently, a Gaussian integer γ exists with

$$\gamma = \mu_0\alpha + \nu_0\beta,$$

where μ_0 and ν_0 are Gaussian integers and $N(\gamma) \leq N(\mu\alpha + \nu\beta)$ for all Gaussian integers μ and ν.

We will show that γ is a greatest common divisor of α and β. First, suppose that $\delta \mid \alpha$ and $\delta \mid \beta$. Then there exist Gaussian integers ρ and σ such that $\alpha = \delta\rho$ and $\beta = \delta\sigma$. It follows that

$$\gamma = \mu_0\alpha + \nu_0\beta = \mu_0\delta\rho + \nu_0\delta\sigma = \delta(\mu_0\rho + \nu_0\sigma).$$

We see that $\delta \mid \gamma$.

To show that $\gamma|\alpha$ and $\gamma|\beta$ we will show that γ divides every Gaussian integer of the form $\mu\alpha + \nu\beta$. So suppose that $\tau = \mu_1\alpha + \nu_1\beta$ for Gaussian integers μ_1 and ν_1. By

Theorem 14.6, the division algorithm for Gaussian integers, we see that

$$\tau = \gamma\eta + \zeta,$$

where η and ζ are Gaussian integers with $0 \leq N(\zeta) < N(\gamma)$. Furthermore, ζ is a Gaussian integer of the form $\mu\alpha + \nu\beta$. To see this note that

$$\zeta = \tau - \gamma\eta = (\mu_1\alpha + \nu_1\beta) - (\mu_0\alpha + \nu_0\beta)\eta = (\mu_1 - \mu_0\eta)\alpha + (\nu_1 - \nu_0\eta)\beta.$$

Recall that γ was chosen as an element with smallest possible norm among the nonzero Gaussian integers of the form $\mu\alpha + \nu\beta$. Consequently, because ζ has this form and $0 \leq N(\zeta) < N(\gamma)$, we know that $N(\zeta) = 0$. By Theorem 14.1, we see that $\zeta = 0$. Consequently, $\tau = \gamma\eta$. We conclude that every element Gaussian integer of the form $\mu\alpha + \nu\beta$ is divisible by γ. ∎

We now show that any two greatest common divisors of two Gaussian integers must be associates.

Theorem 14.8. If both γ_1 and γ_2 are greatest common divisors of the Gaussian integers α and β, not both zero, then γ_1 and γ_2 are associates of each other.

Proof. Suppose that γ_1 and γ_2 are both greatest common divisors of α and β. By part (ii) of the definition of greatest common divisor, it follows that $\gamma_1 \mid \gamma_2$ and $\gamma_2 \mid \gamma_1$. This means there are Gaussian integers ϵ and θ such that $\gamma_2 = \epsilon\gamma_1$ and $\gamma_1 = \theta\gamma_2$. Combining these two equations, we see that

$$\gamma_1 = \theta\epsilon\gamma_1.$$

Divide both sides by γ_1 (which does not equal 0 because 0 is not a common divisor of two Gaussian integers if they are not both zero) to see that

$$\theta\epsilon = 1.$$

We conclude that θ and ϵ are both units. Because $\gamma_1 = \theta\gamma_2$, we see that γ_1 and γ_2 are associates. ∎

The demonstration that the converse of Theorem 14.8 is also true is left as Exercise 5 at the end of this section.

Definition. The Gaussian integers α and β are *relatively prime* if 1 is a greatest common divisor of α and β.

Note that 1 is a greatest common divisor of α and β if and only if the associates of 1, namely -1, i, and $-i$, are also greatest common divisors of α and β. For example, if we know that i is a greatest common divisor of α and β, then these two Gaussian integers are relatively prime.

We can adapt the Euclidean algorithm (Theorem 3.11) to find a greatest common divisor of two Gaussian integers.

Theorem 14.9. ***A Euclidean Algorithm for Gaussian Integers.*** Let $\rho_0 = \alpha$ and $\rho_1 = \beta$ be nonzero Gaussian integers. If the division algorithm for Gaussian integers is

successively applied to obtain $\rho_j = \rho_{j+1}\gamma_{j+1} + r_{j+2}$, with $N(\rho_{j+2}) < N(\rho_{j+1})$ for $j = 0, 1, 2, \ldots, n-2$ and $\rho_{n+1} = 0$, then ρ_n, the last nonzero remainder, is a greatest common divisor of α and β.

We leave the proof of Theorem 14.9 to the reader; it is a straightforward adaption of the proof of Theorem 3.11. Note that we can also work backward through the steps of the Euclidean algorithm for Gaussian integers to express the greatest common divisor found by the algorithm as a linear combination of the two Gaussian integers provided as input to the algorithm. We illustrate this in the following example.

Example 14.9. Suppose that $\alpha = 97 + 210i$ and $\beta = 123 + 16i$. The version of the Euclidean algorithm based on the version of the division algorithm in the proof of Theorem 4.6 can be used to find the greatest common divisors of α and β with the following steps.

$$\begin{aligned}
97 + 210i &= (123 + 16i)(1 + 2i) + (6 - 52i) \\
123 + 16i &= (6 - 52i)(2i) + (19 + 4i) \\
6 - 52i &= (19 + 4i)(-3i) + (-6 + 5i) \\
19 + 4i &= (-6 + 5i)(-2 - 2i) + (-3 + 2i) \\
-6 + 5i &= (-3 + 2i)2 + i \\
-3 + 2i &= i(2 + 3i) + 0
\end{aligned}$$

We conclude that i is a greatest common divisor of $97 + 210i$ and $123 + 16i$. Consequently, all greatest common divisors of these two Gaussian integers are the associates of i, namely 1, -1, i, and $-i$. It follows that $97 + 210i$ and $123 + 6i$ are relatively prime.

Because $97 + 210i$ and $123 + 16i$ are relatively prime, we can express 1 as a linear combination of these Gaussian integers. We can find Gaussian integers μ and ν such that $1 = \mu\alpha + \nu\beta$ by working backward through these steps and then multiplying both sides by $-i$ to obtain 1. These computations, which we leave to the reader, show that

$$(97 + 210i)(-24 + 21i) + (123 + 16i)(57 + 17i) = 1. \quad \blacktriangleleft$$

Unique Factorization for Gaussian Integers

The fundamental theorem of arithmetic states that every rational integer has a unique factorization into primes. Its proof depends on the fact that if the rational prime p divides the product of two rational integers ab, then p divides either a or b. We now prove an analogous fact about the Gaussian integers which will play the crucial role in proving unique factorization for the Gaussian integers.

Lemma 14.1. If π is a Gaussian prime and α and β are Gaussian integers such that $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.

Proof. Suppose that π does not divide α. We will show that π must then divide β. If $\pi \nmid \alpha$, then we also know that $\epsilon\pi \nmid \alpha$ when ϵ is a unit. Because the only divisors of π are $1, -1, i, -i, \pi, -\pi, i\pi$, and $-i\pi$, it follows that a greatest common divisor of π and α must be a unit. This means that 1 is a greatest common divisor of π and α. By Theorem 14.7, we know that there exist Gaussian integers μ and ν such that

$$1 = \mu\pi + \nu\alpha.$$

Multiplying both sides of this equation by β, we see that

$$\beta = \pi(\mu\beta) + \nu(\alpha\beta).$$

By the hypotheses of the theorem, we know that $\pi \mid \alpha\beta$ so that $\pi \mid \nu(\alpha\beta)$. Because $\beta = \pi(\mu\beta) + \nu(\alpha\beta)$, it follows (using Exercise 8 of Section 14.1) that $\pi \mid \beta$. ∎

Lemma 14.1 is a key ingredient in proving that the Gaussian integers enjoy the unique factorization property. Other sets of algebraic integers, such as $Z[\sqrt{-5}]$, the set of quadratic integers of the form $a + b\sqrt{-5}$, do not enjoy a property analogous to Lemma 14.1 and do not enjoy unique factorization.

We can extend Lemma 14.1 to products with more than two terms.

Lemma 14.2. If π is a Gaussian prime and $\alpha_1, \alpha_2, \cdots, \alpha_m$ are Gaussian integers such that $\pi \mid \alpha_1\alpha_2 \cdots \alpha_m$, then there is an integer j such that $\pi \mid \alpha_j$, where $1 \leq j \leq m$.

Proof. We can prove this result using mathematical induction. When $m = 1$, the result is trivial. Now suppose that the result is true for $m = k$, where k is a positive integer. That is, suppose that if

$$\pi \mid \alpha_1\alpha_2 \cdots \alpha_k,$$

where α_i is a Gaussian integer for $i = 1, 2, \ldots, k$, then $\pi \mid \alpha_i$ for some integer i with $1 \leq i \leq k$. Now suppose that

$$\pi \mid \alpha_1\alpha_2 \cdots \alpha_k\alpha_{k+1},$$

where α_i, $i = 1, 2, \ldots, k+1$ are Gaussian integers. Then $\pi \mid \alpha_1(\alpha_2 \cdots \alpha_k\alpha_{k+1})$, so that by Lemma 14.1, we know that $\pi \mid \alpha_1$ or $\pi \mid \alpha_2 \cdots \alpha_k\alpha_{k+1}$. If $\pi \mid \alpha_2 \cdots \alpha_k\alpha_{k+1}$, we can use the induction hypothesis to conclude that $\pi \mid \alpha_j$ for some integer j with $2 \leq j \leq k+1$. It follows that $\pi \mid \alpha_j$ for some integer j with $1 \leq j \leq k+1$, completing the proof. ∎

We can now state and prove the unique factorization theorem for Gaussian integers. Not surprising, Carl Friedrich Gauss was the first to prove this theorem.

Theorem 14.10. ***The Unique Factorization Theorem for Gaussian Integers.*** Suppose that γ is a nonzero Gaussian integer which is not a unit. Then

(i) γ can be written as the product of Gaussian primes; and

(ii) this factorization is unique in the sense that if

$$\gamma = \pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t,$$

where $\pi_1, \pi_2, \ldots, \pi_s, \rho_1, \rho_2, \ldots, \rho_t$ are all Gaussian primes, then $s = t$, and after renumbering the terms, if necessary, π_i and ρ_i are associates for $i = 1, 2, \ldots, s$.

Proof. We will prove part (i) using the second principle of mathematical induction where the variable is $N(\gamma)$, the norm of γ. First note that because $\gamma \neq 0$ and γ is not a unit, by Theorem 14.3, we know that $N(\gamma) \neq 1$. It follows that $N(\gamma) \geq 2$.

When $N(\gamma) = 2$, by Theorem 14.5, we know that γ is a Gaussian prime. Consequently, in this case, γ is the product of exactly one Gaussian prime, itself.

Now assume that $N(\gamma) > 2$. We assume that every Gaussian integer δ with $N(\delta) < N(\gamma)$ can be written as the product of Gaussian primes; this is the induction hypothesis. If γ is a Gaussian prime, it can be written as the product of exactly one Gaussian prime, itself. Otherwise, $\gamma = \eta\theta$, where η and θ are Gaussian integers which are not units. Because η and θ are not units, by Theorem 14.3, we know that $N(\eta) > 1$ and $N(\theta) > 1$. Furthermore, because $N(\gamma) = N(\eta)N(\theta)$, we know that $2 \leq N(\eta) < N(\gamma)$ and $2 \leq N(\theta) < N(\gamma)$. Using the induction hypothesis, we know that both η and θ are products of Gaussian primes. That is, $\eta = \pi_1\pi_2 \cdots \pi_s$, where $\pi_1, \pi_2, \ldots, \pi_k$ are Gaussian primes and $\theta = \rho_1\rho_2 \cdots \rho_t$, where $\rho_1, \rho_2, \ldots, \rho_t$ are Gaussian primes. Consequently,

$$\gamma = \theta\eta = \pi_1\pi_2 \cdots \pi_s\rho_1\rho_2 \cdots \rho_t$$

is the product of Gaussian primes. This finishes the proof that every Gaussian integer can be written as the product of Gaussian primes.

We will also use the second principle of mathematical induction to prove part (ii) of the theorem, the uniqueness of the factorization in the sense described in the statement of the theorem. Suppose that γ is a nonzero Gaussian integer which is not a unit. By Theorem 14.3, we know that $N(\gamma) \geq 2$. To begin the proof by mathematical induction, note that when $N(\gamma) = 2$, γ is a Gaussian prime, so γ can only be written in one way as the product of Gaussian primes, namely the product with one term, γ.

Now assume that part (ii) of the statement of the theorem is true when δ is a Gaussian integer with $N(\delta) < N(\gamma)$. Assume that γ can be written as the product of Gaussian primes in two ways, that is,

$$\gamma = \pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t,$$

where $\pi_1, \pi_2, \ldots, \pi_s, \rho_1, \rho_2, \ldots, \rho_t$ are all Gaussian primes. Note that $s > 1$; otherwise, γ is a Gaussian prime which already can be written uniquely as the product of Gaussian primes.

Because $\pi_1 \mid \pi_1\pi_2 \cdots \pi_s$ and $\pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t$, we see that $\pi_1 \mid \rho_1\rho_2 \cdots \rho_t$. By Lemma 14.2, we know that $\pi_1 \mid \rho_k$ for some integer k with $1 \leq k \leq t$. We can reorder the primes $\rho_1, \rho_2, \ldots, \rho_k$, if necessary, so that $\pi_1 \mid \rho_1$. Because ρ_1 is a Gaussian prime, it

is only divisible by units and associates, so that π_1 and ρ_1 must be associates. It follows that $\rho_1 = \epsilon\pi_1$, where ϵ is a unit. This implies that

$$\pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t = \epsilon\pi_1\rho_2 \cdots \rho_t.$$

We now divide both sides of this last equation by π_1 to obtain

$$\pi_2\pi_3 \cdots \pi_s = (\epsilon\rho_2)\rho_3 \cdots \rho_t.$$

Because π_1 is a Gaussian prime, we know that $N(\pi_1) \geq 2$. Consequently,

$$1 \leq N(\pi_2\pi_3 \cdots \pi_s) < N(\pi_1\pi_2 \cdots \pi_s) = N(\gamma).$$

By the induction hypothesis and the fact that $\pi_2\pi_3 \cdots \pi_s = (\epsilon\rho_2)\rho_3 \cdots \rho_t$, we can conclude that $s - 1 = t - 1$, and that after reordering of terms, if necessary, ρ_i is an associate of π_i for $i = 1, 2, \ldots, s - 1$. This completes the proof of part (ii). ■

Factoring a Gaussian integer into a product of Gaussian primes can be done by computing its norm. For each prime in the factorization of this norm as a rational integer, we look for possible Gaussian prime divisors of the Gaussian integer with this norm. We can perform trial division by each possible Gaussian prime divisor to see whether it divides the Gaussian integer.

Example 14.10. To find the factorization of 20 into Gaussian integers, we note that $N(20) = 20^2 = 400$. It follows that the possible Gaussian prime divisors of 20 have norm 2 or 5. We find that we can divide 20 by $1 + i$ four times, leaving a quotient of -5. Because $5 = (1 + 2i)(1 - 2i)$, we see that

$$20 = -(1 + i)^4(1 + 2i)(1 - 2i).$$ ◄

14.2 Exercises

1. Use the definition of the greatest common divisor of two Gaussian integers to show that if π_1 and π_2 are Gaussian primes that are not associates, then 1 is a greatest common divisor of π_1 and π_2.
2. Use the definition of the greatest common divisor of two Gaussian integers to show that if ϵ is a unit and α is a Gaussian integer, then 1 is a greatest common divisor of α and ϵ.
3. Show that if γ is a greatest common divisor of the Gaussian integers α and β, then $\overline{\gamma}$ is a greatest common divisor of $\overline{\alpha}$ and $\overline{\beta}$.
4. a) By extending the definition of a greatest common divisor of two Gaussian integers, define the greatest common divisor of a set of more than two Gaussian integers.
   b) Show from your definition that a greatest common divisor of three Gaussian integers α, β, and γ is a greatest common divisor of γ and a greatest common divisor of α and β.
5. Show that if α and β are Gaussian integers and γ is a greatest common divisor of α and β, then all associates of γ are also greatest common divisors of α and β.
6. Show that if α and β are Gaussian integers and $N(\alpha)$ and $N(\beta)$ are relatively prime rational integers, then α and β are relatively prime Gaussian integers.

7. Show that the converse of the statement in Exercise 6 is not necessarily true, that is, find Gaussian integers α and β such that α and β are relatively prime Gaussian integers, but $N(\alpha)$ and $N(\beta)$ are not relatively prime positive integers.

8. Show that if α and β are Gaussian integers and γ is a greatest common divisor of α and β, then $N(\gamma)$ divides $((N(\alpha), N(\beta))$.

9. Show if a and b are relatively prime rational integers, then they are also relatively prime Gaussian integers.

10. Show that if α, β, and γ are Gaussian integers and n is a positive integer such that $\alpha\beta = \gamma^n$ and α and β are relatively prime, then $\alpha = \epsilon\delta^n$, where ϵ is a unit and δ is a Gaussian integer.

11. a) Show all steps of the version of the Euclidean algorithm for the Gaussian integers described in the text to find a greatest common divisor of $\alpha = 44 + 18i$ and $\beta = 12 - 16i$.
    b) Use the steps in part (a) to find Gaussian integers μ and ν such that $\mu(44 + 18i) + \nu(12 - 16)$ equals the greatest common divisor found in part (a).

12. a) Show all steps of the version of the Euclidean algorithm for the Gaussian integers described in the text to show that $2 - 11i$ and $7 + 8i$ are relatively prime.
    b) Use the steps in part (a) to find Gaussian integers μ and ν such that $\mu(2 - 11i) + \nu(7 + 8i) = 1$.

13. Show that two consecutive Gaussian Fibonacci numbers G_k and G_{k+1} (defined in the preamble to Exercise 37 of Section 14.1), where k is a positive integer, are relatively prime Gaussian integers.

14. How many divisions are used to find a greatest common divisor of two consecutive Gaussian Fibonacci numbers G_k and G_{k+1} (defined in Exercise 37 of Section 14.1), where k is a positive integer? Justify your answer.

15. Derive a big-O estimate for the number of bit operations required to find a greatest common divisor of two nonzero Gaussian integers α and β, where $N(\alpha) \leq N(\beta)$. (*Hint:* Use the remark following the proof of Theorem 14.6.)

16. For each of these Gaussian integers, find its factorization into Gaussian primes and a unit where each Gaussian prime has a positive real part and a nonnegative imaginary part.

    a) $9 + i$ b) 4 c) $22 + 7i$ d) $210 + 2100i$

17. For each of these Gaussian integers, find its factorization into Gaussian primes and a unit where each Gaussian prime has a positive real part and a nonnegative imaginary part.

    a) $7 + 6i$ b) $3 - 13i$ c) 28 d) $400i$

18. Find the factorization into Gaussian primes of each of the Gaussian integers $k + (7 - k)i$ for $k = 1, 2, 3, 4, 5, 6, 7$, where each Gaussian prime has a positive real part and a nonnegative imaginary part.

19. Determine the number of different Gaussian integers, counting associates separately, that divide

    a) 10. c) 27000.
    b) $256 + 128i$. d) $5040 + 40320i$.

20. Determine the number of different Gaussian integers, counting associates separately, that divide

a) 198. b) $128 + 256i$. c) 169000. d) $4004 + 8008i$.

21. Suppose that $a + ib$ is a Gaussian integer and n is a rational integer. Show that n and $a + ib$ are relatively prime if and only if n and $b + ai$ are relatively prime.

22. Use the unique factorization theorem for Gaussian integers (Theorem 14.10) and Exercise 13 in Section 10.1 to show that every nonzero Gaussian integer can be written uniquely, except for the order of terms, as $\epsilon\pi_1^{e_1}\pi_2^{e_2}\cdots\pi_k^{e_k}$, where ϵ is a unit and for $j = 1, 2, \ldots, k$, $\pi_j = a_j + ib_j$ is a Gaussian prime with $a_j > 0$ and $b_j \geq 0$, and e_j is a positive integer.

23. Adapt Euclid's proof that there are infinitely many primes (Theorem 3.1) to show that there are infinitely many Gaussian primes.

Exercises 24–41 rely on the notion of a congruence for Gaussian integers defined in the preamble to Exercise 33 in Section 14.1.

24. a) Define what it means for β to be an inverse of the α modulo μ, where α, β, and μ are Gaussian integers.

b) Show that if α and μ are relatively prime Gaussian integers, then there exists a Gaussian integer β which is an inverse of α modulo μ.

25. Find an inverse of $1 + 2i$ modulo $2 + 3i$.

26. Find an inverse of 4 modulo $5 + 2i$.

27. Explain how a linear congruence of the form $\alpha x \equiv \beta \pmod{\mu}$ can be solved, where α, β, and μ are Gaussian integers and α and μ are relatively prime.

28. Solve each of these linear congruences in Gaussian integers.

a) $(2 + i)x \equiv 3 \pmod{4 - i}$ c) $2x \equiv 5 \pmod{3 - 2i}$
b) $4x \equiv -3 + 4i \pmod{5 + 2i}$

29. Solve each of these linear congruences in Gaussian integers.

a) $3x \equiv 2 + i \pmod{13}$ c) $(3 + i)x \equiv 4 \pmod{2 + 3i}$
b) $5x \equiv 3 - 2i \pmod{4 + i}$

30. Solve each of these linear congruences in Gaussian integers.

a) $5x \equiv 2 - 3i \pmod{11}$ c) $(2 + 5i)x \equiv 3 \pmod{4 - 7i}$
b) $4x \equiv 7 + i \pmod{3 + 2i}$

31. Develop and prove a version of the Chinese remainder theorem for systems of congruences for Gaussian integers.

32. Find the simultaneous solutions in Gaussian integers of the system of congruences

$$x \equiv 2 \pmod{2 + 3i}$$
$$x \equiv 3 \pmod{1 + 4i}.$$

33. Find the simultaneous solutions in Gaussian integers of the system of congruences

$$x \equiv 1 + 3i \pmod{2 + 5i}$$
$$x \equiv 2 - i \pmod{3 - 4i}.$$

34. Find a Gaussian integer congruent to 1 modulo 11, to 2 modulo $4+3i$, and to 3 modulo $1+7i$.

A *complete residue system* modulo γ, where γ is a Gaussian integer, is a set of Gaussian integers such that every Gaussian integer is congruent modulo γ to exactly one element of this set.

35. Find a complete residue system modulo

a) $1-i$. b) 2. c) $2+3i$.

36. Find a complete residue system modulo

a) $1+2i$. b) 3. c) $4-i$.

37. Prove that a complete residue system of α, where α is a Gaussian integer, has $N(\alpha)$ elements.

A *reduced residue system* modulo γ, where γ is a Gaussian integer, is a set of Gaussian integers such that every Gaussian integer that is relatively prime to γ is congruent to exactly one element of this set.

38. Find a reduced residue system modulo

a) $-1+3i$. b) 2. c) $5-i$.

39. Find a reduced residue system modulo

a) $2+2i$. b) 4. c) $4+2i$.

40. Suppose that π is a Gaussian prime. Determine the number of elements in a reduced residue system modulo π.

41. Suppose that π is a Gaussian prime. Determine the number of elements in a reduced residue system modulo π^e, where e is a positive integer.

42. a) Show that the algebraic integers of the form $r+s\sqrt{-3}$, where r and s are rational numbers, are the numbers of the form $a+b\omega$, where a and b are integers and where $\omega=(-1+\sqrt{-3})/2$. Numbers of this form are called *Eisenstein integers* after Max Eisenstein who studied them in the mid-nineteenth century. (They are also sometimes called *Eisenstein-Jacobi integers* because they were also studied by Carl Jacobi.) The set of Eisenstein integers is denoted by $Z[\omega]$.

b) Show that the sum, difference, and product of two Eisenstein integers is also an Eisenstein integer.

c) Show that if α is an Eisenstein integer, then $\overline{\alpha}$, the complex conjugate of α, is also an Eisenstein integer. (*Hint*: First show that $\overline{\omega}=\omega^2$.)

d) If α is an Eisenstein integer, we define the *norm* of this integer by $N(\alpha)=a^2-ab+b^2$ if $\alpha=a+b\omega$, where a and b are integers. Show that $N(\alpha)=\alpha\overline{\alpha}$ whenever α is an Eisenstein integer.

e) If α and β are Eisenstein integers, we say that α divides β if there exists an element γ in $Z[\omega]$ such that $\beta=\alpha\gamma$. Determine whether $1+2\omega$ divides $1+5\omega$ and whether $3+\omega$ divides $9+8\omega$.

f) An Eisenstein integer ϵ is a *unit* if ϵ divides 1. Find all the Eisenstein integers that are units.

g) An *Eisenstein prime* π in $Z[\omega]$ is an element divisible only by a unit or an associate of π. (An associate of an Eisenstein integer is the product of that integer and a unit.) Determine whether each of the following elements are Eisenstein primes: $1+2\omega$, $3-2\omega$, $5+4\omega$, and $-7-2w$.

*h) Show that if α and $\beta \neq 0$ belong to $Z[\omega]$, there are numbers γ and ρ such that $\alpha = \beta\gamma + \rho$ and $N(\rho) < N(\beta)$. That is, establish a version of the division algorithm for the Eisenstein integers.

i) Using part (h), show that Eisenstein integers can be uniquely written as the product of Eisenstein primes, with the appropriate considerations about associated primes taken into account.

j) Find the factorization into Eisenstein primes of each of the following Eisenstein integers: 6, $5+9\omega$, 114, $37+74\omega$.

43. a) Show that the algebraic integers of the form $r+s\sqrt{-5}$, where r and s are rational numbers, are the numbers of the form $a+b\sqrt{-5}$, where a and b are rational integers. (Recall that we briefly studied such numbers in Chapter 3. In this exercise, we look at these numbers in more detail.)

b) Show that the sum, difference, and product of numbers of the form $a+b\sqrt{-5}$, where a and b are rational integers, is again of this form.

c) We denote the set of numbers $a+b\sqrt{-5}$ by $Z[\sqrt{-5}]$. Suppose that α and β belong to $Z[\sqrt{-5}]$. We say that α *divides* β if there exists a number γ in $Z[\sqrt{-5}]$ such that $\beta = \alpha\gamma$. Determine whether $-9+11\sqrt{-5}$ is divisible by $2+3\sqrt{-5}$ and whether $8+13\sqrt{-5}$ is divisible by $1+4\sqrt{-5}$.

d) We define the *norm* of a number $\alpha = a+b\sqrt{-5}$ to be $N(\alpha) = a^2+5b^2$. Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ whenever α and β belong to $Z[\sqrt{-5}]$.

e) We say ϵ is a *unit* of $Z[\sqrt{-5}]$ if ϵ divides 1. Show that the units in $Z[\sqrt{-5}]$ are 1 and -1.

f) We say that an element α in $Z[\sqrt{-5}]$ is *prime* if its only divisors in $Z(\sqrt{-5}]$ are 1, -1, α, and $-\alpha$. Show that 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$ are all primes, that 2 does not divide either $1+\sqrt{-5}$ or $1-\sqrt{-5}$. Conclude that $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ can be written as the product of primes in two different ways. This means that $Z[\sqrt{-5}]$ does not have unique factorization into primes.

g) Show that there do not exist elements γ and ρ in $Z[\sqrt{-5}]$ such that $7-2\sqrt{-5} = (1+\sqrt{-5})\gamma + \rho$, where $N(\rho) < N(1+\sqrt{-5}) = 6$. Conclude that there is no analog for the division algorithm in $Z[\sqrt{-5}]$.

h) Show that if $\alpha = 3$ and $\beta = 1+\sqrt{-5}$, there do not exist numbers μ and ν in $Z[\sqrt{-5}]$ such that $\alpha\mu + \beta\nu = 1$, even though α and β are both primes, neither of which divides the other.

14.2 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the unique factorization into a unit and a product of Gaussian primes, where each Gaussian prime has a positive real part and a nonnegative imaginary part of $(2007-k)+(2008-k)i$ for all positive integers k with $k \leq 8$.

2. Find a prime factor of smallest norm of each of the Gaussian integers formed by adding 1 to the product of all Gaussian primes with norm less than n for as many n as possible. Do you think that infinitely many of these numbers are Gaussian primes?
3. Determine whether two randomly selected Gaussian integers are relatively prime, and by doing this repeatedly, estimate the probability that two randomly selected Gaussian integers are relatively prime.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Find a greatest common divisor of two Gaussian integers using a version of the Euclidean algorithm for Gaussian integers.
2. Express a greatest common divisor of two Gaussian integers as a linear combination of these Gaussian integers.
3. Keep track of the number of steps used by the version of the Euclidean algorithm for Gaussian integers that uses the construction in the proof of the division algorithm for Gaussian integers to find quotients and remainders.
4. Find the unique factorization of a Gaussian integer into a unit times Gaussian primes, where each Gaussian prime in the factorization is in the first quadrant.

14.3 Gaussian Integers and Sums of Squares

In Section 13.3 we determined which positive integers are the sum of two squares. In this section we will show that we can prove this result using what we have learned about Gaussian primes. We will also be able to determine the number of different ways that a positive integer can be written as the sum of two squares using Gaussian primes.

In Section 13.3 we proved that every prime of the form $4k + 1$ is the sum of two squares. We can prove this fact in a different way using Gaussian primes.

Theorem 14.11. If p is a rational prime of the form $4k + 1$, where k is a positive integer, then p is the sum of two squares.

Proof. Suppose that p is of the form $4k + 1$, where k is a positive integer. To prove that p can be written as the sum of two squares, we show that p is not a Gaussian prime. By Theorem 11.5, we know that -1 is a quadratic residue of p. Consequently, we know that there is a rational integer t such that $t^2 \equiv -1 \pmod{p}$. It follows that $p \mid (t^2 + 1)$. We can use this divisibility relation for rational integers to conclude that $p \mid (t + i)(t - i)$. If p is a Gaussian prime, then by Lemma 14.1, it follows that $p \mid t + i$ or $p \mid t - i$. Both of these cases are impossible because the Gaussian integers divisible by p have the form $p(a + bi) = pa + pbi$, where a and b are rational integers. Neither $t + i$ nor $t - i$ has this form. We can conclude that p is not a Gaussian prime.

Because p is not a Gaussian prime, there are Gaussian integers α and β, neither a unit, such that $p = \alpha\beta$. Taking norms of both sides of this equation, we find that

$$N(p) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta).$$

Because neither α nor β is a unit, $N(\alpha) \neq 1$ and $N(\beta) \neq 1$. This implies that $N(\alpha) = N(\beta) = p$. Consequently, if $\alpha = a + bi$ and $\beta = c + di$, we know that

$$p = N(\alpha) = a^2 + b^2 \quad \text{and} \quad p = N(\beta) = c^2 + d^2.$$

It follows that p is the sum of two squares. ∎

To find which rational integers are the sum of two squares, we will need to determine which rational integers are Gaussian primes and which factor into Gaussian primes. To accomplish that task, we will need the following lemma.

Lemma 14.3. If π is a Gaussian prime, then there is exactly one rational prime p such that π divides p.

Proof. We first factor the rational integer $N(\pi)$ into prime factors, say $N(\pi) = p_1 p_2 \cdots p_t$, where p_j is prime for $j = 1, 2, \ldots, t$. Because $N(\pi) = \pi\overline{\pi}$, it follows that $\pi \mid N(\pi)$, so that $\pi \mid p_1 p_2 \cdots p_t$. By Lemma 14.2, it follows that $\pi \mid p_j$ for some integer j with $1 \leq j \leq t$. We have shown that π divides a rational prime.

To complete the proof, we must show that π cannot divide two different rational primes. So suppose that $\pi \mid p_1$ and $\pi \mid p_2$, where p_1 and p_2 are different rational primes. Because p_1 and p_2 are relatively prime, by Corollary 3.8.1, there are rational integers m and n such that $mp_1 + np_2 = 1$. Moreover, because $\pi \mid p_1$ and $\pi \mid p_2$ we see that $\pi \mid 1$ (using the divisibility property in Exercise 8 of Section 14.1.) But this implies that π is a unit, which is impossible, so π does not divide two different rational primes. ∎

We can now determine which rational primes are also Gaussian primes and the factorization into Gaussian primes of those that are not.

Theorem 14.12. If p is a rational prime, then p factors as a Gaussian integer according to these rules.

(i) If $p = 2$, then $p = -i(1+i)^2 = i(1-i)^2$, where $1+i$ and $1-i$ are both Gaussian primes with norm 2.

(ii) If $p \equiv 3 \pmod 4$, then $p = \pi$ is a Gaussian prime with $N(\pi) = p^2$.

(iii) If $p \equiv 1 \pmod 4$, then $p = \pi\pi'$, where π and π' are Gaussian primes which are not associates with $N(\pi) = N(\pi') = p$.

Proof. To prove (i), we note that $2 = -i(1+i)^2 = i(1-i)^2$, where the factors $-i$ and i are units. Furthermore, $N(1+i) = N(1-i) = 1^2 + 1^2 = 2$. Since $N(1+i) = N(1-i)$ is a rational prime by Theorem 14.3, it follows that $1+i$ and $1-i$ are Gaussian primes.

To prove (ii), let p be a rational prime with $p \equiv 3 \pmod 4$. Suppose that $p = \alpha\beta$, where α and β are Gaussian integers with $\alpha = a + bi$ and $\beta = c + di$ and neither α nor β is a unit. By part (ii) of Theorem 14.1, it follows that $N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$. Because $N(p) = p^2$, $N(\alpha) = a^2 + b^2$, and $N(\beta) = c^2 + d^2$, we see that $p^2 = (a^2 + b^2)(c^2 + d^2)$. Neither α nor β is a unit, so neither has norm 1. It follows that $N(\alpha) = a^2 + b^2 = p$ and $N(\beta) = c^2 + d^2 = p$. However, this is impossible because $p \equiv 3 \pmod 4$, so that p is not the sum of two squares.

To prove (iii), let p be a rational prime with $p \equiv 1 \pmod 4$. By Theorem 14.11, there are integers a and b such that $p = a^2 + b^2$. If $\pi_1 = a - bi$ and $\pi_2 = a + bi$, then $p^2 = N(p) = N(\pi_1)N(\pi_2)$, so that $N(\pi_1) = N(\pi_2) = p$. It follows by Theorem 14.5 that π_1 and π_2 are Gaussian primes.

Next, we show that π_1 and π_2 are not associates. Suppose that $\pi_1 = \epsilon\pi_2$, where ϵ is a unit. Because ϵ is a unit, $\epsilon = 1, -1, i$, or $-i$.

If $\epsilon = 1$, then $\pi_1 = \pi_2$. This means that $x + yi = x - yi$, so that $y = 0$. This implies that $p = x^2 + y^2 = x^2$, which is impossible because p is prime. Similarly, when $\epsilon = -1$, then $\pi_1 = -\pi_2$. This implies that $x + yi = -x + yi$, which makes $x = 0$. This implies that $y^2 = p$, which is also impossible. If $\epsilon = i$, then $x + iy = i(x - iy) = y + ix$, so that $x = y$. Similarly, if $\epsilon = -i$, then $x + iy = -i(x - iy)$, so that $x = -y$. In both of these cases, $p = x^2 + y^2 = 2x^2$, which is impossible because p is an odd prime. We have shown that all four possible values of ϵ are impossible. It follows that π_1 and π_2 are not associates, completing the proof of (iii). ∎

We have all the ingredients we need to determine the number of representations of a positive integer as the sum of two squares using the unique factorization theorem for the Gaussian integers. Recall that we determined which positive integers can be written as the sum of two squares in Section 13.6.

Theorem 14.13. Suppose that n is a positive integer with prime power factorization

$$n = 2^m p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t},$$

where m is a nonnegative integer, $p_1, p_2, \ldots, p_s$ are primes of the form $4k + 1$, $q_1, q_2, \ldots, q_t$ are primes of the form $4k + 3$, $e_1, e_2 \ldots, e_s$ are nonnegative integers, and $f_1, f_2, \ldots, f_t$ are even nonnegative integers. Then there are

$$4(e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$$

ways to express n as the sum of two squares. (Here the order in which squares appear in the sum and the sign of the integer being squared both matter.)

Proof. To count the number of ways to write n as the sum of the squares, that is, the number of solutions of $n = a^2 + b^2$, we can count the number of ways to factor n into Gaussian integers $a + ib$ and $a - ib$, that is, to write $n = (u + iv)(u - iv)$.

We will use the factorization of n to count the number of ways we can factor n as the product of two conjugates, that is, $n = (u + iv)(u - iv)$. First, note that by Theorem 14.11, for each prime p_k of the form $4k + 1$ that divides n, there are integers a_k and b_k such that $p_k = a_k^2 + b_k^2$. Also, note that because $1 + i = i(1 - i)$, we have $2^m = (1 + i)^m(1 - i)^m = (i(1 - i))^m(1 - i)^m = i^m(1 - i)^{2m}$.

Consequently, we have

$$n = i^m(1-i)^{2m}(a_1+b_1i)^{e_1}(a_1-b_1i)^{e_1}(a_2+b_2i)^{e_2}(a_2-b_2i)^{e_2}$$
$$\cdots(a_s-b_si)^{e_s}(a_s+b_si)^{e_s}q_1{}^{f_1}q_2{}^{f_2}\cdots q_t{}^{f_t}.$$

Next, note that $\epsilon = i^m$ is a unit because it takes on one of the values $1, -1, i$, or $-i$. This means that a factorization of n into the product of a unit and Gaussian primes is

$$n = \epsilon(1-i)^{2m}(a_1+b_1i)^{e_1}(a_1-b_1i)^{e_1}(a_2+b_2i)^{e_2}(a_2-b_2i)^{e_2}$$
$$\cdots(a_s-b_si)^{e_s}(a_s+b_si)^{e_s}q_1{}^{f_1}q_2{}^{f_2}\cdots q_t{}^{f_t}.$$

Because the Gaussian integer $u+iv$ divides n, its factorization into a unit and Gaussian primes must have the form

$$u+iv = \epsilon_0(1-i)^w(a_1+b_1i)^{g_1}(a_1-b_1i)^{h_1}(a_2+b_2i)^{g_2}(a_2-b_2i)^{h_2}$$
$$\cdots(a_t-b_si)^{g_s}(a_s-b_si)^{h_s}q_1^{k_1}q_2{}^{k_2}\cdots q_t{}^{k_t},$$

where ϵ_0 is a unit, $w, g_1, \ldots, g_s, h_1, \ldots, h_s$, and $k_1, \ldots, k_t$ are nonnegative integers with $0 \le w \le 2m$, $0 \le g_i \le e_i$, $0 \le h_i \le e_i$ for $i = 1, \ldots, s$, and $0 \le k_j \le f_j$ for $j = 1, \ldots, t$.

Forming the conjugate of $u+iv$, we find

$$u-iv = \overline{\epsilon_0}(1+i)^w(a_1-b_1i)^{g_1}(a_1+b_1i)^{h_1}(a_2-b_2i)^{g_2}(a_2+b_2i)^{h_2}$$
$$\cdots(a_s-b_si)^{g_s}(a_s+b_si)^{h_s}q_1^{k_1}q_2^{k_2}\cdots q_t^{k_t}.$$

We can now rewrite the equation $n = (u+iv)(u-iv)$ as

$$n = 2^w p_1^{g_1+h_1}\cdots p_s^{g_s+h_s}q_1^{2k_1}\cdots q_t^{2k_t}.$$

Comparing this with the factorization of n into a unit and Gaussian primes, we see that $w = m$, $g_i + h_i = e_j$ for $i = 1, \ldots, s$, and $2k_j = f_j$ for $j = 1, \ldots, t$. We see that the values of w and k_i for $j = 1, \ldots, t$ are determined, but we have $e_i + 1$ choices for g_i, namely $g_i = 0, 1, 2, \ldots, e_i$, and that once g_i is determined, so is $h_i = e_i - g_i$. Furthermore, we have four choices for the unit ϵ_0. We conclude that there are $4(e_1+1)(e_2+1)\cdots(e_s+1)$ choices for the factor $u+iv$ and for the number of ways to write n as the sum of two squares. ■

Example 14.11. Suppose that $n = 25 = 5^2$. Then by Theorem 14.13, there are $4 \cdot 3 = 12$ ways to write 25 as the sum of two squares. (These are $(\pm3)^2 + (\pm4)^2$, $(\pm4)^2 + (\pm3)^2$, $(\pm5)^2 + 0^2$, and $0 + (\pm5)^2$. Note that the order in which terms appear matters when we count these representations.)

Suppose that $n = 90 = 2 \cdot 5 \cdot 3^2$. Then by Theorem 14.13, there are $4 \cdot 2 = 8$ ways to write 90 as the sum of two squares. (These are $(\pm3)^2 + (\pm9)^2$ and $(\pm9)^2 + (\pm3)^2$. Note that the order in which terms appear matters when we count these representations.)

Let $n = 16{,}200 = 2^3 \cdot 5^2 \cdot 3^4$. By Theorem 14.13, there are $4 \cdot 3 = 12$ ways to write 16,200 as the sum of two squares. We leave it to the reader to find these representations. ◀

Conclusion

In this section we used the Gaussian integers to study the solutions of the diophantine equation $x^2 + y^2 = n$, where n is a positive integer. The Gaussian integers are useful in studying a variety of other types of diophantine equations. For example, we can find Pythagorean triples using the Gaussian integers (Exercise 7), and we can find the solutions in rational integers of the diophantine equation $x^2 + y^2 = z^3$ (Exercise 8).

14.3 Exercises

1. Determine the number of ways to write each of the following rational integers as the sum of squares of two rational integers.

   a) 5 b) 20 c) 120 d) 1000

2. Determine the number of ways to write each of the following rational integers as the sum of squares of two rational integers.

   a) 16 b) 99 c) 650 d) 1001000

3. Explain how to solve a linear diophantine equation of the form $\alpha x + \beta y = \gamma$, where α, β, and γ are Gaussian integers so that the solution (x, y) is a pair of Gaussian integers.

4. Find all solutions in Gaussian integers of each of these linear diophantine equations.

   a) $(3 + 2i)x + 5y = 7i$ b) $5x + (2 - i)y = 3$

5. Find all solutions in Gaussian integers of each of the following linear diophantine equations.

   a) $(3 + 4i)x + (3 - i)y = 7i$ b) $(7 + i)x + (7 - i)y = 1$

6. In this exercise we will use the Gaussian integers to find the solutions in rational integers of the diophantine equation $x^2 + 1 = y^3$.
   a) Show that if x and y are integers such that $x^2 + 1 = y^3$, then $x - i$ and $x + i$ are relatively prime.
   b) Show that there are integers r and s such that $x = r^3 - 3rs^2$ and $3r^2s - s^3 = 1$. (*Hint*: Use part (a) and Exercise 10 in Section 14.2 to show that there is a unit ϵ and a Gaussian integer δ such that $x + i = (\epsilon\delta)^3$.)
   c) Find all solutions in integers $x^2 + 1 = y^3$ by analyzing the equations for r and s in part (b).

7. Use the Gaussian integers to prove Theorem 13.1 in Section 13.1, which gives primitive Pythagorean triples, that is, solutions of the equation $x^2 + y^2 = z^2$ in integers x, y, and z, where x, y, and z are pairwise relatively prime. (*Hint:* Begin with the factorization $x^2 + y^2 = (x + iy)(x - iy)$. Show that $x + iy$ and $x - iy$ are relatively prime Gaussian integers and then use Exercise 10 in Section 14.1.)

* 8. Use the Gaussian integers to find all solutions of the diophantine equation $x^2 + y^2 = z^3$ in rational integers x, y, and z.

* 9. Prove the analog of Fermat's little theorem for the Gaussian integers, which states that if α and π are relatively prime, then $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$. (*Hint:* Suppose that p is the

unique rational prime with $\pi \mid p$. Consider separately the cases where $p \equiv 1 \pmod 4$, $p \equiv 2 \pmod 4$, and $p \equiv 3 \pmod 4$).

10. Define $\phi(\gamma)$, where γ is a Gaussian integer, to be the number of elements in a reduced residue system modulo γ. Prove the analog of Euler's theorem for the Gaussian integers, which states that if γ is a Gaussian integer and α is a Gaussian integer that is relatively prime to γ, then

$$\alpha^{\phi(\gamma)} \equiv 1 \pmod \gamma.$$

11. Prove the analog of Wilson's theorem for the Gaussian integers, which states that if π is a Gaussian prime and $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ is a reduced system of residues modulo π, then

$$\alpha_1\alpha_2 \cdots \alpha_r \equiv -1 \pmod \pi.$$

12. Show that in the Eisenstein integers (defined in Exercise 42 in Section 14.2)

a) the rational prime 2 is an Eisenstein prime.

b) a rational prime of the form $3k + 2$, where k is a positive integer, is an Eisenstein prime.

c) a rational prime of the form $3k + 1$, where k is a positive integer, factors into the product of two primes that are not associates of one another.

14.3 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. In Chapter 13 we mentioned that Catalan's conjecture has been settled, showing that 2^3 and 3^2 are the only powers of rational integers that differ by 1. An open question for Gaussian integers is to find all powers of Gaussian integers that differ by a unit. Show that $(11 + 11i)^2$ and $(3i)^5$, $(1 - i)^5$ and $(1 + 2i)^2$, and $(78 + 78i)^2$ and $(23i)^3$ are such pairs of powers. Can you find other such pairs?

2. Show that $(3 + 13i)^3 + (7 + i)^3 = (3 + 10i)^3 + (1 + 10i)^3$, $(6 + 3i)^4 + (2 + 6i)^4 = (4 + 2i)^4 + (2 + i)^4$, $(2 + 3i)^5 + (2 - 3i)^5 = 3^5 + 1$, $(1 + 6i)^5 + (3 - 2i)^5 = (6 + i)^5 + (-2 + 3i)^5$, $(9 + 6i)^5 + (3 - 10i)^5 = (6 + i)^5 + (6 - 5i)^5$, and $(15 + 14i)^5 + (5 - 18i)^5 = (18 - 7i)^5 + (2 + 3i)^5$. Can you find other solutions of the equation $x^n + y^n = w^n + z^n$, where x, y, z, and w are Gaussian integers and n is a positive integer?

3. Show that Beal's conjecture, which asserts that there are no nontrivial solutions of the diophantine equation $x^a + y^b = z^c$, where a, b, and c are integers with $a \geq 3$, $b \geq 3$, and $c \geq 3$, does not hold when x, y, and z are allowed to be pairwise relatively prime Gaussian integers by showing that $(-2 + i)^3 + (-2 - i)^3 = (1 + i)^4$. Can you find other counterexamples?

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Find the number of ways to write a positive integer n as the sum of two squares.

2. Find all representations of a positive integer n as the sum of two squares.

A

Axioms for the Set of Integers

In this appendix, we state a collection of fundamental properties for the set of *integers* $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ that we have taken as axioms in the main body of the text. These properties provide the foundations for proving results in number theory. We begin with properties dealing with addition and multiplication. As usual, we denote the sum and product of a and b by $a + b$ and $a \cdot b$, respectively. Following convention, we write ab for $a \cdot b$.

- *Closure:* $a + b$ and $a \cdot b$ are integers whenever a and b are integers.
- *Commutative laws:* $a + b = b + a$ and $a \cdot b = b \cdot a$ for all integers a and b.
- *Associative laws:* $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all integers a, b, and c.
- *Distributive law:* $(a + b) \cdot c = a \cdot c + b \cdot c$ for all integers a, b, and c.
- *Identity elements:* $a + 0 = a$ and $a \cdot 1 = a$ for all integers a.
- *Additive inverse:* For every integer a there is an integer solution x to the equation $a + x = 0$; this integer x is called the *additive inverse* of a and is denoted by $-a$. By $b - a$ we mean $b + (-a)$.
- *Cancellation law:* If a, b, and c are integers with $a \cdot c = b \cdot c$, $c \neq 0$, then $a = b$.

We can use these axioms and the usual properties of equality to establish additional properties of integers. An example illustrating how this is done follows. In the main body of the text, results that are easily proved from these axioms are used without comment.

Example A.1. To show that $0 \cdot a = 0$, begin with the equation $0 + 0 = 0$; this holds because 0 is an identity element for addition. Next, multiply both sides by a to obtain $(0 + 0) \cdot a = 0 \cdot a$. By the distributive law, the left-hand side of this equation equals $(0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. Hence, $0 \cdot a + 0 \cdot a = 0 \cdot a$. Next subtract $0 \cdot a$ from both

sides (which is the same as adding the inverse of $0 \cdot a$). Using the associative law for addition and the fact that 0 is an additive identity element, the left-hand side becomes $0 \cdot a + (0 \cdot a - 0 \cdot a) = 0 \cdot a + 0 = 0 \cdot a$. The right-hand side becomes $0 \cdot a - 0 \cdot a = 0$. We conclude that $0 \cdot a = 0$. ◀

Ordering of integers is defined using the set of *positive integers* $\{1, 2, 3, \ldots\}$. We have the following definition.

Definition. If a and b are integers, then $a < b$ if $b - a$ is a positive integer. If $a < b$, we also write $b > a$.

Note that a is a positive integer if and only if $a > 0$.

The fundamental properties of ordering of integers follow.

- *Closure for the Positive Integers:* $a + b$ and $a \cdot b$ are positive integers whenever a and b are positive integers.
- *Trichotomy law:* For every integer a, exactly one of the statements $a > 0, a = 0$, and $a < 0$ is true.

The set of integers is said to be an *ordered set* because it has a subset that is closed under addition and multiplication and because the trichotomy law holds for every integer.

Basic properties of ordering of integers can now be proved using our axioms, as the following example shows. Throughout the text we have used without proof properties of ordering that easily follow from our axioms.

Example A.2. Suppose that a, b, and c are integers with $a < b$ and $c > 0$. We can show that $ac < bc$. First, note that by the definition of $a < b$ we have $b - a > 0$. Because the set of positive integers is closed under multiplication, $c(b - a) > 0$. Because $c(b - a) = cb - ca$, it follows that $ca < cb$. ◀

We need one more property to complete our set of axioms.

- *The Well-Ordering Property:* Every nonempty set of positive integers has a least element.

We say that the set of positive integers is *well ordered*. On the other hand, the set of all integers is not well ordered, because there are sets of integers that do not have a smallest element (as the reader should verify). Note that the principle of mathematical induction discussed in Section 1.3 is a consequence of the set of axioms listed in this appendix. Sometimes, the principle of mathematical induction is taken as an axiom replacing the well-ordering property. When this is done, the well-ordering property follows as a consequence.

Exercises

1. Use the axioms for the set of integers to prove the following statements for all integers a, b, and c.

   a) $a \cdot (b + c) = a \cdot b + a \cdot c$
   b) $(a + b)^2 = a^2 + 2ab + b^2$
   c) $a + (b + c) = (c + a) + b$
   d) $(b - a) + (c - b) + (a - c) = 0$

2. Use the axioms for the set of integers to prove the following statements for all integers a and b.

   a) $(-1) \cdot a = -a$
   b) $-(a \cdot b) = a \cdot (-b)$
   c) $(-a) \cdot (-1) = ab$
   d) $-(a + b) = (-a) + (-b)$

3. What is the value of -0? Give a reason for your answer.

4. Use the axioms for the set of integers to show that if a and b are integers with $ab = 0$, then $a = 0$ or $b = 0$.

5. Show that an integer a is positive if and only if $a > 0$.

6. Use the definition of the ordering of integers, and the properties of the set of positive integers, to prove the following statements for integers a, b, and c with $a < b$ and $c < 0$.

   a) $a + c < b + c$
   b) $a^2 \geq 0$
   c) $ac > bc$
   d) $c^3 < 0$

7. Show that if a, b, and c are integers with $a > b$ and $b > c$, then $a > c$.

* **8.** Show that there is no positive integer that is less than 1.

B

Binomial Coefficients

Sums of two terms are called *binomial expressions.* Powers of binomial expressions are used throughout number theory and throughout mathematics. In this section we will define the *binomial coefficients* and show that these are precisely the coefficients that arise in expansions of powers of binomial expressions.

Definition. Let m and k be nonnegative integers with $k \leq m$. The *binomial coefficient* $\binom{m}{k}$ is defined by

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}.$$

When k and m are positive integers with $k > m$, we define $\binom{m}{k} = 0$.

In computing $\binom{m}{k}$, we see that there is a good deal of cancellation, because

$$\begin{aligned}\binom{m}{k} = \frac{m!}{k!(m-k)!} &= \frac{1 \cdot 2 \cdot 3 \cdots (m-k)(m-k+1) \cdots (m-1)m}{k!\ 1 \cdot 2 \cdot 3 \cdots (m-k)} \\ &= \frac{(m-k+1) \cdots (m-1)m}{k!}.\end{aligned}$$

Example B.1. To evaluate the binomial coefficient $\binom{7}{3}$, we note that

$$\binom{7}{3} = \frac{7!}{3!4!} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 1 \cdot 2 \cdot 3 \cdot 4} = \frac{5 \cdot 6 \cdot 7}{1 \cdot 2 \cdot 3} = 35. \quad \blacktriangleleft$$

We now prove some simple properties of binomial coefficients.

Theorem B.1. Let n and k be nonnegative integers with $k \leq n$. Then

(i) $\binom{n}{0} = \binom{n}{n} = 1$, and

(ii) $\binom{n}{k} = \binom{n}{n-k}$.

Proof. To see that (i) is true, note that

$$\binom{n}{0} = \frac{n!}{0!n!} = \frac{n!}{n!} = 1$$

and

$$\binom{n}{n} = \frac{n!}{n!0!} = \frac{n!}{n!} = 1.$$

To verify (ii), we see that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}.$$ ∎

An important property of binomial coefficients is the following identity.

Theorem B.2. ***Pascal's Identity.*** Let n and k be positive integers with $n \geq k$. Then

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Proof. We perform the addition

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!}$$

by using the common denominator $k!(n-k+1)!$. This gives

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \\ &= \frac{n!((n-k+1)+k)}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n-k+1)!} \\ &= \binom{n+1}{k}\end{aligned}$$ ∎

Using Theorem B.2, we can construct *Pascal's triangle*, named after French mathematician *Blaise Pascal* who used the binomial coefficients in his analysis of gambling games. In Pascal's triangle, the binomial coefficient $\binom{n}{k}$ is the $(k+1)$st number in the

$(n + 1)$st row. The first nine rows of Pascal's triangle are displayed in Figure B.1. Pascal's triangle appeared in Indian and Islamic mathematics several hundred years before it was studied by Pascal.

```
                1
              1 2 1
            1 3 3 1
          1 4 6 4 1
        1 5 10 10 5 1
      1 6 15 20 15 6 1
    1 7 21 35 35 21 7 1
  1 8 28 56 70 56 28 8 1
```

Figure B.1 *Pascal's triangle.*

We see that the exterior numbers in the triangle are all 1. To find an interior number, we simply add the two numbers in the positions above, and to either side, of the position being filled. From Theorem B.2, this yields the correct integer.

Binomial coefficients occur in the expansion of powers of sums. Exactly how they occur is described by the *binomial theorem.*

Theorem B.3. ***The Binomial Theorem.*** Let x and y be variable, and n be a positive integer. Then,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n,$$

or, using summation notation,

BLAISE PASCAL (1623–1662) exhibited his mathematical talents early even though his father, who had made discoveries in analytic geometry, kept mathematical books from him to encourage his other interests. At 16, Pascal discovered an important result concerning conic sections. At 18, he designed a calculating machine, which he had built and successfully sold. Later, Pascal made substantial contributions to hydrostatics. Pascal, together with Fermat, laid the foundations for the modern theory of probability. It was in his work on probability that Pascal made new discoveries concerning what is now called Pascal's triangle, and gave what is considered to be the first lucid description of the principle of mathematical induction. In 1654, catalyzed by an intense religious experience, Pascal abandoned his mathematical and scientific pursuits to devote himself to theology. He returned to mathematics only once: one night, he had insomnia caused by the discomfort of a toothache and, as a distraction, he studied the mathematical properties of the cycloid. Miraculously, his pain subsided, which he took as a signal of divine approval of the study of mathematics.

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

Proof. We use mathematical induction. When $n = 1$, according to the binomial theorem, the formula becomes

$$(x+y)^1 = \binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1.$$

But because $\binom{1}{0} = \binom{1}{1} = 1$, this states that $(x+y)^1 = x + y$, which is obviously true.

We now assume that the theorem is true for the positive integer n, that is, we assume that

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

We must now verify that the corresponding formula holds with n replaced by $n+1$, assuming the result holds for n. Hence, we have

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n (x+y) \\ &= \left[\sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j \right] (x+y) \\ &= \sum_{j=0}^{n} \binom{n}{j} x^{n-j+1} y^j + \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^{j+1}.\end{aligned}$$

We see by removing terms from the sums and subsequently shifting indices, that

$$\sum_{j=0}^{n} \binom{n}{j} x^{n-j+1} y^j = x^{n+1} + \sum_{j=1}^{n} \binom{n}{j} x^{n-j+1} y^j$$

and

$$\begin{aligned}\sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^{j+1} &= \sum_{j=0}^{n-1} \binom{n}{j} x^{n-j} y^{j+1} + y^{n+1} \\ &= \sum_{j=1}^{n} \binom{n}{j-1} x^{n-j+1} y^j + y^{n+1}.\end{aligned}$$

Hence, we find that

$$(x+y)^{n+1} = x^{n+1} + \sum_{j=1}^{n} \left[\binom{n}{j} + \binom{n}{j-1} \right] x^{n-j+1} y^j + y^{n+1}.$$

By Pascal's identity, we have

$$\binom{n}{j} + \binom{n}{j-1} = \binom{n+1}{j},$$

so we conclude that

$$(x+y)^{n+1} = x^{n+1} + \sum_{j=1}^{n} \binom{n+1}{j} x^{n-j+1} y^j + y^{n+1}.$$

$$= \sum_{j=0}^{n+1} \binom{n+1}{j} x^{n+1-j} y^j.$$

This establishes the theorem. ∎

The binomial theorem shows that the coefficients of $(x+y)^n$ are the numbers in the $(n+1)$st row of Pascal's triangle.

We now illustrate one use of the binomial theorem.

Corollary B.1. Let n be a nonnegative integer. Then

$$2^n = (1+1)^n = \sum_{j=0}^{n} \binom{n}{j} 1^{n-j} 1^j = \sum_{j=0}^{n} \binom{n}{j}.$$

Proof. Let $x = 1$ and $y = 1$ in the binomial theorem. ∎

Corollary B.1 shows that if we add all elements of the $(n+1)$st row of Pascal's triangle, we get 2^n. For instance, for the fifth row, we find that

$$\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 1+4+6+4+1 = 16 = 2^4.$$

Exercises

1. Find the value of each of the following binomial coefficients.

   a) $\binom{100}{0}$ c) $\binom{20}{3}$ e) $\binom{10}{7}$
   b) $\binom{50}{1}$ d) $\binom{11}{5}$ f) $\binom{70}{70}$

2. Find the binomial coefficients $\binom{9}{3}$, $\binom{9}{4}$, and $\binom{10}{4}$, and verify that $\binom{9}{3} + \binom{9}{4} = \binom{10}{4}$.

3. Use the binomial theorem to write out all terms in the expansions of the following expressions.

   a) $(a+b)^5$ c) $(m-n)^7$ e) $(3x-4y)^5$
   b) $(x+y)^{10}$ d) $(2a+3b)^4$ f) $(5x+7)^8$

4. What is the coefficient of $x^{99}y^{101}$ in $(2x+3y)^{200}$?

5. Let n be a positive integer. Using the binomial theorem to expand $(1+(-1))^n$, show that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0.$$

6. Use Corollary B.1 and Exercise 5 to find

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots$$

and

$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots.$$

7. Show that if n, r, and k are integers with $0 \le k \le r \le n$, then

$$\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}.$$

* **8.** What is the largest value of $\binom{m}{n}$, where m is a positive integer and n is an integer such that $0 \le n \le m$? Justify your answer.

9. Show that

$$\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1},$$

where n and r are integers with $1 \le r \le n$.

The binomial coefficients $\binom{x}{n}$, where x is a real number and n is a positive integer, can be defined recursively by the equations $\binom{x}{1} = x$ and

$$\binom{x}{n+1} = \frac{x-n}{n+1}\binom{x}{n}.$$

10. Show from the recursive definition that if x is a positive integer, then $\binom{x}{k} = \frac{x!}{k!(x-k)!}$, where k is a integer with $1 \le k \le x$.

11. Show from the recursive definition that if x is a positive integer, then $\binom{x}{n} + \binom{x}{n+1} = \binom{x+1}{n+1}$, whenever n is a positive integer.

12. Show that the binomial coefficient $\binom{n}{k}$, where n and k are integers with $0 \le k \le n$, gives the number of subsets with k elements of a set with n elements.

13. Use Exercise 12 to give an alternate proof of the binomial theorem.

14. Let S be a set with n elements and let P_1 and P_2 be two properties that an element of S may have. Show that the number of elements of S possessing neither property P_1 nor property P_2 is

$$n - [n(P_1) + n(P_2) - n(P_1, P_2)],$$

where $n(P_1)$, $n(P_2)$, and $n(P_1, P_2)$ are the number of elements of S with property P_1, with property P_2, and both properties P_1 and P_2, respectively.

15. Let S be a set with n elements and let P_1, P_2, and P_3 be three properties that an element S may have. Show that the number of elements of S possessing none of the properties P_1, P_2, and P_3 is

$$\begin{aligned} n - [&n(P_1) + n(P_2) + n(P_3)] \\ &- n(P_1, P_2) - n(P_1, P_3) - n(P_2, P_3) + n(P_1, P_2, P_3)], \end{aligned}$$

where $n(P_{i_1}, \ldots, P_{i_k})$ is the number of elements of S with properties $P_{i_1} \ldots, P_{i_k}$.

* **16.** In this exercise we develop the *principle of inclusion-exclusion*. Suppose that S is a set with n elements and let $P_1, P_2, \ldots, P_t$ be t different properties that an element of S may

have. Show that the number of elements of S possessing *none* of the t properties is

$$\begin{aligned} n &- [n(P_1) + n(P_2) + \cdots + n(P_t)] \\ &+ [n(P_1, P_2) + n(P_1, P_3) + \cdots + n(P_{t-1}, p_t)] \\ &- \quad [n(P_1, P_2, P_3) + n(P_1, P_2, P_4) + \cdots + n(P_{t-2}, P_{t-1}, P_t)] \\ &+ \cdots + (-1)^t n(P_1, P_2, \ldots, P_t), \end{aligned}$$

where $n(P_{i_1}, P_{i_2}, \ldots, P_{i_j})$ is the number of elements of S possessing all of the properties $P_{i_1}, P_{i_2}, \ldots, P_{i_j}$. The first expression in brackets contains a term for each property, the second expression in brackets contains terms for all combinations of two properties, the third expression contains terms for all combinations of three properties, and so forth. (*Hint:* For each element of S, determine the number of times it is counted in the above expression. If an element has k of the properties, show that it is counted $1 - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k}$ times; this is 0 when $k > 0$, by Exercise 5.)

* **17.** What are the coefficients of $(x_1 + x_2 + \cdots + x_m)^n$? These coefficients are called *multinomial coefficients.*

18. Write out all terms in the expansion of $(x + y + z)^7$.

19. What is the coefficient of $x^3y^4z^5$ in the expansion of $(2x - 3y + 5z)^{12}$?

Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica,* or programs you have written, carry out the following computations and explorations.

1. Find the least integer n such that there is a binomial coefficient $\binom{n}{k}$, where k is a positive integer greater than 1,000,000.

Programming Projects

Write computer programs using Maple, *Mathematica,* or a language of your choice to do the following.

1. Evaluate binomial coefficients.

2. Given a positive integer n, print out the first n rows of Pascal's triangle.

3. Expand $(x + y)^n$, given a positive integer n, using the binomial theorem.

C

Using Maple and *Mathematica* for Number Theory

Investigating questions in number theory often requires computations with large integers. Fortunately, there are many tools available today that can be used for such computations. This appendix describes how two of the most popular of these tools, Maple and *Mathematica*, can be used to perform computations in number theory. We will concentrate on existing commands in these two systems, both of which support extensive programming environments that can be used to create useful programs for studying number theory. We will not describe these programming environments here.

C.1 Using Maple for Number Theory

The Maple system is a comprehensive environment for numerical and symbolic computations. It can also be used to develop additional functionality. We will briefly describe some of the existing support for number theory in Maple. For additional information about Maple, consult the Maple Web site at `http://www.maplesoft.com`.

In Maple, commands for computations in number theory can be found in the `numtheory` package. Some useful commands for number theory are included in the standard set of Maple commands, and a few are found in other packages, such as the `combinat` package of combinatorics commands. You need to let Maple know when you want to use one or more commands from a package. This can be done in two ways: You can either load the package and then use any of its commands, or you can prepend the name of the package to a particular command. For example, after running the command `with(numtheory)`, you can use commands from the `numtheory` package as you would standard commands. You can also run commands from this package by simply prepending the name of the package before the command. You will need to do this every time you use a command from the package, unless you run the `with(numtheory)` command.

Additional Maple commands for number theory can be found in the Maple V Share Library, which can be accessed at `http://www.cybermath.com/share_home.html`.

A useful reference for using Maple to explore number theory (and other topics in discrete mathematics) is *Exploring Discrete Mathematics with Maple* [Ro97]. This book explains how to use Maple to find greatest common divisors and least common multiples, apply the Chinese remainder theorem, factor integers, run primality tests, find base b expansions, encrypt and decrypt using classical ciphers and the RSA cryptosystem, and perform other number theoretic computations. Also, Maple worksheets for number theory and cryptography, written by John Cosgrave for a course at St. Patrick's College in Dublin, Ireland, can be found at `http://www.spd.dcu.ie/johnbcos/Maple_3rd_year.htm`.

Maple Number Theory Commands

The Maple commands relevant to material in this text are presented according to the chapter in which that material is covered. These commands are useful for checking computations in the text, for working or checking some exercises, and for the computations and explorations at the end of each section. Furthermore, programs in Maple can be written for many of the explorations and programming projects listed at the end of each section. Consult the appropriate Maple reference materials, such as the *Maple V Programming Guide* [Mo96], for information about writing programs in Maple.

Chapter 1

`combinat[fibonacci](n)` computes the nth Fibonacci number.

`iquo(`int_1`,`int_2`)` computes the quotient when int_1 is divided by int_2.

`irem(`int_1`,`int_2`)` computes the remainder when int_1 is divided by int_2.

`floor(`*expr*`)` computes the largest integer less than or equal to the real expression *expr*.

`numtheory[divisors](`n`)` computes the positive divisors of the integer n.

Maple code for investigating the Collatz $3x + 1$ problem has been written by Gaston Gonnet, and is available in the Maple V Release 5 Share Library.

Chapter 2

`convert(`*int*`, base, `*posint*`)` converts the integer *int* in decimal notation to a list representing its digits base *posint*.

`convert(`*int*`,binary)` converts the integer *int* in decimal notation to its binary equivalent.

`convert(`*int*`,hex)` converts the integer *int* in decimal notation to its hexadecimal equivalent.

`convert(`*bin*`,decimal,binary)` converts the integer *bin* in binary notation to its decimal equivalent.

`convert(`*oct*`,decimal,octal)` converts the integer *oct* in octal notation to its decimal equivalent.

`convert(`*hex*`,decimal,octal)` converts the integer *hex* in hexadecimal notation to its decimal equivalent.

Chapter 3

`isprime(`n`)` tests whether n is prime.

`ithprime(`n`)` calculates the nth prime number where n is a positive integer.

`prevprime(`n`)` calculates the largest prime smaller than the integer n.

`numbertheory[fermat](`n`)` calculates the nth Fermat number.

`ifactor(`n`)` finds the prime-power factorization of an integer n.

`ifactors(`n`)` finds the prime integer factors of an integer n.

`igcd(`$int_1, \ldots, int_n$`)` computes the greatest common divisor of integers $int_1, \ldots, int_n$.

`igcdex(`int_1, int_2`)` computes the greatest common divisor of the integers int_1 and int_2 using the extended Euclidean algorithm, which also expresses the greatest common divisor as a linear combination of int_1 and int_2.

`ilcm(`$int_1, \ldots, int_n$`)` computes the least common multiple of the integers $int_1, \ldots, int_n$.

Chapter 4

The operator `mod` can be used in Maple; for example, 17 `mod` 4 tells Maple to reduce 17 to its least residue modulo 4.

`msolve(`*eqn*`,`m`)` finds the integer solutions modulo m of the equation *eqn*.

`chrem(`$[n_1 \ldots, n_r], [m_1, \ldots, m_r]$`)` computes the unique positive integer *int* such that *int* **mod** $m_i = n_i$ for $i = 1, \ldots, r$.

Chapter 6

`numtheory[phi](`n`)` computes the value of the Euler phi function at n.

Chapter 7

`numtheory[invphi](`n`)` computes the positive integers m with $\phi(m) = n$.

`numtheory[sigma](`n`)` computes the sum of the positive divisors of the integer n.

`numtheory[tau](`n`)` computes the number of positive divisors of the integer n.

`numbertheory[bigomega](`n`)` computes the value of $\Omega(n)$, the number of prime factors of n.

`numtheory[mersenne](`n`)` determines whether the nth Mersenne number $M_n = 2^n - 1$ is prime.

`numtheory[mobius](`n`)` computes the value of the Möbius function at the integer n.

Chapter 9

`numtheory[order](`n_1, n_2`)` computes the order of n_1 modulo n_2.

`numtheory[primroot](`n`)` computes the smallest primitive root modulo n.

`numtheory[mlog]` (n_1, n_2, n_3) computes the index, or discrete logarithmn, of n_1 to the base n_2 modulo n_3. (The function `numtheory[index]` (n_1, n_2, n_3) is identical to this function.)

`numtheory[lambda]` (n) computes the minimal universal exponent of n.

Chapter 11

`numtheory[quadres]` (int_1, int_2) determines whether int_1 is a quadratic residue modulo int_2.

`numtheory[legendre]` (n_1, n_2) computes the value of the Legendre symbol $\left(\frac{n_1}{n_2}\right)$.

`numtheory[jacobi]` (n_1, n_2) computes the value of the Jacobi symbol $\left(\frac{n_1}{n_2}\right)$.

`numtheory[msqrt]` (n_1, n_2) computes the square root of n_1 modulo n_2.

Chapter 12

`numtheory[pdexpand]` (rat) computes the periodic decimal expansion of the rational number *rat*.

`numtheory[cfrac]` (rat) computes the continued fraction of the rational number *rat*.

`numtheory[invcfrac]` (cf) converts a periodic continued fraction cf to a quadratic irrational number.

Chapter 13

`numtheory[sum2sqr]` (n) computes all sums of two squares that sum to n.

Chapter 14

Maple supports a special package for working with Gaussian integers. To use the commands in this package, first run the command

```
with(GaussInt);
```

After running this command you can add, subtract, multiply, and form powers of Gaussian integers using the same operators as you ordinarily do. Maple requires that you enter the Gaussian integer $a + ib$ as a + b*I. (That is, you must include the * operator between b and the letter I, which Maple uses to represent the imaginary number i.)

`GaussInt[GInearest]` (c) returns the Gaussian integer closest to the complex number c, where the Gaussian integer of smallest norm is chosen in the case of ties.

`GaussInt[GIquo]` (m, n) finds the Gaussian integer quotient when m is divided by n.

`GaussInt[GIrem]` (m, n) finds the remainder Gaussian integer divisor when m is divided by n.

`GaussInt[GInorm]` (m) gives the norm of the complex number m.

`GaussInt[GIprime]` (m) returns true when m is a Gaussian prime and false otherwise.

`GaussInt[GIfactor]` (m) returns a factorization of m into a unit and Gaussian primes.

`GaussInt[GIfactors]` (m) finds a unit and Gaussian prime factors and their multiplicities in a factorization of the Gaussian integer m.

`GaussInt[GIsieve]` (m), where m is a positive integer, generates a list of Gauss primes $a + ib$ with $0 \leq a \leq b$ and norm not exceeding m^2.

`GaussInt[GIdivisor]` (m) finds the set of divisors of the Gaussian integer m in the first quadrant.

`GaussInt[GInodiv]` (m) computes the number of nonassociated divisors of m.

`GaussInt[GIgcd]` $(m_1, m_2, \ldots, m_r)$ finds the greatest common divisor in the first quadrant of the Gaussian integers $m_1, m_2, \ldots, m_r$.

`GaussInt[GIgcdex]` $(a, b, \texttt{'}s\texttt{'}, \texttt{'}t\texttt{'})$ finds the greatest common divisor in the first quadrant of the Gaussian integers a and b and finds integers s and t such that as $as + bt$ equals this greatest common divisor.

`GaussInt[GIchrem]` $([a_0, a_1, \ldots, a_r], [u_0, u_1, \ldots, u_r])$ computes the unique Gaussian integer m such that m is congruent to a_i modulo u_i for $i = 1, 2, \ldots, r$.

`GaussInt[GIlcm]` $(a_1, \ldots, a_r)$ finds the least common multiple in the first quadrant (that is, with positive real part and nonnegative part), in terms of norm, of the Gaussian integers $a_1, \ldots, a_r$.

`GaussInt[GIphi]` (n) returns the number of Gaussian integers in a reduced residue set modulo n, where n is a Gaussian integer.

`GaussInt[GIquadres]` (a, b) returns 1 if the Gaussian integer a is a quadratic residue of the Gaussian integer b and -1 if a is a quadratic nonresidue of b.

Appendices

`binomial`(n, r) computes the binomial coefficient n choose r.

C.2 Using *Mathematica* for Number Theory

The *Mathematica* system provides a comprehensive environment for numerical and symbol computations. It can also be used to develop additional functionality. We will describe the existing *Mathematica* support for computations relating to the number theory covered in this text. For additional information on *Mathematica,* consult the *Mathematica* Web site at `http://www.mathematica.com`.

Mathematica supports many number theory commands as part of its basic system. Additional number theory commands can be found in *Mathematica* packages that are collections of programs implementing functions in particular areas. The *Mathematica* system bundles some add-on packages, called standard packages, with its basic offerings. These standard packages include a group supporting commands for functions from number theory, including `ContinuedFractions`, `FactorIntegerECM`, `NumberTheoryFunctions`, and `PrimeQ`. There are other *Mathematica* packages that can be obtained using the Internet; access them at `http://www.mathsource.com`. Consult the *Mathematica Book* [Wo03] to learn how to load and use them.

You cannot use a command form package without having first told *Mathematica* that you want to run commands from this package, which is done by loading it. For example, to load the package `NumberTheoryFunctions`, use the command: `In[1]:=NumberTheory‘NumberTheoryFunctions‘`

Another resource for using *Mathematica* for number theory computations is *Mathematica in Action* by Stan Wagon [Wa99]. This book contains useful discussions of how to use *Mathematica* to investigate large primes, run extended versions of the Euclidean algorithm, solve linear diophantine equations, use the Chinese remainder theorem, work with continued fractions, and generate prime certificates.

Number Theory Commands in *Mathematica*

The *Mathematica* commands relevant to material covered in this book are presented here according to the chapter in which that material is covered. (The command for loading these functions if they are part of add-on packages is also provided.) These commands are useful for checking computations in the text, for working or checking some of the exercises, and for the computations and explorations at the end of each section. Furthermore, it is possible to write programs in *Mathematica* for many of the explorations and programming projects listed at the end of each section. Consult *Mathematica* reference materials, such as the *Mathematica Book* [Wo03], for information about writing programs in *Mathematica*.

Chapter 1

`Fibonacci[`n`]` gives the nth Fibonacci number f_n.

`Quotient[`m, n`]` gives the integer quotient when m is divided by n.

`Mod[m,n]` gives the remainder when m is divided by n.

The Collatz $(3x + 1)$ problem has been implemented in *Mathematica* by Ilan Vardi. You can access this *Mathematica* package at `http://www.mathsource.com /Content/Applications/Mathematics/0200-305`.

Chapter 2

`IntegerDigits[`n, b`]` gives a list of the base b digits of n.

Chapter 3

`PrimeQ[`n`]` produces output `True` if n is prime and `False` if n is not prime.

`Prime[`n`]` gives the nth prime number.

`PrimePi[`x`]` gives the number of primes less than or equal to x.

`In[1]:=NumberTheory‘NumberTheoryFunctions‘`
`NextPrime[`n`]` gives the smallest prime larger than n.

`GCD[`$n_1, n_2, \ldots, n_k$`]` gives the greatest common divisor of the integers $n_1, n_2, \ldots, n_k$.

`ExtendedGCD[`n, m`]` gives the extended greatest common divisor of the integers n and m.

`LCM[`$n_1, n_2, \ldots, n_k$`]` gives the least common multiple of the integers $n_1, n_2, \ldots, n_k$.

`FactorInteger[`n`]` produces a list of the prime factors of n and their exponents.

`Divisors[`n`]` gives a list of the integers that divide n.

`IntegerExponent[`n, b`]` gives the highest power of b that divides n.

`In[1]:=NumberTheory`‘`NumberTheoryFunctions`‘
`SquareFreeQ[`n`]` returns `True` if n contains a squared factor and `False` otherwise.

`In[1]:=NumberTheory`‘`FactorIntegerECM`‘
`FactorIntegerECM[`n`]` gives a factor of a composite integer n produced using Lenstra's elliptic curve factorization method.

Chapter 4

`Mod[`k, n`]` gives the least nonnegative residue of k modulo n.

`Mod[`k, n, `1]` gives the least positive residue of k modulo n.

`Mod[`$k, n, -n/2$`]` gives the absolute least residue of k modulo n.

`PowerMod[`a, b, n`]` gives the value of $a^b \bmod n$. Taking $b = -1$ gives the inverse of a modulo n, if it exists.

`In[1]:=NumberTheory`‘`NumberTheoryFunctions`‘
`ChineseRemainder[`$list_1$, $list_2$`]` gives the smallest nonnegative integer r such that `Mod[`$r, list_2$`]` equals $list_1$. (For example, `ChineseRemainder[`$\{r_1, r_2\}, \{m_1 m_2\}$`]` produces the solution of the simultaneous congruence $x \equiv r_1 \bmod m_1$ and $x \equiv r_2 \bmod m_2$.)

Chapter 6

`EulerPhi[`n`]` gives the value of the Euler phi function at n.

Chapter 7

`DivisorSigma[`k, n`]` gives the value of the sum of the kth powers of divisors function at n. Taking $k = 1$ gives the sum of divisors function at n. Taking $k = 0$ gives the number of divisors of n.

`MoebiusMu[`n`]` gives the value of $\mu(n)$.

Chapter 8

The RSA Public Key Cryptosystem has been implemented in *Mathematica* by Stephan Kaufmann. You can obtain the *Mathematica* package, instructions for how to use it, and a *Mathematica* notebook from the Mathsource Web site at `http://www.mathsource.com/Content/Applications/ComputerScience/0204-130`.

Chapter 9

`MultiplicativeOrder[`k, n`]` gives the order of k modulo n.

`PrimitiveRoot[`n`]` gives a primitive root of n when n has a primitive root, and does not evaluate when it does not.

`In[1]:=NumberTheory'PrimeQ'`
`PrimeQCertificate[`n`]` produces a certificate verifying that n is prime or composite.
`CarmichaelLambda[`n`]` gives the minimal universal exponent $\lambda(n)$.

Chapter 11

`JacobiSymbol[`n, m`]` gives the value of the Jacobi symbol $\left(\frac{n}{m}\right)$.
`SqrtMod[`d, n`]` gives a square root of d modulo n for odd n.

Chapter 12

`RealDigits[`x`]` gives a list of the digits in the decimal expansion of x.
`RealDigits[`x, b`]` gives a list of the digits in the base b expansion of x.

The following functions dealing with decimal expansions are part of the `Number Theory'ContinuedFractions'` package. Load this package using `In[1]:=Number Theory'Continued Fractions'` before using them.

`PeriodicForm[{`$a_0, \ldots, \{a_m, \ldots\}$`}, `*exp*`]` presents a repeated decimal expansion in terms of a preperiodic and a periodic part.
`PeriodicForm[{`$a_0, \ldots, \{a_m, \ldots\}$`}, `*expr*`, `$b$`]` represents a base b expansion.
`Normal[PeriodicForm[`*args*`]]` gives the rational number corresponding to a decimal expansion.

The following functions dealing with continued fractions are part of the `Number Theory'Continued Fractions'` package. Load this package using `In[1]:=Number Theory'Continued Fractions'` before using them.

`ContinuedFraction[`x, n`]` gives the first n terms of the continued fraction expansion of x.
`ContinuedFraction[`x`]` gives the complete continued fraction expansion of a quadratic irrational number.
`FromContinued Fraction[`*list*`]` finds a number from its continued fraction expansion.
`ContinuedFractionForm[{`$a_0, a_1, \ldots$`}]` represents the continued fraction with partial quotients $a_0, a_1 \ldots$
`ContinuedFractionForm[{`$a_0, a_1, \ldots, \{p_0, p_1, \ldots\}$`}]` represents the continued fraction with partial quotients $a_0, a_1 \ldots$ and additional quotients $p_1, p_2, \ldots$.
`Normal[ContinuedFractionForm[`*quotients*`]]` gives the rational or quadratic irrational number corresponding to the given continued fraction.
`Convergents[`*rat*`]` gives the convergents for all terms of the continued fraction of a rational or quadratic irrational x.
`Convergents[`*num*`, `*terms*`]` gives the convergents for the given number of terms of the continued fraction expansion of *num*.
`Convergents[`cf`]` gives the convergents for the particular continued fraction cf returned from `ContinuedFraction` or `ContinuedFractionForm`.

`QuadraticIrrationalQ[`*expr*`]` tests whether *expr* is a quadratic irrational.

Chapter 14

`Divisors[`n, GaussianIntegers `->` `True]` lists all Gaussian integer divisors of the Gaussian integer n.

`DivisorSigma[`k, n, GaussianIntegers `->` `True]` gives the sum of the kth powers of the Gaussian integer divisors of the Gaussian integer n.

`FactorInteger[`n, GaussianIntegers `->` `True]` produces a list of the Gaussian prime factors of the Gaussian integer n with positive real parts, and nonnegative imaginary parts, their exponents, and a unit.

`PrimeQ[`n, GaussianIntegers `->` `True]` returns the value of `True` if n is a Gaussian prime and `False` otherwise.

Appendices

`Binomial[`n, m`]` gives the values of the binomial coefficient $\binom{n}{m}$.

D

Number Theory Web Links

In this appendix we provide an annotated list of key Web sites for number theory. These sites are excellent starting points for an exploration of number theory resources on the Web. At the time of publication of this book, these sites could be found at the URLs listed here. However, with the ephemeral nature of the Web, the addresses of these sites may change, they may cease to exist, or their content may change, and neither the author nor the publisher of this book is able to vouch for the contents of these sites. If you have trouble locating these sites, you may want to try using a search engine to see whether they can be found at a new URL. You will also want to consult the comprehensive guide to all the Web references for this book at `http://www.awlonline.com/rosen`. This guide will help you locate some of the more difficult-to-find sites relevant to number theory and to cryptography.

The Fibonacci Numbers and the Golden Section (`http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/fib.html`)

An amazing collection of information about the Fibonacci numbers, including their history, where they arise in nature, puzzles involving the Fibonacci numbers, and their mathematical properties can be found on this site. Additional material addresses the golden section. An extensive collection of links to other sites makes this an excellent place to start your exploration for information about Fibonacci numbers.

The Prime Pages (`http://www.utm.edu/research/primes/`)

This is the premier site for information about prime numbers. You can find a glossary, primers, articles, the Prime FAQ, current records, conjectures, extensive lists of primes and prime factorizations, as well as links to other sites, including those that provide useful software. This is a great site for exploring the world of primes!

The Great Internet Prime Search (`http://www.mersenne.org`)

Find the latest discoveries about Mersenne primes at this site. You can download software from this site to search for Mersenne primes, as well as primes of other special forms. Links to other sites related to searching for primes and factoring are provided. This is the site to visit to sign up for the communal search for a new prime of world-record size!

The MacTutor History of Mathematics Archives (`http://www-groups.dcs.st-and.ac.uk/history/index.html`)

This is the main site to visit for biographies of mathematicians. Hundreds of important mathematicians from ancient to modern times are covered. You can also find essays on the history of important mathematical topics, including the prime numbers and Fermat's last theorem.

Frequently Asked Questions in Mathematics (`http://db.uwaterloo.ca/alopez-o/math-faq/math-faq.html`)

This is a compilation of the frequently asked questions from the USENET newsgroup `sci.math`. It contains several sections of questions relating to number theory, including primes and Fermat's last theorem, as well as a potpourri of historical information and mathematical trivia.

The Number Theory Web (`http://www.numbertheory.org/ntw/web.html`)

This site provides an amazing collection to links to sites containing information relevant to number theory. You can find links to sites providing software for number theory calculations, course notes, articles, online theses, historical and biographical information, conference information, job postings, and everything else on the Web related to number theory.

RSA Labs—Cryptography FAQ (`http://www.rsasecurity.com/rsalabs/faq/`)

This site provides an excellent overview of modern cryptography. You can find descriptions of cryptographic applications, cryptographic protocols, public and private key cryptosystems, and the mathematics behind them.

The Mathematics of Fermat's Last Theorem (`http://www.best.com/~cgd/home/flt/flt01.htm`)

This site provides an excellent introduction to Fermat's last theorem. It provides discussions of each of the important topics involved in the proof of the theorem.

NOVA Online—The Proof (`http://www.pbs.org/wgbh/nova/proof`)

This site provides material relating to a television program on the proof of Fermat's last theorem. Included are transcripts of the program and of an interview with Andrew Wiles, and links to other sites on Fermat's last theorem.

E Tables

Table E.1 gives the least prime factor of each odd positive integer less than 10,000 and not divisible by 5. The initial digits of the integer are listed to the side and the last digit is at the top of the column. Primes are indicated with a dash. The table is reprinted with permission from U. Dudley, *Elementary Number Theory*, Second Edition, Copyright © 1969 and 1978 by W. H. Freeman and Company. All rights reserved.

Table E.3 gives the least primitive root r modulo p for each prime p, $p < 1000$.

Table E.4 is reprinted with permission from J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill Book Company. Copyright © 1939.

	1	3	7	9
0	—	—	—	3
1	—	—	—	—
2	3	—	3	—
3	—	3	—	3
4	—	—	—	7
5	3	—	3	—
6	—	3	—	3
7	—	—	7	—
8	3	—	3	—
9	7	3	—	3
10	—	—	—	—
11	3	—	3	7
12	11	3	—	3
13	—	7	—	—
14	3	11	3	—
15	—	3	—	3
16	7	—	—	13
17	3	—	3	—
18	—	3	11	3
19	—	—	—	—
20	3	7	3	11
21	—	3	7	3
22	13	—	—	—
23	3	—	3	—
24	—	3	13	3
25	—	11	—	7
26	3	—	3	—
27	—	3	—	3
28	—	—	7	17
29	3	—	3	13
30	7	3	—	3
31	—	—	—	11
32	3	17	3	7
33	—	3	—	3
34	11	7	—	—
35	3	—	3	—
36	19	3	—	3
37	7	—	13	—
38	7	—	3	—
39	17	3	—	3

	1	3	7	9
40	—	13	11	—
41	3	7	3	—
42	—	3	7	3
43	—	—	19	—
44	3	—	3	—
45	11	3	—	3
46	—	—	—	7
47	3	11	3	—
48	13	3	—	3
49	—	17	7	—
50	3	—	3	—
51	7	3	11	3
52	—	—	17	23
53	3	13	3	7
54	—	3	—	3
55	19	7	—	13
56	3	—	3	—
57	—	3	—	3
58	7	11	—	19
59	3	—	3	—
60	—	3	—	3
61	13	—	—	—
62	3	7	3	17
63	—	3	7	3
64	—	—	—	11
65	3	—	3	—
66	—	3	23	3
67	11	—	—	7
68	3	—	3	13
69	—	3	17	3
70	—	19	7	—
71	3	23	3	—
72	7	3	—	3
73	17	—	11	—
74	3	—	3	7
75	—	3	—	3
76	—	7	13	—
77	3	—	3	19
78	11	3	—	3
79	7	13	—	17

	1	3	7	9
80	3	11	3	—
81	—	3	19	3
82	—	—	—	—
83	3	7	3	—
84	29	3	7	3
85	23	—	—	—
86	3	—	3	11
87	13	3	—	3
88	—	—	—	7
89	3	19	3	29
90	17	3	—	3
91	—	11	7	—
92	3	13	3	—
93	7	3	—	3
94	—	23	—	13
95	3	8	3	7
96	31	3	—	3
97	—	7	—	11
98	3	—	3	23
99	—	3	—	3
100	7	17	19	—
101	3	—	3	—
102	—	3	13	3
103	—	—	17	—
104	3	7	3	—
105	—	3	7	3
106	—	—	11	—
107	3	29	3	13
108	23	3	—	3
109	—	—	—	7
110	3	—	3	—
111	11	3	—	3
112	19	—	7	—
113	3	11	3	17
114	7	3	31	3
115	—	—	13	19
116	3	—	3	7
117	—	3	11	3
118	—	7	—	29
119	3	—	3	11

	1	3	7	9
120	—	3	17	3
121	7	—	—	23
122	3	—	3	—
123	—	3	—	3
124	17	11	29	—
125	3	7	3	—
126	13	3	7	3
127	31	19	—	—
128	3	—	3	—
129	—	3	—	3
130	—	—	—	7
131	3	13	3	—
132	—	3	—	3
133	11	31	7	13
134	3	17	3	19
135	7	3	23	3
136	—	29	—	37
137	3	—	3	7
138	—	3	19	3
139	13	7	11	—
140	3	23	3	—
141	17	3	13	3
142	7	—	—	—
143	3	—	3	—
144	11	3	—	3
145	—	—	31	—
146	3	7	3	13
147	—	3	7	3
148	—	—	—	—
149	3	—	3	—
150	19	3	11	3
151	—	17	37	7
152	3	—	3	11
153	—	3	29	3
154	23	—	7	—
155	3	—	3	—
156	7	3	—	3
157	—	11	19	—
158	3	—	3	7
159	37	3	—	3

Table E.1 *Factor table.*

	1	3	7	9
160	—	7	—	—
161	3	—	3	—
162	—	3	—	3
163	7	23	—	11
164	3	31	3	17
165	13	3	—	3
166	11	—	—	—
167	3	7	3	23
168	41	3	7	3
169	19	—	—	—
170	3	13	3	—
171	29	3	17	3
172	—	—	11	7
173	3	—	3	37
174	—	3	—	3
175	17	—	7	—
176	3	41	3	29
177	7	3	—	3
178	13	—	—	—
179	3	11	3	7
180	—	3	13	3
181	—	7	23	17
182	3	—	3	31
183	—	3	11	3
184	7	19	—	43
185	3	17	3	11
186	—	3	—	3
187	—	—	—	—
188	3	7	3	—
189	31	3	7	3
190	—	11	—	23
191	3	—	3	19
192	17	3	41	3
193	—	—	13	7
194	3	29	3	—
195	—	3	19	3
196	37	13	7	11
197	3	—	3	—
198	7	3	—	3
199	11	—	—	—
200	3	—	3	7
201	—	3	—	3
202	43	7	—	—
203	3	19	3	—
204	13	3	23	3
205	7	—	11	29
206	3	—	3	—
207	19	3	31	3
208	—	—	—	—
209	3	7	3	—
210	11	3	7	3
211	—	—	29	13
212	3	11	3	—
213	—	3	—	3
214	—	—	19	7
215	3	—	3	17
216	—	3	11	3
217	13	41	7	—
218	3	37	3	11
219	7	3	13	3
220	31	—	—	47
221	3	—	3	7
222	—	3	17	3
223	23	7	—	—
224	3	—	3	13
225	—	3	37	3
226	7	31	—	—
227	3	—	3	43
228	—	3	—	3
229	29	—	—	11
230	3	7	3	—
231	—	3	7	3
232	11	23	13	17
233	3	—	3	—
234	—	3	—	3
235	—	13	—	7
236	3	17	3	23
237	—	3	—	3
238	—	—	7	—
239	3	—	3	—
240	7	3	29	3
241	—	19	—	41
242	3	—	3	7
243	11	3	—	3
244	—	7	—	31
245	3	11	3	—
246	23	3	—	3
247	7	—	—	37
248	3	13	3	19
249	47	3	11	3
250	41	—	23	13
251	3	7	3	11
252	—	3	7	3
253	—	17	43	—
254	3	—	3	—
255	—	3	—	3
256	13	11	17	7
257	3	31	3	—
258	29	3	13	3
259	—	—	7	23
260	3	19	3	—
261	7	3	—	3
262	—	43	37	11
263	3	—	3	7
264	19	3	—	3
265	11	7	—	—
266	3	—	3	17
267	—	3	—	3
268	7	—	—	—
269	3	—	3	—
270	37	3	—	3
271	—	—	11	—
272	3	7	3	—
273	—	3	7	3
274	—	13	41	—
275	3	—	3	31
276	11	3	—	3
277	17	47	—	7
278	3	11	3	—
279	—	3	—	3
280	—	—	7	53
281	3	29	3	—
282	7	3	11	3
283	19	—	—	17
284	3	—	3	7
285	—	3	—	3
286	—	7	47	19
287	3	13	3	—
288	43	3	—	3
289	7	11	—	13
290	3	—	3	—
291	41	3	—	3
292	23	37	—	29
293	3	7	3	—
294	17	3	7	3
295	13	—	—	11
296	3	—	3	—
297	—	3	13	3
298	11	19	29	7
299	3	41	3	—
300	—	3	31	3
301	—	23	7	—
302	3	—	3	13
303	7	3	—	3
304	—	17	11	—
305	3	43	3	7
306	—	3	—	3
307	37	7	17	—
308	3	—	3	—
309	11	3	19	3
310	7	29	13	—
311	3	11	3	—
312	—	3	53	3
313	31	13	—	43
314	3	7	3	47
315	23	3	7	3
316	29	—	—	—
317	3	19	3	11
318	—	3	—	3
319	—	31	23	7

Table E.1 (continued)

	1	3	7	9
320	3	—	3	—
321	13	3	—	3
322	—	11	7	—
323	3	53	3	41
324	7	3	17	3
325	—	—	—	—
326	3	13	3	7
327	—	3	29	3
328	17	7	19	11
329	3	37	3	—
330	—	3	—	3
331	7	—	31	—
332	3	—	3	—
333	—	3	47	3
334	13	—	—	17
335	3	7	3	—
336	—	3	7	3
337	—	—	11	31
338	3	17	3	—
339	—	3	43	3
340	19	41	—	7
341	3	—	3	13
342	11	3	23	3
343	47	—	7	19
344	3	11	3	—
345	7	3	—	3
346	—	—	—	—
347	3	23	3	7
348	59	3	11	3
349	—	7	13	—
350	3	31	3	11
351	—	3	—	3
352	7	13	—	—
353	3	—	3	—
354	—	3	—	3
355	53	11	—	—
356	3	7	3	43
357	—	3	7	3
358	—	—	17	37
359	3	—	3	59
360	13	3	—	3
361	23	—	—	7
362	3	—	3	19
363	—	3	—	3
364	11	—	7	41
365	3	13	3	—
366	7	3	19	3
367	—	—	—	13
368	3	29	3	7
369	—	3	—	3
370	—	7	11	—
371	3	47	3	—
372	61	3	—	3
373	7	—	37	—
374	3	19	3	23
375	11	3	13	3
376	—	53	—	—
377	3	7	3	—
378	19	3	7	3
379	17	—	—	29
380	3	—	3	31
381	37	3	11	3
382	—	—	43	7
383	3	—	3	11
384	23	3	—	3
385	—	—	7	17
386	3	—	3	53
387	7	3	—	3
388	—	11	13	—
389	3	17	3	7
390	47	3	—	3
391	—	7	—	—
392	3	—	3	—
393	—	3	31	3
394	7	—	—	11
395	3	59	37	3
396	17	3	—	3
397	11	29	41	23
398	3	7	3	—
399	13	3	7	3
400	—	—	—	19
401	3	—	3	—
402	—	3	—	3
403	29	37	11	7
404	3	13	3	—
405	—	3	—	3
406	31	17	7	13
407	3	—	3	—
408	7	3	61	3
409	—	—	17	—
410	3	11	3	7
411	—	3	23	3
412	13	7	—	—
413	3	—	3	—
414	41	3	11	3
415	7	—	—	—
416	3	23	3	11
417	43	3	—	3
418	37	47	53	59
419	3	7	3	13
420	—	3	7	3
421	—	11	—	—
422	3	41	3	—
423	—	3	19	3
424	—	—	31	7
425	3	—	3	—
426	—	3	17	3
427	—	—	7	11
428	3	—	3	—
429	7	3	—	3
430	11	13	59	31
431	3	19	3	7
432	29	3	—	3
433	61	7	—	—
434	3	43	3	—
435	19	3	—	3
436	7	—	11	17
437	3	—	3	29
438	13	3	41	3
439	—	23	—	53
440	3	7	3	—
441	11	3	7	3
442	—	—	19	43
443	3	11	3	23
444	—	3	—	3
445	—	61	—	7
446	3	—	3	41
447	17	3	11	3
448	—	—	7	67
449	3	—	3	11
450	7	3	—	3
451	13	—	—	—
452	3	—	3	7
453	23	3	13	3
454	19	7	—	—
455	3	29	3	47
456	—	3	—	3
457	7	17	23	19
458	3	—	3	13
459	—	3	—	3
460	43	—	17	11
461	3	7	3	31
462	—	3	7	3
463	11	41	—	—
464	3	—	3	—
465	—	3	—	3
466	59	—	13	7
467	3	—	3	—
468	31	3	43	3
469	—	13	7	37
470	3	—	3	17
471	7	3	53	3
472	—	—	29	—
473	3	—	3	7
474	11	3	47	3
475	—	7	67	—
476	3	11	3	19
477	13	3	17	3
478	7	—	—	—
479	3	—	3	—

Table E.1 (continued)

	1	3	7	9
480	—	3	11	3
481	17	—	—	61
482	3	7	3	11
483	—	3	7	3
484	47	29	37	13
485	3	23	3	43
486	—	3	31	3
487	—	11	—	7
488	3	19	3	—
489	67	3	59	3
490	13	—	7	—
491	3	17	3	—
492	7	3	13	3
493	—	—	—	11
494	3	—	3	7
495	—	3	—	3
496	11	7	—	—
497	3	—	3	13
498	17	3	—	3
499	7	—	19	—
500	3	—	3	—
501	—	3	29	3
502	—	—	11	47
503	3	7	3	—
504	71	3	7	3
505	—	31	13	—
506	3	61	3	37
507	11	3	—	3
508	—	13	—	7
509	3	11	3	—
510	—	3	—	3
511	19	—	7	—
512	3	47	3	23
513	7	3	11	3
514	53	37	—	19
515	3	—	3	7
516	13	3	—	3
517	—	7	31	—
518	3	71	3	—
519	29	3	—	3
520	7	11	41	—
521	3	13	3	17
522	23	3	—	3
523	—	—	—	13
524	3	7	3	29
525	59	3	7	3
526	—	19	23	11
527	3	—	3	—
528	—	3	17	3
529	11	67	—	7
530	3	—	3	—
531	47	3	13	3
532	17	—	7	73
533	3	—	3	19
534	7	3	—	3
535	—	53	11	23
536	3	31	3	7
537	41	3	19	3
538	—	7	—	17
539	3	—	3	—
540	11	3	—	3
541	7	—	—	—
542	3	11	3	61
543	—	3	—	3
544	—	—	13	—
545	3	7	3	53
546	43	3	7	3
547	—	13	—	—
548	3	—	3	11
549	17	3	23	3
550	—	—	—	7
551	3	37	3	—
552	—	3	—	3
553	—	11	7	29
554	3	23	3	31
555	7	3	—	3
556	67	—	19	—
557	3	—	3	7
558	—	3	37	3
559	—	7	29	11
560	3	13	3	71
561	31	3	41	3
562	7	—	17	13
563	3	43	3	—
564	—	3	—	3
565	—	—	—	—
566	3	7	3	—
567	53	3	7	3
568	13	—	11	—
569	3	—	3	41
570	—	3	13	3
571	—	29	—	7
572	3	59	3	17
573	11	3	—	3
574	—	—	7	—
575	3	11	3	13
576	7	3	73	3
577	29	23	53	—
578	3	—	3	7
579	—	3	11	3
580	—	7	—	37
581	3	—	3	11
582	—	3	—	3
583	7	19	13	—
584	3	—	3	—
585	—	3	—	3
586	—	11	—	—
587	3	7	3	—
588	—	3	7	3
589	43	71	—	17
590	3	—	3	19
591	23	3	61	3
592	31	—	—	7
593	3	17	3	—
594	13	3	19	3
595	11	—	7	59
596	3	67	3	47
597	7	3	43	3
598	—	31	—	53
599	3	13	3	7
600	17	3	—	3
601	—	7	11	13
602	3	19	3	—
603	37	3	—	3
604	7	—	—	23
605	3	—	3	73
606	11	3	—	3
607	13	—	59	—
608	3	7	3	—
609	—	3	7	3
610	—	17	31	41
611	3	—	311	29
612	—	3	11	3
613	—	—	17	7
614	3	—	3	11
615	—	3	47	3
616	61	—	7	31
617	3	—	3	37
618	7	3	23	3
619	41	11	—	—
620	3	—	3	7
621	—	3	—	3
622	—	7	13	—
623	3	23	3	17
624	79	3	—	3
625	7	13	—	11
626	3	—	3	—
627	—	3	—	3
628	11	61	—	19
629	3	7	3	—
630	—	3	7	3
631	—	59	—	71
632	3	—	3	—
633	13	3	—	3
634	17	—	11	7
635	3	—	3	—
636	—	3	—	3
637	23	—	7	—
638	3	13	3	—
639	7	3	—	3

Table E.1 (continued)

	1	3	7	9
640	37	19	43	13
641	3	11	3	7
642	—	3	—	3
643	59	7	41	47
644	3	19	3	—
645	—	3	11	3
646	7	23	29	—
647	3	—	3	11
648	—	3	13	3
649	—	43	73	67
650	3	7	3	23
651	17	3	7	3
652	—	11	61	—
653	3	47	3	13
654	31	3	—	3
655	—	—	79	7
656	3	—	3	—
657	—	3	—	3
658	—	29	7	11
659	3	19	3	—
660	7	3	—	3
661	11	17	13	—
662	3	37	3	7
663	19	3	—	3
664	29	7	17	61
665	3	—	3	—
666	—	3	59	3
667	7	—	11	—
668	3	41	3	—
669	—	3	37	3
670	—	—	19	—
671	3	7	3	—
672	11	3	7	3
673	53	—	—	23
674	3	11	3	17
675	43	3	29	3
676	—	—	67	7
677	3	13	3	—
678	—	3	11	3
679	—	—	7	13
680	3	—	3	11
681	7	3	17	3
682	19	—	—	—
683	3	—	3	7
684	—	3	41	3
685	13	7	—	19
686	3	—	3	—
687	—	3	13	3
688	7	—	71	83
689	3	61	3	—
690	67	3	—	3
691	—	31	—	11
692	3	7	3	13
693	29	3	7	3
694	11	53	—	—
695	3	17	3	—
696	—	3	—	3
697	—	19	—	7
698	3	—	3	29
699	—	3	—	3
700	—	47	7	43
701	3	—	3	—
702	7	3	—	3
703	79	13	31	—
704	3	—	3	7
705	11	3	—	3
706	23	7	37	—
707	3	11	3	—
708	73	3	19	3
709	7	41	47	31
710	3	—	3	—
711	13	3	11	3
712	—	17	—	—
713	3	7	3	11
714	37	3	7	3
715	—	23	17	—
716	3	13	3	67
717	71	3	—	3
718	43	11	—	7
719	3	—	3	23
720	19	3	—	3
721	—	—	7	—
722	3	31	3	—
723	7	3	—	3
724	13	—	—	11
725	3	—	3	7
726	53	3	13	3
727	11	7	19	29
728	3	—	3	37
729	23	3	—	3
730	7	67	—	—
731	3	71	3	13
732	—	3	17	3
733	—	—	11	41
734	3	7	3	—
735	—	3	7	3
736	17	37	53	—
737	3	73	3	47
738	11	3	83	3
739	19	—	13	7
740	3	11	3	31
741	—	3	—	3
742	41	13	7	17
743	3	—	3	43
744	7	3	11	3
745	—	29	—	—
746	3	17	3	7
747	31	3	—	3
748	—	7	—	—
749	3	59	3	—
750	13	3	—	3
751	7	11	—	73
752	3	—	3	—
753	17	3	—	3
754	—	19	—	—
755	3	7	3	—
756	—	3	7	3
757	67	—	—	11
758	3	—	3	—
759	—	3	71	3
760	11	—	—	7
761	3	23	3	19
762	—	3	29	3
763	13	17	7	—
764	3	—	3	—
765	7	3	13	3
766	47	79	11	—
767	3	—	3	7
768	—	3	—	3
769	—	7	43	—
770	3	—	3	13
771	11	3	—	3
772	7	—	—	59
773	3	11	3	71
774	—	3	61	3
775	23	—	—	—
776	3	7	3	17
777	19	3	7	3
778	31	43	13	—
779	3	—	3	11
780	29	3	37	3
781	73	13	—	7
782	3	—	3	—
783	41	3	17	3
784	—	11	7	47
785	3	—	3	29
786	7	3	—	3
787	17	—	—	—
788	3	—	3	7
789	13	3	53	3
790	—	7	—	11
791	3	41	3	—
792	89	3	—	3
793	7	—	—	17
794	3	13	3	—
795	—	3	73	3
796	19	—	31	13
797	3	7	3	79
798	23	3	7	3
799	61	—	11	19

Table E.1 (continued)

	1	3	7	9		1	3	7	9		1	3	7	9		1	3	7	9
800	3	53	3	—	840	31	3	7	3	880	13	—	—	23	920	3	—	3	—
801	—	3	—	3	841	13	47	19	—	881	3	7	3	—	921	61	3	13	3
802	13	71	23	7	842	3	—	3	—	882	—	3	7	3	922	—	23	—	11
803	3	29	3	—	843	—	3	11	3	883	—	11	—	—	923	3	7	3	—
804	11	3	13	3	844	23	—	—	7	884	3	37	3	—	924	—	3	7	3
805	83	—	7	—	845	3	79	3	11	885	53	3	17	3	925	11	19	—	47
806	3	11	3	—	846	—	3	—	3	886	—	—	—	7	926	3	59	3	13
807	7	3	41	3	847	43	37	7	61	887	3	19	3	13	927	73	3	—	3
808	—	59	—	—	848	3	17	3	13	888	83	3	—	3	928	—	—	37	7
809	3	—	3	7	849	7	3	29	3	889	17	—	7	11	929	3	—	3	17
810	—	3	11	3	850	—	11	47	67	890	3	29	3	59	930	71	3	41	3
811	—	7	—	23	851	3	—	3	7	891	7	3	37	3	931	—	67	7	—
812	3	—	3	11	852	—	3	—	3	892	11	—	79	—	932	3	—	3	19
813	47	3	79	3	853	19	7	—	—	893	3	—	3	7	933	7	3	—	3
814	7	17	—	29	854	3	—	3	83	894	—	3	23	3	934	—	—	13	—
815	3	31	3	41	855	17	3	43	3	895	—	7	13	17	935	3	47	3	7
816	—	3	—	3	856	7	—	13	11	896	3	—	3	—	936	11	3	14	3
817	—	11	13	—	857	3	—	3	23	897	—	3	47	3	937	—	7	—	83
818	3	7	3	19	858	—	3	31	3	898	7	13	11	89	938	3	11	3	41
819	—	3	7	3	859	11	13	—	—	899	3	17	3	—	939	—	3	—	3
820	59	13	29	—	860	3	7	3	—	900	—	3	—	3	940	7	—	23	97
821	3	43	3	—	861	79	3	7	3	901	—	—	71	29	941	3	—	3	—
822	—	3	19	3	862	37	—	—	—	902	3	7	3	—	942	—	3	11	3
823	—	—	—	7	863	3	89	3	53	903	11	3	7	3	943	—	—	—	—
824	3	—	3	73	864	—	3	—	3	904	—	—	83	—	944	3	7	3	11
825	37	3	23	3	865	41	17	11	7	905	3	11	3	—	945	13	3	7	3
826	11	—	7	—	866	3	—	3	—	906	13	3	—	3	946	—	—	—	17
827	3	—	3	17	867	13	3	—	3	907	47	43	29	7	947	3	—	3	—
828	7	3	—	3	868	—	19	7	—	908	3	31	3	61	948	19	3	53	3
829	—	—	—	43	869	3	—	3	—	909	—	3	11	3	949	—	11	—	7
830	3	19	3	7	870	7	3	—	3	910	19	—	7	—	950	3	13	3	37
831	—	3	—	3	871	31	—	23	—	911	3	31	3	11	951	—	3	31	3
832	53	7	11	—	872	3	11	3	7	912	7	3	—	3	952	—	89	7	13
833	3	13	3	31	873	—	3	—	3	913	23	—	—	13	953	3	—	3	—
834	19	3	17	3	874	—	7	—	13	914	3	41	3	7	954	7	3	—	3
835	7	—	61	13	875	3	—	3	193	915	—	3	—	3	955	—	41	19	11
836	3	—	3	—	876	—	3	11	3	916	—	7	89	53	956	3	73	3	7
837	11	3	—	3	877	7	31	67	—	917	3	—	3	67	957	17	3	61	3
838	17	83	—	—	878	3	—	3	11	918	—	3	—	3	958	11	7	—	43
839	3	7	3	37	879	59	3	19	3	919	7	29	17	—	959	3	53	3	29

Table E.1 (continued)

	1	3	7	9
960	—	3	13	3
961	7	—	59	—
962	3	—	3	—
963	—	3	23	3
964	31	—	11	—
965	3	7	3	13
966	—	3	7	3
967	19	17	—	—
968	3	23	3	—
969	11	3	—	3
970	89	31	18	7
971	3	11	3	—
972	—	3	71	3
973	37	—	7	—
974	3	—	3	—
975	7	3	11	3
976	43	13	—	—
977	3	29	3	7
978	—	3	—	3
979	—	7	97	41
980	3	—	3	17
981	—	3	—	3
982	7	11	31	—
983	3	—	3	—
984	13	3	43	3
985	—	59	—	—
986	3	7	3	71
987	—	3	7	3
988	41	—	—	11
989	3	13	3	19
990	—	3	—	3
991	11	23	47	7
992	3	—	3	—
993	—	3	19	3
994	—	61	7	—
995	3	37	3	23
996	7	3	—	3
997	13	—	11	17
998	3	67	3	7
999	97	3	13	3

Table E.1 (continued)

n	$\phi(n)$	$\tau(n)$	$\sigma(n)$
1	1	1	1
2	1	2	3
3	2	2	4
4	2	3	7
5	4	2	6
6	2	4	12
7	6	2	8
8	4	4	15
9	6	3	13
10	4	4	18
11	10	2	12
12	4	6	28
13	12	2	14
14	6	4	24
15	8	4	24
16	8	5	31
17	16	2	18
18	6	6	39
19	18	2	20
20	8	6	42
21	12	4	32
22	10	4	36
23	22	2	24
24	8	8	60
25	20	3	31
26	12	4	42
27	18	4	40
28	12	6	56
29	28	2	30
30	8	8	72
31	30	2	32
32	16	6	63
33	20	4	48
34	16	4	54
35	24	4	48
36	12	9	91
37	36	2	38
38	18	4	60
39	24	4	56
40	16	8	90
41	40	2	42
42	12	8	96
43	42	2	44
44	20	6	84
45	24	6	78
46	22	6	72
47	46	2	48
48	16	10	124
49	42	3	57

Table E.2 *Values of some arithmetic functions.*

n	$\phi(n)$	$\tau(n)$	$\sigma(n)$
50	20	6	93
51	32	4	72
52	24	6	98
53	52	2	54
54	18	8	120
55	40	4	72
56	24	8	120
57	36	4	80
58	28	4	90
59	58	2	60
60	16	12	168
61	60	2	62
62	30	4	96
63	36	6	104
64	32	7	127
65	48	4	84
66	20	8	144
67	66	2	68
68	32	6	126
69	44	4	96
70	24	8	144
71	70	2	72
72	24	12	195
73	72	2	74
74	36	4	114
75	40	6	124
76	36	6	140
77	60	4	96
78	24	8	168
79	78	2	80
80	32	10	186
81	54	5	121
82	40	4	126
83	82	2	84
84	24	12	224
85	64	4	108
86	42	4	132
87	56	4	120
88	40	8	180
89	88	2	90
90	24	12	234
91	72	4	112
92	44	6	168
93	60	4	128
94	46	4	144
95	72	4	120
96	32	12	252
97	96	2	98
98	42	6	171
99	60	6	156
100	40	9	217

Table E.2 (continued)

p	r	p	r	p	r	p	r
2	1	191	19	439	15	709	2
3	2	193	5	443	2	719	11
5	2	197	2	449	3	727	5
7	3	199	3	457	13	733	6
11	2	211	2	461	2	739	3
13	2	223	3	463	3	743	5
17	3	227	2	467	2	751	3
19	2	229	6	479	13	757	2
23	5	233	3	487	3	761	6
29	2	239	7	491	2	769	11
31	3	241	7	499	7	773	2
37	2	251	6	503	5	787	2
41	6	257	3	509	2	797	2
43	3	263	5	521	3	809	3
47	5	269	2	523	2	811	3
53	2	271	6	541	2	821	2
59	2	277	5	547	2	823	3
61	2	281	3	557	2	827	2
67	2	283	3	563	2	829	2
71	7	293	2	569	3	839	11
73	5	307	5	571	3	853	2
79	3	311	17	577	5	857	3
83	2	313	10	587	2	859	2
89	3	317	2	593	3	863	5
97	5	331	3	599	7	877	2
101	2	337	10	601	7	881	3
103	5	347	2	607	3	883	2
107	2	349	2	613	2	887	5
109	6	353	3	617	3	907	2
113	3	359	7	619	2	911	17
127	3	367	6	631	3	919	7
131	2	373	2	641	3	929	3
137	3	379	2	643	11	937	5
139	2	383	5	647	5	941	2
149	2	389	2	653	2	947	2
151	6	397	5	659	2	953	3
157	5	401	3	601	2	967	5
163	2	409	21	673	5	971	6
167	5	419	2	677	2	977	3
173	2	421	2	683	5	983	5
179	2	431	7	691	3	991	6
181	2	433	5	701	2	997	7

Table E.3 *Primitive roots modulo primes.*

	Numbers															
p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	2	1														
5	4	1	3	2							Indices					
7	6	2	1	4	5	3										
11	10	1	8	2	4	9	7	3	6	5						
13	12	1	4	2	9	5	11	3	8	10	7	6				
17	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
19	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4
23	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8
29	28	1	5	2	22	6	12	3	10	23	25	7	18	13	27	4
31	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21	0
37	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4
41	40	26	15	12	22	1	39	38	30	8	3	27	31	25	37	24
43	42	27	1	12	25	28	35	39	2	10	30	13	32	20	26	24
47	46	18	20	36	1	38	32	8	40	19	7	10	11	4	21	26
53	52	1	17	2	47	18	14	3	34	48	6	19	24	15	12	4
59	58	1	50	2	6	51	18	3	42	7	25	52	45	19	56	4
61	60	1	6	2	22	7	49	3	12	23	15	8	40	50	28	4
67	66	1	39	2	15	40	23	3	12	16	59	41	19	24	54	4
71	70	6	26	12	28	32	1	18	52	34	31	38	39	7	54	24
73	72	8	6	16	1	14	33	24	12	9	55	22	59	41	7	32
79	78	4	1	8	62	5	53	12	2	66	68	9	34	57	63	16
83	82	1	72	2	27	73	8	3	62	28	24	74	77	9	17	4
89	88	16	1	32	70	17	81	48	2	86	84	33	23	9	71	64
97	96	34	70	68	1	8	31	6	44	35	86	42	25	65	71	40

	Numbers															
p	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
19	10	9															
23	7	12	15	5	13	11								Indices			
29	21	11	9	24	17	26	20	8	16	19	15	14					
31	7	26	4	8	29	17	27	13	10	5	3	16	9	15			
37	7	17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20
41	33	16	9	34	14	29	36	13	4	17	5	11	7	23	28	10	18
43	38	29	19	37	36	15	16	40	8	17	3	5	41	11	34	9	31
47	16	12	45	37	6	25	5	28	2	29	14	22	35	39	3	44	27
53	10	35	37	49	31	7	39	20	42	25	51	16	46	13	33	5	23
59	40	43	38	8	10	26	15	53	12	46	34	20	28	57	49	5	17
61	47	13	26	24	55	16	57	9	44	41	18	51	35	29	59	5	21
67	64	13	10	17	62	60	28	42	30	20	51	25	44	55	47	5	32
71	49	58	16	40	27	37	15	44	56	45	8	13	68	60	11	30	57
73	21	20	62	17	39	63	46	30	2	67	18	49	35	15	11	40	61
79	21	6	32	70	54	72	26	13	46	38	3	61	11	67	56	20	69
83	56	63	47	29	80	25	60	75	56	78	52	10	12	18	38	5	14
89	6	18	35	14	82	12	57	49	52	39	3	25	59	87	31	80	85
97	89	78	81	69	5	24	77	76	2	59	18	3	13	9	46	74	60

Table E.4 *Indices.*

	Numbers															
p	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
37	8	19	18													
41	19	21	2	32	35	6	20				Indices					
43	23	18	14	7	4	33	22	6	21							
47	34	33	30	42	17	31	9	15	24	13	43	41	23			
53	11	9	36	30	38	41	50	45	32	22	8	29	40	44	21	23
59	41	24	44	55	39	37	9	14	11	33	27	48	16	23	54	36
61	48	11	14	39	27	46	25	54	56	43	17	34	58	20	10	38
67	65	38	14	22	11	58	18	53	63	9	61	27	29	50	43	46
71	55	29	64	20	22	65	46	25	33	48	43	10	21	9	50	2
78	29	34	28	64	70	65	25	4	47	51	71	13	54	31	38	66
79	25	37	10	19	36	35	74	75	58	49	76	64	30	59	17	28
83	57	35	64	20	48	67	30	40	81	71	26	7	61	23	76	16
89	22	63	34	11	51	24	30	21	10	29	28	72	73	54	65	74
97	27	32	16	91	19	95	7	85	39	4	58	45	15	84	14	62

	Numbers															
p	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
53	43	27	26													
59	13	32	47	22	35	31	21	30	29			Indices				
61	45	53	42	33	19	37	52	32	36	31	30					
67	31	37	21	57	52	8	26	49	45	36	56	7	48	35	6	34
71	62	5	51	23	14	59	19	42	4	3	66	69	17	53	36	67
73	10	27	3	53	26	56	57	68	43	5	23	58	19	45	48	60
79	50	22	42	77	7	52	65	33	15	31	71	45	60	55	24	18
83	55	46	79	59	53	51	11	37	13	34	19	66	39	70	6	22
89	68	7	55	78	19	66	41	36	75	43	15	69	47	83	8	5
97	36	63	93	10	52	87	37	55	47	67	43	64	80	75	12	26

	Numbers															
p	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
67	33															
71	63	47	61	41	35						Indices					
78	69	50	37	52	42	44	36									
79	73	48	29	27	41	51	14	44	23	47	40	43	39			
83	15	45	58	50	36	33	65	69	21	44	49	32	68	43	31	42
89	13	56	38	58	79	62	50	20	27	53	67	77	40	42	46	4
97	94	57	61	51	66	11	50	28	29	72	53	21	33	30	41	88

	Numbers															
p	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	
83	41															
89	37	61	26	76	45	60	44					Indices				
97	23	17	73	90	38	83	92	54	79	56	49	20	22	82	48	

Table E.4 (continued)

	Indices															
p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	2	1														
5	2	4	3	1												
7	3	2	6	4	5	1						Numbers				
11	2	4	8	5	10	9	7	3	6	1						
13	2	4	8	3	6	12	11	9	5	10	7	1				
17	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
19	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5
23	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3
29	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25
31	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28
37	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9
41	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18
43	3	9	27	38	28	41	37	25	32	10	30	4	12	36	22	23
47	5	25	31	14	23	21	11	8	40	12	13	18	43	27	41	17
53	2	4	8	16	32	11	22	44	35	17	34	15	30	7	14	28
59	2	4	8	16	32	5	10	20	40	21	42	25	50	41	23	46
61	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11	22
67	2	4	8	16	32	64	61	55	43	19	38	9	18	36	5	10
71	7	49	59	58	51	2	14	27	47	45	31	4	28	54	23	19
73	5	25	52	41	59	3	15	2	10	50	31	9	45	6	30	4
79	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16
83	2	4	8	16	32	64	45	7	14	28	56	29	58	33	66	49
89	3	9	27	81	65	17	51	64	14	42	37	22	66	20	60	2
97	2	25	28	43	21	8	40	6	30	53	71	64	29	48	46	36

	Indices															
p	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
19	10	1															
23	15	6	7	12	14	1						Numbers					
29	21	13	26	23	17	5	10	20	11	22	15	1					
31	22	4	12	5	15	14	11	2	6	18	23	7	21	1			
37	18	36	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14
41	26	33	34	40	35	5	30	16	14	2	12	31	22	9	13	37	17
43	26	35	19	14	42	40	34	16	5	15	2	6	18	11	33	13	39
47	38	2	10	3	15	28	46	42	22	16	33	24	26	36	39	7	35
53	3	6	12	24	48	43	33	13	26	52	51	49	45	37	21	42	31
59	33	7	14	28	56	53	47	35	11	22	44	29	58	57	55	51	43
61	44	27	54	47	33	5	10	20	40	19	38	15	30	60	59	57	53
67	20	40	13	26	52	37	7	14	28	56	45	23	46	25	50	33	66
71	62	8	56	37	46	38	53	16	41	3	21	5	35	32	11	6	42
73	20	27	62	18	17	12	60	8	40	54	51	36	34	24	47	16	7
79	48	65	37	32	17	51	74	64	34	23	69	49	68	46	59	19	57
83	15	30	60	37	74	65	47	11	22	44	5	10	20	40	80	77	71
89	6	18	54	73	41	34	13	39	28	84	74	44	43	40	31	4	12
97	83	27	38	93	77	94	82	22	13	65	34	73	74	79	7	35	78

Table E.4 (continued)

	Indices															
p	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
37	28	19	1													
41	20	38	23	15	8	7	1					Numbers				
43	31	7	21	20	17	8	24	29	1							
47	34	29	4	20	6	30	9	45	37	44	32	19	1			
53	9	18	36	19	38	23	46	39	25	50	47	41	29	5	10	20
59	27	54	49	39	19	38	17	34	9	18	36	13	26	52	45	31
61	45	29	58	55	49	37	13	26	52	43	25	50	39	17	34	7
67	65	63	59	51	35	3	6	12	24	48	29	58	49	31	62	57
71	10	70	64	22	12	13	20	69	57	44	24	26	40	67	43	17
73	35	29	72	68	48	21	32	14	70	58	71	63	23	42	64	28
79	13	39	38	35	26	78	76	70	52	77	73	61	25	75	67	43
83	59	35	70	57	31	62	41	82	81	79	75	67	51	19	38	76
89	36	19	57	82	68	26	78	56	79	59	88	86	80	62	8	24
97	2	10	50	56	86	42	16	80	12	60	9	45	31	58	96	92

	Indices															
p	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
53	40	27	1													
59	3	6	12	24	48	37	15	30	1				Numbers			
61	14	28	56	51	41	21	42	23	46	31	1					
67	47	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34
71	48	52	9	63	15	34	25	33	18	55	30	68	50	66	36	39
73	67	43	69	53	46	11	55	56	61	13	65	33	19	22	37	39
79	50	71	55	7	21	63	31	14	42	47	62	28	5	15	45	56
83	69	55	27	54	25	50	17	34	68	53	23	46	9	18	36	72
89	72	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48
97	72	69	54	76	89	57	91	67	44	26	33	68	49	51	61	14

	Indices															
p	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81
67	1															
71	60	65	29	61	1											
73	49	26	57	66	38	44	1									
79	10	30	11	33	20	60	22	66	40	41	44	53	1			
83	61	39	78	73	63	43	3	6	12	24	48	13	26	52	21	42
89	55	76	50	61	5	15	45	46	49	58	85	77	53	70	32	7
97	70	59	4	20	3	15	75	84	32	63	24	23	18	90	62	19

	Indices															
p	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	
83	1															
89	21	63	11	33	10	30	1					Numbers				
97	95	87	47	41	11	55	81	17	85	37	88	52	66	39	1	

Table E.4 (continued)

d	$\sqrt{d}$	d	$\sqrt{d}$
2	$[1;\overline{2}]$	53	$[7;\overline{3,1,1,3,14}]$
3	$[1;\overline{1,2}]$	54	$[7;\overline{2,1,6,2,14}]$
5	$[2;\overline{4}]$	55	$[7;\overline{2,2,2,14}]$
6	$[2;\overline{2,4}]$	56	$[7;\overline{2,14}]$
7	$[2;\overline{1,1,1,4}]$	57	$[7;\overline{1,1,4,1,1,14}]$
8	$[2;\overline{1,4}]$	58	$[7;\overline{1,1,1,1,1,1,14}]$
10	$[3;\overline{6}]$	59	$[7;\overline{1,2,7,2,1,14}]$
11	$[3;\overline{3,6}]$	60	$[7;\overline{1,2,1,14}]$
12	$[3;\overline{2,6}]$	61	$[7;\overline{1,4,3,1,2,2,1,3,4,1,14}]$
13	$[3;\overline{1,1,1,1,6}]$	62	$[7;\overline{1,6,1,14}]$
14	$[3;\overline{1,2,1,6}]$	63	$[7;\overline{1,14}]$
15	$[3;\overline{1,6}]$	65	$[8;\overline{16}]$
17	$[4;\overline{8}]$	66	$[8;\overline{8,16}]$
18	$[4;\overline{4,8}]$	67	$[8;\overline{5,2,1,1,7,1,1,2,5,16}]$
19	$[4;\overline{2,1,3,1,2,8}]$	68	$[8;\overline{4,16}]$
20	$[4;\overline{2,8}]$	69	$[8;\overline{3,3,1,4,1,3,3,16}]$
21	$[4;\overline{1,1,2,1,1,8}]$	70	$[8;\overline{2,1,2,1,2,16}]$
22	$[4;\overline{1,2,4,2,1,8}]$	71	$[8;\overline{2,2,1,7,1,2,2,16}]$
23	$[4;\overline{1,3,1,8}]$	72	$[8;\overline{2,16}]$
24	$[4;\overline{1,8}]$	73	$[8;\overline{1,1,5,5,1,1,16}]$
26	$[5;\overline{10}]$	74	$[8;\overline{1,1,1,1,16}]$
27	$[5;\overline{5,10}]$	75	$[8;\overline{1,1,1,16}]$
28	$[5;\overline{3,2,3,10}]$	76	$[8;\overline{1,2,1,1,5,4,5,1,1,2,1,16}]$
29	$[5;\overline{2,1,1,2,10}]$	77	$[8;\overline{1,3,2,3,1,16}]$
30	$[5;\overline{2,10}]$	78	$[8;\overline{1,4,1,16}]$
31	$[5;\overline{1,1,3,5,3,1,1,10}]$	79	$[8;\overline{1,7,1,16}]$
32	$[5;\overline{1,1,1,10}]$	80	$[8;\overline{1,16}]$
33	$[5;\overline{1,2,1,10}]$	82	$[9;\overline{18}]$
34	$[5;\overline{1,4,1,10}]$	83	$[9;\overline{9,18}]$
35	$[5;\overline{5,10}]$	84	$[9;\overline{6,18}]$
37	$[6;\overline{12}]$	85	$[9;\overline{4,1,1,4,18}]$
38	$[6;\overline{6,12}]$	86	$[9;\overline{3,1,1,1,8,1,1,1,3,18}]$
39	$[6;\overline{4,12}]$	87	$[9;\overline{3,18}]$
40	$[6;\overline{3,12}]$	88	$[9;\overline{2,1,1,1,2,18}]$
41	$[6;\overline{2,2,12}]$	89	$[9;\overline{2,3,3,2,18}]$
42	$[6;\overline{2,12}]$	90	$[9;\overline{2,18}]$
43	$[6;\overline{1,1,3,1,5,1,3,1,1,12}]$	91	$[9;\overline{1,1,5,1,5,1,1,18}]$
44	$[6;\overline{1,1,1,2,1,1,1,12}]$	92	$[9;\overline{1,1,2,4,2,1,1,18}]$
45	$[6;\overline{1,2,2,2,1,12}]$	93	$[9;\overline{1,1,1,4,6,4,1,1,1,18}]$
46	$[6;\overline{1,3,1,1,2,6,2,1,1,3,1,12}]$	94	$[9;\overline{1,2,3,1,1,5,1,8,1,5,1,1,3,2,1,18}]$
47	$[6;\overline{1,5,1,12}]$	95	$[9;\overline{1,2,1,18}]$
48	$[6;\overline{1,12}]$	96	$[9;\overline{1,3,1,18}]$
50	$[7;\overline{14}]$	97	$[9;\overline{1,5,1,1,1,1,1,1,5,1,18}]$
51	$[7;\overline{7,14}]$	98	$[9;\overline{1,8,1,18}]$
52	$[7;\overline{4,1,2,1,4,14}]$	99	$[9;\overline{1,18}]$

Table E.5 *Simple continued fractions for square roots of positive integers.*

Answers to Odd-Numbered Exercises

Section 1.1

1. a. well-ordered; every subset of this set is also a subset of the set of positive integers and hence must have a least element
b. well-ordered; every subset of this set is also a subset of the set of positive integers and hence must have a least element
c. not well-ordered; the set of positive rational numbers
d. well-ordered; the set of numerators of the numbers in any subset is a subset of the set of positive integers, so it must have a least element b, and then $b/2$ is the least element of the subset
e. not well-ordered; the set of positive rational numbers

3. Let a/b and c/d be the given rational numbers, where a, b, c, and d are integers with b and d nonzero. The sum of the two rational numbers is $(ad + bc)/(bd)$, which is a rational number since the numerator and denominator are integers and the denominator is not 0. Similarly, their product is $(ac)/(bd)$, which is a rational number for the same reasons.

5. Suppose that $\sqrt{3} = a/b$, with a and b positive integers. Then the set $S = \{k\sqrt{3} \mid k \text{ and } k\sqrt{3} \text{ are positive integers}\}$ is nonempty since it contains $a = b\sqrt{3}$. By the well-ordering property, S has a smallest element, say $s = t\sqrt{3}$. Consider $s' = s\sqrt{3} - s = 3t - s$. Since $3t$ and s are both integers, s' must also be an integer. Note that $s' = s(\sqrt{3} - 1)$, so s' is positive since $\sqrt{3} > 1$, and s' is less than s since $\sqrt{3} < 2$. This contradicts the choice of s, so our original assumption that $\sqrt{3}$ is rational is wrong.

7. a. 0 **b.** -1 **c.** 3 **d.** -2 **e.** 0 **f.** -4

9. a. $\{8/5\} = 3/5$ **b.** $\{1/7\} = 1/7$ **c.** $\{-11/4\} = 1/4$ **d.** $\{7\} = 0$

11. 0 if x is an integer; -1 otherwise

13. We have $[x] \le x$ and $[y] \le y$. Adding these two inequalities gives $[x] + [y] \le x + y$. Hence, $[x + y] \ge [[x] + [y]] = [x] + [y]$.

15. Let $x = a + r$ and $y = b + s$, where a and b are integers and r and s are real numbers such that $0 \le r, s < 1$. Then $[xy] = [ab + as + br + sr] = ab + [as + br + sr]$, whereas $[x][y] = ab$. Thus

$[xy] \geq [x][y]$. If x and y are both negative, then $[xy] \leq [x][y]$. If one of x and y is positive and the other negative, then either $[xy]$ or $[x][y]$ could be larger.

17. Let $x = [x] + r$. Since $0 \leq r < 1$, $x + \frac{1}{2} = [x] + r + \frac{1}{2}$. If $r < \frac{1}{2}$, then $[x]$ is the integer nearest to x, and $[x + \frac{1}{2}] = [x]$ since $[x] \leq x + \frac{1}{2} = [x] + r + \frac{1}{2} < [x] + 1$. If $r \geq \frac{1}{2}$, then $[x] + 1$ is the integer nearest to x (choosing this integer if x is midway between $[x]$ and $[x + 1]$), and $[x + \frac{1}{2}] = [x] + 1$ since $[x] + 1 \leq x + r + \frac{1}{2} < [x] + 2$.

19. If x is a positive integer, then the two sides are identical. So suppose that $x = n^2 + m + \epsilon$, where n is the largest perfect square integer less than x, m is a nonnegative integer, and $0 < \epsilon < 1$. Then both $\sqrt{x}$ and $\sqrt{[x]} = \sqrt{n^2 + m}$ are between n and $n + 1$. Therefore, both sides of the equation equal n.

21. **a.** $8n - 5$ **b.** $2^n + 3$ **c.** $[[\sqrt{n}\,]/\sqrt{n}\,]$ **d.** $a_1 = 1$, $a_2 = 3$, and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$

23. $a_n = 2^{n-1}$; $a_n = (n^2 - n + 2)/2$; $a_1 = 1$, $a_2 = 2$, and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 3$

25. This set is exactly the sequence $a_n = n - 100$ and hence is countable.

27. The function $f(a + b\sqrt{2}) = 2^a 3^b$ is a one-to-one map of this set into the set of positive integers, which is countable.

29. Suppose that $\{A_i\}$ is a countable collection of countable sets. Then each A_i can be represented by a sequence: $A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$, $A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$, $A_3 = \{a_{31}, a_{32}, a_{33}, \ldots\}$, . . . Consider the listing $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \ldots$, in which we first list the elements with subscripts adding to 2, then the elements with subscripts adding to 3, and so on. Further, we order the elements with subscripts adding to k in order of the first subscript. Form a new sequence c_i as follows. Let $c_1 = a_1$. Given that c_n is determined, let c_{n+1} be the next element in the listing that is different from each c_i with $i = 1, 2, \ldots, n$. Then this sequence is exactly the elements of $\bigcup_{i=1}^{\infty} A_i$, which is therefore countable.

31. **a.** $a = 4$, $b = 7$ **b.** $a = 7$, $b = 10$ **c.** $a = 7$, $b = 69$ **d.** $a = 1$, $b = 20$

33. The number α lies in an interval of the form $r/k \leq \alpha < (r + 1)/k$, where $0 \leq r \leq k - 1$. If we divide this interval into equal halves, then α must lie in one of the halves, so either $r/k \leq \alpha < (2r + 1)/2k$ or $(2r + 1)/2k \leq \alpha < (r + 1)/k$. In the first case, because $|\alpha - r/k| < 1/2k$, we can take $u = r$. In the second case, we can take $u = r + 1$, because $|\alpha - (r + 1)/k| < 1/2k$.

35. First we have $|\sqrt{2} - 1/1| = 0.414 \ldots < 1/1^2$. Second, by Exercise 30 (a), we have $|\sqrt{2} - 7/5| < 1/50 < 1/5^2$. Third, observing that $3/7 = 0.428 \ldots$ leads us to try $|\sqrt{2} - 10/7| = 0.014 \ldots < 1/7^2 = 0.0204 \ldots$. Fourth, observing that $5/12 = 0.4166 \ldots$ leads us to try $|\sqrt{2} - 17/12| = 0.00245 \ldots < 1/12^2 = 0.00694 \ldots$.

37. Assume that $b > 0$ and $q > 0$. Note that if $q > b$, then $|p/q - a/b| = |pb - aq|/qb \geq 1/qb > 1/q^2$. Therefore, solutions to the inequality have $1 \leq q \leq b$. For a given q, there can be only finitely many p such that the distance between the rational numbers a/b and p/q is less than $1/q^2$ (indeed, there is at most one). Therefore, there are only finitely many p/q satisfying the inequality.

39. **a.** 3, 6, 9, 12, 15, 18, 21, 24, 27, 30 **b.** 1, 3, 5, 6, 8, 10, 12, 13, 15, 17 **c.** 2, 4, 7, 9, 11, 14, 16, 18, 21, 23 **d.** 3, 6, 9, 12, 15, 18, 21, 25, 28, 31

41. Assume that $1/\alpha + 1/\beta = 1$. First, show that the sequences $m\alpha$ and $n\beta$ are disjoint. Then, for an integer k, define $N(k)$ to be the number of elements of the sequences $m\alpha$ and $n\beta$ less than k. Then $N(k) = [k/\alpha] + [k/\beta]$. By definition of the greatest integer function, $k/\alpha - 1 < [k/\alpha] < k/\alpha$ and $k/\beta - 1 < [k/\beta] < k/\beta$. Add these inequalities to deduce that $k - 2 < N(k) < k$. Hence, $N(k) = k - 1$, and the conclusion follows. To prove the converse, note that if $1/\alpha + 1/\beta \neq 1$, then the spectrum sequences cannot partition the integers.

43. Assume that there are only finitely many Ulam numbers. Let the two largest Ulam numbers be u_{n-1} and u_n. Then the integer $u_{n-1} + u_n$ is an Ulam number larger than u_n. It is the unique sum of two distinct Ulam numbers u_i and u_j with $i < j$, since $u_i + u_j < u_{n-1} + u_n$ if $j < n$ or if $j = n$ and $i < n - 1$.

Section 1.2

1. **a.** 55 **b.** -15 **c.** $29/20$

3. **a.** 510 **b.** 24600 **c.** $-255/256$

5. The sum $\sum_{k=1}^{n} [\sqrt{k}]$ counts for every value of k with $\sqrt{k} \geq 1$. There are n such values of k in the range $k = 1, 2, 3, \ldots, n$. It counts another 1 for every value of k with $\sqrt{k} \geq 2$. There are $n - 3$ such values in the range. The sum counts another 1 for each value of k with $\sqrt{k} \geq 3$. There are $n - 8$ such values in the range. In general, for $m = 1, 2, 3, \ldots, [\sqrt{n}]$ the sum counts a 1 for each value of k with $\sqrt{k} \geq m$, and there are $n - (m^2 - 1)$ values in the range. Therefore, $\sum_{k=1}^{n} [\sqrt{k}] = \sum_{m=1}^{[\sqrt{n}]} n - (m^2 - 1) = [\sqrt{n}](n + 1) - \sum_{m=1}^{[\sqrt{n}]} m^2 = [\sqrt{n}](n + 1) - ([\sqrt{n}]([\sqrt{n}] + 1)(2[\sqrt{n}] + 1))/6$.

7. The total number of dots in the n by $n + 1$ rectangle, namely $n(n + 1)$, is $2t_n$ since the rectangle is made from two triangular arrays. Dividing both sides by 2 gives the desired formula.

9. From Exercise 8 we have $p_n = \sum_{k=1}^{n} (3k - 2) = 3 \sum_{k=1}^{n} k - 2 \sum_{k=1}^{n} 1 = 3n(n + 1)/2 - 2n = (3n^2 - n)/2$. On the other hand, $t_{n-1} + n^2 = n(n - 1)/2 + n^2 = (3n^2 - n)/2$ as well.

11. **a.** Consider a regular heptagon which we border successively by heptagons with 3, 4, 5, ... dots on each side. Define the heptagonal number s_k to be the number of dots contained in the k nested heptagons.
b. $(5k^2 - 3k)/2$

13. By Exercise 12 we have $T_n = \sum_{k=1}^{n} t_k = \sum_{k=1}^{n} k(k + 1)/2$. Note that $(k + 1)^3 - k^3 = 3k^2 + 3k + 1 = 3(k^2 + k) + 1$, so that $k^2 + k = (k + 1)^3 = k^3/3 - 1/3$. It follows that $T_n = (1/2) \sum_{k=1}^{n} k(k + 1) = (1/6) \sum_{k=1}^{n} ((k + 1)^3 - k^3) - (1/6) \sum_{k=1}^{n} 1$. Because the first sum telescopes, we conclude that $T_n = (1/6)((n + 1)^3 - 1^3) - 1/6 = (n^3 + 3n^2 + 2n)/6$.

15. Each of these four quantities is the product of 100 integers. The largest product is 100^{100}, since it is the product of 100 factors of 100. The second largest is 100! which is the product of the integers $1, 2, \ldots, 100$, and each of these terms is less than or equal to 100. The third largest is $(50!)^2$ which is the product of $1^2, 2^2, \ldots, 50^2$, and each of these factors j^2 is less than $j(50 + j)$. The smallest is 2^{100} as is easily seen.

17. We have $\sum_{k=1}^{n} 1/(k(k + 1)) = \sum_{k=1}^{n} (1/k - 1/(k + 1))$. Let $a_j = 1/(j + 1)$. Notice that this is a telescoping sum. Using the notation in the text preceding Example 1.19, we have $\sum_{k=1}^{n} (1/k - 1/(k + 1)) = \sum_{j=1}^{n} (a_{j-1} - a_j) = -(a_n - a_0) = 1 - 1/(n + 1)$.

19. We sum both sides of the identity $(k + 1)^3 - k^3 = 3k^2 + 3k + 1$ from $k = 1$ to $k = n$. Then the sum telescopes, as in Example 1.19, yielding $\sum_{k=1}^{n} ((k + 1)^3 - k^3) = (n + 1)^3 - 1$. Also $\sum_{k=1}^{n} (3k^2 + 3k + 1) = 3(\sum_{k=1}^{n} k^2) + 3(\sum_{k=1}^{n} k) + \sum_{k=1}^{n} 1 = 3(\sum_{k=1}^{n} k^2) + 3n(n + 1)/2 + n$. As these two expressions are equal, solving for $\sum_{k=1}^{n} k^2$ yields, after several steps of algebra, $\sum_{k=1}^{n} k^2 = n(n + 1)(2n + 1)/6$.

21. **a.** $10! = (7!)(8 \cdot 9 \cdot 10) = (7!)(720) = (7!)(6!)$
b. $10! = (7!)(6!) = (7!)(5!) \cdot 6 = (7!)(5!)(3!)$
c. $16! = (14!)(15 \cdot 16) = (14!)(240) = (14!)(5!)(2!)$
d. $9! = (7!)(8 \cdot 9) = (7!)(6 \cdot 6 \cdot 2) = (7!)(3!)(3!)(2!)$

23. $x = y = 1, z = 2$

Section 1.3

1. For $n = 1$ we have $1 < 2^1 = 2$. Now assume $n < 2^n$. Then $n + 1 < 2^n + 1 < 2^n + 2^n = 2^{n+1}$.

3. For the basis step, $\sum_{k=1}^{1} 1/k^2 = 1 \leq 2 - \frac{1}{1}$. For the inductive step, we assume that $\sum_{k=1}^{n} 1/k^2 \leq 2 - 1/n$. Then $\sum_{k=1}^{n+1} 1/k^2 = \sum_{k=1}^{n} 1/k^2 + 1/(n+1)^2 \leq 2 - 1/n + 1/(n+1)^2 = 2 - ((n+1)^2 - n)/(n(n+1)^2) = 2 - (n^2 + n + 1)/(n(n+1)^2) \leq 2 - (n^2 + n)/(n(n+1)^2) = 2 - 1/(n+1)$, as desired.

5. $\mathbf{A}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. The basis step is trivial. For the inductive step, assume that $\mathbf{A}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$. Then $\mathbf{A}^{n+1} = \mathbf{A}^n\mathbf{A} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$.

7. For the basis step, $\sum_{j=1}^{1} j^2 = 1 = 1(1+1)(2 \cdot 1 + 1)/6$. For the inductive step, we assume that $\sum_{j=1}^{n} j^2 = n(n+1)(2n+1)/6$. Then $\sum_{j=1}^{n+1} j^2 = \sum_{j=1}^{n} j^2 + (n+1)^2 = n(n+1)(2n+1)/6 + (n+1)^2 = (n+1)((n+1)+1)(2(n+1)+1)/6$.

9. For the basis step, $\sum_{j=1}^{1} j(j+1) = 2 = 1 \cdot 2 \cdot 3/3$. Assume it is true for n. Then $\sum_{j=1}^{n+1} j(j+1) = n(n+1)(n+2)/3 + (n+1)(n+2) = (n+1)(n+2)(n/3+1) = (n+1)(n+2)(n+3)/3$.

11. $2^{n(n+1)/2}$

13. Proof using mathematical induction. We see that $12 = 4 \cdot 3$. Now assume that postage of n cents can be formed, with $n = 4a + 5b$, where a and b are nonnegative integers. To form $n + 1$ cents postage, if $a > 0$ we can replace a 4-cent stamp with a 5-cent stamp; that is, $n + 1 = 4(a - 1) + 5(b + 1)$. If no 4-cent stamps are present, then all 5-cent stamps were used. It follows that there must be at least three 5-cent stamps and these can be replaced by four 4-cent stamps; that is, $n + 1 = 4(a + 4) + 5(b - 3)$.

15. We use mathematical induction. The inequality is true for $n = 0$ since $H_{2^0} = H_1 = 1 \geq 1 = 1 + 0/2$. Now assume that the inequality is true for n, that is, $H_{2^n} \geq 1 + n/2$. Then $H_{2^{n+1}} = \sum_{j=1}^{2^n} 1/j + \sum_{j=2^n+1}^{2^{n+1}} 1/j \geq H_{2^n} + \sum_{j=2^n+1}^{2^{n+1}} 1/2^{n+1} \geq 1 + n/2 + 2^n/2^{n+1} = 1 + n/2 + 1/2 = 1 + (n+1)/2$.

17. For the basis step, $(2 \cdot 1)! = 2 < 2^{2 \cdot 1}(1!)^2 = 4$. For the inductive step, we assume that $(2n)! < 2^{2n}(n!)^2$. Then $(2(n+1))! = (2n)!(2n+1)(2n+2) < 2^{2n}(n!)^2(2n+1)(2n+2) < 2^{2n}(n!)^2(2n+2)^2 = 2^{2(n+1)}((n+1)!)^2$.

19. Let A be such a set. Let $B = \{x - k + 1 \mid x \in A \text{ and } x \geq k\}$, which is clearly a set of positive integers. Since $k \in A$ and $k \geq k$, we know that $k - k + 1 = 1$ is in B. Since $n + 1$ is in A whenever n is, $n + 1 - k + 1$ is in B whenever $n - k + 1$ is. Thus B satisfies the hypothesis for mathematical induction, i.e., B is the set of positive integers. Mapping B back to A in the natural manner, we find that A contains the set of integers greater than or equal to k.

21. For the basis step, $4^2 = 16 < 24 = 4!$. For the inductive step, we assume that $n^2 < n!$. Then $(n+1)^2 = n^2 + 2n + 1 < n! + 2n + 1 < n \cdot n! + n! = (n+1)n! = (n+1)!$

23. We use the second principle of mathematical induction to prove that $n - 1$ moves are necessary and sufficient to assemble a puzzle with n pieces. For the basis step ($n = 1$), if the puzzle has only one piece, then it clearly may be assembled with no moves. For the inductive step, assume that a puzzle of k pieces takes $k - 1$ moves, for all $k \leq n$. To assemble a puzzle of $n + 1$ pieces, first assemble n pieces, using $n - 1$ moves. This leaves two blocks—the assembled n pieces and the last piece. Now make the move consisting of putting these two blocks together. Thus assembling a puzzle of $n + 1$ pieces can be done in $n = (n + 1) - 1$ moves. To see that it cannot be done

in fewer moves, look at the situation just before making any last move, where there are two blocks, say of sizes i and $n+1-i$. By the inductive hypothesis, it required $i-1$ moves to put together the first block and $n+1-i-1=n-i$ moves to put together the second block. Thus $i-1+n-i=n-1$ moves have been required thus far. These, together with the final move, account for n moves, as desired.

25. Suppose that $f(n)$ is defined recursively by specifying the value of $f(1)$ and a rule for finding $f(n+1)$ from $f(n)$. We will prove by mathematical induction that such a function is well-defined. First note that $f(1)$ is well-defined since this value is explicitly stated. Now assume that $f(n)$ is well-defined. Then $f(n+1)$ also is well-defined since a rule is given for determining this value from $f(n)$.

27. 65,536

29. We use the second principle of mathematical induction. The basis step consists of verifying the formula for $n=1$ and $n=2$. For $n=1$ we have $f(1)=1=2^1+(-1)^1$, and for $n=2$ we have $f(2)=5=2^2+(-1)^2$. Now assume that $f(k)=2^k+(-1)^k$ for all positive integers k with $k<n$, where $n>2$. By the inductive hypothesis, $f(n)=f(n-1)+2f(n-2)=(2^{n-1}+(-1)^{n-1})+2(2^{n-2}+(-1)^{n-2})=(2^{n-1}+2^{n-1})+(-1)^{n-2}(-1+2)=2^n+(-1)^n$.

31. We use the second principle of mathematical induction. We see that $a_0=1\le 3^0=1$, $a_1=3\le 3^1=3$, and $a_2=9\le 3^2=9$. These are the basis cases. Now assume that $a_k\le 3^k$ for all integers k with $0\le k<n$. It follows that $a_n=a_{n-1}+a_{n-2}+a_{n-3}\le 3^{n-1}+3^{n-2}+3^{n-3}=3^{n-3}(1+3+9)=13\cdot 3^{n-3}<27\cdot 3^{n-3}=3^n$.

33. Let P_n be the statement for n. Then P_2 is true, since we have $((a_1+a_2)/2)^2-a_1a_2=((a_1-a_2)/2)^2\ge 0$. Assume that P_n is true. Then by P_2, for $2n$ positive real numbers $a_1,\ldots,a_{2n}$ we have $a_1+\cdots+a_{2n}\ge 2(\sqrt{a_1a_2}+\sqrt{a_3a_4}+\cdots+\sqrt{a_{2n-1}a_{2n}})$. Apply P_n to this last expression to get $a_1+\cdots+a_{2n}\ge 2n(a_1a_2\cdots a_{2n})^{1/(2n)}$. This establishes P_n for $n=2^k$ for all k. Again, assume P_n is true. Let $g=(a_1a_2\cdots a_{n-1})^{1/(n-1)}$. Applying P_n, we have $a_1+a_2+\cdots+a_{n-1}+g\ge n(a_1a_2\cdots a_{n-1}g)^{1/n}=n(g^{n-1}g)^{1/n}=ng$. Therefore $a_1+a_2+\cdots+a_{n-1}\ge(n-1)g$, which establishes P_{n-1}. Thus P_n implies P_{n-1}. Putting these two pieces together establishes P_n for all n.

35. We follow the hint. The basis step follows immediately because the algorithm stops after 1 step when applied to a fraction of the form $1/q$. To carry out the induction step, assume that the algorithm terminates for all fractions with numerator less than p. Given a fraction p/q, apply the algorithm and find the unit fraction $1/s$ such that $1/(s-1)>p/q>1/s$. When we subtract $1/s$ from p/q, the remainder is $p/q-1/s=(ps-q)/qs$. On the other hand, when we multiply the inequality $1/(s-1)>p/q>1/s$ by $q(s-1)$, we see that $q>p(s-1)$. This implies that $p>ps-q$, showing that the numerator of $(ps-q)/q$ is less than the numerator of the fraction p/q. Applying the induction hypothesis finishes the proof.

Section 1.4

1. **a.** 55 **b.** 233 **c.** 610 **d.** 2584 **e.** 6765 **f.** 75,025

3. Note that $2f_{n+2}-f_n=f_{n+2}+(f_{n+2}-f_n)=f_{n+2}+f_{n+1}=f_{n+3}$. Add f_n to both sides.

5. For the basis step (when $n=1$ and $n=2$), note that $f_2=f_1^2+2f_0f_1$ because $1=1^2+2\cdot 0\cdot 1$ and $f_4=f_2^2+2f_1f_2$ because $3=1^2+2\cdot 1\cdot 1$. For the induction step, assume that $f_{2k}=f_k^2+2f_{k-1}f_k$ for $k=1,2,\ldots,n$, where $n\ge 3$. Using the induction hypothesis, we have $f_{2n-4}=f_{n-2}^2+2f_{n-3}f_{n-2}$ and $f_{2n-2}=f_{n-1}^2+2f_{n-2}f_{n-1}$. We have $f_{2n}=f_{2n-1}+f_{2n-2}=2f_{2n-2}+f_{2n-3}=3f_{2n-2}-f_{2n-4}$ because $f_{2n-1}=f_{2n-2}+f_{2n-3}$ and $f_{2n-2}=f_{2n-3}+f_{2n-4}$. Using the inductive hypothesis, this last expression equals $3f_{n-1}^2+6f_{n-2}f_{n-1}-f_{n-2}^2-$

$2f_{n-3}f_{n-2} = 3f_{n-1}^2 + 6(f_n - f_{n-1})f_{n-1} - (f_n - f_{n-1})^2 - 2(f_{n-1} - f_{n-2})(f_n - f_{n-1}) = -2f_{n-1}^2 + 6f_nf_{n-1} - f_n^2 + 2f_n(f_n - f_{n-1}) - 2f_{n-1}(f_n - f_{n-1}) = f_n^2 + 2f_{n-1}f_n$, which completes the induction step.

7. $\sum_{j=1}^{n} f_{2j-1} = f_{2n}$. Basis case $n = 1$ is trivial. Now assume that $\sum_{j=1}^{n} f_{2j-1} = f_{2n}$. Using this inductive hypothesis, we have $\sum_{j=1}^{n+1} f_{2j-1} = (\sum_{j=1}^{n} f_{2j-1}) + f_{2n+1} = f_{2n} + f_{2n+1} = f_{2n+2}$.

9. The sum is $f_{n-1} - (-1)^n$. To see this in the case that $n = 2k$ is even, note that the sum is $(f_2 + f_4 + \cdots + f_{2k}) - (f_1 + f_3 + \cdots + f_{2k-1})$, which equals $(f_{2k+1} - 1) - f_{2k} = f_{2k-1} - 1 = f_{n-1} - 1 = f_{n-1} - (-1)^n$ by Exercises 8 and 9. Similarly, when $n = 2k + 1$ is odd, we have $(f_1 + f_3 + \cdots + f_{2k+1}) - (f_2 + f_4 + \cdots + f_{2k}) = f_{2k+2} - (f_{2k+1} - 1) = f_{2k} + 1 = f_{n-1} + 1 = f_{n-1} - (-1)^n$.

11. By Exercise 5, we have $f_{2n} = f_n^2 + 2f_{n-1}f_n = f_n(f_n + f_{n-1} + f_{n-1}) = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) = f_{n+1}^2 - f_{n-1}^2$.

13. We use mathematical induction. To complete the basis step, note that $\sum_{j=1}^{1} f_j^2 = f_1f_2$ because the left-hand side is $f_1^2 = 1^2 = 1$ and the right-hand side is $f_1f_2 = 1 \cdot 1 = 1$. For the induction step, assume that $\sum_{j=1}^{n} f_j^2 = f_nf_{n+1}$. It follows that $\sum_{j=1}^{n+1} f_j^2 = \sum_{j=1}^{n} f_j^2 + f_{n+1}^2 = f_nf_{n+1} + f_{n+1}^2 = f_{n+1}(f_n + f_{n+1}) = f_{n+1}f_{n+2}$, completing the proof.

15. We use mathematical induction and the recursive definition $f_n = f_{n-1} + f_{n-2}$, with $f_0 = 0$ and $f_1 = 1$. For $n = 1$, we have $f_2f_0 - f_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1$. Hence, the basis step holds. Now assume that $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$. Then $f_{n+2}f_n - f_{n+1}^2 = (f_{n+1} + f_n)f_n - f_{n+1}(f_n + f_{n-1}) = f_n^2 - f_{n+1}f_{n-1} = -(-1)^n = (-1)^{n+1}$.

17. For fixed m, we proceed by induction on n. For the basis step, note that when $n = 1$, the identity holds because $f_{m+1} = f_mf_2 + f_1f_{m-1} = f_m + f_{m-1}$. When $n = 2$, the identity holds because $f_{m+2} = f_mf_3 + f_2f_{m-1} = 2f_m + f_{m-1} = f_m + (f_m + f_{m-1}) = f_m + f_{m+1}$. For the induction step, assume that the identity holds for $1, 2, \ldots, k$, where $k \geq 3$. Then $f_{m+k} = f_mf_{k+1} + f_{m-1}f_k$ and $f_{m+k-1} = f_mf_k + f_{m-1}f_{k-1}$. Adding these equations gives us $f_{m+k} + f_{m+k-1} = f_m(f_{k+1} + f_k) + f_{m-1}(f_k + f_{k-1})$. This simplifies to $f_{m+k+1} = f_mf_{k+2} + f_{m-1}f_{k+1}$.

19. $\sum_{i=1}^{n} L_i = L_{n+2} - 3$. We prove this by induction. The basis step is $L_1 = 1 = L_3 - 3$. Assume that the formula holds for n and compute $\sum_{i=1}^{n+1} L_i = \sum_{i=1}^{n} L_i + L_{n+1} = L_{n+2} - 3 + L_{n+1} = L_{n+3} - 3$.

21. $\sum_{i=1}^{n} L_{2i} = L_{2n+1} - 1$. We prove this by induction. The basis step is $L_2 = 3 = L_3 - 1$. Assume that the formula holds for n and compute $\sum_{i=1}^{n+1} L_{2i} = \sum_{i=1}^{n} L_{2i} + L_{2n+2} = L_{2n+1} - 1 + L_{2n+2} = L_{2n+3} - 1$.

23. We proceed by induction. The basis step is $L_1^2 = 1 = L_1L_2 - 2$. Assume that the formula holds for n. Then $\sum_{i=1}^{n+1} L_i^2 = \sum_{i=1}^{n} L_i^2 + L_{n+1}^2 = L_nL_{n+1} - 2 + L_{n+1}^2 = L_{n+1}(L_n + L_{n+1}) - 2 = L_{n+1}L_{n+2} - 2$.

25. For the basis step we check that $L_1f_1 = 1 = f_2$ and $L_2f_2 = 3 = f_4$. Assume that the identity is true for all positive integers up to n. Then $f_{n+1}L_{n+1} = (f_{n+2} - f_n)(f_{n+2} - f_n)$ from Exercise 24. This equals $f_{n+2}^2 - f_n^2 = (f_{n+1} + f_n)^2 - (f_{n-1} + f_{n-2})^2 = f_{n+1}^2 + 2f_{n+1}f_n + f_n^2 - f_{n-1}^2 - 2f_{n-1}f_{n-2} - f_{n-2}^2 = (f_{n+1}^2 - f_{n-1}^2) + (f_n^2 - f_{n-2}^2) + 2(f_{n+1}f_n - f_{n-1}f_{n-2}) = (f_{n+1} - f_{n-1})(f_{n+1} + f_{n-1}) + (f_n - f_{n-2})(f_n + f_{n-2}) + 2f_{2n-1}$, where the last term is obtained from Exercise 16. This equals $f_nL_n + f_{n-1}L_{n-1} + 2f_{2n-1}$. Applying the induction hypothesis yields $f_{2n} + f_{2n-2} + 2f_{2n-1} = (f_{2n} + f_{2n-1}) + (f_{2n-1} + f_{2n-2}) = f_{2n+1} + f_{2n} = f_{2n+2}$, which completes the induction.

27. We prove this by induction on n. If $n = 2$, use induction on m to establish the basis step for n. For the induction step on n, note that $L_{m+n+1} = L_{m+n} + L_{m+n-1} = (f_{m+1}L_n + f_mL_{n-1}) + (f_{m+1}L_{n-1} + f_mL_{n-2}) = f_{m+1}(L_n + L_{n-1}) + f_m(L_{n-1} + L_{n-2}) = f_{m+1}L_{n+1} + f_mL_n$.

29. $50 = f_9 + f_7 + f_4$, $85 = f_{10} + f_8 + f_6 + f_2$, $110 = f_{11} + f_8$, $200 = f_{12} + f_{10} + f_2$

31. We proceed by mathematical induction. The basis steps ($n = 2, 3$) are easily seen to hold. For the inductive step, we assume that $f_n \le \alpha^{n-1}$ and $f_{n-1} \le \alpha^{n-2}$. Now $f_{n+1} = f_n + f_{n-1} \le \alpha^{n-1} + \alpha^{n-2} = \alpha^n$, since α satisfies $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$.

33. We use Theorem 1.3. Note that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$, since α and β are the roots of $x^2 - x - 1 = 0$. Then $f_{2n} = (\alpha^{2n} - \beta^{2n})/\sqrt{5} = (1/\sqrt{5})((\alpha + 1)^n - (\beta + 1)^n) = (1/\sqrt{5})\left(\sum_{j=0}^{n}\binom{n}{j}\alpha^j - \sum_{j=0}^{n}\binom{n}{j}\beta^j\right) = (1/\sqrt{5})\sum_{j=0}^{n}\binom{n}{j}(\alpha^j - \beta^j) = \sum_{j=1}^{n}\binom{n}{j}f_j$ since the first term is 0 in the second-to-last sum.

35. We have $\det(\mathbf{F}^n) = \det(\mathbf{F})^n = (-1)^n$ and $\det\begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix} = f_{n+1}f_{n-1} - f_n^2$.

37. $f_n = f_{n+2} - f_{n+1}$; $f_{-1} = 1$, $f_{-2} = -1$, $f_{-3} = 2$, $f_{-4} = -3$, $f_{-5} = 5$, $f_{-6} = -8$, $f_{-7} = 13$, $f_{-8} = -21$, $f_{-9} = 34$, $f_{-10} = -55$

39. The square has area 64 square units, while the rectangle has area 65 square units. This corresponds to the identity in Exercise 14, which tells us that $f_7f_5 - f_6^2 = 1$. Notice that the slope of the hypotenuse of the triangular piece is $\frac{3}{8}$, while the slope of the top of the trapezoidal piece is $\frac{2}{5}$. We have $\frac{2}{5} - \frac{3}{8} = \frac{1}{40}$. Thus the "diagonal" of the rectangle is really a very skinny parallelogram of area 1, hidden visually by the fact that the two slopes are nearly equal.

41. We solve the equation $r^2 - r - 1 = 0$ to discover the roots $r_1 = (1 + \sqrt{5})/2$ and $r_2 = (1 - \sqrt{5})/2$. Then according to the theory in the preamble, $f_n = C_1r_1^n + C_2r_2^n$. For $n = 0$ we have $0 = C_1r_1^0 + C_2r_2^0 = C_1 + C_2$, and for $n = 1$ we have $1 = C_1r_1 + C_2r_2 = C_1(1 + \sqrt{5})/2 + C_2(1 - \sqrt{5})/2$. Solving these two equations simultaneously yields $C_1 = 1/\sqrt{5}$ and $C_2 = -1/\sqrt{5}$. So the explicit formula is $f_n = (1/\sqrt{5})r_1^n - (1/\sqrt{5})r_2^n = (r_1^n - r_2^n)/\sqrt{5}$.

43. We seek to solve the recurrence relation $L_n = L_{n-1} + L_{n-1}$ subject to the initial conditions $L_1 = 1$ and $L_2 = 3$. We solve the equation $r^2 - r - 1 = 0$ to discover the roots $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Then according to the theory in the preamble to Exercise 41, $L_n = C_1\alpha^n + C_2\beta^n$. For $n = 1$ we have $L_1 = 1 = C_1\alpha + C_2\beta$, and for $n = 2$ we have $3 = C_1\alpha^2 + C_2\beta^2$. Solving these two equations simultaneously yields $C_1 = 1$ and $C_2 = 1$. So the explicit formula is $L_n = \alpha^n + \beta^n$.

45. First check that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. We proceed by induction. The basis steps are $(\alpha - \beta)/\sqrt{5} = \sqrt{5}/\sqrt{5} = 1 = f_1$ and $(\alpha^2 - \beta^2)/\sqrt{5} = ((1 + \alpha) - (1 + \beta))/\sqrt{5} = (\alpha - \beta)/\sqrt{5} = 1 = f_2$. Assume that the identity is true for all positive integers up to n. Then $f_{n+1} = f_n + f_{n-1} = (\alpha^n - \beta^n)/\sqrt{5} + (\alpha^{n-1} - \beta^{n-1})/\sqrt{5} = (\alpha^{n-1}(\alpha + 1) - \beta^{n-1}(\beta + 1))/\sqrt{5} = (\alpha^{n-1}(\alpha^2) - \beta^{n-1}(\beta^2))/\sqrt{5} = (\alpha^{n+1} - \beta^{n+1})/\sqrt{5}$, which completes the induction.

Section 1.5

1. $3 \mid 99$ since $99 = 3 \cdot 33$; $5 \mid 145$ since $145 = 5 \cdot 29$; $7 \mid 343$ since $343 = 7 \cdot 49$; $888 \mid 0$ since $0 = 888 \cdot 0$

3. **a.** yes **b.** yes **c.** no **d.** no **e.** no **f.** no

5. **a.** $q = 5$, $r = 15$ **b.** $q = 17$, $r = 0$ **c.** $q = -3$, $r = 7$ **d.** $q = -6$, $r = 2$

7. By the hypothesis, $b = ra$ and $d = sc$ for some r and s. Thus $bd = rs(ac)$, so $ac \mid bd$.

9. If $a \mid b$, then $b = na$ and $bc = n(ca)$, i.e., $ac \mid bc$. Now suppose that $ac \mid bc$. Then $bc = nac$, and, as $c \neq 0$, $b = na$, i.e., $a \mid b$.

11. The statement is trivially true for $k = 1$. Assume therefore that $a \mid b$ and $a^k \mid b^k$; we want to show that $a^{k+1} \mid b^{k+1}$. But this follows directly from Exercise 7.

13. Let $a = 2x + 1$ and $b = 2y + 1$ be odd, and $c = 2z$ even. Then $ab = (2x + 1)(2y + 1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1$, so ab is odd. On the other hand, if w is any integer, then $cw = (2z)w = 2(zw)$ is even.

15. By the division algorithm $a = bq + r$ with $0 \le r < b$. Thus $-a = -bq - r = -(q + 1)b + b - r$. If $0 \le b - r < b$, then we are done. Otherwise, $b - r = b$, or $r = 0$ and $-a = -qb + 0$.

17. **a.** Note that if $a = bq + r$, then $a = (-b)(-q) + r$. Therefore, to divide by a negative number, just divide by the corresponding positive number and take the negative of the quotient. The remainder stays the same.
b. 3

19. By the division algorithm, let $m = qn + r$, with $0 \le r \le n - 1$ and $q = [m/n]$. Then $[(m + 1)/n] = [(qn + r + 1)/n] = [q + (r + 1)/n] = q + [(r + 1)/n]$. If $r = 0, 1, 2, \ldots, n - 2$, then $m \ne kn - 1$ for any integer k and $1/n \le (r + 1)/n < 1$, and so $[(r + 1)/n] = 0$. In this case, we have $[(m + 1)/n] = q + 0 = [m/n]$. On the other hand, if $r = n - 1$, then $m = qn + n - 1 = n(q + 1) - 1 = nk - 1$, and $[(r + 1)/n] = 1$. In this case, we have $[(m + 1)/n] = q + 1 = [m/n] + 1$.

21. The positive integers divisible by the positive integer d are those integers of the form kd, where k is a positive integer. The number of these that are less than x is the number of positive integers k with $kd \le x$, or equivalently with $k \le x/d$. There are $[x/d]$ such integers.

23. 128, 18

25. 457

27. It costs $11 - 22[-x]$ cents to mail a letter weighing x ounces. It cannot cost \$1.45; a 10-ounce letter costs \$2.31.

29. Multiplying two integers of this form gives us $(4n + 1)(4m + 1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1$. Similarly, $(4n + 3)(4m + 3) = 16mn + 12m + 12n + 9 = 4(4mn + 3m + 3n + 2) + 1$.

31. Every odd integer can be written in the form $4k + 1$ or $4k + 3$. Observe that $(4k + 1)^4 = 16^2k^4 + 4(4k)^3 + 6(4k)^2 + 4(4k) + 1 = 16(16k^4 + 16k^3 + 6k^2 + k) + 1$. Proceeding further, $(4k + 3)^4 = (4k)^4 + 12(4k)^3 + 54(4k)^2 + 108(4k) + 3^4 = 16(16k^4 + 48k^3 + 54k^2 + 27k + 5) + 1$.

33. Of any three consecutive integers, one is a multiple of 3. Also, at least one is even. Therefore, the product is a multiple of $2 \cdot 3 = 6$.

35. The basis case is true: $1^3 + 2^3 + 3^3 = 36$ is divisible by 9. Assume the inductive hypothesis that $n^3 + (n + 1)^3 + (n + 2)^3$ is divisible by 9. Then $(n + 1)^3 + (n + 2)^3 + (n + 3)^3 = (n^3 + (n + 1)^3 + (n + 2)^3) + ((n + 3)^3 - n^3) = (n^3 + (n + 1)^3 + (n + 2)^3) + (9n^2 + 27n + 27)$. In this last expression, the first summand is divisible by 9 by the inductive hypothesis, and the second is clearly divisible by 9, so we are done.

37. We proceed by mathematical induction. The basis step is clear. Assume that $3 \mid f_i$ if and only if $4 \mid i$, for all $i \le 4k$. Since $f_{4k+1} = f_{4k} + f_{4k-1}$, knowing that $3 \mid f_{4k}$ and $3 \nmid f_{4k-1}$ tells us that $3 \nmid f_{4k+1}$. Similarly, $3 \mid f_{4k}$ and $3 \nmid f_{4k+1}$ imply $3 \nmid f_{4k+2}$. Also $f_{4k+3} = 2f_{4k+1} + f_{4k}$, and since $3 \mid f_{4k}$ but $3 \nmid 2f_{4k+1}$, we have $3 \nmid f_{4k+3}$. Finally, as $f_{4k+4} = 3f_{4k+1} + 2f_{4k}$ and $3 \mid 2f_{4k}$ and $3 \mid 3f_{4k+1}$, we see that $3 \mid f_{4k+4}$. This has taken us up to the next value of k, as required.

39. The basis cases ($n = 6$ and $n = 7$) state that $f_6 = 5f_2 + 3f_1$ and $f_7 = 5f_3 + 3f_2$, which are true, since $8 = 5 + 3$ and $13 = 5 \cdot 2 + 3 \cdot 1$. Assume the inductive hypothesis (second principle). Then $f_{n+1} = f_n + f_{n-1} = 5f_{n-4} + 3f_{n-5} + 5f_{n-5} + 3f_{n-6} = 5(f_{n-4} + f_{n-5}) + 3(f_{n-5} + f_{n-6}) =$

$5f_{n-3} + 3f_{n-4}$, as desired. For the second statement, the basis case is the true statement that $f_5 = 5$ is divisible by 5. Assuming the inductive hypothesis that f_n is divisible by 5, we see that f_{n+5} ($n + 5$ being the next multiple of 5 after n) is the sum of two multiples of 5, namely $5f_{n+1}$ and $3f_n$.

41. 39, 59, 89, 134, 67, 101, 152, 76, 38, 19, 29, 44, 22, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1

43. We prove this using the second principle of mathematical induction. Since $T(2) = 1$, the Collatz conjecture is true for $n = 2$. Now assume that the conjecture holds for all integers less than n. By assumption, there is an integer k such that k iterations of the transformation T, starting at n, produces an integer m less than n. By the inductive hypothesis, there is an integer l such that iterating T l times starting at m produces the integer 1. Hence, iterating T $k + l$ times starting with n leads to 1.

45. We first show that $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n$ is an even integer. From the binomial theorem it follows that $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n = \sum_{j=0}^{n} \binom{n}{j} 2^{n-j}\sqrt{3}^j + \sum_{j=0}^{n} \binom{n}{j} 2^{n-j}(-1)^j\sqrt{3}^j = 2(2^n + 3\binom{n}{2}2^{n-2} + 3^2\binom{n}{4}2^{n-4} + \cdots) = 2l$, where l is an integer. Next, note that $(2 - \sqrt{3})^n < 1$. We see that $[(2 + \sqrt{3})^n] = (2 + \sqrt{3})^n + (2 - \sqrt{3})^n - 1$. It follows that $[(2 + \sqrt{3})^2]$ is odd.

Section 2.1

1. $(5554)_7$, $(2112)_{10}$

3. $(175)_{10}$, $(1111100111)_2$

5. $(8F5)_{16}$, $(74E)_{16}$

7. The reason is that we are using the blocks of three digits as one "digit," which has 1000 possible values

9. $-39, 26$

11. If m is any integer weight less than 2^k, then by Theorem 2.1, m has a base 2 expansion $m = a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_1 2^1 + a_0 2^0$, where each a_i is 0 or 1. The 2^i weight is used if and only if $a_i = 1$.

13. Let w be the weight to be measured. By Exercise 12, w has a unique balanced ternary expansion. Place the object in pan 1. If $e_i = 1$, then place a weight of 3^i in pan 2. If $e_i = -1$, then place a weight of 3^i in pan 1. If $e_i = 0$, then do not use the weight of 3^i. Now the pans will be balanced.

15. To convert a number from base r to base r^n, take the number in blocks of size n. To go the other way, convert each digit of a base r^n number to base r, and concatenate the results.

17. $(a_k a_{k-1} \ldots a_1 a_0 00 \ldots 00)_b$, where we have placed m zeros at the end of the base b expansion of n

19. **a.** -6 **b.** 13 **c.** -14 **d.** 0

21. If m is positive, then $a_{n-1} = 0$ and $a_{n-2}a_{n-3} \ldots a_0$ is the binary expansion of m. Hence, $m = \sum_{i=0}^{n-2} a_i 2^i$ as desired. If m is negative, then the one's complement expansion for m has its leading bit equal to 1. By the definition of one's complement, we can think of obtaining the remaining $n - 1$ bits by subtracting $-m$, written in binary, from $111 \ldots 1$ (with $n - 1$ 1s), since subtracting a bit from 1 is the same thing as complementing it. Equivalently, if we view the bit string $(a_{n-2}a_{n-1} \ldots a_0)$ as a binary number, then it represents $(2^{n-1} - 1) - (-m)$. In symbols, this says that $(2^{n-1} - 1) - (-m) = \sum_{i=0}^{n-2} a_i 2^i$. Solving for m gives us the equation we are trying to prove (since $a_{n-1} = 1$).

23. **a.** -7 **b.** 13 **c.** -15 **d.** -1

25. Complement each of the digits in the two's complement representation for m and then add 1.

27. $4n$

29. We first show that every positive integer has a Cantor expansion. To find a Cantor expansion of the positive integer n, let m be the unique positive integer such that $m! \leq n < (m+1)!$. By the division algorithm, there is an integer a_m such that $n = m! \cdot a_m + r_m$, where $0 \leq a_m \leq m$ and $0 \leq r_m < m!$. We iterate, finding that $r_m = (m-1)! \cdot a_{m-1} + r_{m-1}$, where $0 \leq a_{m-1} \leq m-1$ and $0 \leq r_{m-1} < (m-1)!$. We iterate $m-2$ more times, obtaining $r_i = (i-1)! \cdot a_{i-1} + r_{i-1}$, where $0 \leq a_{i-1} \leq i-1$ and $0 \leq r_{i-1} < (i-1)!$ for $i = m+1, m, m-1, \ldots, 2$, with $r_{m+1} = n$. At the last stage, we have $r_2 = 1! \cdot a_1 + 0$, where $r_2 = 0$ or 1 and $r_2 = a_1$.

31. Call a position *good* if the number of ones in each column is even, and *bad* otherwise. Since a player can affect only one row, he or she must change some column sums. Thus any move from a good position produces a bad position. To find a move from a bad position to a good one, construct a binary number by putting a 1 in the place of each column with odd sum, and a 0 in the place of each column with even sum. Subtracting this number of matches from the largest pile will produce a good position.

33. **a.** First show that the result of the operation must yield a multiple of 9. Then it suffices to check only multiples of 9 with decreasing digits. There are only 79 of these. If we perform the operation on each of these 79 numbers and reorder the digits, we will have one of the following 23 numbers: 7551, 9954, 5553, 9990, 9981, 8820, 9810, 9620, 8532, 8550, 9720, 9972, 7731, 6543, 8730, 8640, 8721, 7443, 9963, 7632, 6552, 6642, or 6174. It will suffice to check only 9810, 7551, 9990, 8550, 9720, 8640, and 7632.

b. 8

35. Consider $a_0 = (1234)_6$. We find that T_6 repeats with period 6. Therefore it never goes to a Kaprekar's constant for the base 6. Hence there is no Kaprekar's constant for the base 6.

Section 2.2

1. $(10010110110)_2$

3. $(1011101100)_2$

5. $(10110001101)_2$

7. $q = (11111)_2, r = (1100)_2$

9. $(3314430)_5$

11. $(4320023)_5$

13. $(16665)_{16}$

15. $(B705736)_{16}$

17. Represent $(18235187)_{10}$ using three words, $((018)(235)(187))_{1000}$, and $(22135674)_{10}$ using three words, $((022)(135)(674))_{1000}$, where each base 1000 digit is represented by three base 10 digits in parentheses. To find the sum, difference, and product of these integers from their base 1000 representations we carry out the algorithms for such computations for base 1000.

19. We must assume that the sum actually represents a number in the appropriate range. Assume that n bits are being used, so that numbers strictly between -2^{n-1} and 2^{n-1} can be represented. The answer is almost, but not quite, that to obtain the one's complement representation of the sum of two numbers, we simply add the two strings representing these numbers using the usual grade-school right-to-left algorithm, as in Example 2.4. Instead, after performing this operation, there may be a carry out of the left-most column; in such a case, we then add 1 more to the answer.

21. Let $a = (a_m a_{m-1} \ldots a_2 a_1)_!$ and $b = (b_m b_{m-1} \ldots b_2 b_1)_!$. Then $a + b = (d_{m+1} d_m d_{m-1} \ldots d_2 d_1)_!$ is obtained by adding the digits from right to left with the following rule for producing carries.

If $a_j + b_j + c_{j-1}$, where c_{j-1} is the carry from adding a_{j-1} and b_{j-1}, is greater than j, then $c_j = 1$, and the resulting jth digit is $d_j = a_j + b_j + c_{j-1} - j - 1$. Otherwise, the resulting digit is $d_j = a_j + b_j + c_{j-1}$, and $c_j = 0$. To subtract b from a, assuming $a > b$, we let $d_j = a_j - b_j + c_{j-1}$ and set $c_j = 0$ if $a_j - b_j + c_{j-1}$ is between 0 and j (inclusive). Otherwise, $d_j = a_j - b_j + c_{j-1} + j + 1$ and $c_j = -1$. In this manner, $a - b = (d_m d_{m-1} \ldots d_2 d_1)_1$.

23. We have $(a_n \ldots a_1 5)_{10}^2 = (10(a_n \ldots a_1)_{10} + 5)^2 = 100(a_n \ldots a_1)_{10}^2 + 100(a_n \ldots a_1)_{10} + 25 = 100(a_n \ldots a_1)_{10} \cdot ((a_n \ldots a_1)_{10} + 1) + 25$. The decimal digits of this number consist of the decimal digits of $(a_n \ldots a_1)_{10} \cdot ((a_n \ldots a_1)_{10} + 1)$ followed by 25 since this first product is multiplied by 100, which shifts its decimal expansion two digits.

Section 2.3

1. **a.** yes **b.** no **c.** yes **d.** yes **e.** yes **f.** yes

3. First note that $(n^3 + 4n^2 \log n + 101n^2)$ is $O(n^3)$ and that $(14n \log n + 8n)$ is $O(n \log n)$ as in Example 2.11. Now applying Theorem 2.3 yields the result.

5. Use Exercise 4 and follow Example 2.9, noting that $(\log n)^3 \leq n^3$ whenever n is a positive integer.

7. What we want to show is equivalent to the statement that $\log(n^n)$ is at most a constant times $\log(n!)$, which in turn is equivalent to the statement that n^n is at most a constant power of $n!$ (because of the fact that $C \log A = \log(A^C)$). We will show that in fact $n^n \leq (n!)^2$ for all $n > 1$. To do this, let us write $(n!)^2$ as $(n \cdot 1) \cdot ((n-1) \cdot 2) \cdot ((n-2) \cdot 3) \cdots (2 \cdot (n-1)) \cdot (1 \cdot n)$. Now clearly each product pair $(i+1) \cdot (n-i)$ is at least as big as n (indeed, the ones near the middle are significantly bigger than n). Therefore, the entire product is at least as big as n^n, as desired.

9. Suppose that f is $O(g)$, where $f(n)$ and $g(n)$ are positive integers for every integer n. Then there is an integer C such that $f(n) < Cg(n)$ for all $x \in S$. Then $f^k(n) < C^k g^k(n)$ for all $x \in S$. Hence, f^k is $O(g^k)$.

11. The number of digits in the base b expansion of n is $1 + k$, where k is such that $b^k \leq n < b^{k+1}$, since there is a digit for each of the powers of $b^0, b^1, \ldots, b^k$. Note that this inequality is equivalent to $k \leq \log_b n < k + 1$, so $k = [\log_b n]$. Hence, there are $[\log_b n] + 1$ digits in the base b expansion of n.

13. To multiply an n-digit integer by an m-digit integer in the conventional manner, one must multiply every digit of the first number by every digit of the second number (with carries), to produce an array of about mn digits. Then we need to add these partial products, but this requires only about mn additions as we proceed column by column. In all, the number of operations is at most a constant multiple of mn, as desired.

15. **a.** $O((n \log n)^{1+\epsilon})$ for every $\epsilon > 0$
b. $O((n \log n)^{1+\epsilon})$ for every $\epsilon > 0$

17. $(1100011)_2$

19. **a.** $ab = (10^{2n} + 10^n)A_1B_1 + 10^n(A_1 - A_0)(B_0 - B_1) + (10^n + 1)A_0B_0$, where A_i and B_i are defined as in identity (2.2)
b. 6351 **c.** 11522328

21. That the given equation is an identity may be seen by direct calculation. The seven multiplications necessary to use this identity are $a_{11}b_{11}$, $a_{12}b_{21}$, $(a_{11} - a_{21} - a_{22})(b_{11} - b_{12} - b_{22})$, $(a_{21} + a_{22})(b_{12} - b_{11})$, $(a_{11} + a_{12} - a_{21} - a_{22})b_{22}$, $(a_{11} - a_{21})(b_{22} - b_{12})$, and $a_{22}(b_{11} - b_{21} - b_{12} + b_{22})$.

23. Let $k = [\log_2 n] + 1$. Then the number of multiplications for $2^k \times 2^k$ matrices is $O(7^k)$. But $7^k = 2^{(\log_2 7)([\log_2 n]+1)}$, which is $O(2^{\log_2 n \log_2 7} 2^{\log_2 7}) = O(n^{\log_2 7})$. The other bit operations are absorbed into this term.

Section 3.1

1. **a.** yes **b.** yes **c.** yes **d.** no **e.** yes **f.** no

3. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

5. none

7. If n is not prime, then let $n = kl$, where $1 < k < n$. From the hint (which follows from algebra) we see that $a^k - 1$ is a factor of $a^n - 1$. This means that $a^k - 1 = 1$, whence $a^k = 2$. But this is impossible. Therefore, n is prime. Clearly, $a \neq 1$. Note that n cannot equal 2 unless $a = 2$, since otherwise $a^n - 1$ factors nontrivially as the difference of two squares; so we can assume that n is an odd prime. But then $a^n - 1$ factors algebraically as $(a-1)(a^{n-1} + \cdots + a + 1)$, and this is nontrivial if $a > 2$. We conclude that $a = 2$.

9. We can show that there are infinitely many primes by showing that given an integer n, there is a prime p with $p > n$. We assume that $n \geq 3$. By Lemma 3.1, $S_n = n! - 1$ has a prime divisor p. If $p \leq n$ then $p \mid n!$, and so $p \mid n! - S_n = 1$, a contradiction. It follows that $p > n$.

11. 3, 7, 31, 211, 2311, 59

13. If n is prime, then we are done. Otherwise, $n/p < (\sqrt[3]{n})^2$. If n/p is prime, then we are done. Otherwise, by Theorem 3.2, n/p has a prime factor less than $\sqrt{n/p} < \sqrt[3]{n}$, a contradiction.

15. **a.** 7 **b.** 19 **c.** 71

17. If n is prime, then the statement is true for n. Otherwise, n is composite, so n is the product of two integers a and b such that $1 < a \leq b < n$. Since $n = ab$ and by the inductive hypothesis both a and b are the product of primes, we conclude that n is also the product of primes.

19. 53

21. For $n = 0, 1, 2, \ldots, 10$, the values of the function are 11, 13, 19, 29, 43, 61, 83, 109, 139, 173, 211, each of which is prime. But $2 \cdot 11^2 + 11 = 11(2 \cdot 11 + 1) = 11 \cdot 23$.

23. Assume not. Let x_0 be a positive integer. It follows that $f(x_0) = p$, where p is prime. Let k be an integer. We have $f(x_0 + kp) = a_n(x_0 + kp)^n + \cdots + a_1(x_0 + kp) + a_0$. Note that by the binomial theorem $(x_0 + kp)^j = \sum_{i=0}^{j} \binom{j}{i} x_0^{j-i} (kp)^i$. It follows that $f(x_0 + kp) = \sum_{j=0}^{n} a_j x_0^j + Np = f(x_0) + Np$, for some integer N. Since $p \mid f(x_0)$ it follows that $p \mid (f(x_0) + Np) = f(x_0 + kp)$. Since $f(x_0 + kp)$ is supposed to be prime, it follows that $f(x_0 + kp) = p$ for all integers k. This contradicts the fact that a polynomial of degree n takes on each value no more than n times. Hence, $f(y)$ is composite for at least one integer y.

25. At each stage of the procedure for generating the lucky numbers, the smallest number left, say k, is designated to be a lucky number and infinitely many numbers are left after the deletion of every kth integer left. It follows that there are infinitely many steps, and at each step a new lucky number is added to the sequence. Hence, there are infinitely many lucky numbers.

Section 3.2

1. 24, 25, 26, 27, 28

3. Suppose that p, $p + 2$, and $p + 4$ are all prime. We consider three cases. First, suppose that p is of the form $3k$. Then p cannot be prime unless $k = 1$, and then the prime triplet is 3, 5, 7. Next, suppose

that p is of the form $3k+1$. Then $p+2=3k+3=3(k+1)$ is not prime. We obtain no prime triplets in this case. Finally, suppose that p is of the form $3k+2$. Then $p+4=3k+6=3(k+2)$ is not prime. We obtain no prime triplet in this case either.

5. $(7, 11, 13)$, $(13, 17, 19)$, $(37, 41, 43)$, $(67, 71, 73)$.

7. **a.** 5 **b.** 7 **c.** 29 **d.** 53

9. 127, 149, 173, 197, 227, 257, 293, 331, 367, 401

11. **a.** $7=3+2+2$ **b.** $17=11+3+3$ **c.** $27=23+2+2$
d. $97=89+5+3$ **e.** $101=97+2+2$ **f.** $199=191+5+3$

13. Suppose that $n>5$ and that Goldbach's conjecture is true. Apply it to $n-2$ if n is even or to $n-3$ if n is odd. Conversely, suppose that every integer greater than 5 is the sum of three primes. Let $n>2$ be an even integer. Then $n+2$ is also even and the sum of three primes, not all odd.

15. Let $p<n$ be prime. Using the division algorithm, divide each of the first $p+1$ integers in the sequence by p to get $a=q_0p+r_0$, $a+k=q_1p+r_1, \ldots, a+pk=q_pp+r_p$, with $0\le r_i<p$ for each i. By the pigeonhole principle, at least two of the remainders are equal, say $r_i=r_j$. Subtract the corresponding equations to get $a+ik-a-jk=q_ip+r_i-q_jp-r_j$, which reduces to $(i-j)k=(q_i-q_j)p$. Therefore, $p\mid(i-j)k$, and because p is prime, it must divide one of the factors. But since $(i-j)<p$, we must have $p\mid k$.

17. The difference is 6, achieved with 5, 11, 17, 23.

19. The difference is 30, achieved with 7, 37, 67, 97, 127, 157.

21. If $p^\alpha-q^\beta=1$, with p and q primes, then p or q is even, so that p or q is 2. If $p=2$, there are several cases: we have $2^\alpha-q^\beta=1$. If α is even, say $\alpha=2k$, then $(2^{2k}-1)=(2^k-1)(2^k+1)=q^\beta$. So $q\mid(2^k-1)$ and $q\mid(2^k+1)$; hence $q=1$, a contradiction. If α is odd and β is odd, then $2^\alpha=1+q^\beta=(1+q)(q^{\beta-1}-q^{\beta-2}+\cdots\pm 1)$. Thus $1+q=2^n$ for some n. Then $2^\alpha=(2^n-1)^\beta+1=2^n\cdot$(odd number), since β is odd. So $2^{\alpha-n}$ is odd and therefore $\alpha=n$. Thus $2^\alpha=1+(2^\alpha-1)^\beta$, and so $\beta=1$, which is not allowed. If $\alpha=2k+1$ and $\beta=2n$, then $2^{2k+1}=1+q^{2n}$. Since q is odd, q^2 is of the form $4m+1$, and by the binomial theorem, so is q^{2n}. Thus the right-hand side of the last equation is of the form $4m+2$, but this forces $k=0$, a contradiction. If $q=2$, then $p^\alpha-2^\beta=1$, whence $2^\beta=(p-1)(p^{\alpha-1}+p^{\alpha-2}+\cdots+p+1)$, where the last factor is the sum of α odd terms but must be a power of 2; therefore, $\alpha=2k$ for some k. Then $2^\beta=(p^k-1)(p^k+1)$. These last two factors are powers of 2 that differ by 2; this forces $k=1$, $\alpha=2$, $\beta=3$, $p=3$, and $q=2$ as the only solution: $3^2-2^3=9-8=1$.

23. Since $3p>2n$, we see that p and $2p$ are the only multiples of p that appear as factors in $(2n)!$. Thus p divides $(2n)!$ exactly twice. Since $2p>n$, we know that p is the only multiple of p that appears as a factor in $n!$. Thus p divides $n!$ exactly once. Then since $\binom{2n}{n}=(2n)!/(n!n!)$, the two factors of p in the numerator are canceled by the two in the denominator. and therefore p does not divide the quotient.

25. By Bertrand's postulate, there must be a prime in each interval of the form $(2^{k-1}, 2^k)$, for $k=2, 3, 4, \ldots$. Thus there are at least $k-1$ primes less than 2^k. Since the prime 2 is not counted here, we have at least k primes less than 2^k.

27. First suppose that $m<n$. Then $1/n+1/(n+1)+\cdots+1/(n+m)\le 1/n+1/(n+1)+\cdots+1/(2n-1)<1/n+1/n+\cdots+1/n\le n(1/n)=1$, so the sum cannot be an integer. Now suppose $m\ge n$. By Bertrand's postulate, there is a prime p such that $n<p<n+m$. Let p be the largest such prime. Then $n+m<2p$. Suppose that $1/n+1/(n+1)+\cdots+1/p+\cdots+1/(n+m)=a$, where a is an integer. Note that p occurs as a factor in only one denominator, since $2p>n+m$. Let $Q=\prod_{j=n}^{n+m} j$, and let $Q_i=Q/i$, for $i=n, n+1, \ldots, n+m$. Multiply the equation by Q to get $Q_n+Q_{n+1}+\cdots+Q_p+\cdots+Q_{n+m}=Q_a$. Except for the term Q_p on the left-hand side

of the equation, every term on both sides is divisible by p. When we solve the equation for Q_p and factor p out, we obtain an equation of the form $Q_p = pN$, where N is an integer. But this implies that p divides Q_p, a contradiction.

29. Suppose that n has the stated property and $n \geq p^2$ for some prime p. Since p^2 is not prime, there must be a prime dividing both p^2 and n, and the only possibility is p itself, that is, $p \mid n$. Now if $n \geq 7^2$, then n is greater than 2^2, 3^2, and 5^2 and hence divisible by 2, 3, 5, and 7. This is the basic step for induction. Now assume n is divisible by $p_1, p_2, \ldots, p_k$. By Bonse's inequality, $p_{k+1}^2 < p_1 p_2 \cdots p_k < n$, so $p_{k+1} \mid n$ also. This induction implies that every prime divides n, which is absurd. Therefore, if n has the stated property, it must be less than $7^2 = 49$. To finish, check the remaining cases.

31. First suppose $n \geq 8$. By Bertrand's postulate, we have $p_{n-1} < p_n < 2p_{n-1}$ and $p_{n-2} < p_{n-1} < 2p_{n-2}$. Therefore, $p_n^2 < (2p_{n-1})(2p_{n-1}) < (2p_{n-1})(4p_{n-2}) < p_{n-1}p_{n-2}8 < p_{n-1}p_{n-2}p_5 \leq p_{n-1}p_{n-2}p_{n-3}$, since $n \geq 8$. Now check the cases $n = 6$ and 7.

Section 3.3

1. **a.** 5 **b.** 111 **c.** 6 **d.** 1 **e.** 11 **f.** 2

3. a

5. 1

7. By Theorem 3.8, $(ca, cb) = cma + cnb = |c| \cdot |ma + nb|$, where $cma + cnb$ is as small as possible. Therefore, $|ma + nb|$ is as small a positive integer as possible, i.e., equal to (a, b).

9. 1 or 2

11. Let $a = 2k$. Since $(a, b) \mid b$ and b is odd, (a, b) is odd. But $(a, b) \mid a = 2k$. Thus $(a, b) \mid k$. Therefore $(a, b) = (k, b) = (a/2, b)$.

13. Let $d = (a, b)$. Then $(a/d, b/d) = 1$, so if $g \mid (a/d)$, then $(g, b/d) = 1$. In particular, if we let $e = (a/d, bc/d)$, then $e \mid (a/d)$, so $(e, b/d) = 1$; therefore $e \mid c$. Since $e \mid (a/d)$, we know that $e \mid a$, so $e \mid (a, c)$. Conversely, if $f = (a, c)$, then $(f, b) = 1$, so $(d, f) = 1$; therefore $f \mid (a/d)$, and trivially $f \mid (bc/d)$. Therefore, $f \mid e$, whence $e = f$. Then $(a, b)(a, c) = de = d(a/d, bc/d) = (a, bc)$.

15. 10, 26, 65

17. **a.** 2 **b.** 5 **c.** 99 **d.** 3 **e.** 7 **f.** 1001

19. We proceed by induction, the basis case $n = 2$ being Exercise 7. Then using the basis case and Lemma 3.2, we have $(ca_1, ca_2, \ldots, ca_n) = (ca_1, ca_2, \ldots, ca_{n-2}, (ca_{n-1}, ca_n)) = (ca_1, ca_2, \ldots, ca_{n-2}, c(a_{n-1}, a_n)) = c(a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$ by the inductive hypothesis. But this last expression equals $c(a_1, a_2, \ldots, a_n)$ by Lemma 3.2.

21. Suppose that $(6k + a, 6k + b) = d$. Then $d \mid b - a$. We have $a, b \in \{-1, 1, 2, 3, 5\}$, so if $a < b$ it follows that $b - a \in \{1, 2, 3, 4, 6\}$. Hence, $d \in \{1, 2, 3, 4, 6\}$. To show that $d = 1$ it is sufficient to show that neither 2 nor 3 divides $(6k + a, 6k + b)$. If $p = 2$ or 3 and $p \mid (6k + a, 6k + b)$, then $p \mid a$ and $p \mid b$. However, there are no such pairs a, b in the set $\{-1, 1, 2, 3, 5\}$.

23. We proceed with the Euclidean algorithm: $8a + 3 = 1(5a + 2) + (3a + 1)$, $5a + 2 = 1(3a + 1) + (2a + 1)$, $3a + 1 = 1(2a + 1) + (a)$, $2a + 1 = 2(a) + (1)$. Therefore $(8a + 3, 5a + 2) = 1$.

25. From Exercise 21, we know that $6k - 1$, $6k + 1$, $6k + 2$, $6k + 3$, and $6k + 5$ are pairwise relatively prime. To represent n as the sum of two relatively prime integers greater than 1, let $n = 12k + h$, $0 \leq h < 12$. We now examine the twelve cases, one for each possible value of h: $h = 0$, $n = (6k - 1) + (6k + 1)$; $h = 1$, $n = (6k - 1) + (6k + 2)$; $h = 2$, $n = (6k - 1) + (6k + 3)$; $h = 3$, $n = (6k + 1) + (6k + 2)$; $h = 4$, $n = (6k + 1) + (6k + 3)$; $h = 5$, $n = (6k + 2) + (6k + 3)$;

$h = 6, n = (6k + 1) + (6k + 5)$; $h = 7, n = (6k + 2) + (6k + 5)$; $h = 8, n = (6k + 3) + (6k + 5)$; $h = 9, n = (12k + 7) + 2$; $h = 10, n = (12k + 7) + 3$; $h = 11, n = (12k + 9) + 2$.

27. Let S be the set of all fractions $P/Q = (xa + ye)/(xb + yf)$, where x and y are relatively prime positive integers. Then every element of S lies between a/b and e/f and is in lowest terms. The first element of S to appear in a Farey series will have the smallest Q, i.e., $x = y = 1$. This fraction must be c/d by hypothesis.

29. Since $a/b < (a + c)/(b + d) < c/d$, we have $b + d > n$, or a/b and c/d would not be consecutive, since otherwise $(a + c)/(b + d)$ would have appeared in the Farey series of order n.

31. Since $(a/b) + (c/d) = (ad + bc)/(bd)$ is an integer, $bd \mid ad + bc$. Certainly, then, $bd \mid d(ad + bc) = ad^2 + cbd$. Now since $bd \mid cbd$, we have $bd \mid ad^2$. From this, $bdn = ad^2$ for some integer n, and it follows that $bn = ad$, or $b \mid ad$. Since $(a, b) = 1$, we must have $b \mid d$. Similarly, we can show that $d \mid b$; hence $b = d$.

33. Note that a lattice point lies on the diagonal from $(0, 0)$ to (a, b) if and only if $[bx/a]$ is an integer. Let $d = (a, b)$ and $a = cd$, so that $(c, b) = 1$. There are exactly x multiples of c less than or equal to a since $cd = a$, so there are exactly $d + 1$ lattice points on the diagonal. One way to count the lattice points is to consider the rectangle, which has $(a + 1)(b + 1)$ points, and divide by 2. But we need to add back in half the points on the diagonal, which gives us $(a + 1)(b + 1)/2 + ((a, b) + 1)/2$. Another way is to count each column above the horizontal axis, starting with $i = 1, 2, \ldots, a - 1$. The equation of the diagonal is $y = (ba)x$, so for a given i, the number of points on or below the diagonal is $[bi/a]$. So the total number of interior points in the triangle plus the points on the the diagonal is $\sum_{i=1}^{a-1}[bi/a]$. Then the right-hand boundary has b points and the lower boundary has $a + 1$ points. So in all, we have $\sum_{i=1}^{a-1}[bi/a] + a + b + 1$ points. Equating the two expressions and simplifying gives the identity.

35. Assume there are exactly r primes and consider the $r + 1$ numbers $(r + 1)! + 1$. From Lemma 3.1, each of these numbers has a prime divisor, but from Exercise 34, these numbers are pairwise relatively prime, so these prime divisors must be unique, so we must have at least $r + 1$ different prime divisors, a contradiction.

Section 3.4

1. **a.** 15 **b.** 6 **c.** 2 **d.** 5

3. **a.** $-1 \cdot 75 + 2 \cdot 45$ **b.** $6 \cdot 222 + (-13) \cdot 102$ **c.** $-138 \cdot 666 + 65 \cdot 1414$ **d.** $-1707 \cdot 20785 + 800 \cdot 44350$

5. **a.** 1 **b.** 7 **c.** 5

7. **a.** $1 \cdot 6 + 1 \cdot 10 + (-1) \cdot 15$ **b.** $0 \cdot 70 + (-1) \cdot 98 + 1 \cdot 105$ **c.** $-13 \cdot 280 + 0 \cdot 330 + 9 \cdot 405 + 0 \cdot 490$

9. 2

11. $2n - 2$

13. Suppose that we have the balanced ternary expansions for integers $a \geq b$. If both expansions end in 0, then both are divisible by 3, and we can divide this factor of 3 out by deleting the trailing 0s (a shift), in which case $(a, b) = 3(a/3, b/3)$. If exactly one expansion ends in 0, then we can divide the factor of 3 out by shifting, and we have $(a, b) = (a/3, b)$, say. If both expansions end in 1 or in -1, then we can subtract the larger from the smaller to get $(a, b) = (a - b, b)$, say, and then the expansion for $a - b$ ends in 0. Finally, if one expansion ends in 1 and the other in -1, then we can add the two to get $(a + b, b)$, where the expansion of $a + b$ now ends in 0. Since $a + b$ is no larger than $2a$ and since we can now divide $a + b$ by 3, the larger term is reduced by

a factor of at least 2/3 after two steps. Therefore, this algorithm will terminate in a finite number of steps, when we finally have $a = b = 1$.

15. *Lemma:* If c and d are integers and $c = dq \pm r$, where q and r are integers, then $(c, d) = (d, r)$. [*Proof of lemma:* If an integer e divides both c and d, then since $r = \pm(c - dq)$, Theorem 1.8 shows that $e \mid r$. If $e \mid d$ and $e \mid r$, then since $c = dq + r$, from Theorem 1.8 we see that $e \mid c$. Since the common divisors of c and d are the same as the common divisors of d and r, we see that $(c, d) = (d, r)$.] Let $r_0 = a$ and $r_1 = b$ be positive integers with $a \geq b$. By successively applying the least-remainder division algorithm, we find that $r_0 = r_1q_1 + e_2r_2$, $-r_1/2 < e_2r_2 \leq r_1/2$; $\ldots$; $r_{n-2} = r_{n-1}q_{n-1} + e_nr_n$, $-r_{n-1}/2 < e_nr_n \leq r_{n-1}/2$; $r_{n-1} = r_nq_n$. We eventually obtain a remainder of 0 since the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. By the lemma we see that $(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Hence $(a, b) = r_n$, the last nonzero remainder.

17. Let $v_2 = v_3 = 2$ and $v_i = 2v_{i-1} + v_{i-2}$ for $i \geq 4$.

19. Performing the Euclidean algorithm with $r_0 = m$ and $r_1 = n$, we find that $r_0 = r_1q_1 + r_2, 0 \leq r_2 < r_1$, $r_1 = r_2q_2 + r_3, 0 \leq r_3 < r_2$, $\ldots$, $r_{k-3} = r_{k-2}q_{k-2} + r_{k-1}, 0 \leq r_{k-1} < r_{k-2}$, and $r_{k-2} = r_{k-1}q_{k-1}$. We have $(m, n) = r_{k-1}$. We will use these steps to find the greatest common divisor of $a^m - 1$ and $a^n - 1$. First, we show that if u and v are positive integers, then the least positive residue of $a^u - 1$ modulo $a^v - 1$ is $a^r - 1$, where r is the least positive residue of u modulo v. To see this, note that $u = vq + r$, where r is the least positive residue of u modulo v. It follows that $a^u - 1 = a^{vq+r} - 1 = (a^v - 1)(a^{v(q-1)+r} + \cdots + a^{v+r} + a^r) + (a^r - 1)$. This shows that the remainder is $a^r - 1$ when $a^u - 1$ is divided by $a^v - 1$. Now let $R_0 = a^m - 1$ and $R_1 = a^n - 1$. When we perform the Euclidean algorithm starting with R_0 and R_1 we obtain $R_0 = R_1Q_1 + R_2$, where $R_2 = a^{r_2} - 1$, $R_1 = R_2Q_2 + R_3$, where $R_3 = a^{r_3} - 1, \ldots, R_{k-3} = R_{k-2}Q_{k-2} + R_{k-1}$, where $R_{k-1} = a^{r_{k-1}-1}$. Hence the last nonzero remainder, $R_{k-1} = a^{r_{k-1}} - 1 = a^{(m,n)} - 1$ is the greatest common divisor of $a^m - 1$ and $a^n - 1$.

21. Note that $(x, y) = (x - ty, y)$, as every divisor of x and y is also a divisor of $x - ty$. So, every move in the game of Euclid preserves the g.c.d. of the two numbers. Since $(a, 0) = a$, if the game beginning with $\{a, b\}$ terminates, then it must do so at $\{(a, b), 0)\}$. Since the sum of the two numbers is always decreasing and positive, the game must terminate.

23. Choose m so that d has no more than m bits and q has $2m$ bits, if necessary appending initial zeros to q. By Theorems 2.5 and 2.7, q can be divided by d using $O(m^2) = O(\log_2 q \log_2 d)$ bit operations. Suppose that n is the number of steps used by the Euclidean algorithm to find (a, b). Then by Theorem 3.13, $n = O(\log_2 a)$. The total number of bit operations for divisions in the Euclidean algorithm is $\sum_{i=1}^{n} O(\log_2 q_i \log_2 r_i) = \sum_{i=1}^{n} O(\log_2 q_i \log_2 b) = O(\log_2 b \sum_{i=1}^{n} \log_2 q_i) = O(\log_2 b \log_2 \prod_{i=1}^{n} q_i)$, where q_i and r_i are as in the proof of Theorem 3.13. Dropping the remainder in each step of the Euclidean algorithm, we have inequalities $r_i \geq r_{i+1}q_{i+1}$, for $i = 0, 1, \ldots, n - 1$. Multiplying these inequalities together yields $\prod_{i=0}^{n-1} r_i \geq \prod_{i=1}^{n} r_iq_i$. Cancelling common factors reduces this to $a = r_0 \geq r_n \prod_{i=1}^{n} q_i$. Therefore, the total number of bit operations is $O(\log_2 b \log_2 \prod_{i=1}^{n} q_i) = O(\log_2 b \log_2 a) = O((\log_2 a)^2)$.

25. We apply the Q_i's one at a time. When we multiply $\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_n \\ 0 \end{pmatrix} = \begin{pmatrix} q_nr_n \\ r_n \end{pmatrix} = \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$, the top component is the last equation in the series of equations in the proof of Lemma 3.3. When we multiply this result on the left by the next matrix, we get $\begin{pmatrix} q_{n-1} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} q_{n-1}r_{n-1} + r_n \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}$, which is the matrix version of the last two equations in the proof of Lemma 3.3. In general, at the ith step we have $\begin{pmatrix} q_{n-1} & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-i-1} \\ r_{n-i} \end{pmatrix} =$

$\begin{pmatrix} q_{n-i}r_{n-i-1}+r_{n-i} \\ r_{n-i-1} \end{pmatrix} = \begin{pmatrix} r_{n-i-2} \\ r_{n-i-1} \end{pmatrix}$, so that we inductively work our way up the equations in the proof of Lemma 3.3, until finally we have $\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$.

Section 3.5

1. **a.** $2^2 \cdot 3^2$ **b.** $3 \cdot 13$ **c.** $2^2 \cdot 5^2$ **d.** 17^2 **e.** $2 \cdot 3 \cdot 37$ **f.** 2^8 **g.** $5 \cdot 103$ **h.** $23 \cdot 43$ **i.** $2^4 \cdot 3^2 \cdot 5 \cdot 7$ **j.** $2^6 \cdot 5^3$ **k.** $3 \cdot 5 \cdot 7^2 \cdot 13$ **l.** $3^2 \cdot 11 \cdot 101$

3. $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

5. **a.** 2, 3 **b.** 2, 3, 5 **c.** 2, 3, 5, 7, 11, 13, 17, 19 **d.** 2, 3, 7, 13, 29, 31, 37, 41, 43, 47

7. integers of the form p^2, where p is prime; integers of the form pq or p^3, where p and q are distinct primes

9. Let $n = p_1^{2a_1}p_2^{2a_2}\cdots p_k^{2a_k}q_1^{2b_1+3}q_2^{2b_2+3}\cdots q_l^{2b_l+3}$ be the factorization of a powerful number. Then $n = (p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}q_1^{b_1}q_2^{b_2}\cdots q_l^{b_l})^2(q_1q_2\cdots q_l)^3$ is a product of a square and a cube.

11. Suppose that $p^a \parallel m$ and $p^b \parallel n$. Then $m = p^aQ$ and $n = p^bR$, where both Q and R are products of primes other than p. Hence, $mn = (p^aQ)(p^bR) = p^{a+b}QR$. It follows that $p^{a+b} \parallel mn$ since p does not divide QR.

13. Suppose that $p^a \parallel m$ and $p^b \parallel n$ with $a \neq b$. Then $m = p^aQ$ and $n = p^bR$, where both Q and R are products of primes other than p. Suppose, without loss of generality, that $a = \min(a, b)$. Then $m + n = p^aQ + p^bR = p^{\min(a,b)}(Q + p^{b-a}R)$. Then $p \nmid (Q + p^{b-a}R)$ because $p \nmid Q$ but $p \mid p^{b-a}R$. It follows that $p^{\min(a,b)} \parallel (m + n)$.

15. $2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

17. 300, 301, 302, 303, 304

19. We compute $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Thus $N(\alpha\beta) = (ac - 5bd)^2 + 5(ad + bc)^2 = a^2c^2 - 10acbd + 25b^2d^2 + 5a^2d^2 + 10adbc + 5b^2c^2 = a^2(c^2 + 5d^2) + 5b^2(5d^2 + c^2) = (a^2 + 5b^2)(c^2 + 5d^2) = N(\alpha)N(\beta)$.

21. Suppose $3 = \alpha\beta$. Then from Exercise 19 we know that $9 = N(3) = N(\alpha)N(\beta)$. Then $N(\alpha) = 1$, 3, or 9. Let $\alpha = a + b\sqrt{-5}$. Then we must have $a^2 + 5b^2 = 1$, 3, or 9. So either $b = 0$ and $a = \pm 1$ or ± 3, or $b = \pm 1$ and $a = \pm 2$. Since $a = \pm 1$, $b = 0$ is excluded, and since $a = \pm 3$ forces $\beta = \pm 1$, we must have $b = \pm 1$. That is, $\alpha = \pm 2 \pm \sqrt{-5}$. But then $N(\alpha) = 9$, and hence $N(\beta) = 1$, which forces $\beta = \pm 1$.

23. Note that $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. We know that 3 is prime from Exercise 21. Similarly, if we seek $\alpha = a + b\sqrt{-5}$ such that $N(\alpha) = a^2 + 5b^2 = 7$, then we find there are no solutions. Indeed, $b = 0$ implies $a^2 = 7$, $|b| = 1$ implies $a^2 = 2$, and $|b| > 1$ implies $a^2 < 0$, and in each case there is no such a. Hence, if $\alpha\beta = 7$, then $N(\alpha\beta) = N(\alpha)N(\beta) = N(7) = 49$. So one of $N(\alpha)$ and $N(\beta)$ must be equal to 49 and the other equal to 1. Hence, 7 is also prime. We have shown that there are no numbers of the form $a + b\sqrt{-5}$ with norm 3 or 7. So in a similar fashion to the argument above, if $\alpha\beta = 1 \pm 2\sqrt{-5}$, then $N(\alpha\beta) = N(\alpha)N(\beta) = N(1 \pm 2\sqrt{-5}) = 21$. Since there are no numbers with norm 3 or 7, one of α and β has norm 21 and the other has norm 1. Hence, $1 \pm 2\sqrt{-5}$ is also prime.

25. The product of $4k + 1$ and $4l + 1$ is $(4k + 1)(4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1 = 4m + 1$, where $m = 4kl + k + l$. Hence, the product of two integers of the form $4k + 1$ is also of this form.

27. We proceed by mathematical induction on the elements of H. The first Hilbert number greater than 1, 5, is a Hilbert prime because it is an integer prime. This completes the basis step. For the

inductive step, we assume that all numbers in H less than or equal to n can be factored into Hilbert primes. The next greatest number in H is $n+4$. If $n+4$ is a Hilbert prime, then we are done. Otherwise, $n = hk$, where h and k are less than n and in H. By the inductive hypothesis, h and k can be factored into Hilbert primes. Thus $n+4$ can be written as the product of Hilbert primes.

29. 1, 2, 3, 4, 6, 8, 12, 24

31. **a.** 77 **b.** 36 **c.** 150 **d.** 33633 **e.** 605605 **f.** 277200

33. **a.** $2^2 3^3 5^3 7^2, 2^7 3^5 5^5 7^7$ **b.** $1, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ **c.** $2 \cdot 5 \cdot 11, 2^3 \cdot 3 \cdot 5^7 \cdot 7 \cdot 11^{13} \cdot 13$ **d.** $101^{1000}, 41^{11} 47^{11} 79^{111} 83^{111} 101^{1001}$

35. the year 2121

37. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, where each p_i is a prime and r_i and s_i are nonnegative. Then $(a, b) = p_1^{\min(r_1, s_1)} \cdots p_k^{\min(r_k, s_k)}$ and $[a, b] = p_1^{\max(r_1, s_1)} \cdots p_k^{\max(r_k, s_k)}$. So $[a, b] = (a, b) \cdot p_1^{\max(r_1, s_1) - \min(r_1, s_1)} \cdots p_k^{\max(r_k, s_k) - \min(r_k, s_k)}$. Since $\max(r_i, s_i) - \min(r_i, s_i)$ is clearly nonnegative, we now see that $(a, b) \mid [a, b]$. Clearly, $(a, b) = [a, b]$ if and only if each $r_i = s_i$, which means $a = b$.

39. If $[a, b] \mid c$, then since $a \mid [a, b]$, we have $a \mid c$. Similarly, $b \mid c$. Conversely, suppose that $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, and $c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$. If $a \mid c$ and $b \mid c$, then $\max(a_i, b_i) \leq c_i$ for $i = 1, 2, \ldots, n$. Hence $[a, b] \mid c$.

41. Assume that $p \mid a^n = \pm |a| \cdot |a| \cdots |a|$. Then by Lemma 3.5, $p \mid |a|$ and so $p \mid a$.

43. **a.** Suppose that $(a, b) = 1$ and $p \mid (a^n, b^n)$, where p is a prime. It follows that $p \mid a^n$ and $p \mid b^n$. By Exercise 43, $p \mid a$ and $p \mid b$. But then $p \mid (a, b) = 1$, which is a contradiction.
b. Suppose that a does not divide b, but $a^n \mid b^n$. Then there is some prime power, say p^r, that divides a but does not divide b (else $a \mid b$ by the fundamental theorem of arithmetic). Thus $a = p^r Q$, where Q is an integer. Now $a^n = (p^r Q)^n = p^{rn} Q^n$, so $p^{rn} \mid a^n$ and it follows that $p^{rn} \mid b^n$. Then $b^n = m p^{rn}$, from which it follows that each of the n b's must by symmetry contain at least r p's. But this is a contradiction.

45. Let $x = \sqrt{2} + \sqrt{3}$. Then $x^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 5 + 2\sqrt{6}$. Hence, $x^2 - 5 = 2\sqrt{6}$. It follows that $x^4 - 10x^2 + 25 = 24$. Consequently, $x^4 - 10x^2 + 1 = 0$. From Theorem 3.18 it follows that $\sqrt{2} + \sqrt{3}$ is irrational, since it is not an integer (we can see this since $3 < \sqrt{2} + \sqrt{3} < 4$).

47. Suppose that $m/n = \log_p b$. This implies that $p^{m/n} = b$, from which it follows that $p^m = b^n$. Since b is not a power of p, there must be another prime, say q, such that $q \mid b$. But then $q \mid b^n = p^m = p \cdot p \cdots p$. By Lemma 3.5, $q \mid p$, which is impossible since p is a prime number.

49. Let p be a prime. Define s and t by $p^s \parallel a$ and $p^t \parallel b$, say $a = xp^s$ and $b = yp^t$, where $p \nmid xy$. Without loss of generality, suppose that $s \leq t$. Then $a + b = p^s(x + p^{t-s})$, so $p^s \parallel a + b$. Also, $p^{\max(s,t)} \parallel [a, b]$. But $\max(s, t) = t$, so $p^t \parallel [a, b]$. Therefore $p^{\min(s,t)} \parallel (a + b, [a, b])$. But $p^{\min(s,t)} \parallel (a, b)$, so the same power of p divides both sides of the equation. Since this holds for each p, the two sides must be equal.

51. It suffices to prove this "one prime at a time"; to this end, let r, s, and t be the exponents on the prime p in the prime factorizations of a, b, and c, respectively. We know that the exponent on p in $[a, b]$ is $\max(r, s)$, and so the exponent on p in $([a, b], c)$ is $\min(t, \max(r, s))$. We also know that the exponent on p in (a, c) is $\min(r, t)$ and the exponent on p in (b, c) is $\min(s, t)$, so the exponent on p in $[(a, c), (b, c)]$ is $\max(\min(r, t), \min(s, t))$. But it is not hard to see that $\min(t, \max(r, s))$ and $\max(\min(r, t), \min(s, t))$ always represent the same value. It follows that the exponent on p in the prime factorizations of $([a, b], c)$ and $[(a, c), (b, c)]$ are the same for each prime p, and we conclude therefore that $([a, b], c) = [(a, c), (b, c)]$. In a similar manner, we find that $[(a, b), c] = ([a, c], [b, c])$.

53. Let $c = [a_1, \ldots, a_n]$, $d = [[a_1, \ldots, a_{n-1}], a_n]$, and $e = [a_1, \ldots, a_{n-1}]$. If $c \mid m$, then all a_i's divide m; hence $e \mid m$ and $a_n \mid m$, so $d \mid m$. Conversely, if $d \mid m$, then $e \mid m$ and $a_n \mid m$, so all a_i's divide m; thus $c \mid m$. Since c and d divide all the same numbers, they must be equal.

55. **a.** There are six cases, all handled the same way. So without loss of generality, suppose that $a \le b \le c$. Then $\max(a, b, c) = c$, $\min(a, b) = a$, $\min(a, c) = a$, $\min(b, c) = b$, and $\min(a, b, c) = a$. Hence $c = \max(a, b, c) = a + b + c - \min(a, b) - \min(a, c) - \min(b, c) + \min(a, b, c) = a + b + c - a - a - b + a$.
b. The exponent on a prime p that occurs in the prime factorization of $[a, b, c]$ is $\max(x, y, z)$, where x, y, and z are the exponents on this prime in the factorizations of a, b, and c, respectively. Also $x + y + z$ is the exponent on p in abc, $\min(x, y, z)$ is the exponent on p in (a, b, c), $\min(x, y)$ is the exponent on p in (a, b), $\min(x, z)$ is the exponent on p in (a, c), $\min(y, z)$ is the exponent on p in (b, c), and $\min(x, y, z)$ is the exponent on p in (a, b, c). It follows that $x + y + z + \min(x, y, z) - \min(x, y) - \min(x, z) - \min(y, z)$ is the exponent on p in $abc(a, b, c)/((a, b)(a, c)(b, c))$. Hence from part (a), $[a, b, c] = abc(a, b, c)/((a, b)(a, c)(b, c))$.

57. Let $a = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, $b = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, and $c = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, with p_i prime and r_i, s_i, and t_i nonnegative. Then $p_i^{r_i+s_i+t_i} \parallel abc$, but $p_i^{\min(r_i,s_i,t_i)} \parallel (a, b, c)$ and $p_i^{r_i+s_i+t_i-\min(r_i,s_i,t_i)} \parallel [ab, ac, ab]$, and $p_i^{\min(r_i,s_i,t_i)} \cdot p_i^{r_i+s_i+t_i-\min(r_i,s_i,t_i)} = p_i^{r_i+s_i+t_i}$.

59. It suffices to prove this "one prime at a time"; to this end, let r, s, and t be the exponents on the prime p in the prime factorizations of a, b, and c, respectively. Then, using the facts that the exponent on p in (a, b, c) is $\min(r, s, t)$, and the exponent on p in $[a, b, c]$ is $\max(r, s, t)$, we see that the exponent on p in $([a, b], [a, c], [b, c])$ is $\min(\max(r, s), \max(r, t), \max(s, t))$, whereas the exponent on p in $[(a, b), (a, c), (b, c)]$ is $\max(\min(r, s), \min(r, t), \min(s, t))$. But these two are equal (examine the six orderings $r \ge s \ge t, \ldots$).

61. First note that there are arbitrarily long sequences of composites in the integers. For example, $(n + 2)! + 2, (n + 2)! + 3, \ldots, (n + 2)! + (n + 2)$ is a sequence of n consecutive composites. To find a sequence of n composites in the sequence $a, a + b, a + 2b, \ldots$, look at the integers in $a, a + b, a + 2b, \ldots$ with absolute values between $(nb + 2)! + 2$ and $(nb + 2)! + (nb + 2)$. There are clearly n or $n + 1$ such integers, and all are composite.

63. 103

65. 701

67. Let $a = \prod_{i=1}^{s} p_i^{\alpha_i}$ and $b = \prod_{i=1}^{t} p_i^{\beta_i}$. The condition $(a, b) = 1$ is equivalent to $\min(\alpha_i, \beta_i) = 0$ for all i, and the condition $ab = c^n$ is equivalent to $n \mid \alpha_i + \beta_i$ for all i. Hence $n \mid \alpha_i$ and $\beta_i = 0$, or $n \mid \beta_i$ and $\alpha_i = 0$. Let d be the product of $p_i^{\alpha_i/n}$ over all i of the first kind, and let e be the product of $p_i^{\beta_i/n}$ over all i of the second kind. Then $d^n = a$ and $e^n = b$.

69. Partition the set of integers $S = \{1, 2, 3, \ldots, 2n\}$ into n subsets in the following way. Let $S_1 = \{1, 2, 4, 8, \ldots\} \cap S$; let $S_2 = \{3, 6, 12, 24, \ldots\} \cap S$; let $S_3 = \{5, 10, 20, 40, \ldots\} \cap S$; and so on, with the last set being $S_n = \{2n - 1\}$. In other words, S_i is the set of elements in S whose "odd part" (the number with all factors of 2 divided out) is $2i - 1$, for $i = 1, 2, \ldots, n$. By the pigeonhole principle, at least two of the $n + 1$ given numbers must lie in the same S_i, and clearly the smaller of the two will divide the larger.

71. $m = n$ or $\{m, n\} = \{2, 4\}$

73. For $j \ne i$, $p_i \mid Q_j$, since it is one of the factors. So p_1 must divide $S - \sum_{j \ne i} Q_j = Q_i = p_1 \cdots p_{i-1} p_{i+1} \cdots p_r$, but by the fundamental theorem of arithmetic, p_i must be equal to one of these last factors, a contradiction.

75. Let p be the largest prime less than or equal to n. If $2p < n$, then Bertrand's postulate guarantees another prime q such that $p < q < 2p \le n$, contradicting the choice of p. Therefore, we know that $n < 2p$. Therefore, in the prime factorization of the product $n! = 1 \cdot 2 \cdot 3 \cdots n$, only one multiple of p appears.

77. **a.** Uniqueness follows from the fundmental theorem of arithmetic. Because $e_i \ge 0$, we have $p_1^{e_1} = p_1^{e_1} p_2^0 \cdots p_r^0 \le p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = m$.
b. Because $p_1^{e_i} < p_i^{e_i} \le m \le Q = p_r^n$, taking logarithms it follows that $e_i \log p_1 = n \log p_r$. Dividing by $\log p_1$ gives the first inequality. If $1 \le m \le Q$, then m has a prime-power factorization of the form in part (a), so the r-tuples of exponents count the number of integers in the range $1 \le m \le Q$.
c. To bound the number of r-tuples, by part (b) there are at most $C(n+1)^r$ r-tuples. By part (b) we have $p_r^n \le (Cn+1)^r = (n(C+1/n))^r \le n^r(C+1)^r$.
d. Taking logarithms of both sides of the inequality in part (c), we obtain $n \le r(\log n + \log(C+1))/\log p_r$, but because n grows much faster than $\log n$, the left-hand side must be larger than the right-hand side for large values of n.

79. $S(40) = 5$, $(41) = 41$, $S(43) = 43$

81. $a(n) = 1, 2, 3, 4, 5, 9, 7, 32, 27, 25, 11, \ldots$

83. By Exercise 80, we have $S(p) = p$ whenever p is prime. If $m < p$ and $m \mid S(p)! = p!$, then $m \mid (p-1)!$, so $S(p)$ must be the first time that $S(n)$ takes on the value p.

85. Let n be square-free. Then no prime can appear to a power greater than one in the prime-power factorization of n. So $n = p_1 p_2 \cdots p_r$ for some distinct primes p_i, which implies that $\text{rad}(n) = p_1 p_2 \cdots p_r = n$. Conversely, if n is not square-free, then $d^2 \mid n$ for some integer d with $d > 2$, and some prime factor p_1 of d appears to an even power in the prime-power factorization of n. So $n = p_1^{2a} p_2^{b_2} \cdots p_r^{b_r}$. This implies that $\text{rad}(n) = p_1 p_2 \cdots p_r \ne n$.

87. Since every prime occurring in the prime-power factorization of mn occurs in either the factorization of m or n, every factor in $\text{rad}(mn)$ occurs at least once in the product $\text{rad}(m)\text{rad}(n)$, yielding the inequality. If $m = p_1^{a_1} \cdots p_r^{a_r}$ and $n = q_1^{b_1} \cdots q_s^{b_s}$ are relatively prime, then $\text{rad}(mn) = p_1 \cdots p_r q_1 \cdots q_s = \text{rad}(m)\text{rad}(n)$.

89. First note that if $p \mid \binom{2n}{n}$, then $p \le 2n$. This is true because every factor of the numerator of $\binom{2n}{n} = (2n)!/(n!)^2$ is less than or equal to $2n$. Let $\binom{2n}{n} = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ be the factorization of $\binom{2n}{n}$ into distinct prime powers. By the definition of the function $\pi(x)$, we have $k \le \pi(2n)$. By Exercise 88, $p_i^{r_i} \le 2n$. It now follows that $\binom{2n}{n} = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \le (2n)(2n) \cdots (2n) \le (2n)^{\pi(2n)}$.

91. Note that $\binom{2n}{n} \le \sum_{a=0}^{2n} \binom{2n}{a} = (1+1)^{2n} = 2^{2n}$. Then from Exercise 90, $n^{\pi(2n)-\pi(n)} < \binom{2n}{n} \le 2^{2n}$. Taking logarithms gives $(\pi(2n) - \pi(n)) \log n < \log(2^{2n}) = n \log 4$. Now divide by $\log n$.

93. Note that $2^n = \prod_{a=1}^{n} 2 \le \prod_{a=1}^{n} (n+a)/a = \binom{2n}{n}$. Then by Exercise 89, $2^n \le (2n)^{\pi(2n)}$. Taking logarithms gives $\pi(2n) \ge n \log 2/(\log 2n)$. Hence for a real number x we have $\pi(x) \ge [x/2] \log 2/\log[x] > c_1 x/\log x$. For the other half, Exercise 91 gives $\pi(x) - \pi(x/2) < ax/\log x$, where a is a constant. Then $\log(x/2^m)\pi(x/2^m) - \log(x/2^{m+1})\pi(x/2^{m+1}) < ax/2^m$ for every positive integer m. Thus $(\log x)\pi(x) = \sum_{m=0}^{v} \left(\log(x/2^m)\pi(x/2^m) - \log(x/2^{m+1})\pi(x/2^{m+1})\right) < ax \sum_{m=0}^{v} 1/2^m < c_2 x$, where v is the largest integer such that $2^{v+1} \le x$. Then $\pi(x) < c_2 x/\log x$.

Section 3.6

1. **a.** $3 \cdot 5^2 \cdot 7^3 \cdot 13 \cdot 101$ **b.** $11^3 \cdot 13 \cdot 19 \cdot 641$ **c.** $13 \cdot 17 \cdot 19 \cdot 47 \cdot 71 \cdot 97$

3. **a.** $143 = 12^2 - 1 = (12+1)(12-1) = 13 \cdot 11$
b. $2279 = 48^2 - 5^2 = (48+5)(48-5) = 53 \cdot 43$

c. 43 is prime.
d. $11413 = 107^2 - 6^2 = (107 + 6)(107 - 6) = 113 \cdot 101$

5. Note that $(50 + n)^2 = 2500 + 100n + n^2$ and $(50 - n)^2 = 2500 - 100n + n^2$. The first equation shows that the possible final two digits of squares can be found by examining the squares of the integers $0, 1, \ldots, 49$, and the second equation shows that these final two digits can be found by examining the squares of the integers $0, 1, \ldots, 25$. We find that $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25$, $6^2 = 36$, $7^2 = 49$, $8^2 = 64$, $9^2 = 81$, $10^2 = 100$, $11^2 = 121$, $12^2 = 144$, $13^2 = 169$, $14^2 = 196$, $15^2 = 225$, $16^2 = 256$, $17^2 = 289$, $18^2 = 324$, $19^2 = 361$, $20^2 = 400$, $21^2 = 441$, $22^2 = 484$, $23^2 = 529$, $24^2 = 576$, $25^2 = 625$. It follows that the last two digits of a square are 00, $e1$, $e4$, 25, $o6$, $e9$, where e represents an even digit and o represents an odd digit.

7. Suppose that $x^2 - n$ is a perfect square with $x > (n + p^2)/(2p)$, say a^2. Now, $a^2 = x^2 - n > ((n + p^2)/(2p))^2 - n = ((n - p^2)/(2p))^2$. It follows that $a > (n + p^2)/(2p)$. From these inequalities for x and a, we see that $x + a > n/p$, or $n < p(x + a)$. Also, $a^2 = x^2 - n$ tells us that $(x - a)(x + a) = n$. Now, $(x - a)(x + a) = n < p(x + a)$. Canceling, we find that $x - a < p$. But since $x - a$ is a divisor of n less than p, the smallest prime divisor of n, it follows that $x - a = 1$. In this case, $x = (n + 1)/2$.

9. From the identity in Exercise 8, it is clear that if $n = n_1$ is a multiple of $2k + 1$, then so is n_k, since it is the difference of two multiples of $2k + 1$. If $2k + 1 \mid n_k$, then $2k + 1 \mid r_k$, and it follows from $r_k < 2k + 1$ that $r_k = 0$. Thus $n_k = (2k + 1)q_k$. Continuing, we see that $n = n + 2n_k - 2(2k + 1)q_k = (2k + 1)n + 2(n_k - kn) - 2(2k + 1)q_k$. It follows from Exercise 8 that $n = (2k + 1)n - 2(2k + 1)\sum_{i=1}^{k-1} q_i - 2(2k + 1)q_k = (2k + 1)n - 2(2k + 1)\sum_{i=1}^{k} q_i$. Using Exercise 8 again, we conclude that $n = (2k + 1)(n - 2\sum_{i=1}^{k} q_i) = (2k + 1)m_{k+1}$.

11. To see that u is even, note that $a - c$ is the difference of odd numbers and that $b - d$ is the difference of even numbers. Thus $a - c$ and $b - d$ are even, and u must be as well. That $(r, s) = 1$ follows trivially from Theorem 3.6. To continue, $a^2 + b^2 = c^2 + d^2$ implies that $(a + c)(a - c) = (d - b)(d + b)$. Dividing both sides of this equation by u, we find that $r(a + c) = s(d + b)$. From this it is clear that $s \mid r(a + c)$. But since $(r, s) = 1$, we have $s \mid a + c$.

13. To factor n, observe that $((u/2)^2 + (v/2)^2)(r^2 + s^2) = \frac{1}{4}(u^2r^2 + u^2s^2 + v^2r^2 + v^2s^2)$. Substituting $a - c$, $d - b$, $a + c$, and $d + b$ for ru, su, sv, and rv, respectively, will allow everything to be simplified down to n. As u and v are both even, both of the factors are integers.

15. We have $2^{4n+2} + 1 = 4(2^n)^4 + 1 = (2 \cdot 2^{2n} + 2 \cdot 2^n + 1)(2 \cdot 2^{2n} - 2 \cdot 2^n + 1)$. Using this identity we have the factorization $2^{18} + 1 = 4(2^4)^4 + 1 = (2 \cdot 2^8 + 2 \cdot 2^4 + 1)(2 \cdot 2^8 - 2 \cdot 2^4 + 1) = (2^9 + 2^5 + 1)(2^9 - 2^5 + 1) = 545 \cdot 481$.

17. We can prove that the last digit in the decimal expansion of F_n is 7 for $n \geq 2$ by proving that the last digit in the decimal expansion of 2^{2^n} is 6 for $n \geq 2$. This can be done using mathematical induction. We have $2^{2^2} = 16$ so the result is true for $n = 2$. Now assume that the last decimal digit of 2^{2^n} is 6, i.e., $2^{2^n} \equiv 6 \pmod{10}$. It follows that $2^{2^{n+1}} = (2^{2^n})^{2^{n+1}-2^n} \equiv 6^{2^{n+1}-2^n} \equiv 6 \pmod{10}$. This completes the proof.

19. Since every prime factor of $F_5 = 2^{2^5} + 1 = 4{,}294{,}967{,}297$ is of the form $2^7k + 1 = 128k + 1$, we attempt to factor F_5 by trial division by primes of this form. We find that $128 \cdot 1 + 1 = 129$ is not prime, $128 \cdot 2 + 1 = 257$ is prime but does not divide $4{,}294{,}967{,}297$, $128 \cdot 3 + 1 = 385$ is not prime, $128 \cdot 4 + 1 = 513$ is not prime, and $128 \cdot 5 + 1 = 641$ is prime and does divide $4{,}294{,}967{,}297$, with $4{,}294{,}967{,}297 = 641 \cdot 6{,}700{,}417$. Every factor of $6{,}700{,}417$ is also a factor of $4{,}294{,}967{,}297$. We attempt to factor $6{,}700{,}417$ by trial division by primes of the form $128k + 1$ beginning with 641. We first note that 641 does not divide $6{,}700{,}417$. Among the other integers of the form $128k + 1$ less than $\sqrt{6700417}$, namely the integers 769, 897, 1025, 1153, 1281, 1409, 1537, 1665, 1793, 1921, 2049, 2177, 2305, 2433, and 2561, only 769, 1153, and 1409 are prime,

and none of them divides 6,700,417. Hence 6,700,417 is prime and the prime factorization of F_5 is $641 \cdot 6{,}700{,}417$.

21. $2^n \log_{10} 2$

23. See Exercise 21 of Section 3.2.

Section 3.7

1. **a.** $x = 33 - 5t, y = -11 + 2t$
b. $x = -300 + 13t, y = 400 - 17t$
c. $x = 21 - 2t, y = -21 + 3t$
d. no solutions
e. $x = 889 - 1969t, y = -633 + 1402t$

3. 39 US$ and 94 Can$, or 95 US$ and 33 Can$

5. Solving $111e + 169p = 11798$ yields $e = 53$, $p = 35$.

7. 17 apples and 23 oranges

9. **a.** $(1, 16), (4, 14), (7, 12), \ldots, (22, 2), (25, 0)$
b. no solutions
c. $(0, 37), (3, 35), (6, 33), \ldots, (51, 3), (54, 1)$

11. **a.** $x = -5 + 3s - 2t, y = 5 - 2s, z = t$
b. no solutions
c. $x = -1 + 102s + t, y = 1 - 101s - 2t, z = t$

13. $(9, 9, 0), (19, 8, 0), \ldots, (99, 0, 0); (4, 7, 1), (14, 6, 1), \ldots, (74, 0, 1); (9, 4, 2), (19, 3, 2), \ldots, (49, 0, 2); (4, 2, 3), (14, 1, 3), (24, 0, 3)$

15. **a.** $x = 92 + 6t, y = 8 - 7t, z = t$
b. no solutions
c. $x = 50 - t, y = -100 + 3t, z = 150 - 3t, w = t$

17. 9, 19, 41

19. The quadrilateral with vertices $(b, 0), (0, a), (b - 1, -1)$, and $(-1, a - 1)$ has area $a + b$. Pick's theorem, from elementary geometry, states that the area of a simple polygon whose vertices are lattice points (points with integer coordinates) is given by $\frac{1}{2}x + y - 1$, where x is the number of lattice points on the boundary and y is the number of lattice points inside the polygon. Since $(a, b) = 1$, we have $x = 4$, and therefore by Pick's theorem the quadrilateral contains $a + b - 1$ lattice points. Every point corresponds to a different value of n in the range $ab - a - b < n < ab$. Therefore, every n in the range must get hit, so the equation is solvable.

21. (See the solution for Exercise 19.) The line $ax + by = ab - a - b$ bisects the rectangle with vertices $(-1, a - 1)$, $(-1, -1)$, $(b - 1, a - 1)$, and $(b - 1, -1)$ but contains no lattice points. Hence half the interior points are below the line and half are above. The half below correspond to $n < ab - a - b$, and there are $(a - 1)(b - 1)/2$ of them.

23. $(0, 25, 75), (4, 18, 78), (8, 11, 81), (12, 4, 84)$

Section 4.1

1. **a.** $2 \mid (13 - 1) = 12$ **b.** $5 \mid (22 - 7) = 15$ **c.** $13 \mid (91 - 0) = 91$ **d.** $7 \mid (69 - 62) = 7$
e. $3 \mid (-2 - 1) = -3$ **f.** $11 \mid (-3 - 30) = -33$ **g.** $40 \mid (111 - (-9)) = 120$
h. $37 \mid (666 - 0) = 666$

3. **a.** $1, 2, 11, 22$ **b.** $1, 3, 9, 27, 37, 111, 333, 999$ **c.** $1, 11, 121, 1331$

5. Suppose that a is odd. Then $a = 2k + 1$ for some integer k. Then $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. If k is even, then $k = 2l$, where l is an integer. Then $a^2 = 8l(2l + 1) + 1$. Hence, $a^2 \equiv 1 \pmod 8$. If k is odd, then $k = 2l + 1$ when l is an integer. Then $a^2 = 4(2l + 1)(2l + 2) + 1 = 8(2l + 1)(l + 1)$. Again, $a^2 \equiv 1 \pmod 8$.

7. **a.** 1 **b.** 5 **c.** 9 **d.** 13

9. Since $a \equiv b \pmod m$, there exists an integer k such that $a = b + km$. Thus $ac = (b + km)c = bc + k(mc)$. By Theorem 4.1, $ac \equiv bc \pmod{mc}$.

11. **a.** We proceed by induction on n. It is clearly true for $n = 1$. For the inductive step, we assume that $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod m$ and that $a_{n+1} \equiv b_{n+1} \pmod m$. Now $\sum_{j=1}^{n+1} a_j = (\sum_{j=1}^{n} a_j) + a_{n+1} \equiv (\sum_{j=1}^{n} b_j) + b_{n+1} = \sum_{j=1}^{n+1} b_j \pmod m$ by Theorem 4.5(i).
b. We use induction on n. For $n = 1$, the identity clearly holds. For the inductive step, we assume that $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod m$ and $a_{n+1} \equiv b_{n+1} \pmod m$. Then $\prod_{j=1}^{n+1} a_j = a_{n+1}(\prod_{j=1}^{n} a_j) \equiv b_{n+1}(\prod_{j=1}^{n} b_j) = \prod_{j=1}^{n+1} b_j \pmod m$ by Theorem 4.5(iii).

13. $0 - 0 = 0, 0 - 1 = 5, 0 - 2 = 4, 0 - 3 = 3, 0 - 4 = 2, 0 - 5 = 1$; $1 - 0 = 1, 1 - 1 = 0, 1 - 2 = 5, 1 - 3 = 4, 1 - 4 = 3, 1 - 5 = 2$; $2 - 0 = 2, 2 - 1 = 1, 2 - 2 = 0, 2 - 3 = 5, 2 - 4 = 4, 2 - 5 = 3$; $3 - 0 = 3, 3 - 1 = 2, 3 - 2 = 1, 3 - 3 = 0, 3 - 4 = 5, 3 - 5 = 4$; $4 - 0 = 4, 4 - 1 = 3, 4 - 2 = 2, 4 - 3 = 1, 4 - 4 = 0, 4 - 5 = 5$; $5 - 0 = 5, 5 - 1 = 4, 5 - 2 = 3, 5 - 3 = 2, 5 - 4 = 1, 5 - 5 = 0$

15. **a.** 4 o'clock **b.** 6 o'clock **c.** 4 o'clock

17. $a \equiv \pm b \pmod p$

19. Note that $1 + 2 + 3 + \cdots + (n - 1) = (n - 1)n/2$. If n is odd, then $(n - 1)$ is even, so $(n - 1)/2$ is an integer. Hence, $n \mid 1 + 2 + 3 + \cdots + (n - 1)$ if n is odd, and so $1 + 2 + 3 + \cdots + (n - 1) \equiv 0 \pmod n$. If n is even, then $n = 2k$, where k is an integer. Then $(n - 1)n/2 = (n - 1)k$. We can easily see that n does not divide $(n - 1)k$ since $(n, n - 1) = 1$ and $k < n$. It follows that $1 + 2 + \cdots + (n - 1) \not\equiv 0 \pmod n$ if n is even.

21. those n relatively prime to 6

23. If $n = 1$, then $5 = 5^1 \equiv 1 + 4(1) \pmod{16}$, so the basis step holds. For the inductive step, we assume that $5^n \equiv 1 + 4n \pmod{16}$. Now $5^{n+1} \equiv 5^n 5 \equiv (1 + 4n)5 \pmod{16}$ by Theorem 4.3(iii). Further, $(1 + 4n)5 = 5 + 20n \equiv 5 + 4n \pmod{16}$. Finally, $5 + 4n = 1 + 4(n + 1)$. Thus $5^{n+1} \equiv 1 + 4(n + 1) \pmod{16}$.

25. Note that if $x \equiv 0 \pmod 4$ then $x^2 \equiv 0 \pmod 4$, if $x \equiv 1 \pmod 4$ then $x^2 \equiv 1 \pmod 4$, if $x \equiv 2 \pmod 4$ then $x^2 \equiv 4 \equiv 0 \pmod 4$, and if $x \equiv 3 \pmod 4$ then $x^2 \equiv 9 \equiv 1 \pmod 4$. Hence, $x^2 \equiv 0$ or $1 \pmod 4$ whenever x is an integer. It follows that $x^2 + y^2 \equiv 0$, 1, or $2 \pmod 4$ whenever x and y are integers. Therefore, n is not the sum of two squares when $n \equiv 3 \pmod 4$.

27. By Theorem 4.1, $ap^k = x^2 - x = x(x - 1)$ for some integer a. By the fundamental theorem of arithmetic, p^k is a factor of $x(x - 1)$. Since p cannot divide both x and $x - 1$, we know that $p^k \mid x$ or $p^k \mid x - 1$. Thus $x \equiv 0$ or $x \equiv 1 \pmod{p^k}$.

29. First note that there are m_1 possibilities for a_1, m_2 possibilities for a_2, and in general m_i possibilities for a_i. Thus there are $m_1 m_2 \cdots m_k$ expressions of the form $M_1 a_1 + M_2 a_2 + \cdots + M_k a_k$, where $a_1, a_2, \ldots, a_k$ run through complete systems of residues modulo $m_1, m_2, \ldots, m_k$, respectively. Since this is exactly the size of a complete system of residues modulo M, the result will follow if we can show that each of these expressions is distinct modulo M. Suppose, by way of contradiction, that $M_1 a_1 + M_2 a_2 + \cdots + M_k a_k \equiv M_1 a_1' + M_2 a_2' + \cdots + M_k a_k' \pmod M$. Then $M_1 a_1 \equiv M_1 a_1' \pmod{m_1}$, and therefore $a_1 \equiv a_1' \pmod{m_1}$ since $(M_1, m_1) = 1$. Similarly, $a_i \equiv a_i' \pmod{m_i}$. Thus a_i' is in the same congruence class modulo m_i as a_i, for all i.

31. **a.** Let $\sqrt{n} = a + r$, where a is an integer, and $0 \le r < 1$. We now consider two cases: when $0 \le r < \frac{1}{2}$ and when $\frac{1}{2} \le r < 1$. For the first case, $T = [\sqrt{n} + \frac{1}{2}] = a$, and so $t = T^2 - n = -(2ar + r^2)$. Thus $|t| = 2ar + r^2 < 2a(\frac{1}{2}) + (\frac{1}{2})^2 = a + \frac{1}{4}$. Since both T and n are integers, t is also an integer. It follows that $|t| \le [a + \frac{1}{4}] = a = T$. For the second case, when $\frac{1}{2} \le r < 1$, we find that $T = [\sqrt{n} + \frac{1}{2}] = a + 1$ and $t = 2a(1 - r) + (1 - r^2)$. Since $\frac{1}{2} \le r < 1$, we have $0 < 1 - r \le \frac{1}{2}$ and $0 < 1 - r^2 < 1$. It follows that $t \le 2a(\frac{1}{2}) + (1 - r^2)$. Because t is an integer, we can say that $t \le [a + (1 - r^2)] = a < T$.
b. By the division algorithm, if we divide x by T we get $x = aT + b$, where $0 \le b < T$. If a were negative, then $x = aT + b \le (-1)T + b < 0$; but we assumed x to be nonnegative. This shows that $0 \le a$. Suppose now that $a > T$. Then $x = aT + b \ge (T + 1)T = T^2 + T \ge (\sqrt{n} - \frac{1}{2})^2 + (\sqrt{n} - \frac{1}{2}) = n - \frac{1}{4}$ and, as x and n are integers, $x \ge n$. This is a contradiction, which shows that $a \le T$. Similarly, $0 \le c \le T$ and $0 \le d < T$.
c. $xy = (aT + b)(cT + d) = acT^2 + (ad + bc)T + bd \equiv ac(T^2 - n) + zT + bd \equiv act + zT + bd \pmod{n}$
d. Use part (c), substituting $eT + f$ for ac.
e. The first half is identical to part (b); the second half follows by substituting $gT + h$ for $z + et$ and noting that $T^2 \equiv t \pmod{n}$.
f. Certainly ft and gt can be computed since all three numbers are less than T, which is less than $\sqrt{n} + 1$. So $(f + g)t$ is less than $2n < w$. Similarly, we can compute $j + bd$ without exceeding the word size. Using the same arguments, we can compute $hT + k$ without exceeding the word size.

33. **a.** 1 **b.** 1 **c.** 1 **d.** 1 **e.** Fermat's little theorem (Section 6.1)

35. Since $f_{n-2} + f_{n-1} \equiv f_n \pmod{m}$, if two consecutive numbers recur in the same order, then the sequence must be repeating both as n increases and as it decreases. But there are only m residues and therefore only m^2 ordered sequence of two residues. As the sequence is infinite, some two elements of the sequence must recur by the pigeonhole principle. Thus the sequence of least positive residues of the Fibonacci numbers repeats. It follows that if m divides some Fibonacci number, that is, if $f_n \equiv 0 \pmod{m}$, then m divides infinitely many Fibonacci numbers. To see that m does divide some Fibonacci number, note that $f_0 = 0$.

37. Let a and b be positive integers less than m. Then they have $O(\log m)$ digits (bits). Therefore by Theorem 2.4 we can multiply them using $O(\log^2 m)$ operations. Division by m takes $O(\log^2 m)$ operations by Theorem 2.7. Thus in all we have $O(\log^2 m)$ operations.

39. Let N_i be the number of coconuts the ith man leaves for the next man, with $N_0 = N$. At each stage, the ith man finds N_{i-1} coconuts, gives k coconuts to the monkeys, takes $(1/n)(N_{i-1} - k)$ coconuts for himself, and leaves the rest for the next man. This yields the recursive formula $N_i = (N_{i-1} - k)(n - 1)/n$. For convenience, let $w = (n - 1)/n$. If we iterate this formula a few times, we get $N_1 = (N_0 - k)w$, $N_2 = (N_1 - k)w = ((N_0 - k)w - k)w = N_0w^2 - kw^2 - kw$, $N_3 = N_0w^3 - kw^3 - kw^2 - kw$, ... The general pattern $N_i = N_0w^i - kw^i - kw^{i-1} - \cdots - kw = N_0w^i - kw(w^i - 1)/(w - 1)$ may be proved by induction. When the men rise in the morning they find $N_n = N_0w^n - kw(w^n - 1)/(w - 1)$ coconuts, and we must have $N_n \equiv k \pmod{n}$, that is, $N_n = N_0w^n - kw(w^n - 1)/(w - 1) = k + tn$ for some integer t. Substituting $w = (n - 1)/n$ back in for w, solving for N_0, and simplifying yields $N = N_0 = n^{n+1}(t + k)/(n - 1)^n - kn + k$. For N to be an integer, since $(n, n - 1) = 1$, we must have $(t + k)/(n - 1)^n$ an integer. Since we seek the smallest positive value for N, we take $t + k = (n - 1)^n$, so $t = (n - 1)^n - k$. Substituting this value back into the formula for N yields $N = n^{n+1} - kn + k$.

41. **a.** Let $f_1(x) = \sum_{i=0}^{n} a_i x^i$, $f_2(x) = \sum_{i=1}^{n} b_i x^i$, $g_1(x) = \sum_{i=1}^{n} c_i x^i$, and $g_2(x) = \sum_{i=1}^{n} d_i x^i$, where the leading coefficients may be zero to keep the limits of summation the same for all

polynomials. Then $a_i \equiv c_i \pmod{n}$ and $b_i \equiv d_i \pmod{n}$. Therefore, $a_i + b_1 \equiv c_i + d_i \pmod{n}$ for $i = 0, 1, \ldots, n$. Because $(f_1 + f_2)(x) = \sum_{i=1}^{n}(a_i + b_i)x^i$ and $(g_1 + g_2)(x) = \sum_{i=1}^{n}(c_i + d_i)x^i$, showing the sums of the polynomials are congruent modulo n.
b. The coefficient of x^k in $(f_1 f_2)(x)$ is $a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$, and the corresponding coefficient in $(g_1 g_2)(x)$ is $c_0 d_k + c_1 d_{k-1} + \cdots + c_k d_0$. Because $a_i \equiv c_i \pmod{n}$ and $b_i \equiv d_i \pmod{n}$ for all i, the two expressions are congruent modulo n, and so, therefore, are the polynomials.

43. The basis step for induction on k is Exercise 42. Assume that $f(x) \equiv h(x) \pmod{p}$ and $f(x) = (x - a_1) \cdots (x - a_{k-1})h(x)$. Substituting a_k for x in this equation makes both sides 0, and none of the factors $a_k - a_i$ can be congruent to 0 modulo p, so we must have $h(a_k) \equiv 0 \pmod{p}$. Apply Exercise 42 to $h(x)$ and a_k to get $h(x) \equiv (x - a_k)g(x) \pmod{p}$ and substitute this in the congruence for $f(x)$.

Section 4.2

1. **a.** $x \equiv 6 \pmod{7}$ **b.** $x \equiv 2, 5,$ or $8 \pmod{9}$ **c.** $x \equiv 10 \pmod{40}$ **d.** $x \equiv 20 \pmod{25}$ **e.** $x \equiv 111 \pmod{999}$ **f.** $x \equiv 75 + 80k \pmod{1600}$, where k is an integer

3. $x \equiv 1074 + 3157k \pmod{28{,}927{,}591}$

5. 19 hours

7. 77 solutions when c is a multiple of 77

9. **a.** 13 **b.** 7 **c.** 5 **d.** 16

11. **a.** 1, 7, 11, 13, 17, 19, 23, 29
b. 1, 11, 19, and 29 are their own inverses; 7 and 13 are inverses of each other, as are 23 and 17

13. If $ax + by \equiv c \pmod{m}$, then there exists an integer k such that $ax + by - mk = c$. Because $d = (a, b, m) \mid ax + by - mk$, it follows that $d \mid c$, which shows that there are no solutions when $d \nmid c$. So suppose that $d \mid c$. Let $a = da'$, $b = db'$, $c = dc'$, and $m = dm'$, so that $(a', b', m') = 1$. When we divide both sides of the original congruence by d, we obtain $a'x + b'y \equiv c' \pmod{m'}$, or $a' \equiv c' - b'y \pmod{m'}$. This congruence has solutions if and only if $g = (a', m') \mid c - b'y$, or equivalently, if and only if $b'y \equiv c' \pmod{g}$ has solutions. Because $(a', b', m') = 1$, and $(a', m') = g$, it follows that $(b', g) = 1$. This means that the last congruence has only one incongruent solution y_0 modulo g. But the m'/g solutions, $y_0, y_0 + g, y_0 + 2g, \ldots, y_0 + (m'/g + 1)g$ are incongruent modulo m'. Each of these yields g incongruent values of x in the congruence $a'x \equiv c' - b'y \pmod{m'}$. Therefore, there are $g(m'/g) = m'$ incongruent solutions of $a'x \equiv c' - b'y \pmod{m'}$. Now let (x_1, y_1) be one solution of the original congruence. Then the d values $x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (d - 1)m'$ are congruent modulo m' but incongruent modulo m. Likewise, the d values $y_1, y_1 + m', y_1 + 2m', \ldots, y_1 + (d - 1)m'$ are congruent modulo m' but incongruent modulo m. So for each solution of $a'x \equiv c' - b'y \pmod{m'}$, there are d^2 solutions of the original congruence. This means that there are $d^2 m' = dm$ solutions to the original congruence.

15. Suppose that $x^2 \equiv 1 \pmod{p^k}$, where p is an odd prime and k is a positive integer. Then $x^2 - 1 \equiv (x + 1)(x - 1) \equiv 0 \pmod{p^k}$. Hence $p^k \mid (x + 1)(x - 1)$. Since $(x + 1) - (x - 1) = 2$ and p is an odd prime, p divides at most one of $x - 1$ and $x + 1$. It follows that either $p^k \mid x + 1$ or $p^k \mid x - 1$, so $p \equiv \pm 1 \pmod{p^k}$.

17. To find the inverse of a modulo m, we must solve the diophantine equation $ax + my = 1$, which can be done using the Euclidean algorithm. Using Corollary 3.13.1 we can find the greatest common divisor in $O(\log^3 m)$ bit operations. The back substitution to find x and y will take

no more than $O(\log m)$ multiplications, each taking $O(\log^2 m)$ operations. Therefore, the total number of operations is $O(\log^3 m) + O(\log m)O(\log^2 m) = O(\log^3 m)$.

Section 4.3

1. $x \equiv 1 \pmod 6$
3. $32 + 60k$
5. $x \equiv 1523 \pmod{2310}$
7. 204
9. 1023
11. 2101
13. We can construct a sequence of k consecutive integers each divisible by a square as follows. Consider the system of congruences $x \equiv 0 \pmod{p_1^2}, x \equiv -1 \pmod{p_2^2}, x \equiv -2 \pmod{p_3^2}, \ldots, x \equiv -k + 1 \pmod{p_k^2}$, where p_k is the kth prime. By the Chinese remainder theorem there is a solution to this simultaneous system of congruences since the moduli are relatively prime. It follows that there is a positive integer N that satisfies each of these congruences. Each of the k integers $N, N + 1, \ldots, N + k - 1$ is divisible by a square since p_j^2 divides $N + j - 1$ for $j = 1, 2, \ldots, k$.
15. Suppose that x is a solution to the system of congruences. Then, $x \equiv a_1 \pmod{m_1}$, so that $x = a_1 + km_1$ for some integer k. Substituting this into the second congruence gives $a_1 + km_1 \equiv a_2 \pmod{m_2}$ or $km_1 = (a_2 - a_1) \pmod{m_2}$, which has a solution in k if and only if $(m_1, m_2) \mid (a_1, a_2)$. Now assume such a solution k_0 exists. Then all incongruent solutions are given by $k = k_0 + m_2 t/(m_1, m_2)$, where t is an integer. Then $x = a_1 + km_1 = a_1 + \left(k_0 + \frac{m_2 t}{(m_1, m_2)}\right) m_1 = a_1 + k_0 m_1 + \frac{m_1 m_2}{(m_1, m_2)} t$. Note that $m_1 m_2/(m_1, m_2) = [m_1, m_2]$, so that if we set $x_1 = a_1 + k_0 m_1$, we have $x = x_1 + [m_1, m_2]t \equiv x_1 \pmod{[m_1, m_2]}$, and so the solution is unique modulo $[m_1, m_2]$.
17. **a.** $x = 430 + 2100j$ **b.** $x = 9102 + 10{,}010j$
19. The basis step $r = 2$ is given by Exercise 15. Suppose that the system of the first k congruences has a unique solution A modulo $M = [m_1, \ldots, m_k]$ and $(m_i, m_j) \mid a_j - a_i$ for $1 \le i < j \le k$. Consider the system $x \equiv A \pmod M$, $x \equiv a_{r+1} \pmod{m_{r+1}}$. First suppose that it has a solution B modulo $[[m_1, m_2, \ldots, m_k], m_{k+1}]$. Then by Exercise 15, $([m_1, m_2, \ldots, m_k], m_{r+1}) \mid B - a_{k+1}$. Since $m_i \mid [m_1, m_2, \ldots, m_k]$ for $1 \le i \le k$, we have $(m_i, m_{k+1}) \mid B - a_{kr+1}$. That is, there exists an integer n_i such that $(m_i, m_{k+1})n_i = B - a_{k+1}$. If we reduce this equation modulo m_i, for $1 \le i \le k$, then $(0, m_{k+1})n_i \equiv m_{k+1} \equiv a_i - a_{k+1} \pmod{m_i}$. If we reduce modulo m_{k+1}, then $(m_i, 0)n_i = m_i n_i \equiv 0 \pmod{m_{k+1}}$. In either case, we have that $(m_i, m_j) \mid a_j - a_i$ for $1 \le i < j \le k + 1$. Conversely, suppose that $(m_i, m_j) \mid a_j - a_i$ for $1 \le i < j \le k + 1$. Then as we have just shown, $([m_1, m_2, \ldots, m_k], m_{k+1}) \mid A - a_{k+1}$. Therefore by Exercise 15 there is a unique solution B to the first $k + 1$ congruences. This completes the induction step.
21. 2101
23. 73800 grams
25. 0000, 0001, 0625, 9376
27. none
29. every 85008 quarter-days, starting at 0
31. If the set of distinct congruences cover the integers modulo the least common multiple of the moduli, then that set will cover all integers. Examine the integers modulo 210, the l.c.m. of the moduli in this set of congruences. The first four congruences take care of all numbers containing

a prime divisor of 2, 3, 5, or 7. The remaining numbers can be examined one at a time, and each can be seen to satisfy one (or more) of the congruences.

33. most likely 318 inches

35. $x = 225a_1 + 1000a_2 + 576a_3 + 1800k$, where k is an integer and a_1 is 3 or 7, a_2 is 2 or 7, and a_3 is 14 or 18

Section 4.4

1. **a.** 1 or 2 (mod 7) **b.** 8 or 37 (mod 49) **c.** 106 or 233 (mod 343)

3. 785 or 1615 (mod 2401)

5. 184, 373, 562, 751, 940, 1129, or 1318 (mod 1323)

7. 279 or 3404 (mod 4375)

9. two

11. Since $(a, p) = 1$, we know that a has an inverse b modulo p. Let $f(x) = ax - 1$. Then $x \equiv b \pmod{p}$ is the unique solution to $f(x) \equiv 0 \pmod{p}$. Since $f'(x) = a \not\equiv 0 \pmod{p}$, we know that $r \equiv b$ lifts uniquely to solutions modulo p^k for all natural numbers k. By Corollary 4.14.1, $r_k = r_{k-1} - f(r_{k-1})\overline{f'(b)} = r_{k-1} - (ar_{k-1} - 1)\overline{a} = r_{k-1} - (ar_{k-1} - 1)b = r_{k-1}(1 - ab) + b$. This gives a recursive formula for lifting b to a solution modulo p^k for every k.

13. There are 1, 3, 3, 9, and 18 solutions for $n = 1, 2, 3, 4$, and $n \geq 5$, respectively.

Section 4.5

1. **a.** $x \equiv 2 \pmod 5$ and $y \equiv 2 \pmod 5$

b. no solutions

c. $x \equiv 3 \pmod 5$ and $y \equiv 0 \pmod 5$; $x \equiv 4 \pmod 5$ and $y \equiv 1 \pmod 5$; $x \equiv 0 \pmod 5$ and $y \equiv 2 \pmod 5$; $x \equiv 1 \pmod 5$ and $y \equiv 3 \pmod 5$; $x \equiv 2 \pmod 5$ and $y \equiv 4 \pmod 5$

3. 0, 1, p, or p^2

5. The basis step, where $k = 1$, is clear by assumption. For the inductive hypothesis assume that $\mathbf{A} \equiv \mathbf{B} \pmod m$ and $\mathbf{A}^k \equiv \mathbf{B}^k \pmod m$. Then using Theorem 4.10 we have $\mathbf{A}^{k+1} = \mathbf{A} \cdot \mathbf{A}^k \equiv \mathbf{A} \cdot \mathbf{B}^k \equiv \mathbf{B} \cdot \mathbf{B}^k = \mathbf{B}^{k+1} \pmod m$.

7. false; take $m = 8$ and $\mathbf{A} = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$

9. **a.** $\begin{bmatrix} 4 & 4 & 3 \\ 4 & 3 & 4 \\ 3 & 4 & 4 \end{bmatrix}$ **b.** $\begin{bmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{bmatrix}$ **c.** $\begin{bmatrix} 5 & 5 & 5 & 4 \\ 5 & 5 & 4 & 5 \\ 5 & 4 & 5 & 5 \\ 4 & 5 & 5 & 5 \end{bmatrix}$

11. **a.** 5 **b.** 5 **c.** 5 **d.** 1

13. In Gaussian elimination, the chief operation is to subtract a multiple of one equation or row from another, in order to put a 0 in a desirable place. Given that an entry a must be changed to 0 by subtracting a multiple of b, we proceed as follows: Let $\overline{b}$ be the inverse of $b \pmod k$. Then $a - (a\overline{b})b \equiv 0 \pmod k$, and elimination proceeds as for real numbers. If $\overline{b}$ doesn't exist, and one cannot swap rows to get an invertible b, then the system is underdetermined.

15. Consider summing the ith row. Let $k = xn + y$, where $0 \leq y < n$. Then x and y must satisfy the diophantine equation $i \equiv a + cy + ex \pmod n$, if k is in the ith row. Then $x - ct$ and $y + et$ is also a solution for every integer t. By Exercise 14 there must be n positive solutions, which yield n numbers k between 0 and n^2. Let $s, s + 1, \ldots, s + n - 1$ be the values of t that give these

solutions. Then the sum of the ith row is $\sum_{r=0}^{n-1}(n(x - c(s+r)) + y + e(s+r)) = n(n+1)$, which is independent of i.

Section 4.6

1. **a.** $7 \cdot 19$ **b.** $29 \cdot 41$ **c.** $41 \cdot 47$ **d.** $47 \cdot 173$ **e.** $131 \cdot 277$ **f.** $29 \cdot 1663$

3. Numbers generated by linear functions where $a > 1$ will not be random in the sense that $x_{2s} - x_k = ax_{2s-1} + b - (ax_{s-1} + b) = a(x_{2s-1} - x_{s-1})$ is a multiple of a for all s. If $a = 1$, then $x_{2s} - x_s = x_0 + sb$. In this case, if $x_0 \neq 0$, then we will not notice if a factor of b that is not a factor of x_0 is a divisor of n.

Section 5.1

1. **a.** $2^8 = 256$ **b.** $2^4 = 16$ **c.** $2^{10} = 1024$ **d.** $2^1 = 2$

3. **a.** by 3 but not by 9 **b.** by both 3 and 9 **c.** by both 3 and 9 **d.** by neither 3 nor 9

5. **a.** $2^1 = 2$ **b.** $2^0 = 1$ **c.** $2^6 = 64$ **d.** $2^0 = 1$

7. **a.** no **b.** no **c.** yes **d.** yes

9. **a.** by neither 3 nor 5 **b.** by both 3 and 5 **c.** by neither 3 nor 5 **d.** by 5 but not by 3

11. if and only if the number of digits is a multiple of 3 (respectively, 9)

13. if and only if the number of digits is a multiple of 6 in each case

15. if and only if the number of digits is a multiple of d, where $d \mid b - 1$

17. A palindromic integer with $2k$ digits has the form $(a_k a_{k-1} \ldots a_1 a_1 a_2 \ldots a_k)_{10}$. Using the test for divisibility by 11 developed in this section, we find that $a_k - a_{k-1} + \cdots \pm a_1 \mp a_1 \pm a_2 \mp \cdots - a_k = 0$, and so $(a_k a_{k-1} \ldots a_1 a_1 a_2 \ldots a_k)_{10}$ is divisible by 11.

19. an integer $a_k a_{k-1} \ldots a_1 a_0$ is divisible by 37 if and only if $a_0 a_1 a_2 + a_3 a_4 a_5 + a_6 a_7 a_8 + \cdots$ is; $37 \nmid 443{,}692$; $37 \mid 11{,}092{,}785$

21. **a.** no **b.** by 5 but not by 2 **c.** by neither 5 nor 13 **d.** yes

23. 6

25. no

Section 5.2

1. answer is person-dependent

3. once

5. $W \equiv k + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] - [N/4000] \pmod 7$

7. answer is person-dependent

9. 2500

11. If the 13th falls on the same day of the week on two consecutive months, then the number of days in the first month is congruent to 0 modulo 7, and the only such month is February during a nonleap year. If February 13th is a Friday, then January 1st is a Thursday.

13. Let $W = 5$ and $k = 13$ in the formula for the day of the week to obtain $5 \equiv 13 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \pmod 7$. This implies that $[2.6m - 0.2] \equiv 6 + 2C - Y - [Y/4] - [C/4] \pmod 7$. For every pair of values of C and Y, there is an m satisfying this congruence because $[2.6m - 0.2]$ takes on all possible remainders modulo 7 as the month varies from March to December and m takes on the values from 0 to 10.

15. Months with 31 days are March, May, July, August, October, December, and January (considered to be in the previous year); the corresponding values of m are 1, 3, 5, 6, 8, 10, and 11, respectively. Given Y and C, let $k = 31$ to obtain $W \equiv 31 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \equiv 3 + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \pmod 7$. To determine the days of the week the 31st falls on, first let m equal 1, 3, 5, 6, 8, 10, and reduce modulo 7. Finally, decrease the year by one and find the new values of Y and C, and let $m = 11$ and reduce modulo 7. The values of W we find tell us the days of the week on which the 31st falls.

Section 5.3

1. **a.** Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 7$, with team i drawing a bye if $2i \equiv k \pmod 7$. Round 1: 1-7, 2-6, 3-5, 4-bye; round 2: 2-7, 3-6, 4-5, 1-bye; round 3: 1-2, 3-7, 4-6, 5-bye; round 4: 1-3, 4-7, 5-6, 2-bye; round 5: 1-4, 2-3, 5-7, 6-bye; round 6: 1-5, 2-4, 6-7, 3-bye; round 7: 1-6, 2-5, 3-4, 7-bye.
b. Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 7$, $i, j \neq 8$; team i plays team 8 if $2i \equiv k \pmod 7$.
c. Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 9$, with team i drawing a bye if $2i \equiv k \pmod 9$.
d. Teams i and j are paired in round k if and only if $i + j \equiv k \pmod 9$, $i, j \neq 10$; team i plays team 10 if $2i \equiv k \pmod 9$.

3. **a.** home teams in round 1: 4 and 5; round 2: 2 and 3; round 3: 1 and 5; round 4: 3 and 4; round 5: 1 and 2
b. home teams in round 1: 5, 6, and 7; round 2: 2, 3, and 4; round 3: 1, 6, and 7; round 4: 3, 4, and 5; round 5: 1, 2, and 7; round 6: 4, 5, and 6; round 7: 1, 2, and 3
c. home teams in round 1: 6, 7, 8, and 9; round 2: 2, 3, 4, and 5; round 3: 1, 7, 8, and 9; round 4: 3, 4, 5, and 6; round 5: 1, 2, 8, and 9; round 6: 4, 5, 6, and 7; round 7: 1, 2, 3, and 9; round 8: 5, 6, 7, and 8; round 9: 1, 2, 3, and 4

Section 5.4

1. Let k be the six-digit number on the license plate of a car. We can assign this car the space numbered $h(k) = k \bmod 101$. When a car is assigned the same space as another car we can assign it to the space $(h(k) + g(k)) \bmod 101$, where $g(k) = (k \bmod 99) + 1$. When this space is occupied we next try $(h(k) + 2g(k)) \bmod 101$, then $(h(k) + 3g(k)) \bmod 101$, and so on. All spaces are examined since $(g(k), 101) = 1$.

3. **a.** It is clear that m memory locations will be probed as $j = 0, 1, 2, \ldots, m - 1$. To see that they are all distinct, and hence that every memory location is probed, assume that $h_i(K) \equiv h_j(K) \pmod m$. Then $h(K) + iq \equiv h(K) + jq \pmod m$. From this it follows that $iq \equiv jq \pmod m$, and, as $(q, m) = 1$, we have $i \equiv j \pmod m$ by Corollary 4.4.1. Therefore $i = j$ since i and j are both less than m.
b. It is clear that m memory locations will be probed as $j = 0, 1, 2, \ldots, m - 1$. To see that they are all distinct, and hence that every memory location is probed, assume that $h_i(K) \equiv h_j(K) \pmod m$. Then $h(K) + iq \equiv h(K) + jq \pmod m$. From this it follows that $iq \equiv jq \pmod m$, and, as $(q, m) = 1$, we have $i \equiv j \pmod m$ by Corollary 4.4.1. Therefore $i = j$ since i and j are both less than m.

5. 558, 1002, 2174, 4035

Section 5.5

1. **a.** 0 **b.** 0 **c.** 1 **d.** 1 **e.** 0 **f.** 1

3. a. 0 b. 1 c. 0

5. a. 7 b. 1 c. 4

7. Transposition means that adjacent digits are in the wrong order. Suppose, first, that the first two digits, x_1 and x_2, or, equivalently, the fourth and fifth digits, are exchanged, and the error is not detected. Then $x_7 \equiv 7x_1 + 3x_2 + x_3 + 7x_4 + 3x_5 + x_6 \equiv 7x_2 + 3x_1 + x_3 + 7x_4 + 3x_5 + x_6 \pmod{10}$. It follows that $7x_1 + 3x_2 \equiv 7x_2 + 3x_1 \pmod{10}$ or $4x_1 \equiv 4x_2 \pmod{10}$. By Corollary 4.4.1, $x_1 \equiv x_2 \pmod{5}$. This is equivalent to $|x_1 - x_2| = 5$, as x_1 and x_2 are distinct single digits. Similarly, if the second and third (or fifth and sixth) digits are transposed, then $2x_2 \equiv 2x_3 \pmod{10}$, which again reduces to $x_2 \equiv x_3 \pmod{5}$ by Corollary 4.4.1. Also, if the third and fourth digits are transposed, then $6x_3 \equiv 6x_4 \pmod{10}$ and $x_3 \equiv x_4 \pmod{5}$, similarly as before. The reverse argument will complete the proof.

9. a. 0 b. 3 c. 4 d. X

11. a. valid b. not valid c. valid d. valid e. not valid

13. 0-07-289905-0

15. a. no b. yes c. yes d. no

17. It can.

19. a. yes b. no

21. a. 94

b. If x_i is misentered as y_i, then if the congruence defining x_{10} holds, we see that $ax_i \equiv ay_i \pmod{11}$ by setting the two definitions of x_{10} congruent. From this, it follows from Corollary 4.4.1 that $x_i \equiv y_i \pmod{11}$, and so $x_i = y_i$. If the last digit, x_{11}, is misentered as y_{11}, then the congruence defining x_{11} will hold if and only if $x_{11} = y_{11}$.

c. Suppose that x_i is misentered as y_i and x_j is misentered as y_j, with $i < j < 10$. Suppose that both of the congruences defining x_{10} and x_{11} hold. Then by setting the two versions of each congruence congruent to each other we obtain $ax_i + bx_j \equiv ay_i + by_j \pmod{11}$ and $cx_i + dx_j \equiv cy_i + dy_j \pmod{11}$, where $a \neq b$ and $c \neq d$. If $ad - bc \not\equiv 0 \pmod{11}$, then the coefficient matrix is invertible and we can multiply both sides of this system of congruences by the inverse to obtain $x_i = y_i$ and $x_j = y_j$. Indeed, after (tediously) checking each possible choice of a, b, c, and d, we find that all the matrices are invertible modulo 11.

23. a. 1 b. 1 c. 6

25. Errors involving a difference of 7 cannot be detected: 0 for 7, 1 for 8, 2 for 9, or vice versa. All others can be detected.

27. a. 1 b. X c. 2 d. 8

29. Yes. Assume not and compare the expressions modulo 11, to get a congruence of the form $ad_i + bd_j \equiv ad_j + bd_i \pmod{11}$, which reduces to $(a - b)d_i \equiv (a - b)d_j \pmod{11}$. Because $0 < a - b < 11$ and 11 is prime, it follows that $d_i \equiv d_j \pmod{11}$. Because these are digits between 0 and X, they must be equal.

Section 6.1

1. We have $10! + 1 = 1(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8)10 + 1 = 1 \cdot 12 \cdot 12 \cdot 45 \cdot 56 \cdot 10 + 1 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) + 1 \equiv 0 \pmod{11}$. Therefore, 11 divides $10! + 1$.

3. 9

5. 6

7. 436

9. 2

11. 6

13. $(3^5)^2 \equiv 243^2 \equiv 1^2 \equiv 1 \pmod{11^2}$

15. **a.** $x \equiv 9 \pmod{17}$ **b.** $x \equiv 17 \pmod{19}$

17. Suppose that p is an odd prime. Then Wilson's theorem tells us that $(p-1)! \equiv -1 \pmod{p}$. Since $(p-1)! = (p-3)!(p-1)(p-2) \equiv (p-3)!(-1)(-2) \equiv 2 \cdot (p-3)! \pmod{p}$, this implies that $2 \cdot (p-3)! \equiv -1 \pmod{p}$.

19. Since $(a, 35) = 1$, we have $(a, 7) = (a, 5) = 1$, so we may apply Fermat's little theorem to get $a^{12} - 1 = (a^6)^2 - 1 \equiv 1^2 - 1 = 0 \pmod{7}$, and $a^{12} - 1 = (a^4)^3 - 1 \equiv 1^3 - 1 = 0 \pmod{5}$. Both 5 and 7 divide $a^{12} - 1$, so 35 must also divide it.

21. When n is even, so is n^7, and when n is odd, so is n^7. It follows that $n^7 \equiv n \pmod{2}$. Similarly, since $n^3 \equiv n \pmod{3}$, it follows that $n^7 = (n^3)^2 \cdot n \equiv n^2 \cdot n \equiv n^3 \equiv n \pmod{3}$. We also know by Fermat's little theorem that $n^7 \equiv n \pmod{7}$. Since $42 = 2 \cdot 3 \cdot 7$, it follows that $n^7 \equiv n \pmod{42}$.

23. By Fermat's little theorem, $\sum_{k=1}^{p-1} k^{p-1} \equiv \sum_{k=1}^{p-1} 1 = p - 1 \equiv -1 \pmod{p}$.

25. By Fermat's little theorem, $a \equiv a^p \equiv b^p \equiv b \pmod{p}$; hence $b = a + kp$ for some integer k. Then by the binomial theorem, $b^p = (a + kp)^p = a^p + \binom{p}{1} a^{p-1} kp + p^2 N$, where N is some integer. Then $b^p \equiv a^p + p^2 a^{p-1} k + p^2 N \equiv a^p \pmod{p^2}$.

27. 641 (at $k = 8$)

29. Suppose that p is prime. Then by Fermat's little theorem, $a^p \equiv a \pmod{p}$ for every integer a. Also, by Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$, so $a(p-1)! \equiv -a \pmod{p}$. It follows that $a^p + (p-1)!a \equiv a + (-a) \equiv 0 \pmod{p}$. Consequently, $p \mid a^p + (p-1)!a$.

31. Since $p - 1 \equiv -1$, $p - 2 \equiv -2$, $\ldots$, $(p+1)/2 \equiv -(p-1)/2 \pmod{p}$, we have $((p-1)/2)!^2 \equiv -(p-1)! \equiv 1 \pmod{p}$. (Because $p \equiv 3 \pmod{4}$ the minus signs work out.) If $x^2 \equiv 1 \pmod{p}$, then $p \mid x^2 - 1 = (x-1)(x+1)$, so $x \equiv \pm 1 \pmod{p}$.

33. Suppose that $p \equiv 1 \pmod{4}$. Let $y = \pm((p-1)/2)!$. Then $y^2 \equiv ((p-1)/2)!^2 \equiv ((p-1)/2)!^2(-1)^{(p-1)/2} \equiv (1 \cdot 2 \cdot 3 \cdots (p-1)/2)((-(p-1)/2) \cdots (-3) \cdot (-2) \cdot (-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)/2 \cdot (p+1)/2 \cdots (p-3)(p-2)(p-1) = (p-1)! \equiv -1 \pmod{p}$, where we have used Wilson's theorem. Now suppose that $x^2 \equiv -1 \pmod{p}$. Then $x^2 \equiv y^2 \pmod{p}$. Hence $(x^2 - y^2) = (x - y)(x + y) \equiv 0 \pmod{p}$. It follows that $p \mid x - y$ or $p \mid x + y$, so $x \equiv \pm y \pmod{p}$.

35. If n is composite and $n \neq 4$, then Exercise 16 shows that $(n-1)!/n$ is an integer, so $[((n-1)! + 1)/n - [(n-1)!/n]] = [(n-1)!/n + 1/n - (n-1)!/n] = [1/n] = 0$. If $n = 4$, then the same expression is also equal to 0. But if n is prime, then by Wilson's theorem, $(n-1)! = Kn - 1$ for some integer K. So $[((n-1)! + 1)/n - [(n-1)!/n]] = [(Kn - 1 + 1)/n - [(Kn - 1)/n]] = [K - (K-1)] = 1$. Therefore, the sum increases by 1 exactly when n is prime, so it equals $\pi(n)$.

37. Suppose that n and $n + 2$ are twin primes. Then by Wilson's theorem, $(n-1)! \equiv -1 \pmod{n}$. Hence, $4((n-1)! + 1) + n \equiv 4 \cdot 0 + n \equiv 0 \pmod{n}$. Also, since $n + 2$ is prime it follows from Wilson's theorem that $(n+1)! \equiv -1 \pmod{n+2}$, so $(n+1)n \cdot (n-1)! \equiv (-1)(-2)(n-1)! \equiv 2(n-1)! \equiv -1 \pmod{n+2}$. Hence $4((n-1)! + 1) + n \equiv 2(2 \cdot (n-1)!) + 4 + n \equiv 2 \cdot (-1) + 4 + n = n + 2 \equiv 0 \pmod{n+2}$. Since $(n, n+2) = 1$ it follows that $4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}$.

39. Note that $1 \cdot 2 \cdots (p-1) \equiv (p+1)(p+2) \cdots (2p-1) \pmod{p}$. Each factor is relatively prime to p, so $1 \equiv (p+1)(p+2) \cdots (2p-1)/(1 \cdot 2 \cdots (p-1)) \pmod{p}$. Thus $2 \equiv (p+1)(p+2) \cdots (2p-1)2p/(1 \cdot 2 \cdots (p-1)p) = \binom{2p}{p} \pmod{p}$.

41. We first note that $1^p \equiv 1 \pmod{p}$. Now suppose that $a^p \equiv a \pmod{p}$. Then by Exercise 40 we see that $(a+1)^p \equiv a^p + 1 \pmod{p}$. But by the inductive hypothesis $a^p \equiv a \pmod{p}$, so $a^p + 1 \equiv a + 1 \pmod{p}$. Hence, $(a+1)^p \equiv a + 1 \pmod{p}$.

43. **a.** If $c < 26$, then c extra cards are put into the deck above the card, so it ends up in the $(2c)$th position; $2c < 52$, so $b = 2c$. If $c \geq 26$, then $c - 26 - 1$ extra cards are put into the deck above the card, but 26 cards are taken away above it, so it ends up in the $b = (c - 26 - 1 + c - 26) = (2c - 53)$th place. Then $b = 2c - 53 \equiv 2c \pmod{53}$.
b. 52

45. There are two cases. Assume first that $a_k \equiv 0 \pmod{p}$ and $b_j \equiv 0 \pmod{p}$, where $k \neq j$. Then two of the products $a_i b_i \equiv 0 \pmod{p}$, and this would contradict Wilson's theorem if the $a_i b_i$ formed a complete system, since the product of all but one of them must be $-1 \pmod{p}$, not 0. For the second case, assume without loss of generality that $a_p \equiv b_p \equiv 0 \pmod{p}$. Then by Wilson's theorem, $a_1 a_2 \cdots a_{p-1} \equiv b_1 b_2 \cdots b_{p-1} \equiv -1 \pmod{p}$. Then $a_1 b_1 \cdots a_{p-1} b_{p-1} \equiv (-1)^2 = 1 \pmod{p}$. If the set were a complete system, the last product would have been $\equiv -1 \pmod{p}$.

47. The basis step for induction is Wilson's theorem. Assume $(p-1)!^{p^{k-1}} \equiv -1 \pmod{p^k}$. Then $(p-1)!^{p^k} \equiv ((p-1)!^{p^{k-1}})^p \equiv (-1 + mp^k)^p \equiv -1 + \binom{p}{1} mp^k + \cdots + (mp^k)^p \equiv -1 \pmod{p^{k+1}}$, where we have used the fact that $p \mid \binom{p}{j}$ for $j \neq 0$ or p.

49. If n is prime, then n divides the binomial coefficient $\binom{n}{r}, r = 1, 2, \ldots, n-1$. It follows that $(x-a)^n$ and $x^n - a^n$ are congruent modulo n as polynomials because the coefficient of x^r in $(x-a)^n$ is congruent to 0 modulo n for $r = 1, 2, \ldots, n-1$. By Fermat's little theorem, it follows that $a^n \equiv a \pmod{n}$, so that $(x-a)^n$ and $x^n - a$ are congruent modulo n as polynomials. Now suppose that n is a composite integer with $n > 1$. We know that n has a prime divisor q. Suppose that q^k is the greatest power of q dividing n. A short argument shows that $q^k \nmid \binom{n}{q} = n(n-1)\cdots(n-q+1)/q!$ and $(q^k, a^{n-q}) = 1$. It follows that the coefficient of x^q in $(x-a)^n$ is not congruent to 0 modulo p, but the coefficient of $x^n - a$ is 0. It follows that $(x-a)^n$ and $x^n - a$ are not congruent as polynomials modulo n.

Section 6.2

1. $3^{90} \equiv 1 \pmod{91}$, but $91 = 7 \cdot 13$

3. Either computation by hand or a computational program shows that $2^{161038} \equiv 2 \pmod{161038}$.

5. $(n-a)^n \equiv (-a)^n \equiv -(a^n) \equiv -a \equiv (n-a) \pmod{n}$

7. Raise the congruence $2^{2^m} ; \equiv ; -1 \pmod{F_m}$ to the $(2^{2^m} - m)$th power, to obtain $2^{2^{2^m}} ; \equiv ; 1 \pmod{2^{2^m}} ; + ; 1)$, which says that $2^{F_m - 1} \equiv 1 \pmod{F_m}$.

9. Suppose that n is a pseudoprime to the bases a and b. Then $b^n \equiv b \pmod{n}$ and $a^n \equiv a \pmod{n}$. It follows that $(ab)^n \equiv a^n b^n \equiv ab \pmod{n}$. Hence, n is a pseudoprime to the base ab.

11. **a.** If n is a pseudoprime to the base ab, then $(ab)^{n-1} \equiv 1 \pmod{n}$, so $1 \equiv a^{n-1} b^{n-1} \equiv 1 \cdot b^{n-1} \pmod{n}$, which implies that n is a pseudoprime to the base b, a contradiction.
b. Let $a_1, a_2, \ldots, a_r$ be the bases to which n is a pseudoprime and for which $(a_i, n) = 1$ for each i. Then by part (a) we know that, for each i, n is not a pseudoprime to the base ba_i. Thus we have $2r$ different elements relatively prime to n. Then by the definition of $\phi(n)$, we have $r \leq \phi(n)/2$.

13. A computation shows that $2^{1387} \equiv 2 \pmod{1387}$, so 1387 is a pseudoprime. But $1387 - 1 = 2 \cdot 693$ and $2^{693} \equiv 512 \pmod{1387}$, which is all that must be checked, since $s = 1$. Thus 1387 fails Miller's test and hence is not a strong pseudoprime.

15. Note that $25{,}326{,}001 - 1 = 2^4 \cdot 1{,}582{,}875 = 2^s t$. With this value of t, we see with the help of computational software that $2^t \equiv -1 \pmod{25{,}326{,}001}$, $3^t \equiv -1 \pmod{25{,}326{,}001}$, and $5^t \equiv 1 \pmod{25{,}326{,}001}$.

17. Suppose that $c = 7 \cdot 23 \cdot q$, with q an odd prime, is a Carmichael number. Then by Theorem 6.7 we must have $7 - 1 \mid c - 1$, so $c = 7 \cdot 23 \cdot q \equiv 1 \pmod 6$. Solving this yields $q \equiv 5 \pmod 6$. Similarly, $23 - 1 \mid c - 1$, so $7 \cdot 23 \cdot q \equiv 1 \pmod{22}$. Solving this yields $q \equiv 19 \pmod{22}$. If we apply the Chinese remainder theorem to these two congruences, we obtain $q \equiv 41 \pmod{66}$, that is, $q = 41 + 66k$ for some k. Then we must have $q - 1 \mid c - 1$, which is $40 + 66k \mid 7 \cdot 23 \cdot (41 + 66k) - 1$. So there is an integer m such that $m(40 + 66k) = 6600 + 10626k = 160 + 6440 + 10626k = 160 + 161(40 + 66k)$. Therefore, 160 must be a multiple of $40 + 66k$, which happens only when $k = 0$. Therefore, $q = 41$ is the only such prime.

19. We have $32{,}111{,}197{,}185 - 1 = 321{,}197{,}184 = 4 \cdot 80{,}299{,}296 = 18 \cdot 17{,}844{,}288 = 22 \cdot 14{,}599{,}872 = 28 \cdot 11{,}471{,}328 = 36 \cdot 8{,}922{,}144 = 136 \cdot 2{,}361{,}744$, so $p - 1 \mid 321{,}197{,}185 - 1$ for every prime p that divides 321,197,185. Therefore, by Theorem 5.7, 321,197,185 is a Carmichael number.

21. We can assume that $b < n$. Then b has fewer than $\log_2 n$ bits. Also, $t < n$, so t has fewer than $\log_2 n$ bits. It takes at most $\log_2 n$ multiplications to calculate b^{2^s}, so it takes $O(\log_2 n)$ multiplications to calculate $b^{2^{\log_2 t}} = b^t$. Each multiplication is of two $(\log_2 n)$-bit numbers and so takes $O((\log_2 n)^2)$ operations. In all, we have $O((\log_2 n)^3)$ operations.

Section 6.3

1. **a.** $\{1, 5\}$ **b.** $\{1, 2, 4, 5, 7, 8\}$ **c.** $\{1, 3, 7, 9\}$ **d.** $\{1, 3, 5, 9, 11, 13\}$
e. $\{1, 3, 5, 7, 9, 11, 13, 15\}$ **f.** $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$

3. If $(a, m) = 1$, then $(-a, m) = 1$, so $-c_i$ must appear among the c_j. Also $c_i \not\equiv -c_i \pmod m$, else $2c_i \equiv 0 \pmod m$ and so $(c_i, m) \neq 1$. Hence, the elements in the sum can be paired so that each pair sums to 0 (mod m), and thus the entire sum is 0 (mod m).

5. 1

7. 11

9. Since $a^2 \equiv 1 \pmod 8$ whenever a is odd, $a^{12} = (a^2)^6 \equiv 1 \pmod 8$ whenever $(a, 32{,}760) = 1$. Euler's theorem tells us that $a^{\phi(9)} = a^6 \equiv 1 \pmod 9$ whenever $(a, 9) = 1$, so $a^{12} = (a^6)^2 \equiv 1 \pmod 9$ whenever $(a, 32{,}760) = 1$. Furthermore, Fermat's little theorem tells us that $a^4 \equiv 1 \pmod 5$ whenever $(a, 5) = 1$, $a^6 \equiv 1 \pmod 7$ whenever $(a, 7) = 1$, and $a^{12} \equiv 1 \pmod{13}$ whenever $(a, 13) = 1$. It follows that $a^{12} \equiv (a^4)^3 \equiv 1 \pmod 5$, $a^{12} \equiv (a^6)^2 \equiv 1 \pmod 7$, and $a^{12} \equiv 1 \pmod{13}$ whenever $(a, 32{,}760) = 1$. Since $32{,}760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ and the moduli 8, 9, 5, 7, and 13 are pairwise relatively prime, we see that $a^{12} \equiv 1 \pmod{32{,}760}$.

11. **a.** $x \equiv 9 \pmod{14}$ **b.** $x \equiv 13 \pmod{15}$ **c.** $x \equiv 7 \pmod{16}$

13. **a.** $x \equiv 37 \pmod{187}$ **b.** $x \equiv 23 \pmod{30}$ **c.** $x \equiv 6 \pmod{210}$ **d.** $x \equiv 150{,}999 \pmod{554{,}268}$

15. 1

17. $\phi(13) = 12$, $\phi(14) = 6$, $\phi(15) = 8$, $\phi(16) = 8$, $\phi(17) = 16$, $\phi(18) = 6$, $\phi(19) = 18$, $\phi(20) = 8$

19. If $(a, b) = 1$ and $(a, b - 1) = 1$, then $a \mid (b^{k\phi(a)} - 1)/(b - 1)$, which is a base b repunit. If $(a, b - 1) = d > 1$, then d divides every repunit of length $k(b - 1)$ and $(a/d) \mid (b^{k\phi(a/d)} - 1)/(b - 1)$, and these sets intersect infinitely often.

Section 7.1

1. **a.** f is completely multiplicative since for all positive integers m and n, $f(mn) = 0 = 0 \cdot 0 = f(m) \cdot f(n)$.
b. f is not completely multiplicative since $f(6) = 2$, but $f(2) \cdot f(3) = 2 \cdot 2 = 4$.
c. f is not completely multiplicative since $f(6) = 3$, but $f(2) \cdot f(3) = \frac{2}{2} \cdot \frac{3}{2} = \frac{3}{2}$.
d. f is not completely multiplicative since $f(4) = \log(4) > 1$, but $f(2) \cdot f(2) = \log(2) \cdot \log(2) < 1$.
e. f is completely multiplicative since for every positive integer m and n, $f(mn) = (mn)^2 = m^2n^2 = f(m) \cdot f(n)$.
f. f is not completely multiplicative since $f(4) = 4! = 24$, but $f(2) \cdot f(2) = 2!2! = 4$.
g. f is not completely multiplicative since $f(6) = 7$, but $f(2) \cdot f(3) = 3 \cdot 4 = 12$.
h. f is not completely multiplicative since $f(4) = 4^4 = 256$, but $f(2) \cdot f(2) = 2^2 2^2 = 16$.
i. f is completely multiplicative since for every positive integer m and n, $f(mn) = \sqrt{mn} = \sqrt{m}\sqrt{n} = f(m) \cdot f(n)$.

3. We have the following prime factorizations of 5186, 5187, and 5188: $5186 = 2 \cdot 2593$, $5187 = 3 \cdot 7 \cdot 13 \cdot 19$, and $5188 = 2^2 1297$. Hence, $\phi(5186) = \phi(2)\phi(2593) = 1 \cdot 2592 = 2592$, $\phi(5187) = \phi(3)\phi(7)\phi(13)\phi(19) = 2 \cdot 6 \cdot 12 \cdot 18 = 2592$, and $\phi(5188) = \phi(2^2)\phi(1297) = 2 \cdot 1296 = 2592$. It follows that $\phi(5186) = \phi(5187) = \phi(5188)$.

5. 7, 9, 14, 18

7. 35, 39, 45, 52, 56, 70, 72, 78, 84, 90

9. The nth term of this sequence is $\phi(2n)$.

11. multiples of 3

13. powers of 2 greater than 1

15. If n is odd, then $(2, n) = 1$ and $\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n)$. If n is even, say $n = 2^s t$ with t odd, then $\phi(2n) = \phi(2^{s+1}t) = \phi(2^{s+1})\phi(t) = 2^s\phi(t) = 2(2^{s-1}\phi(t)) = 2(\phi(2^s)\phi(t)) = 2(\phi(2^s t)) = 2\phi(n)$.

17. $n = 2^k p_1 p_2 \cdots p_r$, where each p_i is a distinct Fermat prime

19. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the prime-power factorization for n. If $n = 2\phi(n)$, then $p_1^{a_1} \cdots p_r^{a_r} = 2\prod_{j=1}^{r} p_j^{a_j - 1}(p_j - 1)$. This implies that $p_1 \cdots p_r = 2\prod_{j=1}^{r}(p_j - 1)$. If any p_j is an odd prime, then the factor $(p_j - 1)$ is even and must divide the product on the left-hand side. But there can be at most one factor of 2 on the left-hand side and it is accounted for by the factor of 2 in front of the product on the right-hand side. Therefore, no odd primes appear in the product. That is, $n = 2^j$ for some j.

21. Since $(m, n) = p$, p divides one of the terms, say n, exactly once, so $n = kp$ with $(m, k) = 1 = (n, k)$. Then $\phi(n) = \phi(kp) = \phi(k)\phi(p) = \phi(k)(p - 1)$, and $\phi(mp) = p\phi(m)$ by the formula in Example 7.7. Consequently, $\phi(mn) = \phi(mkp) = \phi(mp)\phi(k) = (p\phi(m))(\phi(n)/(p - 1))$.

23. Let $p_1, \ldots, p_r$ be those primes dividing a but not b. Let $q_1, \ldots, q_s$ be those primes dividing b but not a. Let $r_1, \ldots, r_t$ be those primes dividing a and b. Let $P = \prod(1 - (1/p_i))$, $Q = \prod(1 - (1/q_i))$, and $R = \prod(1 - (1/r_i))$. Then $\phi(ab) = abPQR = aPRbQR/R = \phi(a)\phi(b)/R$. But $\phi((a, b)) = (a, b)R$, so $R = \phi((a, b))/(a, b)$ and we have $\phi(ab) = \phi(a)\phi(b)/R = (a, b)\phi(a)\phi(b)/\phi((a, b))$, as desired. The final conclusion now follows immediately from the obvious fact that $\phi((a, b)) < (a, b)$ when $(a, b) > 1$.

25. Assume that there are only finitely many primes, $2, 3, \ldots, p$. Let $N = 2 \cdot 3 \cdot 5 \cdots p$. Then $\phi(N) = 1$ since there is exactly one positive integer less than N that is relatively prime to N, namely 1, because

every prime is a factor of N. However, $\phi(N) = \phi(2)\phi(3)\phi(5)\cdots\phi(p) = 1 \cdot 2 \cdot 4 \cdots (p-1) > 1$. This contradiction shows that there must be infinitely many primes.

27. From the formula for the ϕ function, we see that if $p \mid n$, then $p - 1 \mid \phi(n)$. Since $\phi(n)$ is finite, there are only finitely many possibilities for prime divisors of n. Further, if p is prime and $p^a \mid n$, then $p^{a-1} \mid \phi(n)$. Hence, $a \leq \log_p \phi(n) + 1$. Therefore, each of the finitely many primes that might divide n may appear to only finitely many exponents. This gives only finitely many possibilities for n.

29. As suggested, we take $k = 2 \cdot 3^{6j+1}$ with $j \geq 1$ and suppose that $\phi(n) = k$. From the formula for $\phi(n)$ we see that $\phi(n)$ has a factor of $p - 1$, which is even, for every odd prime that divides n. Since there is only one factor of 2 in k, there is at most one odd prime divisor of n. Further, since $2 \parallel k$ and $n > 4$, we know that $4 \nmid n$. Since k is not a power of 2, we know that an odd prime p must divide n. So n is of the form p^a or $2p^a$. Recall that $\phi(p^a) = \phi(2p^a)$. It remains to discover the values of p and a. If $a = 1$, then $\phi(p^a) = p - 1 = 2 \cdot 3^{6j+1}$. But then $p = 2 \cdot 3^{6j+1} + 1 = 6 \cdot (3^6)^j + 1 \equiv (-1)(1)^j + 1 \equiv 0 \pmod 7$. Hence, $p = 7$. But $\phi(7) = 6 = 2 \cdot 3^{6j+1}$ implies that $j = 0$, contrary to hypothesis, so this is not a solution. Therefore, $a > 1$ and we have $\phi(p^a) = (p-1)p^{a-1} = 2 \cdot 3^{6j+1}$, from which we conclude that $p = 3$ and $a = 6j + 2$. Therefore, the only solutions are $n = 3^{6j+2}$ and $n = 2 \cdot 3^{6j+2}$.

31. If $n = p^r m$, where $p \nmid m$, then $\phi(p^r m) = (p^r - p^{r-1})\phi(m) \mid p^r m - 1$; hence, $p \mid 1$ or $r = 1$. So n is square-free. If $n = pq$, then $\phi(pq) = (p-1)(q-1) \mid pq - 1$. Then $p - 1 \mid (pq - 1) - (p-1)q = q - 1$. Similarly, $q - 1 \mid p - 1$, a contradiction.

33. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Let P_i be the property that an integer is divisible by p_i. Let S be the set $\{1, 2, \ldots, n-1\}$. To compute $\phi(n)$ we need to count the elements of S with none of the properties $P_1, P_2, \ldots, P_k$. Let $n(P_{i_1}, P_{i_2}, \ldots, P_{i_m})$ be the number of elements of S with all of properties $P_{i_1}, P_{i_2}, \ldots, P_{i_m}$. Then $n(P_{i_1}, \ldots, P_{i_m}) = n/(p_{i_1} p_{i_2} \cdots p_{i_m})$. By the principle of inclusion–exclusion, we have $\phi(n) = n - (n/p_1 + n/p_2 + \cdots + n/p_k) + (n/(p_1p_2) + n/(p_1p_3) + \cdots + n/(p_{k-1}p_k)) - \cdots + (-1)^k \cdot n/(p_1 \cdots p_k) = n(1 - \sum_{p_i \mid n} 1/p_i + \sum_{p_{i_1}p_{i_2} \mid n} 1/(p_{i_1}p_{i_2}) - \sum_{p_{i_1}p_{i_2}p_{i_3} \mid n} 1/(p_{i_1}p_{i_2}p_{i_3}) + \cdots + (-1)^k \cdot n/(p_1 \cdots p_k))$. On the other hand, notice that each term in the expansion of $(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$ is obtained by choosing either 1 or $-1/p_i$ from each factor and multiplying the choices together. This gives each term the form $(-1)^m/(p_{i_1}p_{i_2} \cdots p_{i_m})$. Note that each term can occur in only one way. Thus $n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k) = n(1 - \sum_{p_i \mid n} 1/p_i + \sum_{p_{i_1}p_{i_2} \mid n} 1/(p_{i_1}p_{i_2}) - \cdots + (-1)^k n/(p_1 \cdots p_k)) = \phi(n)$.

35. Note that $1 \leq \phi(m) \leq m - 1$ for $m > 1$. Hence, if $n \geq 2$, then $n > n_1 > n_2 > \cdots \geq 1$, where $n_1 = \phi(n)$ and $n_i = \phi(n_{i-1})$ for $i > 1$. Since n_i, $i = 1, 2, 3, \ldots$, is a decreasing sequence of positive integers, there must be a positive integer r such that $n_r = 1$.

37. Note that the definition of $f * g$ can also be expressed as $(f * g)(n) = \sum_{a \cdot b = n} f(a)g(b)$. Then the fact that $f * g = g * f$ is evident.

39. **a.** If either $m > 1$ or $n > 1$, then $mn > 1$ and one of $\iota(m)$ or $\iota(n)$ is equal to 0. Then $\iota(mn) = 0 = \iota(m)\iota(n)$. Otherwise, $m = n = 1$ and we have $\iota(mn) = 1 = 1 \cdot 1 = \iota(m)\iota(n)$. Therefore, $\iota(n)$ is multiplicative.

b. $(\iota * f)(n) = \sum_{d \mid n} \iota(d) f(n/d) = \iota(1) f(n/1) = f(n)$ since $\iota(d) = 0$ except when $d = 1$; $(f * \iota)(n) = (\iota * f)(n) = f(n)$ by Exercise 37

41. Let $h = f * g$ and let $(m, n) = 1$. Then $h(mn) = \sum_{d \mid mn} f(d)g(mn/d)$. Since $(m, n) = 1$, each divisor d of mn can be expressed in exactly one way as $d = ab$, where $a \mid m$ and $b \mid n$. Then $(a, b) = 1$ and $(m/a, n/b) = 1$. Thus there is a one-to-one correspondence between the divisors d of mn

and the pairs of products ab, where $a \mid m$ and $b \mid n$. Then $h(mn) = \sum_{a|m,\, b|n} f(ab)g(mn/(ab)) = \sum_{a|m,\, b|n} f(a)f(b)g(m/a)g(n/b) = \sum_{a|m} f(a)g(m/a) \cdot \sum_{b|n} f(b)g(n/b) = h(m)h(n)$.

43. **a.** -1 **b.** -1 **c.** 1 **d.** 1 **e.** -1 **f.** -1 **g.** 1

45. Let $f(n) = \sum_{d|n} \lambda(d)$. Then by Theorem 7.8, f is multiplicative. Now $f(p^t) = \lambda(1) + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^t) = 1 - 1 + 1 - \cdots + (-1)^t = 0$ if t is odd and $= 1$ if t is even. Then $f(p_1^{a_1}p_2^{a_2} \cdots p_r^{a_r}) = \prod f(p_i^{a_i}) = 0$ if any a_i is odd (n is not a square) and $= 1$ if all a_i are even (n is a square).

47. If f and g are completely multiplicative and m and n are positive integers, then $(fg)(mn) = f(mn) \cdot g(mn) = f(m) \cdot f(n) \cdot g(m) \cdot g(n) = f(m) \cdot g(m) \cdot f(n) \cdot g(n) = (fg)(m) \cdot (fg)(n)$, so fg is also completely multiplicative.

49. $f(mn) = \log mn = \log m + \log n = f(m) + f(n)$

51. **a.** 2 **b.** 3 **c.** 1 **d.** 4 **e.** 8 **f.** 15

53. Let $(m, n) = 1$. Then by the additivity of f we have $f(mn) = f(m) + f(n)$. Thus $g(mn) = 2^{f(mn)} = 2^{f(m)+f(n)} = 2^{f(m)}2^{f(n)} = g(m)g(n)$.

Section 7.2

1. **a.** 48 **b.** 399 **c.** 2340 **d.** $2^{101} - 1$ **e.** 6912 **f.** 813,404,592 **g.** 15,334,088 **h.** 13,891,399,238,731,734,720

3. perfect squares

5. **a.** 6, 11 **b.** 10, 17 **c.** 14, 15, 23 **d.** 33, 35, 47 **e.** none **f.** 44, 65, 83

7. Note that $\tau(p^{k-1}) = k$ whenever p is prime and k is an integer greater than 1. Hence the equation $\tau(n) = k$ has infinitely many solutions.

9. squares of primes

11. $n^{\tau(n)/2}$

13. **a.** The nth term is $\sigma(2n)$.
b. The nth term is $\sigma(n) - \tau(n)$.
c. The nth term is the least positive integer m with $\tau(m) = n$.
d. The nth term is the number of solutions to the equation $\sigma(x) = n$.

15. 2, 4, 6, 12, 24, 36

17. Let a be the largest highly composite integer less than or equal to n. Note that $2a$ is less than or equal to $2n$ and has more divisors than a, and hence $\tau(2a) > \tau(a)$. By Exercise 16 there must be a highly composite integer b with $a < b \leq 2a$. If $b \leq n$, this contradicts the choice of a. Therefore, $n < b \leq 2n$. It follows that there must be a highly composite integer k with $2^m < k \leq 2^{m+1}$ for every nonnegative integer m. Therefore, there are at least m highly composite integers less than or equal to 2^m. Thus the mth highly composite integer is less than or equal to 2^m.

19. 1, 2, 4, 6, 12, 24, 36, 48

21. $1 + p^k$

23. Suppose that a and b are positive integers with $(a, b) = 1$. Then $\sum_{d|ab} d^k = \sum_{d_1|a,\, d_2|b} (d_1d_2)^k = \sum_{d_1|a} d_1^k \cdot \sum_{d_2|b} d_2^k = \sigma_k(a)\sigma_k(b)$.

25. prime numbers

27. Let $n = p_1^{a_1}p_2^{a_2} \cdots p_r^{a_r}$, and let x and y be integers such that $[x, y] = n$. Then $x \mid n$ and $y \mid n$, so $x = p_1^{b_1}p_2^{b_2} \cdots p_r^{b_r}$ and $y = p_1^{c_1}p_2^{c_2} \cdots p_r^{c_r}$, where b_i and c_i are between 0 and a_i. Since $[x, y] = n$, we must have $\max(b_i, c_i) = a_i$ for each i. Then one of b_i and c_i must be equal to

a_i and the other can range over $0, 1, 2, \ldots, a_i$. Therefore, we have $2a_i + 1$ ways to choose the pair (b_i, c_i) for each i. Thus in total we can choose the exponents $b_1, b_2, \ldots, b_r, c_1, c_2, \ldots, c_r$ in $(2a_1 + 1)(2a_2 + 1) \cdots (2a_r + 1) = \tau(n^2)$ ways.

29. Suppose that n is composite. Then $n = ab$, where a and b are integers with $1 < a \leq b < n$. It follows that either $a \geq \sqrt{n}$ or $b \geq \sqrt{n}$. Consequently, $\sigma(n) \geq 1 + a + b + n > 1 + \sqrt{n} + n > n + \sqrt{n}$. Conversely, suppose that n is prime. Then $\sigma(n) = n + 1$, so $\sigma(n) \leq n + \sqrt{n}$. Hence, $\sigma(n) > n + \sqrt{n}$ implies that n is composite.

31. For $n = 1$, the statement is true. Suppose that $\sum_{j=1}^{n-1} \tau(j) = 2\sum_{j=1}^{[\sqrt{n-1}]}[(n-1)/j] - [\sqrt{n-1}]^2$. For the induction step, if n is not a perfect square, it suffices to show that $\tau(n) = 2\sum_{j=1}^{[\sqrt{n-1}]}([n/j] - [(n-1)/j]) = 2\sum_{j \leq [\sqrt{n-1}],\, j|n} 1$, which is true by the definition of $\tau(n)$, since there is one factor less than $\sqrt{n}$ for every factor greater than $\sqrt{n}$. Note that if n is a perfect square, we must add the term $2\sqrt{n} - (2\sqrt{n} - 1) = 1$ to the last two sums. For $n = 100$, we have $\sum_{j=1}^{100} \tau(j) = 2\sum_{j=1}^{10}[100/j] - 100 = 482$.

33. Let $a = \prod p_i^{a_i}$ and $b = \prod p_i^{b_i}$, and let $c_i = \min(a_i, b_i)$ for each i. We first prove that the product $\prod_{p_i} \sum_{j=0}^{c_i} p_i^j \sigma(p_i^{a_i+b_i-2j}) = \sum_{d|(a,b)} d\sigma(ab/d^2)$. To see this, let d be any divisor of (a, b), say $d = \prod p_i^{d_i}$. Then $d_i \leq c_i$ for each i, so each of the terms $p_i^{d_i}\sigma(p_i^{a_i+b_i-2d_i})$ appears in exactly one of the sums in the product. Therefore, if we expand the product, we will find, exactly once, the term $\prod_{p_i} p_i^{d_i}\sigma(p_i^{a_i+b_i-2d_i}) = d\sigma\left(\prod_{p_i} p_i^{a_i+b_i-2d_i}\right) = d\sigma\left(\prod_{p_i}(p_i^{a_i}/p_i^{d_i})(p_i^{b_i}/p_i^{d_i})\right) = d\sigma((a/d)(b/d))$. This proves the first identity. Next, consider the sum $\sum_{j=0}^{c}(p^{a+b-j} + p^{a+b-j-1} + \cdots + p^j)$, where $c = \min(a, b)$. The term p^k appears in this sum once each time that $k = a + b - j$, which happens exactly when $a + b - c \leq k \leq a + b$, that is, $c + 1$ times. On the other hand, in the expansion of the product $(p^a + p^{a-1} + \cdots + 1)(p^b + p^{b-1} + \cdots + 1) = \sigma(p^a)\sigma(p^b)$, the same term p^k appears whenever $k = (a - m) + (b - n)$, where $0 \leq m \leq a$ and $0 \leq n \leq b$. Each of m and n determines the other, so p^k appears exactly $\min(a + 1, b + 1) = c + 1$ times. Given this identity, we have $\sigma(a)\sigma(b) = \prod_{p_i}(p_i^{a_i} + p_i^{a_i-1} + \cdots + 1)(p_i^{b_i} + p_i^{b-1} + \cdots + 1) = \prod_{p_i} \sum_{j=0}^{c_i}(p_i^{a_i+b_i-j} + p_i^{a_i+b_i-j-1} + \cdots + p_i^j)$, which is the right side of the identity, as we proved above.

35. From Exercises 52 and 53 in Section 7.1, we know that the arithmetic function $f(n) = 2^{\omega(n)}$ is multiplicative. Therefore, the Dirichlet product $h(n) = \sum_{d|n} 2^{\omega(d)} = f * g(n)$, where $g(n) = 1$, is also multiplicative (see Exercise 41 in Section 7.1). Since $\tau(n)$ and n^2 are multiplicative, so is $\tau(n^2)$. Therefore, it is sufficient to prove the identity for n equal to a prime power, p^a. We have $\tau(p^{2a}) = 2a + 1$. On the other hand, $\sum_{d|p^a} 2^{\omega(d)} = \sum_{i=0}^{a} 2^{\omega(p^i)} = 1 + \sum_{i=1}^{a} 2^1 = 2a + 1$.

37. $\phi(1)\phi(2) \cdots \phi(n)$

39. If p and $p + 2$ are prime, then $\phi(p + 2) = p + 1 = \sigma(p)$. If $2^p - 1$ is prime, then $\phi(2^{p+1}) = 2^p = \sigma(2^p - 1)$.

Section 7.3

1. 6, 28, 496, 8128, 33,550,336, 8,589,869,056

3. **a.** 31 **b.** 127 **c.** 127

5. 12, 18, 20, 24, 30, 36

7. Suppose that $n = p^k$, where p is prime and k is a positive integer. Then $\sigma(p^k) = (p^{k+1} - 1)/(p - 1)$. Note that $2p^k - 1 < p^{k+1}$ since $p \geq 2$. It follows that $p^{k+1} - 1 < 2(p^{k+1} - p^k) = 2p^k(p - 1)$, so $(p^{k+1} - 1)/(p - 1) < 2p^k = 2n$. It follows that $n = p^k$ is deficient.

9. Suppose that n is abundant or perfect. Then $\sigma(n) \geq 2n$. Suppose that $m = nk$ for some integer $k > 1$. The divisors of m include the integers kd whenever $d \mid n$, as well as the number 1. Hence, $\sigma(m) \geq 1 + \sum_{d|n} kd = 1 + k\sum_{d|n} d = 1 + k\sigma(n) \geq 1 + 2nk > 2kn = 2m$. Hence, m is abundant.

11. If p is any prime, then $\sigma(p) = p + 1 < 2p$, so p is deficient; and we know that there are infinitely many primes.

13. (See Exercises 6 and 9.) For a positive integer a, let $n = 3^a \cdot 5 \cdot 7$, and compute $\sigma(n) = \sigma(3^a \cdot 5 \cdot 7) = ((3^{a+1} - 1)/(3 - 1))(5 + 1)(7 + 1) = (3^{a+1} - 1)24 = 3^{a+1}24 - 24 = 2 \cdot 3^a(36) - 24 = 2 \cdot 3^a(35) + 2 \cdot 3^a - 24 = 2n + 2 \cdot 3^a - 24$, which will be greater than $2n$ whenever $a \geq 3$. This demonstrates infinitely many odd abundant integers.

15. **a.** The prime factorizations of 220 and 284 are $220 = 2^2 \cdot 5 \cdot 11$ and $284 = 2^2 \cdot 71$. Hence, $\sigma(220) = \sigma(2^2)\sigma(5)\sigma(11) = 7 \cdot 6 \cdot 12 = 504$ and $\sigma(284) = \sigma(2^2)\sigma(71) = 7 \cdot 72 = 504$. Since $\sigma(220) = \sigma(284) = 220 + 284 = 504$, it follows that 220 and 284 form an amicable pair.
b. The prime factorizations of 1184 and 1210 are $1184 = 2^5 \cdot 37$ and $1210 = 2 \cdot 5 \cdot 11^2$. Hence, $\sigma(1184) = \sigma(2^5)\sigma(37) = 63 \cdot 38 = 2394$ and $\sigma(1210) = \sigma(2)\sigma(5)\sigma(11^2) = 3 \cdot 6 \cdot 133 = 2394$. Since $\sigma(1184) = \sigma(1210) = 1184 + 1210 = 2394$, 1184 and 1210 form an amicable pair.
c. The prime factorizations of 79,750 and 88,730 are $79{,}750 = 2 \cdot 5^3 \cdot 11 \cdot 29$ and $88{,}730 = 2 \cdot 5 \cdot 19 \cdot 467$. Hence, $\sigma(79{,}750) = \sigma(2)\sigma(5^3)\sigma(11)\sigma(29) = 3 \cdot 156 \cdot 12 \cdot 30 = 168{,}480$ and similarly $\sigma(88{,}730) = \sigma(2)\sigma(5)\sigma(19)\sigma(467) = 3 \cdot 6 \cdot 20 \cdot 468 = 168{,}480$. Since $\sigma(79{,}750) = \sigma(88{,}730) = 79{,}750 + 88{,}730 = 168{,}480$, it follows that 79,750 and 88,730 form an amicable pair.

17. $\sigma(120) = \sigma(2^3 \cdot 3 \cdot 5) = \sigma(2^3)\sigma(3)\sigma(5) = 15 \cdot 4 \cdot 6 = 360 = 3 \cdot 120$

19. $\sigma(2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19) = (2^8 - 1) \cdot (3^5 - 1)/2 \cdot (5 + 1) \cdot (7 + 1) \cdot (11^3 - 1)/10 \cdot (17 + 1) \cdot (19 + 1) = 255 \cdot 121 \cdot 6 \cdot 8 \cdot 133 \cdot 18 \cdot 20 = 70{,}912{,}195{,}200 = 5 \cdot 14{,}182{,}439{,}040$

21. Suppose that n is 3-perfect and 3 does not divide n. Then $\sigma(3n) = \sigma(3)\sigma(n) = 4 \cdot 3n = 12n = 4 \cdot 3n$. Hence, $3n$ is 4-perfect.

23. 908,107,200

25. $\sigma(\sigma(16)) = \sigma(31) = 32 = 2 \cdot 16$

27. Certainly if r and s are integers greater than 1, then $\sigma(rs) \geq rs + s + 1$. Suppose $n = 2^q t$ is superperfect with t odd and $t > 1$. Then $2n = 2^{q+1}t = \sigma(\sigma(2^q t)) = \sigma\left(\left(2^{q+1} - 1\right)\sigma(t)\right) \geq (2^{q+1} - 1)\sigma(t) + \sigma(t) + 1 > 2^{q+1}\sigma(t) \geq 2^{q+t}(t + 1)$. Then $t > t + 1$, a contradiction. Therefore, we must have $n = 2^q$, in which case we have $2n = 2^{q+1} = \sigma(\sigma(2^q)) = \sigma\left(2^{q+1} - 1\right) = \sigma(2n - 1)$. Therefore, $2n - 1 = 2^{q+1} - 1$ is prime.

29. **a.** yes **b.** no **c.** yes **d.** no

31. **a.** Note that $M_n(M_n + 2) = (2^n - 1)(2^n + 1) = 2^{2n} - 1$. If $2n + 1$ is prime, then $\phi(2n + 1) = 2n$ and $2^{2n} \equiv 1 \pmod{2n + 1}$. Thus $2n + 1 \mid 2^{2n} - 1 = M_n(M_n + 2)$. Therefore, $2n + 1 \mid M_n$ or $2n + 1 \mid M_n + 2$.
b. $23 \nmid 2049$, so $23 \mid 2047 = M_{11}$; $47 \nmid 8{,}388{,}609$ so $47 \mid 8{,}388{,}607 = M_{23}$

33. Since m is odd, $m^2 \equiv 1 \pmod 8$, so $n = p^a m^2 \equiv p^a \pmod 8$. By Exercise 32(a), $a \equiv 1 \pmod 4$, so $p^a \equiv p^{4k} p \equiv p \pmod 8$, since p^{4k} is an odd square. Therefore, $n \equiv p \pmod 8$.

35. First suppose that $n = p^a$, where p is an odd prime and a is a positive integer. Then $\sigma(n) = (p^{a+1} - 1)/(p - 1) < p^{a+1}/(p - 1) = np/(p - 1) = n/(1 - (1/p)) \leq n/(\frac{2}{3}) = 3n/2$, so $\sigma(n) \neq 2n$ and n is not perfect. Next suppose that $n = p^a q^b$, where p and q are primes and a and b are positive integers. Then $\sigma(n) = (p^{a+1} - 1)/(p - 1) \cdot (q^{b+1} - 1)/(q - 1) < p^{a+1}q^{b+1}/((p - 1)(q - 1)) = npq/((p - 1)(q - 1)) = n/((1 - (1/p))(1 - (1/q))) \leq n/(\frac{2}{3} \cdot \frac{4}{5}) = 15n/8 < 2n$. Hence, $\sigma(n) \neq 2n$ and n is not perfect.

37. integers of the form p^5 and p^2q, where p and q are primes

39. Suppose that $M_n = 2^n - 1 = a^k$, with n and k integers greater than 1. Then a must be odd. If $k = 2j$, then $2^n - 1 = (a^j)^2$. Since $n > 1$ and the square of an odd integer is congruent to 1 modulo 4, reduction of the last equation modulo 4 yields the contradiction $-1 \equiv 1 \pmod 4$. Therefore, k must be odd. Then $2^n = a^k + 1 = (a+1)(a^{k-1} - a^{k-2} + \cdots + 1)$. So $a + 1 = 2^m$ for some integer m. Then $2^n - 1 = (2^m - 1)^k \geq 2^{mk} - k2^{m(k-1)} \geq 2^{m(k-1)} \geq 2^{2m}$, so $n \geq 2m$. Then reduction modulo 2^{2m} gives $-1 \equiv k2^m - 1 \pmod{2^{2m}}$, or, since k is odd, $2^m \equiv 0 \pmod{2^{2m}}$, a contradiction.

Section 7.4

1. **a.** 0 **b.** 1 **c.** -1 **d.** 0 **e.** -1 **f.** 1 **g.** 0

3. 0, -1, -1, -1, 0, -1, 1, -1, 0, -1, -1, respectively

5. 1, 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95

7. 1, 0, -1, -1, -2, -1, -2, -2, -2, -1, respectively

9. Since $\mu(n)$ is 0 for non-square-free n, is 1 for n a product of an even number of distinct primes, and is -1 for n a product of an odd number of distinct primes, the sum $M(n) = \sum_{i=1}^{n} \mu(i)$ is unaffected by the non-square-free numbers, but counts 1 for every even product and -1 for every odd product. Thus $M(n)$ counts how many more even products than odd products there are.

11. For any nonnegative integer k, the numbers $n = 36k + 8$ and $n + 1 = 36k + 9$ are consecutive and divisible by $4 = 2^2$ and $9 = 3^2$, respectively. Therefore, $\mu(36k + 8) + \mu(36k + 9) = 0 + 0 = 0$.

13. 3

15. Let $h(n) = n$ be the identity function. Then from Theorem 7.7 we have $h(n) = n = \sum_{d|n} \phi(n)$. Then by the Möbius inversion formula $\phi(n) = \sum_{d|n} \mu(d)h(n/d) = \sum_{d|n} \mu(d)(n/d) = n \sum_{d|n} \mu(d)/d$.

17. Since μ and f are multiplicative, so is their product μf, by Exercise 46 of Section 7.1. The summatory function $\sum_{d|n} \mu(d)f(d)$ is also multiplicative by Theorem 7.17. Therefore, it suffices to prove the proposition for n a prime power. We compute $\sum_{d|p^a} \mu(d)f(d) = \mu(p^a)f(p^a) + \mu(p^{a-1})f(p^{a-1}) + \cdots + \mu(p)f(p) + \mu(1)f(1)$. But for exponents j greater than 1, $\mu(p^j) = 0$, so this sum equals $\mu(p)f(p) + \mu(1)f(1) = -f(p) + 1$.

19. $\phi(n)/n$

21. $(-1)^k \prod_{i=1}^{k} p_i$

23. Since both sides of the equation are known to be multiplicative (see the solution to Exercise 35 in Section 7.2, Exercise 46 in Section 7.1, Theorem 7.17, and Theorem 7.14), it suffices to prove the identity for $n = p^a$, a prime power. On one hand, $\sum_{d|p^a} \mu^2(d) = \mu^2(p) + \mu^2(1) = 1 + 1 = 2$. On the other hand, $\omega(p^a) = 1$, so the right side is $2^1 = 2$.

25. Let λ play the role of f in the identity of Exercise 17. Then the left side equals $\prod_{j=1}^{k}(1 - \lambda(p_j)) = \prod_{j=1}^{k}(1 - (-1)) = 2^k = 2^{\omega(n)}$.

27. By Theorem 7.15, $\mu * \nu(n) = \sum_{d|n} \mu(d)\nu(n/d) = \sum_{d|n} \mu(d) = \iota(n)$.

29. Since $\nu(n)$ is identically 1, we have $F(n) = \sum_{d|n} f(d) = \sum_{d|n} f(d)\nu(n/d) = f * \nu(n)$. If we Dirichlet multiply both sides on the right by μ, then $F * \mu = f * \nu * \mu = f * \iota = f$.

31. From the Möbius inversion formula, Exercise 30, and Theorem 7.15, $\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) = \sum_{d|n} \mu(d)(\log n - \log d) = \sum_{d|n} \mu(d) \log(n) - \sum_{d|n} \mu(d) \log(d) = \log n \sum_{d|n} \mu(d) -$

$\sum_{d|n} \mu(d) \log(d) = (\log n)\nu(n) - \sum_{d|n} \mu(d) \log(d) = -\sum_{d|n} \mu(d) \log(d)$, since $\nu(n) = 0$ if $n \neq 1$ and $\log n = 0$ if $n = 1$.

Section 8.1

1. DWWDF NDWGD ZQ
3. IEXXK FZKXC UUKZC STKJW
5. READ MY LIPS
7. 12
9. AN IDEA IS LIKE A CHILD NONE IS BETTER THAN YOUR OWN FROM CHINESE FORTUNE COOKIE
11. 9, 12
13. THIS MESSAGE WAS ENCIPHERED USING AN AFFINE TRANSFORMATION
15. $C \equiv 7P + 16 \pmod{26}$

Section 8.2

1. VSPFXH HIPKLB KIPMIE GTG
3. TJEVT EESPZ TJIAN IARAB GSHWQ HASBU BJGAO XYACF XPHML AWVMO XANLB GABMS HNEIA TIEZV VWNQF TLEZF HJWPB WKEAG AENOF UACIH LATPR RDADR GKTJR XJDWA XXENB KA
5. Let n be the key length, and suppose that $k_1, k_2, \ldots, k_n$ are the numerical equivalents of the letters of the keyword. If $p_i = p_j$ are two plaintext characters separated by a multiple of the key length, when we break the plaintext into blocks of length n, p_i and p_j will be in the same position in their respective blocks, say the mth position. So when we encrypt them, we get $c_i \equiv p_i + k_m \equiv p_j + k_m \equiv c_j \pmod{26}$.
7. The key is YES, and the plaintext is MISTA KESAR EAPAR TOFBE INGHU MANAP PRECI ATEYO URMIS TAKES FORWH ATTHE YAREP RECIO USLIF ELESS ONSTH ATCAN ONLYB ELEAR NEDTH EHARD WAYUN LESSI TISAF ATALM ISTAK EWHIC HATLE ASTOT HERSC ANLEA RNFRO M.
9. The key is BIRD, and the plaintext is IONCE HADAS PARRO WALIG HTUPO NMYSH OULDE RFORA MOMEN TWHIL EIWAS HOEIN GINAV ILLAG EGARD ENAND IFELT THATI WASMO REDIS TINGU ISHED BYTHA TCIRC UMSTA NCETH ATISH OULDH AVEBE ENBYA NYEPA ULETI COULD HAVEW ORN.
11. The key is SAGAN, and the plaintext is BUTTH EFACT THATS OMEGE NIUSE SWERE LAUGH EDATD OESNO TIMPL YTHAT ALLWH OAREL AUGHE DATAR EGENI USEST HEYLA UGHED ATCOL UMBUS THEYL AUGHE DATFU LTONT HEYLA UGHED ATTHE WRIGH TBROT HERSB UTTHE YALSO LAUGH EDATB OZOTH ECLOW N.
13. RL OQ NZ OF XM CQ KG QI VD AZ
15. TO SLEEP PERCHANCE TO DREAM
17. 3, 24, 24, 25
19. $\mathbf{C} \equiv \mathbf{AP} \pmod{26}$. Multiplying both sides on the left by $\mathbf{A}$ gives $\mathbf{AC} \equiv \mathbf{A^2P} \equiv \mathbf{IP} \equiv \mathbf{P} \pmod{26}$. The congruence $\mathbf{A^2} \equiv \mathbf{I} \pmod{26}$ follows since $\mathbf{A}$ is involutory. It follows that $\mathbf{A}$ is also a decrypting matrix.
21. $C \equiv \begin{bmatrix} 11 & 6 \\ 2 & 13 \end{bmatrix} P \pmod{26}$

23. If the plaintext is grouped into blocks of size m, we may take $[m, n]/m$ of these blocks to form a super-block of size $[m, n]$. If $\mathbf{A}$ is the $m \times m$ encrypting matrix, form the $[m, n] \times [m, n]$ matrix $\mathbf{B}$ with $[m, n]/m$ copies of $\mathbf{A}$ on the diagonal and zeros elsewhere. Then $\mathbf{B}$ will encrypt $[m, n]/m$ blocks of size m at once. Similarly, if $\mathbf{C}$ is the $n \times n$ encrypting matrix, form the corresponding $[m, n] \times [m, n]$ matrix $\mathbf{D}$. Then by Exercise 22, $\mathbf{BD}$ is an $[m, n] \times [m, n]$ encrypting matrix which does everything at once.

25. Multiplication of $[\,0 \quad \ldots \quad 0 \quad 1 \quad 0 \quad \ldots \quad 0\,]$, with the 1 in the ith place, by $[P_1 \quad P_2 \quad \ldots \quad P_n]^T$ yields the 1×1 matrix $[\,P_i\,]$ (T denotes transpose). If the jth row of a matrix $\mathbf{A}$ is $[\,0 \quad \ldots \quad 0 \quad 1 \quad 0 \quad \ldots \quad 0\,]$, then $\mathbf{A}\,[\,P_1 \quad P_2 \quad \ldots \quad P_n\,]^T = [\,C_1 \quad C_2 \quad \ldots \quad C_n\,]$ gives $C_j = P_i$. So if every row of $\mathbf{A}$ has its 1 in a different column, then each C_j is equal to a different P_i. Hence, $\mathbf{A}$ is a "permutation" matrix.

27. $P \equiv \begin{bmatrix} 17 & 4 \\ 1 & 7 \end{bmatrix} C + \begin{bmatrix} 22 \\ 15 \end{bmatrix} \pmod{26}$

29. TOXIC WASTE

31. Make a frequency count of the trigraphs and use a published English language count of frequencies of trigraphs. Then proceed as in Exercise 30. There are 12 variables to determine, so four guesses are needed.

33. yes

35. 01 1101 1010

37. RENDEZVOUZ

39. Let $p_1p_2 \cdots p_m$ and $q_1q_2 \cdots q_m$ be two different plaintext bit streams. Let $k_1, k_2, \ldots, k_m$ be the keystream by which these two plaintexts are encrypted. Note that for $i = 1, 2, \ldots, m$, $E_{k_i}(p_i) + E_{k_i}(q_i) = k_i + p_i + k_i + q_i = 2k_i + p_i + q_i \equiv p_i + q_i \pmod 2$. Therefore, by adding corresponding bits of the ciphertext streams, we get the sums of the corresponding bits of the plaintext streams. This partial information may lead to successful cryptanalysis of encrypted messages.

Section 8.3

1. 14 17 17 27 11 17 65 76 07 76 14

3. BEAM ME UP

5. We encrypt messages using the transformation $C \equiv P^{11} \pmod{31}$. The decrypting exponent is the inverse of 11 modulo 30 since $\phi(31) = 30$. But 11 is its own inverse modulo 30 since $11 \cdot 11 \equiv 121 \equiv 1 \pmod{30}$. It follows that 11 is both the encrypting and decrypting exponent.

Section 8.4

1. 151, 97

3. Since a block of ciphertext p is less than n, we must have $(p, n) = p$ or q. Therefore, the cryptanalyst has a factor of n.

5. 1215 1224 1471 0023 0116

7. GREETINGS

9. 2145 0672 0724 1404 1630

11. No. This is the same as using the RSA cryptosystem with encryption key (e_1e_2, n). It is no easier, or more difficult, to discover the inverse of $e = e_1e_2$ than it is to discover the inverse of either of the factors modulo $\phi(n)$.

13. Suppose that P is a plaintext message and the two encrypting exponents are e_1 and e_2. Let $a = (e_1, e_2)$. Then there exist integers x and y such that $e_1x + e_2y = a$. Let $C_1 \equiv P^{e_1} \pmod{n}$ and $C_2 \equiv P^{e_2} \pmod{n}$ be the two ciphertexts. Since C_1, C_2, e_1, and e_2 are known to the decipherer, and since x and y are relatively easy to compute, it is also easy to compute $C_1^x C_2^y \equiv P^{e_1x} P^{e_2y} = P^{e_1x+e_2y} = P^a \pmod{n}$. If $a = 1$, then P has been recovered. If a is fairly small, then it may not be too difficult to compute ath roots of P^a and thereby recover P.

15. Encryption works the same as for the two-prime case. For decryption, we must compute an inverse d for e modulo $\phi(n) = (p-1)(q-1)(r-1)$, where $n = pqr$ the product of three primes. Then we proceed as in the case with two primes.

Section 8.5

1. **a.** yes **b.** no **c.** yes **d.** no

3. Proceed by induction. Certainly, $a_1 < 2a_1 < a_2$. Suppose $\sum_{j=1}^{n-1} a_j < a_n$. Then $\sum_{j=1}^{n} a_j = \sum_{j=1}^{n-1} a_j + a_n < a_n + a_n = 2a_n < a_{n+1}$.

5. $(17, 51, 85, 7, 14, 45, 73)$

7. NUTS

9. If the multipliers and moduli are $(w_1, m_1), (w_2, m_2), \ldots, (w_r, m_r)$, then the inverses $\overline{w_1}, \overline{w_2}, \ldots, \overline{w_r}$ can be computed with respect to their corresponding moduli. Then we multiply and reduce successively by $(\overline{w_r}, m_r), (\overline{w_{r-1}}, m_{r-1}), \ldots, (\overline{w_1}, m_1)$. The result will be the plaintext sequence of easy knapsack problems.

11. $8 \cdot 21 \cdot 95$

13. For $i = 1, 2, 3, \ldots, n$, we have $b^{\alpha_i} \equiv a_i \pmod{m}$. Then $b^S \equiv P \equiv (b^{\alpha_1})^{x_1} (b^{\alpha_2})^{x_2} \cdots (b^{\alpha_n})^{x_n} \equiv b^{\alpha_1 x_1 + \cdots + \alpha_n x_n} \pmod{m}$. Then $S \equiv \alpha_1 x_1 + \cdots + \alpha_n x_n \pmod{\phi(m)}$. Since $S + k\phi(m)$ is also a logarithm of P to the base b, we may take the congruence to be an equation. Since each x_i is 0 or 1, this becomes an additive knapsack problem on the sequence $(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Section 8.6

1. 90

3. 476

5. Let $k_1, k_2, \ldots, k_n$ be the private keys for parties 1 through n, respectively. There are n steps in this protocol. The first step is for each party i to compute the least positive residue of $r^{k_i} \pmod{p}$ and send this value y_i to the $(i+1)$th party. (The nth party sends his value to the first party.) Now the ith party has the value y_{i-1} (where we take y_0 to be y_n). The second step is for each party i to compute the least positive residue of $y_{i-1}^{k_i} \pmod{p}$ and send this value to the $(i+1)$th party. Now the ith party has the least positive residue of $r^{k_{i-1}+k_{i-2}} \pmod{p}$. This process is continued for a total of n steps. However, at the nth step, the computed value is not sent on to the next party. Then the ith party will have the least positive residue of $r^{k_{i-1}+k_{i-2}+\cdots+k_1+k_n+k_{n-1}+\cdots+k_{i+1}+k_i} \pmod{p}$, which is exactly the value of K desired.

7. **a.** 0371 0354 0858 0858 0087 1369 0354 0000 0087 1543 1797 0535
b. 0833 0475 0074 0323 0621 0105 0621 0865 0421 0000 0746 0803 0105 0621 0421

9. **a.** If $n_i < n_j$, the block sizes are chosen small enough so that each block is unique modulo n_i. Since $n_i < n_j$, each block will be unique modulo n_j after applying the transformation D_{k_j}. Therefore, we can apply E_{k_j} to $D_{k_i}(P)$ and retain uniqueness of blocks. The argument is similar when $n_i > n_j$.

b. If $n_i < n_j$, individual j receives $E_{k_j}(D_{k_i}(P))$ and knows an inverse for e_j modulo $\phi(n_j)$. So he can apply $D_{k_j}(E_{k_j}(D_{k_i}(P))) = D_{k_i}(P)$. Since he also knows e_i, he can apply $E_{k_i}(D_{k_i}(P)) = P$ and discover the plaintext P. If $n_i > n_j$, individual j receives $D_{k_i}(E_{k_j}(P))$. Since he knows e_i he can apply $E_{k_i}(D_{k_i}(E_{k_j}(P))) = E_{k_j}(P)$. Since he also knows $\overline{e_j}$ he can apply $D_{k_j}(E_{k_j}(P)) = P$ and discover the plaintext P.
c. Since only individual i knows $\overline{e_i}$, only he can apply the transfomation D_{k_i} and thereby make $E_{k_i}(D_{k_i}(P))$ intelligible.
d. We have $n_i = 2867 > n_j = 2537$, so we compute $D_{k_i}(E_{k_j}(P))$. Both n_i and n_j are greater than 2525, so we use blocks of 4. REGARDS FRED becomes 1704 0600 1703 1805 1704 0323 (adding an X to fill out the last block). Now $e_i = 11$ and $\phi(n_i) = 2760$, so $\overline{e_i} = 251$. We apply $E_{k_j}(P) \equiv P^{e_j} \equiv P^{13} \pmod{2537}$ to each block and get 1943 0279 0847 0171 1943 0088. Then we apply $D_{k_i}(E) \equiv E^{251} \pmod{2867}$ and get 0479 2564 0518 1571 0479 1064. Now since $n_j < n_i$ individual j must send $E_{k_i}(D_{k_j}(P))$, $e_j = 13$, $\phi(2537) = 2436$, and $\overline{e_j} = 937$. Then $D_{k_j}(P) \equiv P^{937} \pmod{2537}$ and $E_{k_i}(D) = D^{11} \pmod{2867}$. The ciphertext for REGARDS ZELDA is 1609 1802 0790 2508 1949 0267.

11. $k_1 \equiv 4 \pmod 8$, $k_2 \equiv 5 \pmod 9$, $k_3 \equiv 2 \pmod{11}$

13. The three shadows from Exercise 11 are $k_1 = 4$, $k_2 = 5$, and $k_3 = 2$. We solve the system $K_0 \equiv 4 \pmod 8$, $K_0 \equiv 5 \pmod 9$, and $K_0 \equiv 2 \pmod{11}$, where the moduli are the m_i's. The Chinese remainder theorem yields $K_0 \equiv 68 \pmod{8 \cdot 9 \cdot 11}$. Then $K = K_0 - tp = 68 - 13 \cdot 5 = 3$.

Section 9.1

1. **a.** 4 **b.** 4 **c.** 6 **d.** 4

3. **a.** $\phi(6) = 2$, and $5^2 \equiv 1 \pmod 6$
b. $\phi(11) = 10$, and $2^2 \equiv 4$, $2^5 \equiv -1$, $2^{10} \equiv 1 \pmod{11}$

5. Only 1, 5, 7, 11 are relatively prime to 12. Each one squared is congruent to 1, but $\phi(12) = 4$.

7. There are 2: 3 and 5.

9. That $\operatorname{ord}_n a = \operatorname{ord}_n \overline{a}$ follows from the fact that $a^t \equiv 1 \pmod n$ if and only if $\overline{a}^t \equiv 1 \pmod n$. To see this, suppose that $a^t \equiv 1 \pmod n$. Then $\overline{a}^t \equiv \overline{a}^t a^t a^t \equiv (\overline{a}^t a^t) a^t \equiv (a\overline{a})^t a^t \equiv 1^t \cdot 1 \equiv 1 \pmod n$. The converse is shown in a similar manner.

11. $[r, s]/(r, s) \le \operatorname{ord}_n ab \le [r, s]$, where $r = \operatorname{ord}_n a$ and $s = \operatorname{ord}_n b$

13. Let $r = \operatorname{ord}_m a^t$. Then $a^{tr} \equiv 1 \pmod m$; hence, $tr \ge ts$ and $r \ge s$. Since $1 \equiv a^{st} \equiv (a^t)^s \pmod m$, we have $s \ge r$.

15. Suppose that r is a primitive root modulo the odd prime p. Then $r^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors q of $p - 1$ since no smaller power than the $(p - 1)$th of r is congruent to 1 modulo p. Conversely, suppose that $r^{(p-1)/q} \not\equiv 1 \pmod p$ for all prime divisors of $p - 1$. Suppose that r is not a primitive root of p. Then there is an integer t such that $r^t \equiv 1 \pmod p$ with $t < p - 1$. Since t must divide $p - 1$, we have $p - 1 = st$ for some positive integer s greater than 1. Then $(p - 1)/s = t$. Let q be a prime divisor of s. Then $(p - 1)/q = ts/q$, so $r^{(p-1)/q} = r^{ts/q} = (r^t)^{s/q} \equiv 1 \pmod p$. This contradicts the original assumption, so r is a primitive root modulo p.

17. Since $2^{2^n} + 1 \equiv 0 \pmod{F_n}$, we have $2^{2^n} \equiv -1 \pmod{F_n}$. Squaring gives $(2^{2^n})^2 = 2^{2^n \cdot 2} \equiv 1 \pmod{F_n}$. Thus $\operatorname{ord}_{F_n} 2 \le 2^n \cdot 2 = 2^{n+1}$.

19. Note that $a^t < m = a^n - 1$ whenever $1 \le t < n$. Hence, a^t cannot be congruent to 1 modulo m when t is a positive integer less than n. However, $a^n \equiv 1 \pmod m$ since $m = a^n - 1 \mid a^n - 1$. It follows that $\operatorname{ord}_m a = n$. Since $\operatorname{ord}_m a \mid \phi(m)$, we see that $n \mid \phi(m)$.

21. First suppose that pq is a pseudoprime to the base 2. By Fermat's little theorem, $2^p \equiv 2 \pmod{p}$, so there exists an integer k such that $2^p - 2 = kp$. Then $2^{M_p - 1} - 1 = 2^{2^p - 2} - 1 = 2^{kp} - 1$. This last expression is divisible by $2^p - 1 = M_p$ by Lemma 6.1. Hence, $2^{M_p - 1} \equiv 1 \pmod{M_p}$, or $2^{M_p} \equiv 2 \pmod{M_p}$. Since pq is a pseudoprime to the base 2, we have $2^{pq} \equiv 2 \pmod{pq}$, so $2^{pq} \equiv 2 \pmod{p}$. But $2^{pq} \equiv (2^p)^q \equiv 2^q \pmod{p}$. Therefore, $2^q \equiv 2 \pmod{p}$. Thus there exists an integer l such that $M_q - 1 = 2^q - 2 = lp$. Then $2^{M_q - 1} - 1 = 2^{2^q - 2} = 2^{lp} - 1$, so $2^p - 1 = M_p$ divides $2^{M_q - 1} - 1$. Therefore, $2^{M_q} \equiv 2 \pmod{M_p}$. Then we have $2^{M_p M_q} \equiv (2^{M_p})^{M_q} \equiv 2^{M_q} \equiv 2 \pmod{M_p}$. Similarly, $2^{M_p M_q} \equiv 2 \pmod{M_q}$. By the Chinese remainder theorem, noting that M_p and M_q are relatively prime, we have $2^{M_p M_q} \equiv 2 \pmod{M_p M_q}$. Therefore, $M_p M_q$ is a pseudoprime to the base 2. Conversely, suppose that $M_p M_q$ is a pseudoprime to the base 2. From the reasoning in the proof of Theorem 6.6, $2^{M_p} \equiv 2 \pmod{p}$. Therefore, $2^{M_p M_q} \equiv 2^{(M_p - 1)M_q + M_q} \equiv 2^{M_q} \equiv 2 \pmod{p}$. But since $M_p = 2^p - 1 \equiv 0 \pmod{M_p}$, the order of 2 modulo M_p is p. Therefore, $p \mid M_q - 1$. In other words, $2^q \equiv 2 \pmod{p}$. Then $2^{pq} \equiv 2^q \equiv 2 \pmod{p}$. Similarly, $2^{pq} \equiv 2 \pmod{q}$. Therefore, by the Chinese remainder theorem, $2^{pq} \equiv 2 \pmod{pq}$. Since pq is composite, it is a pseudoprime to the base 2.

23. Let $j = \text{ord}_{\phi(n)} e$. Then $e^j \equiv 1 \pmod{\phi(n)}$. Since $\text{ord}_n P \mid \phi(n)$, we have $e^j \equiv 1 \pmod{\text{ord}_n P}$. Then by Theorem 9.2, $P^{e^j} \equiv P \pmod{n}$, so $C^{e^{j-1}} \equiv (P^e)^{e^{j-1}} \equiv P^{e^j} \equiv P \pmod{n}$ and $C^{e^j} \equiv P^e \equiv C \pmod{n}$.

Section 9.2

1. **a.** 2 **b.** 4 **c.** 8 **d.** 6 **e.** 12 **f.** 22

3. 2, 6, 7, 11

5. 2, 3, 10, 13, 14, 15

7. By Lagrange's theorem there are at most two solutions to $x^2 \equiv 1 \pmod{p}$, and we know that $x \equiv \pm 1$ are the two solutions. Since $p \equiv 1 \pmod{4}$, we have $4 \mid p - 1 = \phi(p)$, so by Theorem 9.8 there is an element x of order 4 modulo p. Then $x^4 = (x^2)^2 \equiv 1 \pmod{p}$, so $x^2 \equiv \pm 1 \pmod{p}$. If $x^2 \equiv 1 \pmod{p}$, then x does not have order 4. Therefore, $x^2 \equiv -1 \pmod{p}$.

11. **a.** Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, and let k be the largest integer such that p does not divide a_k. Let $g(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$. Then $f(x) \equiv g(x) \pmod{p}$ for every value of x. In particular, $g(x)$ has the same set of roots modulo p as $f(x)$. Since the number of roots is greater than $n > k$, this contradicts Lagrange's theorem. Therefore, no such k exists, and p must divide every coefficient of $f(x)$.

b. Note that the degree of $f(x)$ is $p - 2$ (the x^{p-1} terms cancel). By Fermat's little theorem we have that $x^{p-1} - 1 \equiv 0 \pmod{p}$ for $x = 1, 2, \ldots, p - 1$. Further, each x in the same range is patently a zero for $(x - 1)(x - 2) \cdots (x - p + 1)$. Therefore, each such x is a root of $f(x)$. Since $f(x)$ has degree $p - 2$ and $p - 1$ roots, part (a) tells us that all the coefficients of $f(x)$ are divisible by p.

c. From part (b) we know that the constant term of $f(x)$ is divisible by p. The constant term is $f(0)$. Thus $f(0) = (-1)(-2) \cdots (-p + 1) + 1 = (-1)^{p-1}(p - 1)! + 1 = (p - 1)! + 1 \equiv 0 \pmod{p}$, which is Wilson's theorem.

13. **a.** Since $q_i^{t_i} \mid \phi(p) = p - 1$, by Theorem 9.8 there exist $\phi(q_i^{t_i})$ elements of order $q_i^{t_i}$ for each $i = 1, 2, \ldots, r$. Let a_i be a fixed element of this order.

b. Using mathematical induction and Exercise 10 of Section 9.1, we have $\text{ord}_p(a) = \text{ord}_p(a_1 \cdots a_r) = \text{ord}_p(a_1 \cdots a_{r-1}) \cdot \text{ord}_p(a_r) = \cdots = \text{ord}_p(a_1) \cdots \text{ord}_p(a_r)$ since

$\{\text{ord}_p(a_1), \ldots, \text{ord}_p(a_r)\} = \{q_1^{t_1}, \ldots, q_r^{t_r}\}$ are pairwise relatively prime.
c. 18

15. If n is odd, composite, and not a power of 3, then the product in Exercise 14 is $\prod_{j=1}^{r}(n-1, p_j - 1) \geq (n-1, 3-1)(n-1, 5-1) \geq 2 \cdot 2 = 4$. Therefore, there must be two bases other than -1 and $+1$.

17. **a.** Suppose that $f(x)$ is a polynomial of degree $n-1$ with integer coefficients. Suppose that $x_1, x_2, \ldots, x_n$ are incongruent modulo p, where p is prime. Consider the polynomial $g(x) = f(x) - \sum_{j=1}^{n}(f(x_j) \cdot \prod_{i \neq j}(x - x_i)\overline{(x_j - x_i)})$. Note that x_j, $j = 1, 2, \ldots, n$, is a root of this polynomial modulo p since its value at x_j is $f(x_j) - (0 + 0 + \cdots + f(x_j)\prod_{i \neq j}(x_j - x_i)(x_j - x_i) + \cdots + 0) \equiv f(x_j) - f(x_j) \cdot 1 \equiv 0 \pmod{p}$. Since $g(x)$ has n incongruent roots modulo p and since it is of degree $n-1$ or less, we can easily use Lagrange's theorem to see that $g(x) \equiv 0 \pmod{p}$ for every integer x.
b. 10

19. By Exercise 23 of Section 9.1, $j \mid \text{ord}_{\phi(n)} e$. Here $\phi(n) = \phi(pq) = 4p'q'$, so $j \mid \phi(4p'q') = 2(p'-1)(q'-1)$. Choose e to be a primitive root modulo p'. Then $p' - 1 = \phi(p') \mid \phi(\phi(n))$, so $p' - 1 \mid \text{ord}_{\phi(n)} e$. The decrypter needs $e^j \equiv 1 \pmod{n}$, but this choice of e forces $j = p' - 1$, which will take quite some time to find.

Section 9.3

1. 4, 10, 22

3. **a.** 2 **b.** 2 **c.** 5 **d.** 2

5. **a.** 2 **b.** 2 **c.** 2 **d.** 3

7. **a.** 3 **b.** 3 **c.** 3 **d.** 3

9. 7, 13, 17, 19

11. 3, 13, 15, 21, 29, 33

13. Suppose that r is a primitive root of m and suppose further that $x^2 \equiv 1 \pmod{m}$. Let $x \equiv r^t \pmod{m}$, where $0 \leq t \leq p-1$. Then $r^{2t} \equiv 1 \pmod{m}$. Since r is a primitive root, $\phi(m) \mid 2t$, so $2t = k\phi(m)$ and $t = k\phi(m)/2$ for some integer k. Then $x \equiv r^t = r^{k\phi(m)/2} = r^{(\phi(m)/2)k} \equiv (-1)^k \equiv \pm 1 \pmod{m}$. Conversely, suppose that m has no primitive root. Then m is not of one of the forms 2, 4, p^a, or $2p^a$, with p an odd prime. So either two distinct odd primes divide m, or $m = 2^b p^\alpha$ with p an odd prime and $b > 1$, or $m = 2^b$ with $b > 2$. Let p be an odd prime dividing m, say $p^\alpha \parallel m$. Then the solution to the system $x \equiv 1 \pmod{p^\alpha}$, $x \equiv -1 \pmod{m/p^\alpha}$ cannot be congruent to $\pm 1 \pmod{m}$. But $x^2 \equiv 1 \pmod{p^\alpha}$ and $x^2 \equiv 1 \pmod{m/p^\alpha}$, so by the Chinese remainder theorem $x^2 \equiv 1 \pmod{m}$. If no odd prime divides m, then $m = 2^b$ with $b \geq 3$. From Theorem 9.12, we know there are at least three solutions y_1, y_2, and y_3 to $y^2 \equiv 1 \pmod{2^b}$. So in each case, there is at least one solution that is not congruent to $\pm 1 \pmod{m}$.

15. By Theorem 9.12 we know that $\text{ord}_{2^k} 5 = \phi(2^k)/2 = 2^{k-2}$. Hence, the 2^{k-2} integers 5^j, $j = 0, 1, \ldots, 2^{k-2} - 1$, are incongruent modulo 2^k. Similarly, the 2^{k-2} integers -5^j, $j = 0, 1, \ldots, 2^{k-2} - 1$, are incongruent modulo 2^k. Note that 5^j cannot be congruent to -5^i modulo 2^k since $5^j \equiv 1 \pmod{4}$ but $-5^i \equiv 3 \pmod{4}$. It follows that the integers $1, 5, \ldots, 5^{2^{k-2}-1}, -1, -5, \ldots, -5^{2^{k-2}-1}$ are 2^{k-1} incongruent integers modulo 2^k. Since $\phi(2^k) = 2^{k-1}$ and every integer of the form $(-1)^\alpha 5^\beta$ is relatively prime to 2^k, it follows that every odd integer is congruent to an integer of this form with $\alpha = 0$ or 1 and $0 \leq \beta \leq 2^{k-2} - 1$.

Section 9.4

1. The values of $\text{ind}_5 i$, $i = 1, 2, \ldots, 22$, are 22, 2, 16, 4, 1, 18, 19, 6, 10, 3, 9, 20, 14, 21, 17, 8, 7, 12, 15, 5, 13, 11, respectively.

3. **a.** 7, 18 **b.** none

5. 8, 9, 20, 21, 29 (mod 29)

7. All positive integers $x \equiv 0$ 1, 12, 23, 24, 45, 46, 47, 67, 69, 70, 78, 89, 91, 92, 93, 100, 111, 115, 116, 133, 137, 138, 139, 144, 155, 161, 162, 177, 183, 184, 185, 188, 199, 207, 208, 210, 221, 229, 230, 231, 232, 243, 253, 254, 265, 275, 276, 277, 287, 299, 300, 309, 321, 322, 323, 331, 345, 346, 353, 367, 368, 369, 375, 386, 391, 392, 397, 413, 414, 415, 419, 430, 437, 438, 441, 459, 460, 461, 463, 483, 484, 485, 496, or 505 (mod 506)

9. Let r be a primitive root of p. Suppose that $x^4 \equiv -1 \pmod{p}$, and let $y = \text{ind}_r x$. Then $-x$ is also a solution, and by Exercise 8, $\text{ind}_r(-x) \equiv \text{ind}_r(-1) + \text{ind}_r(x) \equiv (p-1)/2 + y \pmod{p-1}$. So without loss of generality we may take $0 < y < (p-1)/2$, or $0 < 4y < 2(p-1)$. Taking indices of both sides of the congruence yields $4y \equiv \text{ind}_r(-1) \equiv (p-1)/2 \pmod{p-1}$, again using Exercise 8. So $4y = (p-1)/2 + m(p-1)$ for some m. But $4y < 2(p-1)$, so either $4y = (p-1)/2$ and so $p = 8y + 1$, or $4y = 3(p-1)/2$. In the latter case, 3 must divide y, so we have $p = 8(y/3) + 1$. In either case, p is of the desired form. Conversely, suppose that $p = 8k + 1$, and let r be a primitive root of p. Take $x = r^k$. Then $x^4 \equiv r^{4k} \equiv r^{(p-1)/2} \equiv -1 \pmod{p}$ by Exercise 8. So this x is a solution.

11. (1, 2); (0, 2)

13. $x \equiv 29 \pmod{32}$; $x \equiv 4 \pmod{8}$

15. (0, 0, 1, 1); (0, 0, 1, 4)

17. $x \equiv 17 \pmod{60}$

19. We seek a solution to $x^k \equiv a \pmod{2^e}$. We take indices as described before Exercise 11. Suppose that $a \equiv (-1)^\alpha 5^\beta$ and $x \equiv (-1)^\gamma 5^\delta$. Then the index system of x^k is $(k\gamma, k\delta)$, and the index system of a is (α, β), so $k\gamma \equiv \alpha \pmod{2}$ and $k\delta \equiv \beta \pmod{2^{e-2}}$. Since k is odd, both congruences are solvable for γ and δ, which determine x.

21. First we show that $\text{ord}_{2^e} 5 = 2^{e-2}$. Indeed, $\phi(2^e) = 2^{e-1}$, so it suffices to show that the highest power of 2 dividing $5^{2^{e-2}} - 1$ is 2^e. We proceed by induction. The basis step is the case $e = 2$, which is true. Note that $5^{2^{e-2}} - 1 = (5^{2^{e-3}} - 1)(5^{2^{e-3}} + 1)$. The first factor is exactly divisible by 2^{e-1} by the induction hypothesis. The second factor differs from the first by 2, so it is exactly divisible by 2; therefore, $5^{2^{e-2}} - 1$ is exactly divisible by 2^e, as desired. Hence if k is odd, then the numbers $(\pm 5)^k$, $(\pm 5)^{2k}$, $\ldots$, $(\pm 5)^{2^{e-2}k}$ are 2^{e-1} incongruent kth power residues, which is the number given by the formula. If 2^m exactly divides k, then $5^k \equiv (-5)^k \pmod{2^e}$, so the formula must be divided by 2, hence the factor $(k, 2)$ in the denominator. Further, 5^{2^m} has order $2^{e-2}/2^m$ if $m \leq e - 2$ and order 1 if $m > e - 2$, so the list must repeat modulo 2^e every $\text{ord}_{2^e} 5^{2^m}$ terms, whence the other factor in the denominator.

23. **a.** From the first inequality in the proof, if n is not square-free, then the probability is strictly less than $2n/9$, which is substantially smaller than $(n-1)/4$ for large n. If n is square-free, the argument following (9.6) shows that if n has 4 or more factors, then the probability is less than $n/8$. The next inequality shows that the worst case for $n = p_1 p_2$ is when $s_1 = s_2$ and s_1 is as small as possible, which is the case stated in the exercise.
b. 0.24999249 . . .

Section 9.5

1. We have $2^2 \equiv 4 \pmod{101}$, $2^5 \equiv 32 \pmod{101}$, $2^{10} \equiv (2^5)^2 \equiv 32^2 \equiv 14 \pmod{101}$, $2^{20} \equiv (2^{10})^2 \equiv 14^2 \equiv 95 \pmod{101}$, $2^{25} \equiv (2^5)^5 \equiv 32^5 \equiv (32^2)^2 \cdot 32 \equiv 1024^2 \cdot 32 \equiv 14^2 \cdot 32 \equiv 196 \cdot 32 \equiv -6 \cdot 32 \equiv -192 \equiv 10 \pmod{101}$, $2^{50} \equiv (2^{25})^2 \equiv 10^2 = 100 \equiv -1 \pmod{101}$, $2^{100} \equiv (2^{50})^2 \equiv (-1)^2 \equiv 1 \pmod{101}$. Since $2^{(101-1)/q} \not\equiv 1 \pmod{101}$ for every proper divisor q of 100 but $2^{101-1} \equiv 1 \pmod{101}$, it follows that 101 is prime.

3. $233 - 1 = 2^3 \cdot 29$, $3^{116} \equiv -1 \pmod{233}$, $3^8 \equiv 37 \not\equiv 1 \pmod{233}$

5. The first condition implies that $x^{F_n - 1} \equiv 1 \pmod{F_n}$. The only prime dividing $F_n - 1 = 2^{2^n}$ is 2, and $(F_n - 1)/2 = 2^{2^n - 1}$, so the second condition implies that $2^{(F_n-1)/2} \not\equiv 1 \pmod{F_n}$. Then by Theorem 9.18, F_n is prime.

7. See [Le80].

9. Since $n - 1 = 9928 = 2^3 \cdot 17 \cdot 73$, we take $F = 2^3 \cdot 17 = 136$ and $R = 73$, noting that $F > R$. We apply Pocklington's test with $a = 3$. We check (using a calculator or computational software) that $3^{9928} \equiv 1 \pmod{9929}$ and that $(3^{9928/2} - 1, 9929) = 1$ and $(3^{9928/17} - 1, 9929) = 1$, since 2 and 17 are the only primes dividing F. Therefore, n passes Pocklington's test and so is prime.

11. Note that $3329 = 2^8 \cdot 13 + 1$ and $13 < 2^8$, so it is of the form that can be tested by Proth's test. With the help of computational software, we compute $3^{(3329-1)/2} \equiv -1 \pmod{3329}$, which shows that 3329 is prime.

13. We apply Pocklington's test to this situation. Note that $n - 1 = hq^k$, so we let $F = q^k$ and $R = h$ and observe that by hypothesis $F > R$. Since q is the only prime dividing F, we need only check that there is an integer a such that $a^{n-1} \equiv 1 \pmod{n}$ and $(a^{(n-1)/q} - 1, n) = 1$. But both of these conditions are hypotheses.

Section 9.6

1. **a.** 20 **b.** 12 **c.** 36 **d.** 48 **e.** 180 **f.** 388,080 **g.** 8640 **h.** 125,411,328,000

3. 65,520

5. Suppose that $m = 2^{t_0} p_1^{t_1} \cdots p_s^{t_s}$. Then $\lambda(m) = [\lambda(2^{t_0}), \phi(p_1^{t_1}), \ldots, \phi(p_s^{t_s})]$. Furthermore, $\phi(m) = \phi(2^{t_0})\phi(p_1^{t_1}) \cdots \phi(p_s^{t_s})$. Since $\lambda(2^{t_0}) = 1, 2$, or 2^{t_0-2} when $t_0 = 1, 2$, or $t_0 \geq 3$, respectively, we have $\lambda(2^{t_0}) \mid \phi(2^{t_0}) = 2^{t_0-1}$. Since the least common multiple of a set of numbers divides the product of these numbers, or their multiples, we see that $\lambda(m) \mid \phi(m)$.

7. For any integer x with $(x, n) = (x, m) = 1$ we have $x^a \equiv 1 \pmod{n}$ and $x^a \equiv 1 \pmod{m}$. Then the Chinese remainder theorem gives us $x^a \equiv 1 \pmod{[n, m]}$. But since n is the largest integer with this property, we must have $[n, m] = n$, so $m \mid n$.

9. Suppose that $ax \equiv b \pmod{m}$. Multiplying both sides of this congruence by $a^{\lambda(m)-1}$ gives $a^{\lambda(m)}x \equiv a^{\lambda(m)-1}b \pmod{m}$. Since $a^{\lambda(m)} \equiv 1 \pmod{m}$, it follows that $x \equiv a^{\lambda(m)-1}b \pmod{m}$. Conversely, let $x_0 \equiv a^{\lambda(m)-1}b \pmod{m}$. Then $ax_0 \equiv aa^{\lambda(m)-1}b = a^{\lambda(m)}b \equiv b \pmod{m}$, so x_0 is a solution.

11. **a.** First, suppose that $m = p^a$. Then $x(x^{c-1} - 1) \equiv 0 \pmod{p^a}$. Let r be a primitive root for p^a. Then the solutions to $x^{c-1} \equiv 1 \pmod{p^a}$ are the powers r^k with $(c-1)k \equiv 1 \pmod{\phi(p^a)}$; there are $(c - 1, \phi(p^a))$ of these. Since 0 is a solution, there are $1 + (c - 1, \phi(p^a))$ solutions. If $m = p_1^{a_1} \cdots p_t^{a_t}$, the result follows by the Chinese remainder theorem since there is a one-to-one correspondence between solutions modulo m and the set of t-tuples of solutions to the system of congruences modulo each of the prime powers.
b. If $(c - 1, \phi(m)) = 2$, then $c - 1$ is even. Since $\phi(p^a)$ is even for all prime powers, except 2, $(c - 1, \phi(p_i^{a_i})) = 2$ for each i. By (a) the number of solutions is 3^r. If 2^1 is a prime-power factor,

then $\phi(m) = \phi(m/2)$, and since x^c and x have the same parity, x is a solution modulo m if and only if it is a solution modulo $m/2$, so the result still holds.

13. Let $n = 3pq$, with $p < q$ odd primes, be a Carmichael number. Then by Theorem 9.23, $p - 1 \mid 3pq - 1 = 3(p-1)q + 3q - 1$, so $p - 1 \mid 3q - 1$, say $(p-1)a = 3q - 1$. Since $q > p$, we must have $a \geq 4$. Similarly, there is an integer b such that $(q-1)b = 3p - 1$. Solving these two equations for p and q yields $q = (2a + ab - 3)/(ab - 9)$ and $p = (2b + ab - 3)/(ab - 9) = 1 + (2b + 6)/(ab - 9)$. Then since p is an odd prime greater than 3, we must have $4(ab - 9) \leq 2b + 6$, which reduces to $b(2a - 1) \leq 21$. Since $a \geq 4$, this implies that $b \leq 3$. Then $4(ab - 9) \leq 2b + 6 \leq 12$, so $ab \leq 21/4$, so $a \leq 5$. Therefore, $a = 4$ or 5. If $b = 3$, then the denominator in the expression for q is a multiple of 3, so the numerator must be a multiple of 3, but that is impossible since there is no choice for a that is divisible by 3. Thus $b = 1$ or 2. The denominator of q must be positive, so $ab > 9$, which eliminates all remaining possibilities except $a = 5$, $b = 2$, in which case $p = 11$ and $q = 17$. So the only Carmichael number of this form is $561 = 3 \cdot 11 \cdot 17$.

15. Assume that $q < r$. By Theorem 9.23, $q - 1 \mid pqr - 1 = (q-1)pr + pr - 1$. Therefore, $q - 1 \mid pr - 1$, say $a(q-1) = pr - 1$. Similarly, $b(r-1) = pq - 1$. Since $q < r$, we must have $a > b$. Solving these two equations for q and r yields $r = (p(a-1) + a(b-1))/(ab - p^2)$ and $q = (p(b-1) + b(a-1))/(ab - p^2) = 1 + (p^2 + pb - p - b)/(ab - p^2)$. Since this last fraction must be an integer, $ab - p^2 \leq p^2 + pb - p - b$, which reduces to $a(b-1) \leq 2p^2 + p(b-1)$ or $a - 1 \leq (2p^2/b) + (p(b-1)/b) \leq 2p^2 + p$. So there are only finitely many values for a. Likewise, the same inequality gives us $b(a-1) \leq 2p^2 + pb - p$ or $b(a - 1 - p) \leq 2p^2 - p$. Since $a > b$ and the denominator of the expression for q must be positive, $a \geq p + 1$. If $a = p + 1$, then $(p+1)(q-1) = pq - p + q - 1 = pr - 1$, which implies that $p \mid q$, a contradiction. Therefore, $a > p + 1$, and so $a - 1 - p$ is a positive integer. The last inequality gives us $b \leq b(a - 1 - p) \leq 2p^2 - p$. Therefore, there are only finitely many values for b. Since a and b determine q and r, there can be only finitely many Carmichael numbers of this form.

17. We have $q_n(ab) \equiv ((ab)^{\lambda(n)} - 1)/n = (a^{\lambda(n)}b^{\lambda(n)} - a^{\lambda(n)} - b^{\lambda(n)} + 1 + a^{\lambda(n)} + b^{\lambda(n)} - 2)/n = (a^{\lambda(n)} - 1)(b^{\lambda(n)} - 1)/n + ((a^{\lambda(n)} - 1) + (b^{\lambda(n)} - 1))/n \equiv q_n(a) + q_n(b) \pmod{n}$. At the last step, we use the fact that n^2 must divide $(a^{\lambda(n)} - 1)(b^{\lambda(n)} - 1)$, since $\lambda(n)$ is the universal exponent.

Section 10.1

1. 69, 76, 77, 92, 46, 11, 12, 14, 19, 36, 29, 84, 05, 02, 00, 00, 00, ...

3. 10

5. **a.** $a \equiv 1 \pmod{20}$ **b.** $a \equiv 1 \pmod{30{,}030}$ **c.** $a \equiv 1 \pmod{111111}$ **d.** $a \equiv 1 \pmod{2^{25} - 1}$

7. **a.** 31 **b.** 715,827,882 **c.** 31 **d.** 195,225,786 **e.** 1,073,741,823 **f.** 1,073,741,823

9. 8, 64, 15, 71, 36, 64, 15, 71, 36, ...

11. First we find that $\text{ord}_{77} 8$ is 10 so that $t = 1$ and $s = 5$. Since $\text{ord}_5 2 = 4$, the period length is 4.

13. Using the notation of Theorem 10.4, we have $\phi(77) = 60$, so $\text{ord}_{77} x_0$ is a divisor of $60 = 2^2 \cdot 3 \cdot 5$. Thus the only possible values for s are the odd divisors of 60, which are 3, 5, and 15. But $\text{ord}_3 2 = 2$, $\text{ord}_5 2 = 4$, and $\text{ord}_{15} 2 = 4$. Hence, by Theorem 10.4 the maximum period length is 4.

15. 24, 25, 18, 12, 30, 11, 10, 21

17. Check that 7 has maximal order 1800 modulo $2^{25} - 1$. To make a large enough multiplier, raise 7 to a power relatively prime to $\phi(2^{25} - 1) = 32{,}400{,}000$, for example, to the 11th power.

19. 665

21. **a.** 8, 2, 8, 2, 8, 2, ... **b.** 9, 12, 6, 13, 8, 18, 2, 4, 16, 3, 9, 12, 6, 13, 8, 18, 2, 4, 16, 3, ...

Section 10.2

1. We select $k = 1234$ for our random integer. Converting the plaintext into numerical equivalents results in 0700 1515 2401 0817 1907 0300 2423, where we filled out the last block with an X. With the help of a computational program, we find $\gamma \equiv r^k = 6^{1234} \equiv 517 \pmod{2551}$. Then for each block P we compute $\delta \equiv P \cdot b^k = P \cdot 33^{1234} \equiv P \cdot 651 \pmod{2551}$. The resulting blocks are $0700 \cdot 651 \equiv 1622 \pmod{2551}$, $1515 \cdot 651 \equiv 1579 \pmod{2551}$, $2401 \cdot 651 \equiv 1839 \pmod{2551}$, $0817 \cdot 651 \equiv 1259 \pmod{2551}$, $1907 \cdot 651 \equiv 1671 \pmod{2551}$, $0300 \cdot 651 \equiv 1424 \pmod{2551}$, and $2423 \cdot 651 \equiv 855 \pmod{2551}$. Therefore, the ciphertext is (517, 1622), (517, 1579), (517, 1839), (517, 1259), (517, 1671), (517, 1424), (517, 855). To decrypt this ciphertext, we compute $\gamma^{p-1-a} = 517^{2551-1-13} = 517^{2537} \equiv 337 \pmod{2551}$. Then for each block of the ciphertext we compute $P \equiv 337 \cdot \delta \pmod{2551}$. For the first block we have $337 \cdot 1622 \equiv 0700 \pmod{2551}$, which was the first block of the plaintext; and so on.

3. RABBIT

5. $(\gamma, s) = (2022, 833)$; to verify this signature, we use a computational program to find that $V_1 \equiv 2022^{833} \cdot 801^{2022} \equiv 1014 \equiv 3^{823} \equiv V_2 \pmod{2657}$

7. Let $\delta_1 = P_1 b^k$ and $\delta_2 = P_2 b^k$ in the ElGamal cryptosystem. If P_1 is known, then it is easy to compute an inverse for P_1 modulo p. Then $b^k \equiv \overline{P_1}\delta_1 \pmod{p}$. Then it is also easy to compute an inverse for $b^k \pmod{p}$. Then $P_2 \equiv \overline{b^k}\delta_2 \pmod{p}$. Hence the plaintext P_2 is recovered.

Section 10.3

1. **a.** 8 **b.** 5 **c.** 2 **d.** 6 **e.** 30 **f.** 20

3. **a.** At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $3k - 2 \pmod{50}$.
   b. At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $21k + 56 \pmod{76}$.
   c. At each stage of the splicing, the kth wire of one section is connected to the $S(k)$th wire, where $S(k)$ is the least positive residue of $2k - 1 \pmod{125}$.

Section 11.1

1. **a.** 1 **b.** 1, 4 **c.** 1, 3, 4, 9, 10, 12 **d.** 1, 4, 5, 6, 7, 9, 11, 16, 17

3. $1, -1, -1, 1$

5. **a.** $\left(\frac{7}{11}\right) \equiv 7^{\frac{11-1}{2}} \equiv 7^5 \equiv 49^2 \cdot 7 \equiv 5^2 \cdot 7 \equiv 3 \cdot 7 \equiv -1 \pmod{11}$
   b. $(7, 14, 21, 28, 35) \equiv (7, 3, 10, 6, 2) \pmod{11}$ and three of these are greater than $\frac{11}{2}$, so $\left(\frac{7}{11}\right) = (-1)^3 = -1$

7. We have $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ by Theorem 11.4. Using Theorems 11.5 and 11.6, we have: If $p \equiv 1 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (1)(1) = 1$; if $p \equiv 3 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (-1)(-1) = 1$; if $p \equiv -1 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (-1)(1) = -1$; if $p \equiv -3 \pmod{8}$, then $\left(\frac{-2}{p}\right) = (1)(-1) = -1$.

9. Since $p - 1 \equiv -1$, $p - 2 \equiv -2$, $\ldots$, $(p + 1)/2 \equiv (p - 1)/2 \pmod{p}$, we have $((p - 1)/2)!^2 \equiv -(p - 1)! \equiv 1 \pmod{p}$ by Wilson's theorem (since $p \equiv 3 \pmod 4$ the minus signs cancel). By Euler's criterion $((p - 1)/2)!^{(p-1)/2} \equiv \left(\frac{1}{p}\right)\left(\frac{2}{p}\right) \cdots \left(\frac{(p-1)/2}{p}\right) \equiv (-1)^t \pmod{p}$, by definition of the Legendre symbol. Since $((p - 1)/2)! \equiv \pm 1 \pmod{p}$ and $(p - 1)/2$ is odd, we have the result.

11. If $p \equiv 1 \pmod 4$, then $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = 1 \cdot 1 = 1$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1) \cdot 1 = -1$.

13. **a.** $x \equiv 4$ or $2 \pmod 7$ **b.** $x \equiv 1 \pmod 7$ **c.** no solutions

15. Suppose that p is a prime greater than 6. At least one of the three incongruent integers 2, 3, and 6 is a quadratic residue of p, because if neither 2 nor 3 is a quadratic residue of p, then $2 \cdot 3 = 6$ is a quadratic residue of p. If 2 is a quadratic residue, then 2 and 4 are quadratic residues that differ by 2; if 3 is a quadratic residue, then 1 and 3 are quadratic residues that differ by 2; while if 6 is a quadratic residue, then 4 and 6 are quadratic residues that differ by 2.

17. **a.** Since $p = 4n + 3$, we have $2n + 2 = (p + 1)/2$. Then $x^2 \equiv (\pm a^{n+1})^2 \equiv a^{2n+2} \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv 1 \cdot a \equiv a \pmod p$ using the fact that $a^{(p-1)/2} \equiv 1 \pmod p$ since a is a quadratic residue of p. By Lemma 11.1, there are only these two solutions.
b. By Lemma 11.1, there are exactly two solutions to $y^2 \equiv 1 \pmod p$, namely $y \equiv \pm 1 \pmod p$. Since $p \equiv 5 \pmod 8$, we know that -1 is a quadratic residue of p and 2 is a quadratic nonresidue of p. Since $p = 8n + 5$, we have $4n + 2 = (p - 1)/2$ and $2n + 2 = (p + 3)/4$. Then $(\pm a^{n+1})^2 \equiv a^{(p+3)/4} \pmod p$ and $(\pm 2^{2n+1}a^{n+1})^2 \equiv 2^{(p-1)/2}a^{(p+3)/4} \equiv -a^{(p+3)/4} \pmod p$ by Euler's criterion. We must show that one of $a^{(p+3)/4}$ or $-a^{(p+3)/4}$ is congruent to $a \pmod p$. Now a is a quadratic residue of p, so $a^{(p-1)/2} \equiv 1 \pmod p$, and therefore $a^{(p-1)/4}$ solves $x^2 \equiv 1 \pmod p$. But then $a^{(p-1)/4} \equiv \pm 1 \pmod p$, that is, $a^{(p+3)/4} \equiv \pm a \pmod p$ or $\pm a^{(p+3)/4} \equiv a \pmod p$, as desired.

19. $x \equiv 1, 4, 11,$ or $14 \pmod{15}$

21. 47, 96, 135, 278, 723, 866, 905, 954 (mod 1001)

23. If $x_0^2 \equiv a \pmod{p^{e+1}}$, then $x_0^2 \equiv a \pmod{p^e}$. Conversely, if $x_0^2 \equiv a \pmod{p^e}$, then $x_0^2 = a + bp^e$ for some integer b. We can solve the linear congruence $2x_0y \equiv -b \pmod p$, say $y = y_0$. Let $x_1 = x_0 + y_0p^e$. Then $x_1^2 \equiv x_0^2 + 2x_0y_0p^e = a + p^e(b + 2x_0y_0) \equiv a \pmod{p^{e+1}}$ since $p \mid 2x_0y_0 + b$. This is the induction step in showing that $x^2 \equiv a \pmod{p^e}$ has solutions if and only if $\left(\frac{a}{p}\right) = 1$.

25. **a.** 4 **b.** 8 **c.** 0 **d.** 16

27. Suppose that $p_1, p_2, \ldots, p_n$ are the only primes of the form $4k + 1$. Let $N = 4(p_1p_2 \cdots p_n)^2 + 1$. Let q be an odd prime factor of N. Then $q \neq p_i$ for $i = 1, 2, \ldots, n$, but $N \equiv 0 \pmod q$, so $4(p_1p_2 \cdots p_n)^2 \equiv -1 \pmod q$. Therefore $\left(\frac{-1}{q}\right) = 1$, so $q \equiv 1 \pmod 4$ by Theorem 11.5.

29. Let b_1, b_2, b_3, and b_4 be the four modular square roots of a modulo pq. Then each b_i is a solution to exactly one of the four systems of congruences given in the text. For convenience let the subscripts correspond to the lowercase Roman numerals of the systems. Suppose that two of the b_i's were quadratic residues modulo pq. Without loss of generality, say $b_1 \equiv y_1^2 \pmod{pq}$ and $b_2 \equiv y_2^2 \pmod{pq}$. Then from systems (i) and (ii) we have that $y_1^2 \equiv b_1 \equiv x_2 \pmod q$ and $y_2^2 \equiv b_2 \equiv -x_2 \pmod q$. Therefore, both x_2 and $-x_2$ are quadratic residues modulo q, but this is impossible since $q \equiv 3 \pmod 4$. The other cases are identical.

31. Let r be a primitive root for p, and let $a \equiv r^s \pmod p$ and $b \equiv r^t \pmod p$ with $1 \leq s, t \leq p - 1$. If $a \equiv b \pmod p$, then $s = t$, and so s and t have the same parity; by Theorem 11.2, we have part (i). Further, $ab \equiv r^{s+t} \pmod p$. Thus the right-hand side of (ii) is 1 exactly when s and t have the same parity, which is exactly when the left-hand side is 1. This proves part (ii). Finally, since $a^2 \equiv r^{2s} \pmod p$ and $2s$ is even, a^2 must be a quadratic residue modulo p, proving part (iii).

33. If r is a primitive root of q, then the set of all primitive roots is given by $\{r^k \mid (k, \phi(q)) = (k, 2p) = 1\}$. Thus the $p - 1$ numbers $\{r^k \mid k \text{ is odd}, k \neq p, 1 \leq k < 2p\}$ are all the primitive roots of q.

On the other hand, q has $(q-1)/2 = p$ quadratic residues, which are given by $\{r^2, r^4, \ldots, r^{2p}\}$. This set has no intersection with the first one.

35. First suppose that $p = 2^{2^n} + 1$ is a Fermat prime, and let r be a primitive root for p. Then $\phi(p) = 2^{2^n}$. An integer a is a nonresidue if and only if $a = r^k$ with k odd. But then $(k, \phi(p)) = 1$, so a is also a primitive root. Conversely, suppose that p is an odd prime and every quadratic nonresidue of p is also a primitive root of p. Let r be a particular primitive root of p. Then r^k is a quadratic nonresidue and hence a primitive root for p if and only if k is odd. But this implies that every odd number is relatively prime to $\phi(p)$, so $\phi(p)$ must be a power of 2. Thus $p = 2^b + 1$ for some b. If b had a nontrivial odd divisor, then we could factor p, contradicting the primality of p. Therefore, b is a power of 2, and so p is a Fermat prime.

37. **a.** We have $q = 2p + 1 = 2(4k + 3) + 1 = 8k + 7$, so $\left(\frac{2}{q}\right) = 1$ by Theorem 11.6. Then by Euler's criterion, $2^{(q-1)/2} \equiv 2^p \equiv 1 \pmod{q}$. Therefore, $q \mid 2^p - 1$.
b. $11 = 4(2) + 3$ and $23 = 2(11) + 1$, so $23 \mid 2^{11} - 1 = M_{11}$, by part (a); $23 = 4(5) + 3$ and $47 = 2(23) + 1$, so $47 \mid M_{23}$; $251 = 4(62) + 3$ and $503 = 2(251) + 1$, so $503 \mid M_{251}$

39. Let $q = 2k + 1$. Since q does not divide $2^p + 1$, we must have, by Exercise 38, that $k \equiv 0$ or $3 \pmod 4$. That is, $k \equiv 0, 3, 4$, or $7 \pmod 8$. Then $q \equiv 2 \cdot (0, 3, 4, \text{or } 7) + 1 \equiv \pm 1 \pmod 8$.

41. Note that $\left(\frac{j(j+1)}{p}\right) = \left(\frac{j^2(1+\bar{j})}{p}\right) = \left(\frac{1+\bar{j}}{p}\right)$ since j^2 is a perfect square. Then $\sum_{j=1}^{p-2}\left(\frac{j(j+1)}{p}\right) = \sum_{j=1}^{p-2}\left(\frac{\bar{j}+1}{p}\right) = \sum_{j=2}^{p-1}\left(\frac{j}{p}\right) = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right) - 1 = -1$. Here we have used the method in the solution to Exercise 10 to evaluate the last sum, and the fact that as j runs through the values 1 through $p-2$, so does $\bar{j}$.

43. Let r be a primitive root of p. Then the congruence $x^2 \equiv a \pmod p$ has a solution in x if and only if the congruence $2 \cdot \text{ind}_r x \equiv \text{ind}_r a \pmod{p-1}$ has a solution in $\text{ind}_r x$. Since $p-1$ is even, the last congruence is solvable if and only if $\text{ind}_r a$ is even, which happens when $a = r^2, r^4, \ldots, r^{p-1}$, i.e., $(p-1)/2$ times.

45. We have $q = 2(4k + 1) + 1 = 8k + 3$, so 2 is a quadratic nonresidue of q. By Exercise 33, 2 is a primitive root.

47. Check that $q \equiv 3 \pmod 4$, so -1 is a quadratic nonresidue of q. Since $4 = 2^2$, we have $\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2^2}{q}\right) = (-1)(1) = -1$. Therefore, -4 is a nonresidue of q. By Exercise 33, -4 is a primitive root.

49. **a.** By adding $(\overline{2}b)^2$ to both sides, we complete the square.
b. There are four solutions to $x^2 \equiv C + a \pmod{pq}$. From each, subtract $\overline{2}b$.
c. DETOUR

51. **a.** -1 **b.** -1 **c.** -1 **d.** -1 **e.** 1 **f.** 1

53. 1, 3, 4

Section 11.2

1. **a.** -1 **b.** 1 **c.** 1 **d.** 1 **e.** 1 **f.** 1

3. If $p \equiv 1 \pmod 6$, then there are two cases: If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$, so $\left(\frac{-3}{p}\right) = 1$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, so $\left(\frac{-3}{p}\right) = (-1)(-1) = 1$. If $p \equiv -1 \pmod 6$ and $p \equiv 1 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$. If $p \equiv 3 \pmod 4$, then $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)\left(-\left(\frac{p}{3}\right)\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$.

5. $p \equiv 1, 3, 9, 19, 25,$ or $27 \pmod{28}$

7. **a.** $F_1 = 2^{2^1} + 1 = 5$. We find that $3^{(F_1-1)/2} = 3^{(5-1)/2} = 3^2 = 9 \equiv -1 \pmod{F_1}$. Hence, by Pepin's test, $F_1 = 5$ is prime.
b. $F_3 = 2^{2^3} + 1 = 257$. We find that $3^{(F_3-1)/2} = 3^{(257-1)/2} = 3^{128} \equiv (3^8)^{16} \equiv 136^{16} \equiv (136^4)^4 \equiv 64^4 \equiv (64^2)^2 \equiv 241^2 \equiv 256 \equiv -1 \pmod{257}$.
c. $3^{32,768} \equiv 3^{255 \cdot 128} \cdot 3^{128} \equiv 94^{128} \cdot 3^{128} \equiv -1 \pmod{F_4}$

9. The lattice points in the rectangle are the points (i, j), where $0 < i < p/2$ and $0 < j < q/2$. These are the lattice points (i, j) with $i = 1, 2, \ldots, (p-1)/2$ and $j = 1, 2, \ldots, (q-1)/2$. Consequently, there are $((p-1)/2)((q-1)/2)$ such lattice points.
b. The points on the diagonal connecting **O** and **C** are the points (x, y), where $y = (q/p)x$. Suppose that x and y are integers with $y = (q/p)x$. Then $py = qx$. Since $(p, q) = 1$, it follows that $p \mid x$, which is impossible if $0 < x < p/2$. Hence, there are no lattice points on this diagonal.
c. The number of lattice points in the triangle with vertices **O**, **A**, and **C** is the number of lattice points (i, j) with $i = 1, 2, \ldots, (p-1)/2$ and $1 \le j \le iq/p$. For a fixed value of i in the indicated range, there are $[iq/p]$ lattice points (i, j) in the triangle. Hence, the total number of lattice points in the triangle is $\sum_{i=1}^{(p-1)/2} [iq/p]$.
d. The number of lattice points in the triangle with vertices **O**, **B**, and **C** is the number of lattice points (i, j) with $j = 1, 2, \ldots, (q-1)/2$ and $1 \le i < jp/q$. For a fixed value of j in the indicated range, there are $[jp/q]$ lattice points (i, j) in the triangle. Hence, the total number of lattice points in the triangle is $\sum_{j=1}^{(q-1)/2} [jp/q]$.
e. Since there are $((p-1)/2)((q-1)/2)$ lattice points in the rectangle and no points on the diagonal **OC**, the sum of the numbers of lattice points in the triangles **OBC** and **OAC** is $((p-1)/2)((q-1)/2)$. From parts (b) and (c), it follows that $\sum_{j=1}^{(p-1)/2} [jq/p] + \sum_{j=1}^{(q-1)/2} [jp/q] = ((p-1)/2)((q-1)/2)$. From Lemma 11.3, it follows that $\left(\frac{p}{q}\right) = (-1)^{T(p,q)}$ and $\left(\frac{q}{p}\right) = (-1)^{T(q,p)}$, where $T(p, q) = \sum_{j=1}^{(p-1)/2} [jp/q]$ and $T(q, p) = \sum_{j=1}^{(q-1)/2} [jq/p]$. We conclude that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}$. This is the law of quadratic reciprocity.

11. First suppose that $a = 2$. Then $p \equiv \pm q \pmod 8$, and so $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ by Theorem 11.6. Now suppose that a is an odd prime. If $p \equiv q \pmod{4a}$, then $p \equiv q \pmod a$, and so $\left(\frac{q}{a}\right) = \left(\frac{p}{a}\right)$. Since $p \equiv q \pmod 4$, we have $(p-1)/2 \equiv (q-1)/2 \pmod 2$. Then by Theorem 11.7, $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{((p-1)/2)((a-1)/2)} = \left(\frac{q}{a}\right)(-1)^{((q-1)/2)((a-1)/2)} = \left(\frac{a}{q}\right)$. But if $p \equiv -q \pmod{4a}$, then $p \equiv -q \pmod a$, and so $\left(\frac{-q}{a}\right) = \left(\frac{p}{a}\right)$. Since $p \equiv -q \pmod 4$, we have $(p-1)/2 \equiv ((q-1)/2) + 1 \pmod 2$. Then by Theorem 11.7, $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{((p-1)/2)((a-1)/2)} = \left(\frac{-q}{a}\right)(-1)^{((q-1)/2+1)((a-1)/2)} = \left(\frac{-1}{a}\right)(-1)^{(a-1)/2}\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right)$. The general case follows from the multiplicativity of the Legendre symbol.

13. **a.** Recall that $e^{xi} = 1$ if and only if x is a multiple of 2π. First we compute $(e^{(2\pi i/n)k})^n = e^{(2\pi i/n)nk} = (e^{2\pi i})^k = 1^k = 1$, so $e^{(2\pi i/n)k}$ is an nth root of unity. Now if $(k, n) = 1$, then $((2\pi i/n)k)a$ is a multiple of $2\pi i$ if and only if $n \mid a$. Therefore, $a = n$ is the least positive integer for which $(e^{(2\pi i/n)k})^a = 1$. Therefore, $e^{(2\pi i/n)k}$ is a primitive nth root of unity. Conversely, suppose that $(k, n) = d > 1$. Then $(e^{(2\pi i/n)k})^{n/d} = e^{(2\pi i)k/d} = 1$, since k/d is an integer, and so in this case, $e^{(2\pi i/n)k}$ is not a primitive nth root of unity.
b. Let $m = l + kn$, where k is an integer. Then $\zeta^m = \zeta^{l+kn} = \zeta^l \zeta^{kn} = \zeta^l$. Now suppose that ζ is a primitive nth root of unity and that $\zeta^m = \zeta^l$, and without loss of generality, assume that $m \ge l$. From the first part of this exercise, we may take $0 \le l \le m < n$. Then $0 = \zeta^m - \zeta^l = \zeta^l(\zeta^{m-l} - 1)$.

Hence, $\zeta^{m-l} = 1$. Since n is the least positive integer such that $\zeta^n = 1$, we must have $m - l = 0$.
c. First, $f(z+1) = e^{2\pi i(z+1)} - e^{-2\pi i(z+1)} = e^{2\pi iz}e^{2\pi i} - e^{-2\pi iz}e^{-2\pi i} = e^{2\pi iz} \cdot 1 - e^{-2\pi iz} \cdot 1 = f(z)$. Next, $f(-z) = e^{-2\pi iz} - e^{2\pi iz} = -(e^{2\pi iz} - e^{-2\pi iz}) = -f(z)$. Finally, suppose that $f(z) = 0$. Then $0 = e^{2\pi iz} - e^{-2\pi iz} = e^{-2\pi iz}(e^{4\pi iz} - 1)$, so $e^{4\pi iz} = 1$. Therefore, $4\pi iz = 2\pi in$ for some integer n, and so $z = n/2$.
d. Fix y, and consider $g(x) = x^n - y^n$ and $h(x) = (x - y)(\zeta x - \zeta^{-1}y) \cdots (\zeta^{n-1}x - \zeta^{-(n-1)}y)$ as polynomials in x. Both polynomials have degree n. The leading coefficient in $h(x)$ is $\zeta^{1+2+\cdots+(n-1)} = \zeta^{n(n-1)/2} = (\zeta^n)^{(n-1)/2} = 1$, since $n - 1$ is even. So both polynomials are monic. Further, note that $g(\zeta^{-2k}y) = (\zeta^{-2k}y)^n - y^n = y^n - y^n = 0$ for $k = 0, 1, 2, \ldots, n-1$. Also $h(\zeta^{-2k}y)$ has $\zeta^k\zeta^{-2k}y - \zeta^{-k}y = \zeta^{-k}y - \zeta^{-k}y = 0$ as one of its factors. So g and h are monic polynomials sharing these n distinct zeros (since $-2k$ runs through a complete set of residues modulo n). By the fundamental theorem of algebra, g and h are identical.
e. Let $x = e^{2\pi iz}$ and $y = e^{-2\pi iz}$ in the identity from part (d). Then the right-hand side becomes $\prod_{k=0}^{n-1}\left(\zeta^k e^{2\pi iz} - \zeta^{-k}e^{-2\pi iz}\right) = \prod_{k=0}^{n-1}\left(e^{2\pi i(z+k/n)} - e^{-2\pi i(z+k/n)}\right) = \prod_{k=0}^{n-1} f\left(z + k/n\right) = f(z) \cdot \prod_{k=1}^{(n-1)/2} f\left(z + k/n\right) \cdot \prod_{k=(n+1)/2}^{n-1} f\left(z + k/n\right)$. From part (c), this last product is equal to $\prod_{k=(n+1)/2}^{n-1} f\left(z + k/n\right) = \prod_{k=1}^{(n-1)/2} f\left(z + (n-k)/n\right) = \prod_{k=1}^{(n-1)/2} f\left(z + 1 - k/n\right) = \prod_{k=1}^{(n-1)/2} f\left(z - k/n\right)$. So the product above is equal to $f(z) \cdot \prod_{k=1}^{(n-1)/2} f\left(z + k/n\right) \cdot \prod_{k=1}^{(n-1)/2} f\left(z - k/n\right) = f(z) \cdot \prod_{k=1}^{(n-1)/2} f\left(z + k/n\right) \cdot f\left(z - k/n\right)$. Then noting that the left side of the identity in part (d) is $(e^{2\pi iz})^n - (e^{-2\pi iz})^n = e^{2\pi inz} - e^{-2\pi inz} = f(nz)$ finishes the proof.
f. For $l = 1, 2, \ldots, (p-1)/2$, let k_l be the least positive residue of la modulo p. Then $\prod_{l=1}^{(p-1)/2} f\left(la/p\right) = \prod_{l=1}^{(p-1)/2} f\left(k_l/p\right)$ by the periodicity of f established in part (c). We break this product into two pieces: $\prod_{k_l<p/2} f\left(k_l/p\right) \cdot \prod_{k_l>p/2} f\left(k_l/p\right) = \prod_{k_l<p/2} f\left(k_l/p\right) \cdot \prod_{k_l>p/2} -f\left(-k_l/p\right) = \prod_{k_l<p/2} f\left(k_l/p\right) \cdot \prod_{k_l>p/2} -f\left((p-k_l)/p\right) = \prod_{l=1}^{(p-1)/2} f\left(l/p\right)(-1)^N$, where N is the number of k_l exceeding $p/2$. But by Gauss's lemma, $(-1)^N = \left(\frac{a}{p}\right)$. This establishes the identity.
g. Let $z = l/p$ and $n = q$ in the identities in parts (e) and (f). Then we have $\left(\frac{q}{p}\right) = \prod_{l=1}^{(p-1)/2} f\left(lq/p\right) / f\left(l/p\right) = \prod_{l=1}^{(p-1)/2}\prod_{k=1}^{(q-1)/2} f\left(l/p + k/q\right) \cdot f\left(l/p - k/q\right) = \prod_{l=1}^{(p-1)/2}\prod_{k=1}^{(q-1)/2} f\left(k/q + l/p\right) \cdot f\left(k/q - l/p\right) \cdot (-1)^{(p-1)/2 \cdot (q-1)/2}$, where we have used the fact that $f(-z) = -f(z)$ and the fact that there are exactly $((p-1)/2) \cdot ((q-1)/2)$ factors in the double product. But by symmetry, this is exactly the expression for $\left(\frac{q}{p}\right)(-1)^{((p-1)/2)\cdot((q-1)/2)}$.

15. Since $p \equiv 1 \pmod 4$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. And since $p \equiv 1 \pmod q$ for all primes $q \leq 23$, we have $\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1$. If a is an integer with $0 < a < 29$ and prime factorization $a = p_1p_2 \cdots p_k$, then each $p_i < 29$ and $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_k}{p}\right) = 1^k = 1$. So there are no quadratic nonresidues modulo p less than 29. Further, since a quadratic residue must be an even power of any primitive root r, we know that $r = r^1$ cannot be less than 29.

17. **a.** If $a \in T$, then $a = qk$ for some $k = 1, 2, \ldots (p-1)/2$. So $1 \leq a \leq q(p-1)/2 \leq (pq-1)/2$. Furthermore, $(p, k) = 1$ because $k \leq (p-1)/2$, and p is prime. Because $(q, p) = 1$, it follows that $(a, p) = (qk, p) = 1$, so that $a \in S$, and hence, $T \subset S$. Now suppose $a \in S - T$. Then $1 \leq a \leq (pq-1)/2$ and $(a, p) = 1$. Because $a \notin T$, it follows that $a \neq qk$ for any k. We conclude that $(a, q) = 1$, which means that $(a, pq) = 1$, and so $a \in R$. Thus $S - T \subset R$. Conversely, if $a \in R$, then $1 \leq a \leq (pq-1)/2$ and $(a, pa) = 1$. This implies that $(a, q) = 1$, and so a is not a multiple of q. Hence, $a \notin T$, so that $a \in S - T$. It follows that $R \subset S - T$. Therefore, $R = S - T$.

b. By part (a), $R = S - T$, so that by Euler's criterion, $\prod_{a\in S} a = \prod_{a\in R} a \prod_{a\in T} a = A(q \cdot 2q \cdots ((p-1)/2)a)) = Aq^{(p-1)/2}((p-1)/2)! \equiv A\left(\frac{q}{p}\right)((p-1)/2)! \pmod p$. Note that $(pq-1)/2 = p(q-1)/2 + (p-1)/2$, so that we can evaluate $\prod_{a\in S} a \equiv ((p-1)!)^{(q-1)/2}((p-1)/2!) \equiv (-1)^{(q-1)/2}((p-1)/2)! \pmod p$ by Wilson's theorem. When we set these two expressions congruent to each other modulo p and simplify, we obtain $A \equiv (-1)^{(q-1)/2}\left(\frac{q}{p}\right) \pmod p$ as desired.

c. Because the roles of p and q are identical in the hypotheses and in parts (a) and (b), the result follows by symmetry.

d. Assume that $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$. Then $A = \pm 1$, so that $A \equiv \pm 1 \pmod{pq}$. Conversely, suppose that $A \equiv 1 \pmod{pq}$. Then $A \equiv 1 \pmod p$ and $A \equiv 1 \pmod q$. By parts (b) and (c), we have $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = A = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$. The same argument works if $A \equiv -1 \pmod{pq}$.

e. If a is an integer in R, it satisfies $1 \le a \le (pq-1)/2$. Therefore, its additive inverse modulo pq is in the range $(pq+1)/2 \le -a \le pq - 1$ and in the set of reduced residue classes. By the Chinese remainder theorem, the congruence $a^2 \equiv 1 \pmod{pq}$ has exactly four solutions, 1, -1, b, and $-b$ $\pmod{pq}$ and the congruence $a^2 \equiv -1 \pmod{pq}$ has solutions if and only if $p \equiv q \equiv 1 \pmod 4$, and in this case, it has exactly four solutions, i, $-i$, ib, and $-ib \pmod{pq}$. For each element $a \in R$, $(a, pq) = 1$, so a has a multiplicative inverse u. It follows that exactly one of $u, -u$ is in R. Let $U = \{a \in R \mid a^2 \equiv \pm 1 \pmod{pq}\}$. Then when we compute A, all other elements will be paired with an element that is either its inverse or the negative of its inverse. Thus, $A \equiv \prod_{a\in R} a \equiv \prod_{a\in U} a \pmod{pq}$. So if $p \equiv q \equiv 1 \pmod{pq}$, then $A \equiv \prod_{a\in U} a \equiv \pm(1 \cdot c \cdot i \cdot ic) \equiv c^2 i^2 \equiv \mp 1 \pmod{pq}$. Conversely, in the other case, $A \equiv \prod_{a\in U} a \equiv \pm(1 \cdot c) \not\equiv \pm 1 \pmod{pq}$, which completes the proof.

f. By parts (d) and (e), we have $(-1)^{(q-1)/2}\left(\frac{q}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right)$ if and only if $p \equiv q \equiv 1 \pmod 4$. So if $p \equiv q \equiv 1 \pmod 4$, we have $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. But if $p \equiv 1 \pmod 4$ while $q \equiv 3 \pmod 4$, then we must have $-\left(\frac{q}{p}\right) \ne \left(\frac{p}{q}\right)$, which means we must change the sign, yielding $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. The case where $p \equiv 3 \pmod 4$ but $q \equiv 1 \pmod 4$ is identical. If $p \equiv q \equiv 3 \pmod 4$, then we have $-\left(\frac{q}{p}\right) \ne -\left(\frac{p}{q}\right)$ so that we have $-\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, which concludes the proof.

Section 11.3

1. **a.** 1 **b.** -1 **c.** 1 **d.** 1 **e.** -1 **f.** 1

3. 1, 7, 13, 17, 19, 29, 37, 49, 71, 83, 91, 101, 103, 107, 113, or 119 (mod 120)

5. The pseudo-squares modulo 21 are 5, 17, and 20.

7. The pseudo-squares modulo 143 are 1, 3, 4, 9, 12, 14, 16, 23, 25, 27, 36, 38, 42, 48, 49, 52, 56, 64, 69, 75, 81, 82, 92, 100, 103, 108, 113, 114, 126, and 133.

9. Since n is odd and square-free, n has prime factorization $n = p_1 p_2 \cdots p_r$. Let b be one of the $(p-1)/2$ quadratic nonresidues of p_1, so that $\left(\frac{b}{p_1}\right) = -1$. By the Chinese remainder theorem, let a be a solution to the system of linear congruences $x \equiv b \pmod{p_1}$ and $x \equiv 1 \pmod{p_i}$, $2 \le i \le r$. Then $\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$, $\left(\frac{a}{p_2}\right) = \left(\frac{1}{p_2}\right) = 1$, $\ldots$, $\left(\frac{a}{p_r}\right) = \left(\frac{1}{p_r}\right) = 1$. Therefore, $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = (-1) \cdot 1 \cdots 1 = -1$.

11. **a.** Note that $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = 1$, and, since the q_i are even, the r_i are odd. Since $r_0 = b$ and $a \equiv \epsilon_1 r_1 \pmod{b}$, $\left(\frac{a}{b}\right) = \left(\frac{\epsilon_1 r_1}{r_0}\right) = \left(\frac{\epsilon_1}{r_0}\right)\left(\frac{r_1}{r_0}\right) = \left(\frac{\epsilon_1}{r_0}\right)\left(\frac{r_0}{r_1}\right) \cdot \left(-1\right)^{((r_0-1)/2)((r_1-1)/2)}$ by Theorem 11.11. If $\epsilon_1 = 1$, then $\left(\frac{a}{b}\right) = (-1)^{((r_0-1)/2)((\epsilon_1 r_1-1)/2)}\left(\frac{r_0}{r_1}\right)$. If $\epsilon_1 = -1$, then $\left(\frac{\epsilon_1}{r_0}\right) = (-1)^{((r_0-1)/2)}$, and so we have $\left(\frac{a}{b}\right) = (-1)^{((r_0-1)/2)((r_1+1)/2)}\left(\frac{r_0}{r_1}\right) = (-1)^{((r_0-1)/2)((-r_1-1)/2)}\left(\frac{r_0}{r_1}\right) = (-1)^{((r_0-1)/2)((\epsilon_1 r_1-1)/2)}\left(\frac{r_0}{r_1}\right)$ since $(r_1 + 1)/2$ and $-(r_1 - 1)/2$ have the same parity. Similarly, $\left(\frac{r_0}{r_1}\right) = (-1)^{((r_1-1)/2)((\epsilon_2 r_2-1)/2)}\left(\frac{r_1}{r_2}\right)$, so that $\left(\frac{a}{b}\right) = (-1)^{((r_0-1)/2)((\epsilon_1 r_1-1)/2)+((r_1-1)/2)((\epsilon_2 r_2-1)/2)}\left(\frac{r_1}{r_2}\right)$. Proceed inductively until the last step, when $\left(\frac{r_n}{r_{n-1}}\right) = \left(\frac{1}{r_{n-1}}\right) = 1$.
b. If either $r_{i-1} \equiv 1 \pmod 4$ or $\epsilon_i r_i \equiv 1 \pmod 4$, then $((r_{i-1} - 1)/2)((\epsilon_i r_i - 1)/2)$ is even. Otherwise, that is, if $r_{i-1} \equiv \epsilon_i r_i \equiv 3 \pmod 4$, then $((r_{i-1} - 1)/2)((\epsilon_i r_i - 1)/2)$ is odd. Then $((r_{n-1} - 1)/2)((\epsilon_n r_n - 1)/2)$, the exponent in part (a), is even or odd as T is even or odd.

13. **a.** -1 **b.** -1 **c.** -1

15. Let $n_1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ and $n_2 = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$ be the prime factorizations of n_1 and n_2. Then by the definition of the Kronecker symbol, $\left(\frac{a}{n_1 n_2}\right) = \left(\frac{a}{p_1}\right)^{a_1} \cdots \left(\frac{a}{p_r}\right)^{a_r}\left(\frac{a}{q_1}\right)^{b_1} \cdots \left(\frac{a}{q_s}\right)^{b_s} = \left(\frac{a}{n_1}\right)\left(\frac{a}{n_2}\right)$.

17. If $a \equiv 1 \pmod 4$, then by Exercise 16, we have $\left(\frac{a}{n_1}\right) = \left(\frac{n_1}{|a|}\right)$. This last is equivalent to the Jacobi symbol, so by Theorem 11.10(i), we have $\left(\frac{n_1}{|a|}\right) = \left(\frac{n_2}{|a|}\right) = \left(\frac{a}{n_2}\right)$, using Exercise 16 again. If $a \equiv 0 \pmod 4$, say $a = 2^s t$ with t odd and $s \geq 2$, then Exercise 16 gives $\left(\frac{a}{n_1}\right) = \left(\frac{2}{n_1}\right)^s (-1)^{((t-1)/2)\cdot((n_1-1)/2)}\left(\frac{n_1}{|a|}\right)$ and $\left(\frac{a}{n_2}\right) = \left(\frac{2}{n_2}\right)^s (-1)^{((t-1)/2)\cdot((n_2-1)/2)}\left(\frac{n_2}{|t|}\right)$. Since $n_1 \equiv n_2 \pmod{|t|}$, we have $\left(\frac{n_1}{|t|}\right) = \left(\frac{n_2}{|t|}\right)$, and since $4 \mid a$, we have $n_1 \equiv n_2 \pmod 4$, and so $(-1)^{((t-1)/2)\cdot((n_1-1)/2)} = (-1)^{((t-1)/2)\cdot((n_2-1)/2)}$. If $s = 2$, then certainly $\left(\frac{2}{n_1}\right)^2 = \left(\frac{2}{n_2}\right)^2$. If $s > 2$, then $8 \mid a$ and $n_1 \equiv n_2 \pmod 8$, and hence $n_1^2 \equiv n_2^2 \pmod 8$. So $\left(\frac{2}{n_1}\right) = (-1)^{(n_1^2-1)/8} = (-1)^{(n_2^2-1)/8} = \left(\frac{2}{n_2}\right)$. Therefore, $\left(\frac{a}{n_1}\right) = \left(\frac{a}{n_2}\right)$.

19. If $a \equiv 1 \pmod 4$, then $|a| \equiv 1 \pmod 4$ if $a > 0$ and $|a| \equiv -1 \pmod 4$ if $a < 0$, so by Exercise 16, $\left(\frac{a}{|a|-1}\right) = \left(\frac{|a|-1}{|a|}\right) = \left(\frac{-1}{|a|}\right) = (-1)^{\frac{|a|-1}{2}} = 1$ if $a > 0$ and $= -1$ if $a < 0$. If $a \equiv 0 \pmod 4$, then $a = 2^s t$ with t odd and $t \geq 2$, so by Exercise 16, $\left(\frac{a}{|a|-1}\right) = \left(\frac{2}{|a|-1}\right)^s (-1)^{\frac{t-1}{2}}\left(\frac{|a|-1}{|t|}\right)$. Since $s \geq 2$, check that $\left(\frac{2}{|a|-1}\right)^s = 1$. (Indeed, $|a| - 1 \equiv 7 \pmod 8$ if $s > 2$.) Also $(-1)^{\frac{t-1}{2}}\left(\frac{|a|-1}{|t|}\right) = (-1)^{\frac{t-1}{2}}\left(\frac{-1}{|t|}\right) = (-1)^{\frac{t-1}{2}+\frac{|t|-1}{2}} = 1$ if $t > 0$ and $= -1$ if $t < 0$.

Section 11.4

1. We have $2^{(561-1)/2} = 2^{280} = (2^{10})^{28} \equiv (-98)^{28} \equiv ((-98)^2)^{14} \equiv 67^{14} \equiv (67^2)^7 \equiv 1^7 = 1 \pmod{561}$. Furthermore, we see that $\left(\frac{2}{561}\right) = 1$ since $561 \equiv 1 \pmod 8$. But $561 = 3 \cdot 11 \cdot 17$ is not prime.

3. Suppose that n is an Euler pseudoprime to both the bases a and b. Then $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ and $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$. It follows that $(ab)^{(n-1)/2} \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) = \left(\frac{ab}{n}\right)$. Hence, n is an Euler pseudoprime to the base ab.

5. Suppose that $n \equiv 5 \pmod 8$ and n is an Euler pseudoprime to the base 2. Since $n \equiv 5 \pmod 8$ we have $\left(\frac{2}{n}\right) = -1$. Since n is an Euler pseudoprime to the base 2, we have $2^{(n-1)/2} \equiv \left(\frac{2}{n}\right) \equiv -1 \pmod n$. Write $n - 1 = 2^2 t$, where t is odd. Since $2^{(n-1)/2} \equiv 2^{2t} \equiv -1 \pmod n$, n is a strong pseudoprime to the base 2.

7. $n \equiv 5 \pmod{40}$

9. 80

Section 11.5

1. 1229

3. Since $p, q \equiv 3 \pmod 4$, we know that -1 is not a quadratic residue modulo p or q. If the four square roots are found using the method in Example 11.19, then only one of each possibility for choosing $+$ or $-$ can yield a quadratic residue in each congruence, so there is only one system that results in a square.

5. If Paula chooses $c = 13$, then $v \equiv 713$, which is a quadratic residue of 1411, and which has square root $u \equiv 837 \pmod{1411}$. Her random number is 822, so she computes $x \equiv 822^2 \equiv 1226 \pmod{1411}$ and $y \equiv v\overline{x} \equiv 713 \cdot 961 \equiv 858 \pmod{1411}$. She sends $x \equiv 1226$, $y \equiv 858$ to Vince. Vince checks that $xy \equiv 1226 \cdot 858 \equiv 713 \pmod{1411}$ and then sends the bit $b = 1$ to Paula, so she computes $\overline{r} \equiv \overline{822} \equiv 1193 \pmod{1411}$ and then $u\overline{r} \equiv 837 \cdot 1193 \equiv 964 \pmod{1411}$, which she sends to Vince. Since Vince sent $b = 1$, he computes $964^2 \equiv 858 \pmod{1411}$ and notes that it is indeed equal to y.

7. The prover sends $x = 1403^2 \equiv 1968409 \equiv 519 \pmod{2491}$. The verifier sends $\{1, 5\}$. The prover sends $y = 1425$. The verifier computes $y^2 \cdot s_1 \cdot s_5 = 1425^2 \cdot 197 \cdot 494 \equiv 519 \equiv x \pmod{2491}$.

9. **a.** 959, 1730, 2895, 441, 2900, 2684 **b.** 1074 **c.** $1074^2 \cdot 959 \cdot 1730 \cdot 441 \cdot 2684 \equiv 336 \equiv 403^2 \pmod{3953}$

11. If Paula sends back a to Vince, then $a^2 \equiv w^2 \pmod n$, with $a \not\equiv w \pmod n$. Then $a^2 - w^2 = (a - w)(a + w) \equiv 0 \pmod n$. By computing $(a - w, n)$ and $(a + w, n)$, Vince can produce a nontrivial factor of n.

Section 12.1

1. **a.** .4 **b.** $.41\overline{6}$ **c.** $\overline{.923076}$ **d.** $.5\overline{3}$ **e.** $\overline{.009}$ **f.** $\overline{.000999}$

3. **a.** 3/25 **b.** 11/90 **c.** 4/33

5. $b = 2^r 3^s 5^t 7^u$, with r, s, t, and u positive integers

7. **a.** pre-period 1, period 0 **b.** pre-period 2, period 0 **c.** pre-period 1, period 4 **d.** pre-period 2, period 0 **e.** pre-period 11, period 1 **f.** pre-period 2, period 4

9. **a.** 3 **b.** 11 **c.** 37 **d.** 101 **e.** 41, 271 **f.** 7, 13

11. Using the construction from Theorem 12.2 and Example 12.1, we show by mathematical induction that $c_k = k - 1$ and $\gamma_k = (kb - k + 1)/(b - 1)^2$. The inductive step is as follows: $c_{k+1} = \lfloor b\gamma_k \rfloor = \left\lfloor (kb^2 - bk + b)/(b - 1)^2 \right\rfloor = \left\lfloor (k(b - 1)^2 + b(k + 1) - k)/(b - 1)^2 \right\rfloor = \left\lfloor k + (b(k + 1) - k)/(b - 1)^2 \right\rfloor = k$, and $\gamma_{k+1} = (k + 1)b - k$, if $k \neq b - 2$. If $k = b - 2$, then

$c_{b-2} = b$, so we have determined $b - 1$ consecutive digits of the expansion. From the binomial theorem, $(x + 1)^a \equiv ax + 1 \pmod{x^2}$, so $\text{ord}_{(b-1)^2} b = b - 1$, which is the period length. Therefore, we have determined the entire expansion.

13. The base b expansion is $(.100100001\ldots)_b$, which is nonrepeating and therefore, by Theorem 12.4, represents an irrational number.

15. Let γ be a real number. Set $c_0 = [\gamma]$ and $\gamma_1 = \gamma - c_0$. Then $0 \le \gamma_1 < 1$ and $\gamma = c_0 + \gamma_1$. From the condition that $c_k < k$ for $k = 1, 2, 3, \ldots$, we must have $c_1 = 0$. Let $c_2 = [2\gamma_1]$ and $\gamma_2 = 2\gamma_1 - c_2$. Then $\gamma_1 = (c_2 + \gamma_2)/2$, so $\gamma = c_0 + c_1/1! + c_2/2! + \gamma_2/2!$. Now let $c_3 = [3\gamma_2]$ and $\gamma_3 = 3\gamma_2 - c_3$. Then $\gamma_2 = (c_3 + \gamma_3)/3$ and so $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \gamma_3/3!$. Continuing in this fashion, for each $k = 2, 3, \ldots$, define $c_k = [k\gamma_{k-1}]$ and $\gamma_k = k\gamma_{k-1} - c_k$. Then $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \cdots + c_k/k! + \gamma_k/k!$. Since each $\gamma_k < 1$, we know that $\lim_{k\to\infty} \gamma_k/k! = 0$, so we conclude that $\gamma = c_0 + c_1/1! + c_2/2! + c_3/3! + \cdots + c_k/k! + \cdots$.

17. In the proof of Theorem 12.2, the numbers $p\gamma_n$ are the remainders of b^n upon division by p. The process recurs as soon as some γ_i repeats a value. Since $1/p = (.\overline{c_1 c_2 \ldots c_{p-1}})$ has period length $p - 1$, we have, by Theorem 12.4, that $\text{ord}_p b = p - 1$, so there is an integer k such that $b^k \equiv m \pmod{p}$. So the remainders of mb^n upon division by p are the same as the remainders of $b^k b^n$ upon division by p. Hence, the nth digit of the expansion of m/p is determined by the remainder of b^{k+n} upon division by p. Therefore, it will be the same as the $(k + n)$th digit of $1/p$.

19. n must be prime with 2 a primitive root.

21. Let $\gamma b^{j-1} = a + \epsilon$, where a is an integer and $0 \le \epsilon < 1$. Then $[\gamma b^j] - b[\gamma b^{j-1}] = [(a + \epsilon)b] - b[a + \epsilon] = ab + [\epsilon b] - ab = [\epsilon b]$. Since $0 \le \epsilon < 1$, this last expression is an integer between 0 and $b - 1$. Therefore, $0 \le [\gamma b^j] - b[\gamma b^{j-1}] \le b - 1$. Now consider the sum $\sum_{j=1}^{N}([\gamma b^j] - b[\gamma b^{j-1}])/b^j$. Factor out $1/b^N$ to clear fractions and this becomes $(1/b^N)\sum_{j=1}^{N}(b^{N-j}[\gamma b^j] - b^{N-(j-1)}[\gamma b^{j-1}])$. This sum telescopes to $(-b^N[\gamma] + [\gamma b^N])/b^N = [\gamma b^N]/b^N$ since $[\gamma] = 0$. But $[\gamma b^N]/b^N = (\gamma b^N - \gamma b^N + [\gamma b^N])/b^N = \gamma - (\gamma b^N - [\gamma b^N])/b^N$. But $0 \le \gamma b^N - [\gamma b^N] < 1$, so taking limits as $N \to \infty$ of both sides of this equation yields $\gamma = \sum_{j=1}^{\infty}([\gamma b^j] - b[\gamma b^{j-1}])/b^j$. By the uniqueness of the base b expansion given in Theorem 12.1, we must have $c_j = [\gamma b^j] - b[\gamma b^{j-1}]$ for each j.

23. Let $\alpha = \sum_{i=1}^{\infty}(-1)^{a_i}/10^{i!}$ and $p_k/q_k = \sum_{i=1}^{k}(-1)^{a_i}/10^{i!}$. Then $|\alpha - p_k/q_k| = \left|\sum_{i=k+1}^{\infty}(-1)^{a_i}/10^{i!}\right| \le \sum_{i=k+1}^{\infty} 1/10^{i!}$. As in the proof of Corollary 12.5.1, it follows that $|\alpha - p_k/q_k| < 2/10^{(k+1)!}$, which shows that there can be no real number C, as in Theorem 12.5. Hence, α must be transcendental.

25. Suppose that $e = h/k$. Then $k!(e - 1 - 1/1! - 1/2! - \cdots - 1/k!)$ is an integer. But this is equal to $k!(1/(k + 1)! + 1/(k + 2)! + \cdots) = 1/(k + 1) + 1/((k + 1)(k + 2)) + \cdots < 1/(k + 1) + 1/(k + 1)^2 + \cdots = 1/k < 1$. But $k!(e - 1 - 1/1! - 1/2! - \cdots - 1/k!)$ is positive, and therefore cannot be an integer, a contradiction.

Section 12.2

1. **a.** 15/7 **b.** 10/7 **c.** 6/31 **d.** 355/113 **e.** 2 **f.** 3/2 **g.** 5/3 **h.** 8/5

3. **a.** [1; 2, 1, 1, 2] **b.** [1; 1, 7, 2] **c.** [2; 9] **d.** [3; 7, 1, 1, 1, 1, 2] **e.** [−1; 13, 1, 1, 2, 1, 1, 2, 2] **f.** [0, 9, 1, 3, 6, 2, 4, 1, 2]

5. **a.** 1, 3/2, 4/3, 7/5, 18/13 **b.** 1, 2, 15/8, 32/17 **c.** 2, 19/9
d. 3, 22/7, 25/8, 47/15, 72/23, 119/38, 310/99
e. −1, −12/13, −13/14, −25/27, −63/68, −88/95, −151/163, −390/421, −931/1005
f. 0, 1/9, 1/10, 4/39, 25/244, 54/527, 241/2352, 295/2879, 831/8110

7. **a.** $3/2 > 7/5$ and $1 < 4/3 < 18/13$ **b.** $2 > 32/17$ and $1 < 15/8$ **c.** vacuous
d. $22/7 > 47/15 > 119/38$ and $3 < 25/8 < 72/23 < 310/99$
e. $-12/13 > -25/27 > -88/95 > -390/421$ and $-1 < -13/14 < -63/68 < -151/163 < -931/1005$
f. $1/9 > 4/39 > 54/527 > 295/2879$ and $0 < 1/10 < 25/244 < 241/2352 < 831/8110$

9. Let $\alpha = r/s$. The Euclidean algorithm for $1/\alpha = s/r < 1$ gives $s = 0(r) + s$, $r = a_0(s) + a_1$, and continues just as for r/s.

11. Proceed by induction. The basis case is trivial. Assume that $q_j \geq f_j$ for $j < k$. Then $q_k = a_k q_{k-1} + q_{k-2} \geq a_k f_{k-1} + f_{k-2} \geq f_{k-1} + f_{k-2} = f_k$, as desired.

13. By Exercise 10, we have $p_n/p_{n-1} = [a_n; a_{n-1}, \ldots, a_0] = [a_0; a_1, \ldots, a_n] = p_n/q_n = r/s$ if the continued fraction is symmetric. Then $q_n = p_{n-1} = s$ and $p_n = r$, so by Theorem 12.10, we have $p_n q_{n-1} - q_n p_{n-1} = r q_{n-1} - s^2 = (-1)^{n-1}$. Then $r q_{n-1} = s^2 + (-1)^{n-1}$, and so $r \mid s^2 + (-1)^{n-1}$. Conversely, if $r \mid s^2 + (-1)^{n-1}$, then $(-1)n - 1 = p_n q_{n-1} - q_n p_{n-1} = r q_{n-1} - p_{n-1}s$. Therefore, $r \mid p_{n-1}s + (-1)^{n-1}$, and hence, $r \mid (s^2 + (-1)^{n-1}) - (p_{n-1}s + (-1)^{n-1}) = s(s - p_{n-1})$. Since $s, p_{n-1} < r$ and $(r, s) = 1$, we have $s = p_{n-1}$. Then $[a_n; a_{n-1}, \ldots, a_0] = p_n/p_{n-1} = r/s = [a_0; a_1, \ldots, a_n]$.

15. Note that the notation $[a_0; a_1, \ldots, a_n]$ makes sense, even if the a_j are not integers. Use induction. Assume that the statement is true for k odd and prove it for $k + 2$. Define $a'_k = [a_k; a_{k+1}, a_{k+2}]$ and check that $a'_k < [a_k; a_{k+1}, a_{k+2} + x] = a'_k + x'$. Then $[a_0; a_1, \ldots, a_{k+2}] = [a_0; a_1, \ldots, a'_k] > [a_0; a_1, \ldots, a'_k + x'] = [a_0; a_1, \ldots, a_{k+2} + x]$. Proceed similarly for k even.

Section 12.3

1. **a.** $[1; 2, 2, 2, \ldots]$ **b.** $[1; 1, 2, 1, 2, \ldots]$ **c.** $[2; 4, 4, 4, \ldots]$ **d.** $[1; 1, 1, 1, \ldots]$

3. $312689/99532$

5. If $a_1 > 1$, let $A = [a_2; a_3, \ldots]$. Then $[a_0; a_1, \ldots] + [-a_0 - 1; 1, a_1 - 1, a_2, a_3, \ldots] = a_0 + 1/(a_1 + 1/A) + \big(-a_0 - 1 + 1/(1 + 1/(a_1 - 1 + 1/A))\big) = 0$. Similarly if $a_1 = 1$.

7. If $\alpha = [a_0; a_1, a_2, \ldots]$, then $1/\alpha = 1/[a_0; a_1, a_2, \ldots] = 0 + 1/(a_0 + 1/(a_1 + \cdots)) = [0; a_0, a_1, a_2, \ldots]$. Then the kth convergent of $1/\alpha$ is $[0; a_0, a_1, a_2, \ldots, a_{k-1}] = 1/[a_0; a_1, a_2, \ldots, a_{k-1}]$, which is the reciprocal of the $(k-1)$th convergent of α.

9. By Theorem 12.19, such a p/q is a convergent of α. Now $(\sqrt{5}+1)/2 = [1; 1, 1, \ldots]$, so $q_n = f_n$ (Fibonacci) and $p_n = q_{n+1}$. Then $\lim_{n\to\infty} q_{n-1}/q_n = \lim_{n\to\infty} q_{n-1}/p_{n-1} = 2/(\sqrt{5}+1) = (\sqrt{5}-1)/2$. Therefore, $\lim_{n\to\infty}((\sqrt{5}+1)/2 + q_{n-1}/q_n) = (\sqrt{5}+1)/2 + (\sqrt{5}-1)/2 = \sqrt{5}$. So $(\sqrt{5}+1)/2 + q_{n-1}/q_n > c$ only finitely often, whence $1/(((\sqrt{5}+1)/2 + q_{n-1}/q_n)q_n^2) < 1/(cq_n^2)$. The following identity finishes the proof. Note that $\alpha_n = \alpha$ for all n. Then $\left|\alpha - p_n/q_n\right| = \left|(\alpha_{n+1}p_n + p_{n-1})/(\alpha_{n+1}q_n + q_{n-1}) - p_n/q_n\right| = \left|-(p_n q_{n-1} - p_{n-1}q_n)/(q_n(\alpha q_n + q_{n-1}))\right| = 1/(q_n^2(\alpha + q_{n-1}/q_n))$.

11. If β is equivalent to α, then $\beta = (a\alpha + b)/(c\alpha + d)$. Solving for α gives $\alpha = (-d\beta + b)/(c\beta - a)$, so α is equivalent to β.

13. By symmetry and transitivity (Exercises 11 and 12), it suffices to show that every rational number $\alpha = m/n$ (which we can assume is in lowest terms) is equivalent to 1. By the Euclidean algorithm, we can find a and b such that $ma + nb = 1$. Let $d = m + b$ and $c = a - n$. Then $(a\alpha + b)/(c\alpha + d) = 1$.

15. Note that $p_{k,t}q_{k-1} - q_{k,t}p_{k-1} = t(p_{k-1}q_{k-1} - q_{k-1}p_{k-1}) + (p_{k-2}q_{k-1} - p_{k-1}q_{k-2}) = \pm 1$. Thus $p_{k,t}$ and $q_{k,t}$ are relatively prime.

17. See, for example, the classic work by O. Perron, *Die Lehre von den Kettenbrüchen*, Leipzig, Teubner (1929).

19. 179/57

21. Note first that if $b < d$, then $|a/b - c/d| < 1/2d^2$ implies that $|ad - bc| < b/2d < 1/2$. Because $b \neq d$, $|ad - bc|$ is a positive integer, and so is greater than $1/2$. Thus $b \geq d$. Now assume that c/d is not a convergent of the continued fraction for a/b. Since the denominators of the convergents increase to b, there must be two successive convergents p_n/q_n and p_{n+1}/q_{n+1} such that $q_n < d < q_{n+1}$. Next, by the triangle inequality, $\frac{1}{2d^2} > \left|\frac{a}{b} - \frac{c}{d}\right| = \left|\frac{c}{d} - \frac{p_n}{q_n}\right| - \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \geq \left|\frac{c}{d} - \frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|$, because the $(n+1)$st convergent is on the other side of a/b from the nth convergent. Because the numerator of the first difference is a nonzero integer, applying Corollary 12.10.2 to the second difference shows that the last expression is greater than or equal to $1/dq_n - 1/q_{n+1}q_n$. If we multiply through by d^2, we obtain $\frac{1}{2} > \frac{d}{q_n}\left(1 - \frac{d}{q_{n+1}}\right) > 1 - \frac{d}{q_{n+1}}$ because $d/q_n > 1$. We deduce that $1/2 < d/q_{n+1}$.

The convergents p_n/q_n and p_{n+1}/q_{n+1} divide the line into three regions. As c/d could be in any of these, there are three cases.

Case 1: If c/d is between the convergents, then $\frac{1}{dq_n} \leq \left|\frac{c}{d} - \frac{p_n}{q_n}\right|$, because the numerator of the fraction is a positive integer and the denominators on both sides of the inequality are the same. This last term is less than or equal to $\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n}$, because the $n+1$st convergent is further from the nth convergent than c/d, where we have applied Corollary 12.10.2. But this implies that $d \geq q_{n+1}$, a contradiction.

Case 2: If c/d is closer to p_n/q_n, then we also have $\frac{1}{dq_n} \leq \left|\frac{c}{d} - \frac{p_n}{q_n}\right| \leq \left|\frac{a}{b} - \frac{c}{d}\right|$, because a/b is on the other side of the nth convergent from c/d. But this last term is less than $1/2d^2$, and if we multiply through by d we have $1/q_n < 1/2d$, which implies that $q_n > d$, a contradiction.

Case 3: If c/d is closer to p_{n+1}/q_{n+1}, then with the same reasoning as in Case 2, we have $\frac{1}{dq_{n+1}} \leq \left|\frac{c}{d} - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\frac{a}{b} - \frac{c}{d}\right| < 1/2d^2$. But this implies that $d/q_{n+1} < 1/2$, contradicting the inequality established above. Having exhausted all the cases, we must conclude that c/d must be a convergent of the continued fraction for a/b.

Section 12.4

1. **a.** $[2; \overline{1, 1, 1, 4}]$ **b.** $[3; \overline{3, 6}]$ **c.** $[4; \overline{1, 3, 1, 8}]$ **d.** $[6; \overline{1, 5, 1, 12}]$ **e.** $[7; \overline{1, 2, 7, 2, 1, 14}]$ **f.** $[9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}]$

3. **a.** $[2; \overline{2}]$ **b.** $[1; \overline{2, 2, 2, 1, 12, 1}]$ **c.** $[0; 1, 1, \overline{2, 3, 10, 3}]$

5. **a.** $(23 + \sqrt{29})/10$ **b.** $(-1 + 3\sqrt{5})/2$ **c.** $(8 + \sqrt{82})/6$

7. **a.** $\sqrt{10}$ **b.** $\sqrt{17}$ **c.** $\sqrt{26}$ **d.** $\sqrt{37}$

9. **a.** We have $\alpha_0 = \sqrt{d^2 - 1}$, $a_0 = d - 1$, $P_0 = 0$, $Q_0 = 1$, $P_1 = d - 1$, $Q_1 = 2d - 2$, $\alpha_1 = \frac{1}{2} + \frac{1}{2}\sqrt{(d+1)/(d-1)}$, $a_1 = 1$, $P_2 = d - 1$, $Q_2 = 1$, $\alpha_2 = d - 1 + \sqrt{d^2 - 1}$, $a_2 = 2d - 2$, $P_3 = d - 1 = P_1$, $Q_3 = 2d - 2 = Q_1$, so $\alpha = [d - 1; \overline{1, 2(d-1)}]$.
b. We have $\alpha_0 = \sqrt{d^2 - d}$, $a_0 = d - 1$ since $(d-1)^2 < d^2 - d < d^2$. Then $P_0 = 0$, $Q_0 = 1$, $P_1 = d - 1$, $Q_1 = d - 1$, $\alpha_1 = 1 + \sqrt{d/(d-1)}$, $a_1 = 2$, $P_2 = d - 1$, $Q_2 = 1$, $\alpha_2 = (d-1) + \sqrt{d^2 - d}$, $a_2 = 2(d-1)$, $P_3 = P_1$, $Q_3 = Q_1$. Therefore, $\sqrt{d^2 - d} = [d - 1; \overline{2, 2(d-1)}]$.
c. $[9; \overline{1, 18}]$, $[10; \overline{2, 20}]$, $[16; \overline{2, 32}]$, $[24; \overline{2, 48}]$

11. **a.** Note that $d < \sqrt{d^2 + 4} < d + 1$. Then $\alpha_0 = \sqrt{d^2 + 4}$, $a_0 = d$, $P_0 = 0$, $Q_0 = 1$, $P_1 = d$, $Q_1 = 4$, $\alpha_1 = (d + \sqrt{d^2 + 4})/4$, $a_1 = \lfloor 2d/4 \rfloor = (d-1)/2$, since d is odd. Also, $P_2 = d - 2$,

$Q_2 = d$, $\alpha_2 = (d - 2 + \sqrt{d^2+4})/d$, $((d-2)+d)/d < \alpha_2 < (d-2+d+1)/d$, so $a_2 = 1$, $P_3 = 2$, $Q_3 = d$, $\alpha_3 = (2 + \sqrt{d^2+4})/d$, $a_3 = 1$, $P_4 = d-2$, $Q_4 = 4$, $\alpha_4 = (d - 2 + \sqrt{d^2+4})/4$, $(d-2+d)/4 = (d-1)/2 < \alpha_4 < (d-2+d+1)/4$, so $a_4 = (d-1)/2$, $P_5 = d$, $Q_5 = 1$, $\alpha_5 = d + \sqrt{d^2+4}$, $a_5 = 2d$, $P_6 = d = P_1$, $Q_6 = 4 = Q_1$. Thus $\alpha = [d; \overline{(d-1)/2, 1, 1, (d-1)/2, 2d}]$.

b. Note that $d - 1 < \sqrt{d^2-4} < d$. Then $\alpha_0 = \sqrt{d^2-4}$, $a_0 = d-1$, $P_0 = 0$, $Q_0 = 1$, $P_1 = d-1$, $Q_1 = 2d-5$, $\alpha_1 = (d - 1 + \sqrt{d^2-4})/(2d-5)$, $(d-1+d-1)/(2d-5) < \alpha_0 < (d-1+d)/(2d-5)$ and $d > 3$, so $a_1 = 1$, $P_2 = d-4$, $Q_2 = 4$, $a_2 = (d - 4 + \sqrt{d^2-4})/4$, $a_2 = (d-3)/2$, $P_3 = d-2$, $Q_3 = d-2$, $\alpha_3 = (d - 2 + \sqrt{d^2-4})/(d-2)$, $a_3 = 2$, $P_4 = d-2$, $Q_4 = 4$, $\alpha_4 = (d - 2 + \sqrt{d^2-4})/4$, $a_4 = (d-3)/2$, $P_5 = d-4$, $Q_5 = 2d-5$, $\alpha_5 = (d - 4 + \sqrt{d^2-4})/(2d-5)$, $a_5 = 1$, $P_6 = d-1$, $Q_6 = 1$, $\alpha_6 = d - 1 + \sqrt{d^2-4}$, $a_6 = 2d-2$, $P_7 = d-1 = P_1$, $Q_7 = 2d-5 = Q_1$. Thus $\alpha = [d-1; \overline{1, (d-3)/2, 2, (d-3)/2, 1, 2d-2}]$.

13. Suppose that $\sqrt{d}$ has period length two. Then $\sqrt{d} = [a; \overline{c, 2a}]$ from the discussion preceding Example 12.15. Then $\sqrt{d} = [a; y]$ with $y = [\overline{c; 2a}] = [c; 2a, y] = c + 1/(2a + 1/y) = (2acy + c + y)/(2ay + 1)$. Then $2ay^2 - 2acy - c = 0$, and since y is positive, $y = (2ac + \sqrt{(2ac)^2 + 4(2a)c})/(4a) = (ac + \sqrt{(ac)^2 + 2ac})/(2a)$. Then $\sqrt{d} = [a; y] = a + 1/y = a + 2a/(ac + \sqrt{(ac)^2 + 2ac}) = \sqrt{a^2 + 2a/c}$, so $d = a^2 + 2a/c$, and $b = 2a/c$ is an integral divisor of $2a$. Conversely, let $\alpha = \sqrt{a^2+b}$ and $b \mid 2a$, say $kb = 2a$. Then $a_0 = [\sqrt{a^2+b}] = a$, since $a^2 < a^2 + b < (a+1)^2$. Then $P_0 = 0$, $Q_0 = 1$, $P_1 = a$, $Q_1 = b$, $\alpha_1 = (a + \sqrt{a^2+b})/b$, $a_1 = 4k$, $P_2 = a$, $Q_2 = 1$, $\alpha_2 = a + \sqrt{a^2+b}$, $a_2 = 2a$, $P_3 = a = P_1$, $Q_3 = b = Q_1$, so $\alpha = [a; \overline{4k, 2a}]$, which has period length two.

15. **a.** no **b.** yes **c.** yes **d.** no **e.** yes **f.** no

17. Let $\alpha = (a + \sqrt{b})/c$. Then $-1/\alpha' = -c/(a - \sqrt{b}) = (ca + \sqrt{bc^2})/(b - a^2) = (A + \sqrt{B})/C$, say. By Exercise 16, $0 < a < \sqrt{b}$ and $\sqrt{b} - a < c < \sqrt{b} + a < 2\sqrt{b}$. Multiplying by c gives $0 < ca < \sqrt{bc^2}$ and $\sqrt{bc^2} - ca < c^2 < \sqrt{bc^2} + ca < 2\sqrt{bc^2}$. That is, $0 < A < \sqrt{B}$ and $\sqrt{B} - A < c^2 < \sqrt{B} + A < 2\sqrt{B}$. Multiply $\sqrt{b} - a < c$ by $\sqrt{b} + a$ to get $C = b - a^2 < \sqrt{bc^2} + ca = A + \sqrt{B}$. Multiply $c < \sqrt{b} + a$ by $\sqrt{b} - a$ to get $\sqrt{B} - A = \sqrt{bc^2} - ac < b - a^2 = C$. So, $-1/\alpha'$ satisfies all the inequalities in Exercise 16 and therefore is reduced.

19. Start with $\alpha_0 = \sqrt{D_k} + 3^k + 1$ (this will have the same period since it differs from $\sqrt{D_k}$ by an integer) and use induction. Apply the continued fraction algorithm to show that $\alpha_{3i} = \sqrt{D_k} + 3^k - 2 \cdot 3^{k-i} + 2/(2 \cdot 3^{k-i})$ for $i = 1, 2, \ldots, k$, but $\alpha_{3k+3i} = \sqrt{D_k} + 3^k - 2/(2 \cdot 3^i)$ for $i = 1, 2, \ldots, k-1$, and $\alpha_{6k} = \sqrt{D_k} + 3^k + 1 = \alpha_0$. Since $\alpha_i \neq \alpha_0$ for $i < 6k$, the period is $6k$.

Section 12.5

1. Note that $19^2 - 2^2 = (19-2)(19+2) \equiv 0 \pmod{119}$. Then $(19-2, 119) = (17, 119) = 17$ and $(19+2, 119) = (21, 119) = 7$ are factors of 119.

3. $3119 \cdot 4261$

5. We have $17^2 = 289 \equiv 3 \pmod{143}$ and $19^2 = 361 \equiv 3 \cdot 5^2 \pmod{143}$. Combining these, we have $(17 \cdot 19)^2 \equiv 3^2 5^2 \pmod{143}$. Hence, $323^2 \equiv 15^2 \pmod{143}$. It follows that $323^2 - 15^2 = (323 - 15)(323 + 15) \equiv 0 \pmod{143}$. This produces the two factors $(323 - 15, 143) = (308, 143) = 11$ and $(323 + 15, 143) = (338, 143) = 13$ of 143.

7. $3001 \cdot 4001$

Section 13.1

1. **a.** (3, 4, 5), (5, 12, 13), (15, 8, 17), (7, 24, 25), (21, 20, 29), (35, 12, 37)
b. those in part (a) and (6, 8, 10), (9, 12, 15), (12, 16, 20), (15, 20, 25), (18, 24, 30), (21, 28, 35), (24, 32, 40), (10, 24, 26), (15, 36, 39), (30, 16, 34)

3. By Lemma 13.1, 5 divides at most one of x, y, and z. If $5 \not| x$ or y, then $x^2 \equiv \pm 1 \pmod 5$ and $y^2 \equiv \pm 1 \pmod 5$. Then $z^2 \equiv 0$, 2, or $-2 \pmod 5$. But ± 2 is not a quadratic residue modulo 5, so $z^2 \equiv 0 \pmod 5$, whence $5 \not| z$.

5. Let k be an integer ≥ 3. If $k = 2n + 1$, let $m = n + 1$. Then m and n have opposite parity, $m > n$ and $m^2 - n^2 = 2n + 1 = k$, so m and n define the desired triple. If k has an odd divisor $d > 1$, then use the construction above for d and multiply the result by k/d. If k has no odd divisors, then $k = 2^j$ for some integer $j > 1$. Let $m = 2^{j-1}$ and $n = 1$. Then $k = 2mn$, $m > n$, and m and n have opposite parity, so m and n define the desired triple.

7. Substituting $y = x + 1$ into the Pythagorean equation gives us $2x^2 + 2x + 1 = z^2$, which is equivalent to $m^2 - 2z^2 = -1$, where $m = 2x + 1$. Dividing by z^2 yields $m^2/z^2 - 2 = -1/z^2$. Note that $m/z \geq 1$ and $1/z^2 = 2 - m^2/z^2 = (\sqrt{2} + m/z)(\sqrt{2} - m/z) < 2(\sqrt{2} - m/z)$. So by Theorem 12.19, m/z must be a convergent of the continued fraction expansion of $\sqrt{2}$. Further, by the proof of Theorem 12.13, it must be one of even-subscripted convergents. Therefore, each solution is given by the recurrence $m_{n+1} = 3m_n + 2z_n$, $z_{n+1} = 2m_n + 3m_n$. (See, for example, Theorem 13.11.) Substituting x back in yields the recurrences of Exercise 6.

9. see Exercise 15 with $p = 3$

11. (9, 12, 15), (35, 12, 37), (5, 12, 13), (12, 16, 20)

13. $x = 2m$, $y = m^2 - 1$, $z = m^2 + 1$, $m > 1$

15. primitive solutions given by $x = (m^2 - pn^2)/2$, $y = mn$, $z = (m^2 + pn^2)/2$, where $m > \sqrt{p}n$

17. Substituting $f_n = f_{n+2} - f_{n+1}$ and $f_{n+3} = f_{n+2} + f_{n+1}$ into $(f_n f_{n+3})^2 + (2f_{n+1}f_{n+2})^2$ yields $(f_{n+2} - f_{n+1})^2(f_{n+2} + f_{n+1})^2 + 4f_{n+1}^2 f_{n+2}^2 = (f_{n+2}^2 - f_{n+1}^2)^2 + 4f_{n+1}^2 f_{n+2}^2 = f_{n+2}^4 - 2f_{n+1}^2 f_{n+2}^2 + f_{n+1}^4 + 4f_{n+1}^2 f_{n+2}^2 = f_{n+2}^4 + 2f_{n+1}^2 f_{n+2}^2 + f_{n+1}^4 = (f_{n+2}^2 + f_{n+1}^2)^2$, proving the result.

Section 13.2

1. Assume without loss of generality that $x < y$. Then $x^n + y^n = x^2 x^{n-2} + y^2 y^{n-2} < (x^2 + y^2)y^{k-2} = z^2 y^{n-2} < z^2 z^{n-2} = z^n$.

3. **a.** If $p \mid x$, y, or z, then certainly $p \mid xyz$. If not, then by Fermat's little theorem $x^{p-1} \equiv y^{p-1} \equiv z^{p-1} \equiv 1 \pmod p$. Hence $1 + 1 \equiv 1 \pmod p$, which is impossible.
b. We know that $a^p \equiv a \pmod p$ for every integer a. Then $x^p + y^p \equiv z^p \pmod p$ implies $x + y \equiv z \pmod p$, so $p \mid x + y - z$.

5. Let x and y be the lengths of the legs and z be the hypotenuse. Then $x^2 + y^2 = z^2$. If the area is a perfect square, we have $A = \frac{1}{2}xy = r^2$. Then if $x = m^2 - n^2$ and $y = 2mn$, we have $r^2 = mn(m^2 - n^2)$. All of these factors are relatively prime, so $m = a^2$, $n = b^2$, and $m^2 - n^2 = c^2$, say. Then $a^4 - b^4 = c^2$, which contradicts Exercise 4.

7. We use the method of infinite descent. Assume that there is a nonzero solution where $|x|$ is minimal. Then $(x, y) = 1$. Also, x and z cannot both be even, because then y would be odd and then $z^2 \equiv 8 \pmod{16}$, but 8 is not a quadratic residue modulo 16. Therefore x and z are both odd, since $8y^4$ is even. From here it is easy to check that $(x, z) = 1$. We may also assume (by negating if necessary) that $x \equiv 1 \pmod 4$ and $z \equiv 3 \pmod 4$. Clearly $x^2 > |z|$. We have $8y^4 = x^4 - z^2 = (x^2 - z)(x^2 + z)$. Since $z \equiv 3 \pmod 4$, we have $x^2 - z \equiv 2 \pmod 4$, so

$m = (x^2 - z)/2$ is odd, and $n = (x^2 + z)/4$ is an integer. Since no odd prime can divide both m and n, we have $(m, n) = 1$, $m, n > 0$, and $mn = y^4$, whence $m = r^4$ and $n = s^4$, with $(r, s) = 1$. So now $r^4 + 2s^4 = m + 2n = x^2$. This implies $(x, r) = 1$, since no odd prime divides r and x but not s, and r and x are both odd. Also, $|x| > r^2 > 0$. Now consider $2s^4 = (x^2 - r^4) = (x - r^2)(x + r^2)$. Then s must be even since a difference of squares is not congruent to 2 (mod 4), so $s = 2t$ and $32t^4 = (x - r^2)(x + r^2)$. Recalling that $x \equiv 1 \pmod 4$ and r is odd, we know that $U = (x + r^2)/2$ is odd and $V = (x - r^2)/16$ is an integer. Again $(U, V) = 1$ and $UV = t^4$, but we don't know the sign of x. So $U = \pm u^4$ and $V = \pm v^4$, depending on the sign of x. Now $r^2 = \pm(u^4 - 8v^4)$. But since u is odd, the sign can't be $-$ (or else $r^2 \equiv 7 \pmod 8$). So the sign is $+$ (hence x is positive), and $u^4 - 8v^4 = r^2$. Finally, $|v| > 0$ because $|x + r^2| > 0$, so we have not reduced to a trivial case. Then $u^4 = U < |x + r^2|/2 < x$, so $|u| < x$, and so $|x|$ was not minimal. This contradiction shows that there are no nontrivial solutions.

9. Suppose that $x = a/b$, where a and b are relatively prime integers with $b \neq 0$. Then $y^2 = (a^4 + b^4)/b^4$, from which we can deduce that $y = z/b^2$ for some integer z. Then $z^2 = a^4 + b^4$, which has no nonzero solutions by Theorem 13.3. Because $b \neq 0$, it follows that $z \neq 0$. Therefore, $a = 0$, and hence $x = 0$, and consequently $y = \pm 1$. These are the only solutions.

11. If x were even, then $y^2 = x^3 + 23 \equiv 3 \pmod 4$, which is impossible, so x must be odd, making y even, say $y = 2v$. If $x \equiv 3 \pmod 4$, then $y^2 \equiv 3^3 + 23 \equiv 2 \pmod 4$, which is also impossible, so $x \equiv 1 \pmod 4$. Next, add 4 to both sides of the equation to get $y^2 + 4 = 4v^2 + 4 = x^3 + 27 = (x + 3)(x^2 - 3x + 9)$. Then $z = x^2 - 3x + 9 \equiv 1 - 3 + 9 \equiv 3 \pmod 4$, so a prime $p \equiv 3 \pmod 4$ must divide z. Then $4v^2 + 4 \equiv 0 \pmod p$ or $v^2 \equiv -1 \pmod p$. But this shows that a prime congruent to 3 modulo 4 has -1 as a quadratic residue, which contradicts Theorem 11.5. Therefore, the equation has no solutions.

13. This follows from Exercise 4 and Theorem 13.2.

15. Assume that $n \nmid xyz$ and $(x, y, z) = 1$. Now $(-x)^n = y^n + z^n = (y + z)(y^{n-1} - y^{n-2}z + \cdots + z^{n-1})$, and these factors are relatively prime, so they are nth powers, say $y + z = a^n$ and $y^{n-1} - y^{n-2}z + \cdots + z^{n-1} = \alpha^n$, whence $-x = a\alpha$. Similarly, $z + x = b^n$, $z^{n-1} - z^{n-2}x + \cdots + x^{n-1} = \beta^n$, $-y = b\beta$, $x + y = c^n$, $x^{n-1} - x^{n-2}y + \cdots + y^{n-1} = \gamma^n$, and $-z = c\gamma$. Since $x^n + y^n + z^n \equiv 0 \pmod p$, we have $p \mid xyz$, say $p \mid x$. Then $\gamma^n = x^{n-1} - x^{n-2}y + \cdots + y^{n-1} \equiv y^{n-1} \pmod p$. Also $2x \equiv b^n + c^n + (-a)^n \equiv 0 \pmod p$, so by the condition on p, we have $p \mid abc$. If $p \mid b$, then $y = -b\beta \equiv 0 \pmod p$, but then $p \mid x$ and y, a contradiction. Similarly, p cannot divide c. Therefore, $p \mid a$, so $y \equiv -z \pmod p$, and so $\alpha^n \equiv y^{n-1} - y^{n-2}z + \cdots + z^{n-1} \equiv ny^{n-1} \equiv n\gamma^n \pmod p$. Let g be the inverse of γ modulo p; then $(ag)^n \equiv n \pmod p$, which contradicts the condition that there is no solution to $w^n \equiv n \pmod p$.

17. 3, 4, 5, 6

19. If $m \geq 3$, then modulo 8 we have $3^n \equiv -1 \pmod 8$, which is impossible, so $m = 1$ or 2. If $m = 1$, then $3^n = 2 - 1 = 1$, which implies that $n = 0$, which is not a positive integer, so that we have no solutions in this case. If $m = 2$, then $3^n = 2^2 - 2 = 3$, which implies that $n = 1$, and this is the only solution.

21. **a.** Substituting the expressions into the left-hand side of the equation yields $a^2 + b^2 + (3ab - c)^2 = a^2 + b^2 + 9a^2b^2 - 6abc + c^2 = (a^2 + b^2 + c^2) + 9a^2b^2 - 6abc$. Since (a, b, c) is a solution to Markov's equation, we substitute $a^2 + b^2 + c^2 = 3abc$ to get the last expression equal to $3abc + 9a^2 + b^2 - 6abc = 9a^2b^2 - 3abc = 3ab(3ab - c)$, which is the right-hand side of Markov's equation evaluated at these expressions.

b. *Case 1:* If $x = y = z$, then Markov's equation becomes $3x^2 = 3xyz$ so that $1 = yz$. Then $y = z = 1$ and then $x = 1$, so the only solution in this case is (1, 1, 1).

Case 2: If $x = y \neq z$, then $2x^2 + z^2 = 3x^2z$, which implies that $x^2 \mid z^2$ or $x \mid z$, say $dx = z$. Then $2x^2 + d^2x^2 = 3dx^3$ or $2 + d^2 = 3dx$ or $2 = d(3x - d)$. So $d \mid 2$, but because $x \neq z$, we must have

$d = 2$. Then $3x - d = 1$ so that $x = 1 = y$ and $z = 2$. It follows that the only solution in this case is $(1, 1, 2)$.

Case 3: Assume that $x < y < z$. From $z^2 - 3xyz + x^2 = y^2 + z^2$ we apply the quadratic formula to get $2z = 3xy \pm \sqrt{9x^2y^2 - 4(x^2 + y^2)}$. Note that $8x^2y^2 - 4x^2 - 4y^2 = 4x^2(y^2 - 1) + 4y^2(x^2 - 1) > 0$, so in the "minus" case of the quadratic formula, we have $2z < 3xy - \sqrt{9x^2y^2 - 8x^2y^2} = 3xy - xy = 2xy$, or $z < xy$. But $3xyz = x^2 + y^2 + z^2 < 3z^2$ so that $xy < z$, a contradiction, therefore we must have the case corresponding to the plus sign in the quadratic formula and $2z = 3xy + \sqrt{9x^2y^2 - 4(x^2 + y^2)} > 3xy$, so that $z > 3xy - z$. This last expression is the formula for the generation of z in part (a). Therefore, by successive use of the formula in part (a), we will reduce the value of $x + y + z$ until it is one of the solutions in Case 1 and Case 2.

23. Let $\epsilon > 0$ be given. Then the abc conjecture implies that $\max(|a|, |b|, |c|) \leq K(\epsilon)\text{rad}(abc)^{1+\epsilon}$ for integers $(a, b) = 1$ and $a + b = c$. Set $M = \log K / \log 2 + (3 + 3\epsilon)$. Suppose x, y, z, a, b, c are positive integers with $(x, y) = 1$ and $x^a + y^b = c^z$, so that we have a solution to Beal's equation. Assume $\min(a, b, c) > M$. From the abc conjecture we have $\max(x^a, y^b, z^c) \leq K(\epsilon)\text{rad}(xyz)^{1+\epsilon} \leq K(\epsilon)(xyz)^{1+\epsilon}$. If $\max(x, y, z) = x$, then we would have $x^a \leq K(\epsilon)x^{3(1+\epsilon)}$. Taking algorithms of both sides yields $a \leq \log K / \log x + (3 + 3\epsilon) < \log K / \log 2 + (3 + 3\epsilon) = M$, a contradiction. A similar argument applies if the maximum is y or z. Therefore, if the *abc* conjecture is true, then there are no solutions to the Beal conjecture for sufficiently large exponents.

25. **a.** If 1 is a congruent number, then there exist rational numbers r, s, and t such that $r^2 + s^2 = t^2$ and $rs/2 = 1$. Let $r = a/d$, $s = b/d$, and $t = c/d$, where a, b, c, and d are integers and d is the least common denominator of the rational numbers r, s, and t. Then $a^2 + b^2 = (rd)^2 + (sd)^2 = d^2t^2 = c^2$, so that (a, b, c) is a Pythagorean triple, consisting of the lengths of the sides of a right triangle with area $ab/2 = (rd)(sd)/2 = (d^2)(rs/2) = d^2$, a perfect square. Conversely, if there is a right triangle with area a perfect square, d^2, then its side lengths form a Pythagorean triple (a, b, c), and $a^2 + b^2 + c^2$. We can divide through by d^2 to get $(a/d)^2 + (b/d)^2 = (c/d)^2$ and so this represents a right triangle with sides $(a/d, b/d, c/d)$ and area $1/2(a/d)(b/d) = (ab/2)(1/d^2) = d^2/d^2 = 1$.

b. Suppose that 1 is a congruent number. Then, by part (a), there exist integers a, b, c, and d, such that $a^2 + b^2 = c^2$ and $ab/2 = d^2$. If we add and subtract 4 times the second equation from the first we get $a^2 + 2ab + b^2 = (a + b)^2 = c^2 + (2d)^2$ and $a^2 - 2ab + b^2 = (a - b)^2 = c^2 - (2d)^2$. Since the right-hand sides of both equations are squares, then so is their product, and we have $(c^2 + (2d)^2)(c^2 - (2d)^2) = c^4 - (2d)^4 = (a + b)^2(a - b)^2$, but this is a solution to $x^4 - y^4 = z^2$, which contradicts Exercise 4. Therefore 1 is not a congruent number.

Section 13.3

1. **a.** $19^2 + 4^2$ **b.** $23^2 + 11^2$ **c.** $37^2 + 9^2$ **d.** $137^2 + 9^2$

3. **a.** $5^2 + 3^2$ **b.** $9^2 + 3^2$ **c.** $10^2 + 1^2$ **d.** $21^2 + 7^2$ **e.** $133^2 + 63^2$ **f.** $448^2 + 352^2$

5. **a.** $1^2 + 1^2 + 1^2$ **b.** not possible **c.** $3^2 + 1^2 + 1^2$ **d.** $3^2 + 3^2 + 0^2$ **e.** not possible **f.** not possible

7. Let $n = x^2 + y^2 + z^2 = 4^m(8k + 7)$. If $m = 0$, then see Exercise 6. If $m \geq 1$, then n is even, so zero or two of x, y, z are odd. If two are odd, then $x^2 + y^2 + z^2 \equiv 2$ or 6 (mod 8), but then $4 \nmid n$, a contradiction, so all of x, y, z are even. Then $4^{m-1}(8k + 7) = (x/2)^2 + (y/2)^2 + (z/2)^2$ is the sum of three squares. Repeat until $m = 0$ and use Exercise 6 to get a contradiction.

9. **a.** $10^2 + 1^2 + 0^2 + 2^2$ **b.** $22^2 + 4^2 + 1^2 + 3^2$ **c.** $14^2 + 4^2 + 1^2 + 5^2$ **d.** $56^2 + 12^2 + 17^2 + 1^2$

11. Let $m = n - 169$. Then m is the sum of four squares: $m = x^2 + y^2 + z^2 + w^2$. If, say, x, y, z are 0, then $n = w^2 + 169 = w^2 + 10^2 + 8^2 + 2^2 + 1^2$. If, say, x, y are 0, then $n = z^2 + w^2 + 169 =$

$z^2 + w^2 + 12^2 + 4^2 + 3^2$. If, say, x is 0, then $n = y^2 + z^2 + w^2 + 169 = y^2 + z^2 + w^2 + 12^2 + 5^2$. If none are 0, then $n = x^2 + y^2 + z^2 + w^2 + 13^2$.

13. If k is odd, then 2^k is not the sum of four positive squares. Suppose that $k \geq 3$ and $2^k = x^2 + y^2 + z^2 + w^2$. Modulo 8 we have $0 \equiv x^2 + y^2 + z^2 + w^2$, and since an odd square is congruent to 1 (mod 8), the only possibility is to have x, y, z, w all even. But then we can divide by 4 to get $2^{k-2} = (x/2)^2 + (y/2)^2 + (z/2)^2 + (w/2)^2$. Either $k - 2 \geq 3$ and we can repeat the argument, or $k - 2 = 1$, in which case we have 2 equal to the sum of four positive squares, a contradiction.

15. If $p = 2$, the theorem is obvious. Otherwise, $p = 4k + 1$, whence -1 is a quadratic residue modulo p, say $a^2 \equiv -1 \pmod{p}$. Let x and y be as in Thue's lemma. Then $x^2 < p$ and $y^2 < p$ and $-x^2 \equiv (ax)^2 \equiv y^2 \pmod{p}$. Thus $p \mid x^2 + y^2 < 2p$, so $p = x^2 + y^2$, as desired.

17. The left sum runs over all pairs of integers $i < j$ for $1 \leq i < j \leq 4$, so there are six terms. Each integer subscript 1, 2, 3, and 4 appears in exactly three pairs, so $\sum_{1 \leq i < j \leq 4}((x_i + x_j)^4 + (x_i - x_j)^4) = \sum_{1 \leq i < j \leq 4}(2x_i^4 + 12x_i^2x_j^2 + 2x_j^4) = \sum_{k=1}^{4} 6x_k^4 + \sum_{1 \leq i < j \leq 4} 12x_i^2x_j^2 = 6\left(\sum_{k=1}^{4} x_k^2\right)^2$.

19. If m is positive, then $m = \sum_{k=1}^{4} x_k^2$ for some x_k's. Then $6m = 6\sum_{k=1}^{4} x_k^2 = \sum_{k=1}^{4} 6x_k^2$. Each term of the last sum is the sum of 12 fourth powers by Exercise 18. Therefore $6m$ is the sum of 48 fourth powers.

21. For $n = 1, 2, \ldots, 50$ we have $n = \sum_1^n 1^4$. For $n = 51, 52, \ldots, 81$, we have $n - 48 = n - 3(2^4) = \sum_1^{n-48} 1^4$, so $n = 2^4 + 2^4 + 2^4 + \sum_1^{n-48} 1^4$ is the sum of $n - 45$ fourth powers, and $n - 45 \leq 36 \leq 50$. This result, coupled with the result from Exercise 20, shows that all positive integers can be written as the sum of 50 or fewer fourth powers. That is, $g(4) \leq 50$.

23. The only quartic residues modulo 16 are 0 and 1. Therefore, the sum of fewer than 15 fourth powers must have a least nonnegative residue between 0 and 14 (mod 16), which excludes any integer congruent to 15 (mod 16).

Section 13.4

1. **a.** $(\pm 2, 0), (\pm 1, \pm 1)$ **b.** none **c.** $(\pm 1, \pm 2)$

3. **a.** yes **b.** no **c.** yes **d.** yes **e.** yes **f.** no

5. (73, 12), (10,657, 1752), (1,555,849, 255,780)

7. (6,239,765,965,720,528,801, 798,920,165,762,330,040)

9. Reduce modulo p to get $x^2 \equiv -1 \pmod{p}$. Since -1 is a quadratic nonresidue modulo p if $p = 4k + 3$, there is no solution.

11. Let $p_0 = 0$, $p_1 = 3$, $p_k = 2p_{k-1} + 2p_{k-2}$, $q_0 = 1$, $q_1 = 1$, and $q_k = 2q_{k-1} + q_{k-2}$. Then the legs are $x = p_k^2 + 2p_kq_k$ and $y = 2p_kq_k + 2q_k^2$.

13. Suppose that (x, y) is a solution of $x^4 - 2y^2 = -1$. Note that x must be odd. Furthermore, note that $(x^2 + 1)^2 = x^4 + 2x^2 + 1 = 2y^2 + 2x^2$ and $(x^2 - 1)^2 = x^4 - 2x^2 + 1 = 2y^2 - 2x^2$. Multiplying these equations together yields $(x^4 - 1)^2 = 4(y^4 - x^4)$ so that $((x^4 - 1)/2)^2 = y^4 - x^4$. Since $(x^4 - 1)/2$ is an integer, this contradicts Exercise 4 in Section 13.2.

Section 14.1

1. **a.** $5+15i$ **b.** $-46-9i$ **c.** $-26-18i$

3. **a.** yes **b.** yes **c.** no **d.** yes

5. $(4a-3b)+(3a+4b)i$, where a and b are rational integers (see the *Student Solutions Manual* for the display of such integers)

7. Because $\alpha|\beta$ and $\beta|\gamma$, there are Gaussian integers μ and ν with $\mu\alpha=\beta$ and $\nu\beta=\gamma$, and hence, $\gamma=\nu\beta=\nu\mu\alpha$. Because the product of Gaussian integers is a Gaussian integer, $\nu\mu$ is also a Gaussian integer. It follows that $\alpha|\gamma$.

9. Note that $x^5=x$ if and only if $x^5-x=x(x-1)(x+1)(x-i)(x+i)=0$. The solutions of this last equation are 0, 1, -1, i, and $-i$. These are the four Gaussian integers that are units, together with 0.

11. Since $\alpha|\beta$ and $\beta|\alpha$, there are Gaussian integers μ and ν such that $\alpha\mu=\beta$ and $\beta\nu=\alpha$. It follows that $\alpha=\alpha\mu\nu$. By Theorem 14.1, this implies that $N(\alpha)=N(\alpha\mu\nu)=N(\alpha)N(\mu\nu)$. This means that $N(\mu)N(\nu)=1$, and because the norm of a Gaussian integer is a nonnegative rational integer, $N(\mu)=N(\nu)=1$. Consequently μ and ν are units, and hence, α and β are associates.

13. The pair $\alpha=2+i$, $\beta=1+2i$ is a counterexample.

15. We first whow that such an associate exists. If $a>0$ and $b\geq 0$, the desired inequalities are met; if $a<0$ and $b>0$, multiply by $-i$ to get $-i\alpha=b-ai=c+di$; if $a<0$ and $b\leq 0$, multiply by -1 to get $-\alpha=-a-bi=c+di$; and if $a\geq 0$ and $b<0$, multiply by i to get $i\alpha=-b+ai=c+di$. In all cases, $c>0$ and $d\geq 0$. To prove uniqueness, note that when we multiply $c+di$ with $c>0$ and $d\geq 0$ by a unit other than 1, we obtain $-c-di$, which has $-c<0$, $-d+ci$, which has $-d\leq 0$, or $d-ci$, which has $-c<0$.

17. **a.** $\gamma=3-5i$, $\rho=-3i$, $N(\rho)=3^2+0^2=9<N(\beta)=3^2+3^2=18$
b. $\gamma=5-i$, $\rho=-1-2i$, $N(\rho)=5<N(\beta)=25$
c. $i\gamma=-1+8i$, $\rho=-5-3i$, $N(\rho)=5^2+3^2=34<N(\beta)=11^2+2^2=125$

19. **a.** $\gamma=2-5i$, $\rho=3$ **b.** $\gamma=4-i$, $\rho=2+2i$ **c.** $\gamma=-2+8i$, $\rho=6-5i$

21. 1, 2, and 4.

23. When a and b are both even, $2|a+ib$ because $a+ib=2((a/2)+i(b/2))$, and $(a/2)+i(b/2)$ is a Gaussian integer. Because $1+i|2$, we conclude that $1+i|a+ib$. When a and b are both odd, note that $a+bi=(1+i)+(a-1)+(b-1)i$, where $a-1$ and $b-1$ are both even. Because $1+i$ and $(a-1)+(b-1)i$ are both multiples of $1+i$, so is their sum. On the other hand, if a is odd and b is even, then $(a-1)+bi$ is a multiple of $1+i$. Hence, if $a+bi$ is a multiple of $a+bi$, then $(a+bi)-(a-1+bi)=1$ is a multiple of $1+i$, a contradiction. A similar argument shows that if a is even and b is odd, then $1+i$ does not divide $a+bi$.

25. $\pm 1\pm 2i$

27. Suppose that $7=(a+bi)(c+di)$, where $a+bi$ and $c+di$ are not units. Taking norms of both sides yields $49=(a^2+b^2)(c^2+d^2)$. Because neither $a+bi$ nor $c+di$ is a unit, both factors on the right-hand side must equal 7. However, 7 is not the sum of 2 squares.

29. Because α is neither a unit nor a prime, there exist nonunit Gaussian integers α and β with $\alpha=\beta\gamma$, where neither β nor γ is a unit, so that $N(\alpha)=N(\beta)N(\gamma)$, $N(\beta)>1$, and $N(\gamma)>1$. If $N(\beta)>\sqrt{N(\alpha)}$, then $N(\gamma)=N(\alpha)/N(\beta)<N(\alpha)/\sqrt{N(\alpha)}=\sqrt{N(\alpha)}$. Consequently, either β or γ divides α and has norm not exceeding $\sqrt{N(\alpha)}$.

31. The Gaussian primes with norm less than 100 are 3, 7, $1+i$, $1+2i$, $1+4i$, $1+6i$, $2+3i$, $2+5i$, $2+7i$, $3+8i$, $4+5i$, $4+9i$, $5+6i$, and $5+8i$, together with their associates and conjugates.

33. **a.** Note that $\alpha - \alpha = 0 = 0 \cdot \mu$, so that $\mu | \alpha - \alpha$. Thus, $\alpha \equiv \alpha \pmod{\mu}$.
b. Because $\alpha \equiv \beta \pmod{\mu}$, $\mu | \alpha - \beta$. Hence, there is a Gaussian integer γ with $\mu\gamma = \alpha - \beta$. This means that $\mu(-\gamma) = \beta - \alpha$, so that $\mu | \beta - \alpha$. Therefore, $\beta \equiv \alpha \pmod{\mu}$.
c. Because $\alpha \equiv \beta \pmod{\mu}$ and $\beta \equiv \gamma \pmod{\mu}$, there are Gaussian integers δ and ϵ such that $\mu\delta = \alpha - \beta$ and $\mu\epsilon = \beta - \gamma$. It follows that $\alpha - \gamma = \alpha - \beta + \beta - \gamma = \mu\delta + \mu\epsilon = \mu(\delta + \epsilon)$. Therefore, $\alpha \equiv \gamma \pmod{\mu}$.

35. Let $\alpha = a_1 + ib_1$, $\beta = a_2 + ib_2$, and $(a_1 + b_1)(a_2 + b_2) = R + Si$. We have $R = a_1a_2 - b_1b_2$ and $S = a_1b_2 + a_2b_1$. We compute $m_1 = b_2(a_1 + b_1)$, $m_2 = a_2(a_1 - b_1)$, and $m_3 = b_1(a_2 - b_2)$ using a total of three multiplications. We use these three products to find R and S using the equations $R = m_2 + m_3$ and $S = m_1 + m_3$.

37. **a.** $i, 1 + i, 1 + 2i, 2 + 3i, 3 + 5i, 5 + 8i$
b. Using the definition of G_k and the recursive definition of the Fibonacci sequence, we have $G_k = f_k + if_{k+1} = (f_{k-1} + f_{k-2}) + (f_k + f_{k-1})i = (f_{k-1} + f_ki) + (f_{k-2} + f_{k-1}i) = G_{k-1} + G_{k-2}$.

39. We proceed by induction. For the basis step, note that $G_2G_1 - G_3G_0 = (1 + 2i)(1 + i) - (2 + 3i)(i) = 2 + i$. Now assume the identity holds for values less than n. Using the identity in Exercise 37(b), we see that $G_{n+2}G_{n+1} - G_{n+3}G_n = (G_{n+1} + G_n)G_{n+1} - (G_{n+2} + G_{n+1})G_n = G_{n+1}^2 - G_{n+2}G_n = G_{n+1}^2 - (G_{n+1} + G_n)G_n = G_{n+1}^2 - G_n^2 - G_{n+1}G_n = (G_{n+1} + G_n)(G_{n+1} - G_n) - G_{n+1}G_n = G_{n+2}G_{n-1} - G_{n+1}G_n = -(-1)^{n-1}(2 + i) = (-1)^n(2 + i)$, which completes the induction step.

41. Suppose that $r + si$, where r and $s \neq 0$ are rational, is a root of the monic quadratic polynomial $z^2 + az + b$, where a and b are integers. The other root of the quadratic polynomial must be $r - si$; the polynomial must be $(z - (r + si))(z - (r - si)) = z^2 - 2rz + r^2 + s^2$. Hence, the coefficients $a = 2r$ and $b = r^2 + s^2$ are integers. Solving for r and s, we see that $r = a/2$ and $s^2 = (4b - r^2)/4$. This implies that $s = c/2$ for some integer c. Multiplying by 4, we find that $a^2 + c^2 \equiv 0 \pmod{4}$. This implies that both a and c are even. Hence, r and s are integers and $r + si$ is a Gaussian integer.

43. By the proof of the division algorithm in the text, given a Gaussian integer α, there are Gaussian integers γ and ρ such that $\alpha = \gamma(1 + 2i) + \rho$ such that $N(\rho) \leq N(1 + 2i)/2 = 5/2$. Therefore, the only possible values of ρ are $1 + 2i$ are 0, 1, i, $1 + i$ and their associates. Observing that $\alpha = (1 + 2i)\gamma + (1 + i) = (1 + 2i)(\gamma + 1) + (1 + i) - (1 + 2i) = (1 + 2i)(\gamma + 1) - i$, by modifying the quotient if necessary, all Gaussian integers can be written as a multiple of $1 + 2i$ plus a remainder equal to 0, 1, -1, i, or $-i$. Now consider dividing each of the Gaussian primes $\pi_1, \ldots, \pi_4$, by $1 + 2i$. If two of these can be written as a multiple of $1 + 2i$ plus the same remainder, then $1 + 2i$ divides their difference. But these differences are either 2 or $1 \pm i$, which are not divisible by $1 + 2i$. Furthermore, none of these remainders are 0 because each of these four numbers is prime. Therefore, we may rule out 0 as a possible remainder. Now divide the Gaussian integer $a + bi$ by $1 + 2i$ so that the remainder is one of 0, 1, -1, i, or $-i$; let the remainder be ρ. I this remainder is not 0, one of $\pi_1, \ldots, \pi_4$ leaves the same remainder when divided by $1 + 2i$, where the quotient is selected so that the remainder is one of 0, 1, -1, i, or $-i$, say π_k. It follows that $1 + 2i$ divides $\pi_k - (a + bi)$, which is impossible because this difference equals 1, -1, i, or -1. Therefore, $\rho = 0$, so that $1 + 2i \mid a + bi$. A similar argument shows that $1 - 2i \mid a + bi$. Therefore, the product of these primes $(1 - 2i)(1 + 2i) = 5$ also divides $a + bi$, which implies that $5 \mid a$ and $5 \mid b$. Note that b cannot be 0; if it were, $a - 1$, a, and $a + 1$ would all be prime, which is impossible and a cannot be zero. If $a = 0$ and if b is odd, then $(b - 1)i$ and $(b + 1)i$ are both divisible by 2, while if $a = 0$ and b is even, either $b - 1$ or $b + 1$ is congruent to 1 modulo 4. This implies that either $b - 1$ or $b + 1$ is not a Gaussian prime, and consequently, either $(b - 1)i$ or $(b + 1)i$ is not a Gaussian prime.

45. Because $\alpha\beta\gamma = 1$, $N(\alpha\beta\gamma) = N(\alpha)N(\beta)N(\gamma) = 1$. This implies that $N(\alpha) = N(\beta) = N(\gamma) = 1$, which shows that α, β, and γ are all units in the Gaussian integers. This means that the only possible values for these three values are $1, -1, i$, and $-i$. Check all possible values for these three variables in the equation $\alpha + \beta + \gamma = 1$, show that the possible solutions, up to permutation are $(1, 1, -1)$ and $(1, i, -i)$, but the first solution does not satisfy $\alpha\beta\gamma = 1$. This shows that $(1, i, -i)$ and its permutations are the only six solutions.

Section 14.2

1. Certainly, $1 \mid \pi_1$ and $1 \mid \pi_2$. Suppose that $\delta \mid \pi_1$ and $\delta \mid \pi_2$. Because π_1 and π_2 are Gaussian primes, δ must be either a unit or an associate of both primes. But because π_1 and π_2 are not associates, no Gaussian integer can be an associate of both, so that δ must be a unit if $\delta \mid 1$. Therefore, 1 satisfies the definition of a greatest common divisor for π_1 and π_2.

3. Because γ is a greatest common divisor of α and β, $\gamma \mid \alpha$ and $\gamma \mid \beta$. Hence, there exist Gaussian integers μ and ν such that $\mu\gamma = \alpha$ and $\nu\gamma = \beta$. It follows that $\overline{\mu\gamma} = \overline{\mu} \cdot \overline{\gamma} = \overline{\alpha}$ and $\overline{\nu\gamma} = \overline{\nu} \cdot \overline{\gamma} = \overline{\beta}$, which implies that $\overline{\gamma}$ is a common divisor of $\overline{\alpha}$ and $\overline{\beta}$. Furthermore, if $\delta \mid \overline{\alpha}$ and $\delta \mid \overline{\beta}$, then $\overline{\delta} \mid \alpha$ and $\overline{\delta} \mid \beta$. Consequently, $\overline{\delta} \mid \gamma$ by the definition of greatest common divisor. But this implies that $\overline{\overline{\delta}} = \delta \mid \overline{\gamma}$, which shows that $\overline{\gamma}$ is a greatest common divisor for $\overline{\alpha}$ and $\overline{\beta}$.

5. Let $\epsilon\gamma$, where ϵ is a unit, be an associate of γ. Because $\gamma \mid \alpha$, there is a Gaussian integer μ such that $\mu\gamma = \alpha$. Because ϵ is a unit, $1/\epsilon$ is also a Gaussian integer. Then $(1/\epsilon)\mu(\epsilon\gamma) = \alpha$, so that $\epsilon\gamma \mid \alpha$. Similarly, $\epsilon\gamma \mid \beta$. If $\delta \mid \alpha$ and $\delta \mid \beta$, then $\delta \mid \gamma$ by the definition of greatest common divisor. Consequently, there exists a Gaussian integer ν such that $\nu\delta = \gamma$. This implies that $\epsilon\nu\delta = \epsilon\gamma$, and because $\epsilon\nu$ is a Gaussian integer, we have $\delta \mid \epsilon\gamma$. Thus, $\epsilon\gamma$ satisfies the definition of a greatest common divisor.

7. Take $3 - 2i$ and $3 + 2i$, for example.

9. Because a and b are relatively prime rational integers, there exist rational integers m and n such that $am + bn = 1$. Let δ be a greatest common divisor of the Gaussian integers a and b. Then δ divides $am + bn = 1$. Therefore, δ is a unit in the Gaussian integers. Hence, a and b are relatively prime Gaussian integers.

11. **a.** We have $44 + 18i = (12 - 16i)(1 + 2i) + 10i$; $12 - 16i = (10i)(-2 - i) + (2 + 4i)$; $10i = (2 + 4i)(2 + i) + 0$. The last nonzero remainder, $2 + 4i$, is a greatest common divisor.
b. By part (a), $2 + 4i = (12 - 16i) - (10i)(-2 - i) = (12 - 16i) - ((44 + 18i) - (12 - 16i)(1 + 2i))(-2 - i) = (2 + i)(44 + 18i) + (1 + (1 + 2i)(-2 - i))(12 - 16i) = (2 + i)(44 + 18i) + (1 - 5i)(12 - 16i)$. Take $\mu = 2 + i$ and $\nu = 1 - 5i$.

13. We proceed by induction. We have $G_0 = i$ and $G_1 = 1 + i$. Because G_0 is a unit, G_0 and G_1 are relatively prime, completing the basis step. For the induction step, assume that G_k and G_{k-1} are relatively prime. Suppose that $\delta \mid G_k$ and $\delta \mid G_{k+1}$. Then $\delta \mid (G_{k+1} - G_k) = (G_k + G_{k-1} - G_k) = G_{k-1}$, so that δ is a common divisor of G_k and G_{k-1}, which are relatively prime. Hence, $\delta \mid 1$. Hence, 1 is a greatest common divisor of G_{k+1} and G_k.

15. Because the norm of the remainder in each step of the Euclidean algorithm for Gaussian integers based on the division algorithm described in the text does not exceed half of the norm of the divisor and the norm of the remainder is a positive integer, the maximum number of steps used to find a greatest common divisor of α and β is the largest number of times we can divide $N(\alpha)$ by 2 and obtain a positive integer. It follows that there cannot be more than $[\log_2 N(\alpha)] + 1$ divisions. This means that the number of steps is at most $O(\log_2 N(\alpha))$.

17. **a.** $(-1)(1 - 2i)(1 - 4i)$ **b.** $(-1)(1 + i)(5 + 8i)$ **c.** $(-1)(1 + i)^4 7$
d. $i(1 + i)^8(1 + 2i)^2(1 - 2i)^2$

19. **a.** 48 **b.** 120 **c.** 1792 **d.** 2592

21. Assume that n and $a + bi$ are relatively prime. Then, there exist Gaussian integers μ and ν such that $\mu n + \nu(a + bi) = 1$. Taking conjugates of both sides, and recalling that the conjugate of a rational integer is itself, we have $\overline{\mu} n + \overline{\nu}(a - bi) = 1$. This implies that n is also relatively prime to $a - bi$. Since $a - bi = -i(b + ai)$ is an associate of $b + ai$, n and $b + ai$ are relatively prime. The converse follows by symmetry.

23. Suppose that $\pi_1, \pi_2, \ldots, \pi_k$ are all the Gaussian primes. Form the Gaussian integer $Q = \pi_1\pi_2 \ldots \pi_k + 1$. By Theorem 14.10, Q has a unique factorization into Gaussian primes, and hence, is divisible by some Gaussian prime ρ. Because we have assumed that $\pi_1, \ldots, \pi_k$ are all the Gaussian primes, ρ must be somewhere in this list. It follows that $\rho \mid Q$ and $\rho \nmid \pi_1\pi_2 \ldots \pi_k$, which implies that ρ divides $1 = Q - \pi_1\pi_2 \ldots \pi_k$, a contradiction. It follows that $\pi_1, \pi_2, \ldots \pi_k$ cannot be a list of all the Gaussian primes. Consequently, there must be infinitely many Gaussian primes.

25. $-2i$

27. Because α and μ are relatively prime, there exist Gaussian integers σ and τ such that $\sigma\alpha + \tau\mu = 1$. When we multiply both sides of this equation by β, we obtain $\beta\sigma\alpha + \beta\tau\mu = \beta$, so that $\alpha(\beta\sigma) \equiv \beta \pmod{\mu}$. Thus, $x \equiv \beta\sigma \pmod{\mu}$ is the solution.

29. **a.** $x \equiv 5 - 4i \pmod{13}$ **b.** $x \equiv 1 + i \pmod{4 + i}$ **c.** $x \equiv 3i \pmod{2 + 3i}$.

31. *Chinese Remainder Theorem for the Gaussian Integers.* Let $\mu_1, \mu_2, \ldots, \mu_r$ be pairwise relatively prime Gaussian integers and let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be Gaussian integers. Then the system of congruences $x \equiv \alpha_i \pmod{\mu_i}, i = 1, \ldots, r$ has a unique solution modulo $M = \mu_1\mu_2 \cdots \mu_r$. *Proof:* To construct a solution, for each $k = 1, \ldots, r$, let $M_k = M/\mu_k$. Then M_k and μ_k are relatively prime, because μ_k is relatively prime to the factors of M_k. By Exercise 24, M_k has an inverse λ_k modulo μ_k, so that $M_k\lambda_k \equiv 1 \pmod{\mu_k}$. Now let $x = \alpha_1 M_1\lambda_1 + \cdots + \alpha_r M_r\lambda_r$. We show that x is the solution to the system. Because $\mu_k \mid M_j$ whenever $j \neq k$, we have $\alpha_j M_j\lambda_k \equiv 0 \pmod{\mu_k}$ whenever $j \neq k$. Therefore, $x \equiv \alpha_k M_k\lambda_k \pmod{\mu_k}$. Also, because λ_k is an inverse for M_k modulo μ_k, we have $x \equiv \alpha_k \pmod{\mu_k}$ for every k, as desired. Now suppose there is another solution y to the system. Then $x \equiv \alpha_k \equiv y \pmod{\mu_k}$ and so $\mu_k \mid x - y$ for every k. Because the μ_k are pairwise relatively prime, no Gaussian prime appears in more than one of their prime factorizations. Therefore, if a Gaussian prime power $\pi^e \mid x - y$, it divides exactly one μ_k. Therefore, the product M also divides $x - y$. Hence, $x \equiv y \pmod{M}$, which proves that x is unique modulo M.

33. $x \equiv 9 + 23i \pmod{26 + 7i}$

35. **a.** $\{0, 1\}$ **b.** $\{0, 1, i, 1 + i\}$ **c.** $\{0, 1, -1, i, 2i, 3i, -i, -2i, -3i, 1 + i, 1 + 2i, 1 - i, -1 + i\}$

37. Let $\alpha = a + bi$ and $d = \gcd(a, b)$. We assert that the set $S = \{p + qi \mid 0 \leq p < N(\alpha)/d - 1, 0 \leq q < d - 1\}$ is a complete residue system. This set consists of lattice points inside a rectangle in the plane. To see this, first note that $N(\alpha)/d = \alpha(\overline{\alpha}/d)$ is a real number and is also a multiple of α. Second, note that there exist rational integers r and s such that $ra + sb = d$. All multiples of α are given by $v = (s + ir)\alpha = (s + ir)(a + bi) = (as - br) + di$, where s and r are integers. Any Gaussian integer is congruent modulo α to an integer in the rectangle S, because we can add or subtract multiples of v until the imaginary part is between 0 and $d - 1$, and we can add and subtract multiples of $N(\alpha)/d$ until the real part is between 0 and $N(\alpha)/d - 1$. It remains to show that the elements of S are incongruent to each other modulo α. Suppose that β and γ are in S and congruent modulo α. Then the imaginary part of $\beta - \gamma$ is divisible by d, but since β and γ must lie in the interval from 0 to $d - 1$, they are equal. Therefore the difference between β and γ is real and divisible by α, and hence, by $\overline{\alpha}$, and hence, by $\alpha\overline{\alpha}/d = N(\alpha)/d$, proving they are equal. Since S has $N(\alpha)$ elements, we are done.

39. **a.** $\{1, i, 2+i, 3\}$ **b.** $\{i, 3i, 1, 1+2i, 2+i, 2+3i, 3, 3+2i\}$ **c.** $\{i, 1, 3, 4+i, 6+i, 7, 8+i, 9\}$

41. By the properties of the norm of Gaussian integers and Exercise 37, there are $N(\pi^e) = N(\pi)^e$ residue classes modulo π^e. Let $\pi = r + si$, and $d = \gcd(r, s)$. Also, by Exercise 37, a complete residue system modulo π^e is given by the lattice points $S = \{p + qi \mid 0 \le p < N(\pi^e)/d - 1, 0 \le q < d - 1\}$, while a complete residue system modulo π is given by the set of lattice points $T = \{p + qi \mid 0 \le p < N(\pi)/d - 1, 0 \le q < d - 1\}$. Note that in T there is exactly one element not relatively prime to π, and that there are $N(\pi)^{e-1}$ copies of T, congruent modulo π, inside of S. Therefore, there are exactly $N(\pi)^{e-1}$ elements in S not relatively prime to π. Thus there are $N(\pi)^e - N(\pi)^{e-1}$ elements in a reduced residue system modulo π^e.

43. **a.** First note that because $r + s\sqrt{-5}$ is a root of a monic polynomial with integer coefficients, the other root must be $r - s\sqrt{-5}$ and the polynomial is $(x - (r + s\sqrt{-5}))(x - (r - s\sqrt{-5})) = x^2 - 2rx + (r^2 + 5s^2) = x^2 - ax + b$, where a and b are rational integers. Then $r = a/2$ and $5s^2 = (4b - a^2)/4$, so that $s = c/2$ for some integer c. (Note that 5 cannot appear in the denominator of s, else when we square it, the single factor of 5 in the expression leaves a remaining factor in the denominator, which does not appear on the right side of the equation.) Substituting these expressions for r and s, we have $(a/2)^2 + 5(c/2)^2 = b^2$, or, upon multiplication by 4, $a^2 + 5c^2 = 4b^2 \equiv 0 \bmod 4$, which has solutions only when a and c are even. Therefore, r and s are rational integers.

b. Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$, where a, b, c, and d are rational integers. Then $(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5}$, $(a + b\sqrt{-5}) - (c + d\sqrt{-5}) = (a - c) + (b - d)\sqrt{-5}$, and $(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac + bc\sqrt{-5} + ad\sqrt{-5} - 5bd = (ac - 5bd) + (bc + ad)\sqrt{-5}$. Each of these results is again of desired form.

c. yes, no

d. Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then $N(\alpha)N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$. On the other hand, $\alpha\beta = (ac - 5bd) + (ad + bc)\sqrt{-5}$, so that $N(\alpha\beta) = N((ac - 5bd) + (ad + bc)\sqrt{-5}) = (ac - 5bd)^2 + 5(ad + bc)^2 = a^2c^2 - 10acbd + 25b^2d^2 + 5(a^2d^2 + 2adbc + b^2c^2) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$. It follows that $N(\alpha\beta) = N(\alpha)N(\beta)$.

e. If ϵ is a unit in $\mathbf{Z}[\sqrt{-5}]$, then there exists an η such that $\epsilon\eta = 1$. From part (d), we have $N(\epsilon\eta) = N(\epsilon)N(\eta) = N(1) = 1$, so that $N(\epsilon) = 1$. Now suppose that $\epsilon = a + b\sqrt{-5}$. Then $N(\epsilon) = a^2 + 5b^2 = 1$, which implies that $b = 0$ and $a = \pm 1$. Therefore, the only units are 1 and -1.

f. If an integer α in $\mathbf{Z}[\sqrt{-5}]$ is not a unit and not prime, it must have two nonunit divisors of β and γ such that $\alpha = \beta\gamma$. This implies that $N(\beta)N(\gamma) = N(\alpha)$. To see that 2 is prime, suppose that $\beta \mid 2$, where $\beta = a + b\sqrt{-5}$. It follows that $N(\beta) = a^2 + 5b^2 \mid N(2) = 4$. This implies that $b = 0$, and because β is not a unit, we have $a = \pm 2$. However, if $a = \pm 2$, then γ is a unit, which is a contradiction. Hence, 2 is prime. To see that 3 is prime, we seek divisors of $N(3) = 9$ among integers of the form $a^2 + 5b^2$. We see that b can be only 0 or ± 1. If $b = \pm 1$, then $a = \pm 3$. But this implies that the remaining factor is a unit. If $b = 0$, then $a = \pm 3$, and so 3 is prime. To see that $1 \pm \sqrt{-5}$ is prime, note that its norm is 6. A divisor $a + bi$ can have $b = 0$ or $b = \pm 1$, else its norm is too large. If $b = 0$, then $a^2 \mid 6$, a contradiction, so $b = \pm 1$. But then $a^2 + 5 \mid 6$, which implies that $a = \pm 1$. But $N(\pm 1 \pm \sqrt{-5}) = 6$ so the other divisor is a unit, and so $1 \pm \sqrt{-5}$ is also prime. Note then that $2 \cdot 3 = 6$ and $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$, so that we do not have unique factorization into primes in $\mathbf{Z}[\sqrt{-5}]$.

g. Suppose γ and ρ exist. Note first that $(7 - 2\sqrt{-5})/(1 + \sqrt{-5}) = -1/2 - 3/2\sqrt{-5}$, so $\rho \neq 0$. Let $\gamma = a + b\sqrt{-5}$ and $\rho = c + d\sqrt{-5}$. Then from $7 - 2\sqrt{-5} = (1 + \sqrt{-5})(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a - 5b + c) + (a + b + d)\sqrt{-5}$, we get $7 = a - 5b + c$ and $-2 = a + b + d$. If we subtract the second equation from the first, we have $9 = -6b + c - d$ or $c - d = 6b + 9$. Therefore, $3 \mid c - d$, and since $\rho \neq 0$, $c - d \neq 0$, so $|c - d| \ge 3$. We consider $N(\rho) = c^2 + 5d^2$.

If $d = 0$, then $N(\rho) \geq c^2 \geq 3^2 > 6$. If $d = \pm 1$, then $|c| \geq 2$ and $N(\rho) = c^2 + 5d^2 \geq 4 + 5 > 6$. If $|d| \geq 2$, then $N(\rho) \geq 5d^2 \geq 5 \cdot 2^2 = 20 > 6$, so in every case the norm of ρ is greater than 6. So no such γ and ρ exist, and there is no analog for the division algorithm in $\mathbf{Z}[\sqrt{-5}]$.

h. Suppose $\mu = a + b\sqrt{-5}$ and $\nu = c + d\sqrt{-5}$ is a solution to the equation. Then $3(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = (3a + c - 5d) + (3b + c + d)\sqrt{-5} = 1$. So we must have $3a + c - 5d = 1$ and $3b + c + d = 0$. If we subtract the second equation from the first, we get $3a - 3b - 6d = 1$, which implies that $3|1$, a contradiction. Therefore, no such solution exists.

Section 14.3

1. a. 8 **b.** 8 **8.** 8 **d.** 16

3. We first check that a greatest common divisor δ of α and β divides γ, otherwise no solution exists. If a solution exists, use the Euclidean algorithm and back substitution to express δ as a linear combination of α and β as $\alpha\mu + \beta\nu = \delta$. Because $\delta \mid \gamma$, there is a Gaussian integer η such that $\delta\eta = \gamma$. When we multiply the equation $\alpha\mu + \beta\nu = 1$ by η, we have $\alpha\mu\eta + \beta\nu\eta = \delta\eta = \gamma$, so we may take $x_0 = \mu\eta$ and $y_0 = \nu\eta$ as a solution. The set of all solutions is given by $x = x_0 + \beta\tau/\delta$, $y = y_0 - \alpha\tau/\delta$, where τ ranges over the Gaussian integers.

5. a. no solutions **b.** no solutions

7. Suppose x, y, z is a primitive Pythagorean triple with y even, so that x and z are odd. Then $z^2 = x^2 + y^2 = (x + iy)(x - iy)$. If a rational prime p divides $x + iy$, it divides both x and y, contradicting the fact that the triple is primitive. Therefore, the only Gaussian primes that divide $x + iy$ are of the form $m + in$ with $n \neq 0$. Also, if $1 + i \mid x + iy$, then $1 - i \mid x - iy$, which implies that $2 = (1 - i)(1 + i)$ divides z^2, which is odd, a contradiction. Therefore, we conclude that $1 + i$ does not divide $x + iy$, and hence, neither does 2. Suppose δ is a common divisor of $x + iy$ and $x - iy$. Then δ divides the sum $2x$ and the difference $2iy$. Because 2 is not a common factor, δ must divide both x and y, which are relatively prime. Hence, δ is a unit and $x + iy$ and $x - iy$ are also relatively prime. Every prime that divides $x + iy$ is of the form $\pi = u + iv$, and so $\overline{\pi} = u - iv$ divides $x - iy$. Because their product equals a square, each factor is a square. Thus, $x + iy = (m + in)^2$ and $x - iy = (m - in)^2$ for some Gaussian integer $m + in$. But then $x + iy = m^2 - n^2 + 2mni$ so $x = m^2 - n^2$ and $y = 2mn$. And if $z^2 = (m + ni)^2(m - ni)^2 = (m^2 + n^2)^2$, so $z = m^2 + n^2$. Further, if m and n were both odd or both even, we would have z even, a contradiction. It follows that m and n have opposite parity. Finally, having found m and n, if $m < n$, we can multiply by i and reverse their roles to get $m > n$. The converse is exactly as shown in Section 13.1.

9. By Lemma 14.3, there is a unique rational prime p such that $\pi \mid p$. Let $\alpha = a + bi$. We separately consider three cases: $p = 2$, $p \equiv 3 \pmod 4$, and $p \equiv 1 \pmod 4$.

Case 1: If $p = 2$, then π is an associate of $1 + i$ and $N(\pi) - 1 = 1$. Because there are only two congruence classes modulo $1 + i$ and because α and $1 + i$ are relatively prime, we have $\alpha^{N(\pi)-1} = \alpha \equiv 1 \pmod{1 + i}$.

Case 2: If $p \equiv 3 \pmod 4$, then $\pi = p$ and $N(\pi) - 1 = p^2 - 1$. Also, $i^p = -i$. By the binomial theorem, we can show that $\alpha^p = (a + bi)^p \equiv a^p + (bi)^p \equiv a^p - ib^p \equiv a - bi \equiv \alpha \pmod p$, using Fermat's little theorem. Similarly, $\overline{\alpha}^p \equiv \alpha \pmod p$, so that $\alpha^{p^2} \equiv \overline{\alpha}^p \equiv \alpha \pmod p$, and because $p = \pi$ and α and π are relatively prime, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod p$.

Case 3: If $p \equiv 1 \pmod 4$, then $\pi\overline{\pi} = p$, $i^p = i$, and $N(\pi) - 1 = p - 1$. By the binomial theorem, we can show that $\alpha^p = (a + bi)^p \equiv a^p + (bi)^p \equiv a + bi \equiv \alpha \pmod p$, using Fermat's little theorem. This implies that $\alpha^{p-1} \equiv 1 \pmod p$, and because $\pi \mid p$, we have $\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$, concluding the proof.

11. Let π be a Gaussian prime. If $\alpha^2 \equiv 1 \pmod{\pi}$, then $\pi \mid \alpha^2 - 1 = (\alpha - 1)(\alpha + 1)$, so that either $\alpha \equiv 1$ or $\alpha \equiv -1 \pmod{\pi}$. Therefore, only 1 or -1 can be its own inverse modulo π. Now let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_{r-1}, \alpha_r = -1$ be a reduced residue system modulo π. For each α_k, $k = 2, 3, \ldots, r-1$, there is a multiplicative inverse modulo π, α'_k, such that $\alpha_k \alpha'_k \equiv 1 \pmod{\pi}$. If we group together the two numbers in all such pairs in the reduced residue system, then the product is easy to evaluate: $\alpha_1\alpha_2 \ldots \alpha_r = 1(\alpha_2\alpha'_2)(\alpha_3\alpha'_3) \ldots (\alpha_{r-1})(\alpha'_{r-1})(-1) \equiv -1 \pmod{\pi}$, which proves the theorem.

Appendix A

1. **a.** $a(b+c) = (b+c)a = ba + ca = ab + ac$
b. $(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2 = a^2 + ab \cdot 1 + ab \cdot 1 + b^2 = a^2 + ab \cdot 2 + b^2 = a^2 + 2ab + b^2$.
c. $a + (b + c) = a + (c + b) = (a + c) + b = (c + a) + b$
d. $(b - a) + (c - b) + (a - c) = (-a + b) + (-b + c) + (-c + a) = -a + (b - b) + (c - c) + a = -a + 0 + 0 + a = -a + a = 0$

3. $-0 = 0 + -0 = 0$

5. Let a be a positive integer. Since $a = a - 0$ is positive, $a > 0$. Now let $a > 0$. Then $a - 0 = a$ is positive.

7. $a - c = a + (-b + b) - c = (a - b) + (b - c)$, which is positive from our hypothesis and the closure of the positive integers.

Appendix B

1. **a.** 1 **b.** 50 **c.** 1140 **d.** 462 **e.** 120 **f.** 1

3. **a.** $a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$
b. $x^{10} + 10x^9y + 45x^8y^2 + 120x^7y^3 + 210x^6y^4 + 252x^5y^5 + 210x^4y^6 + 120x^3y^7 + 45x^2y^8 + 10xy^9 + y^{10}$
c. $m^7 - 7m^6n + 21m^5n^2 - 35m^4n^3 + 35m^3n^4 - 21m^2n^5 + 7mn^6 - n^7$
d. $16a^4 + 96a^3b + 216a^2b^2 + 216ab^3 + 81b^4$
e. $243x^5 - 1620x^4y + 4320x^3y^2 - 5760x^2y^3 + 3840xy^4 - 1024y^5$
f. $390{,}625x^8 + 4{,}375{,}000x^7 + 21{,}437{,}500x^6 + 60{,}025{,}000x^5 + 105{,}043{,}750x^4 + 117{,}649{,}000x^3 + 82{,}354{,}300x^2 + 32{,}941{,}720x + 5{,}764{,}801$

5. On the one hand, $(1 + (-1))^n = 0^n = 0$. On the other hand, by the binomial theorem, $(1 + (-1))^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$.

7. $\binom{n}{r}\binom{r}{k} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!(n-k)!}{k!(n-k)!(n-r)!(n-k-n+r)!} = \binom{n}{k}\binom{n-k}{n-r}$

9. We proceed using the second principle of mathematical induction on the variable n. The basis step $n = r = 1$ is clear. For the inductive step, we assume that $\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}$ is true whenever r is an integer with $1 \le r \le n$. We will now examine the formula with $n + 1$ in the place of n. If $r < n + 1$, then $\binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} + \binom{n+1}{r} = \binom{n+1}{r+1} + \binom{n+1}{r} = \binom{n+2}{r+1}$ by Theorem A.2, so the formula holds in this case. If $r = n + 1$, then $\binom{r}{r} + \cdots + \binom{n+1}{r} = \binom{n+1}{n+1} = 1 = \binom{n+2}{n+2}$.

11. Using Exercise 10, $\binom{x}{n} + \binom{x}{n+1} = \frac{x!}{n!(x-n)!} + \frac{x!}{(n+1)!(x-n-1)!} = \frac{x!(n+1)}{(n+1)!(x-n)!} + \frac{x!(x-n)}{(n+1)!(x-n)!} = \frac{x!(x-n+n+1)}{(n+1)!(x-n)!} = \frac{(x+1)!}{(n+1)!(x-n)!} = \binom{x+1}{n+1}$.

13. Let S be a set of n copies of $x + y$. Consider the coefficient of $x^k y^{n-k}$ in the expansion of $(x + y)^n$. Choosing the x from each element of a k-element subset of S, we notice that the coefficient of $x^k y^{n-k}$ is the number of k-element subsets of S, $\binom{n}{k}$.

15. By counting elements with exactly 0, 1, 2, and 3 properties, we see that only elements with 0 properties are counted in $n - (n(P_1) + n(P_2) + n(P_3)) + (n(P_1, P_2) + n(P_1, P_3) + n(P_2, P_3)) - n(P_1, P_2, P_3)$, and those only once.

17. A term of the sum is of the form $ax_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}$, where $k_1 + k_2 + \cdots + k_m = n$ and $a = n!/(k_1!k_2!\cdots k_m!)$.

19. 56133000000

Bibliography

An extensive bibliography of printed resources on number theory and its applications is provided here. Materials listed include both books and articles. To learn more about number theory, you may want to consult other number theory textooks, such as [AdGo76], [An94], [Ar70], [Ba69], [Be66], [Bo70], [BoSh66], [Bu01], [Da99], [Di57], [Du78], [ErSu03], [Fl89], [Gi70], [Go98], [Gr82], [Gu80], [HaWr79], [Hu82], [IrRo95], [Ki74], [La58], [Le90], [Le96], [Lo95], [Ma–], [Na81], [NiZuMo91], [Or67], [Or88], [PeBy70], [Ra77], [Re96], [Ro77], [Sh85], [Sh83], [Sh67], [Si87], [Si64], [Si70], [St78], [St64], [UsHe39], [Va01], [Vi54], and [Wr39].

Printed resources listed in this bibliography also include books and articles covering particular aspects of number theory and its applications, including factorization and primality testing, the history of number theory, and cryptography.

Additional information on number theory, including the latest discoveries, can be found on the many Web sites containing relevant information. Appendix D lists the top number theory and cryptography Web sites. A comprehensive set of links to relevant Web sites can be found on the Web site for this book `www.awlonline.com/rosen`.

[AdGo76] W.W. Adams and L.J. Goldstein, *Introduction to Number Theory,* Prentice Hall, Englewood Cliffs, New Jersey, 1976.

[Ad79] L.M. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," *Proceedings of the 20th Annual Symposium on the Foundations of Computer Science*, 1979, 55–60.

[AdPoRu83] L.M. Adleman, C. Pomerance, and R.S. Rumely, "On distinguishing prime numbers from composite numbers," *Annals of Mathematics*, Volume 117 (1983).

[AgKaSa02] M.A. Agrawal, N. Kayal, N. Saxena, "PRIMES is in P," Department of Computer Science & Engineering, Indian Institute of Technology, Kanpur, India, August 6, 2002.

[AiZi03] M. Aigner and G.M. Ziegler, *Proofs from THE BOOK*, 3rd ed., Springer-Verlag, Berlin, 2003.

[AlWi03] S. Alaca and K. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, 2003.

[AlGrPo94] W.R. Alford, A. Granville, and C. Pomerance, "There are infinitely many Carmichael Numbers," *Annals of Mathematics*, Volume 140 (1994), 703–722.

[An94] G.E. Andrews, *Number Theory*, Dover, New York, 1994.

[Ap76] T.A. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[Ar70] R.G. Archibald, *An Introduction to the Theory of Numbers*, Merrill, Columbus, Ohio, 1970.

[BaSh96] E. Bach and J. Shallit, *Algorithmic Number Theory*, MIT Press, Cambridge, Massachusetts, 1996.

[Ba94] P. Bachmann, *Die Analytische Zahlentheorie*, Teubner, Leipzig, Germany, 1894.

[Ba03] E.J. Barbeau, *Pell's Equation*, Springer-Verlag, New York, 2003.

[Ba69] I.A. Barnett, *Elements of Number Theory*, Prindle, Weber, and Schmidt, Boston, 1969.

[Be66] A.H. Beiler, *Recreations in the Theory of Numbers*, 2nd ed., Dover, New York, 1966.

[BePi82] H. Beker and F. Piper, *Cipher Systems*, Wiley, New York, 1982.

[Be65] E.T. Bell, *Men of Mathematics*, Simon & Schuster, New York, 1965.

[Bl82] M. Blum, "Coin-flipping by telephone—a protocol for solving impossible problems," *IEEE Proceedings, Spring Compcon 82*, 133–137.

[Bo70] E.D. Bolker, *Elementary Number Theory*, Benjamin, New York, 1970.

[Bo99] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *American Mathematical Society Notices*, Volumn 46 (1999), 203–213.

[Bo82] B. Bosworth, *Codes, Ciphers, and Computers*, Hayden, Rochelle Park, New Jersey, 1982.

[Bo91] C.B. Boyer, *A History of Mathematics*, 2nd ed., Wiley, New York, 1991.

[BoSh66] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[Br91] R.P. Brent, "Improved techniques for lower bounds for odd perfect numbers," *Mathematics of Computation*, Volume 57 (1991), 857–868.

[Br00] R.P. Brent, "Recent progress and prospects for integer factorization algorithms," *Proc. COCOON* 2000, LNCS 1858, pages 3–22, Springer-Verlag, 2000.

[BrCote93] R.P. Brent, G.L. Cohen, and H.J.J. te Riele, "Improved techniques for lower bounds for odd perfect numbers," *Mathematics of Computation*, Volume 61 (1993), 857–868.

[Br89] D.M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.

[BrWa00] D. Bressoud and S. Wagon, *A Course in Computational Number Theory*, Key College Publishing, Emeryville, California, 2000.

[Br81] J. Brillhart, "Fermat's factoring method and its variants," *Congressus Numerantium*, Volume 32 (1981), 29–48.

[Br88] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, revised ed., American Mathematical Society, Providence, Rhode Island, 1988.

[Bu01] D.M. Burton, *Elementary Number Theory*, 5th ed., McGraw-Hill, New York, 2001.

[Bu02] D.M. Burton, *The History of Mathematics*, 5th ed., McGraw-Hill, New York, 2002.

[Ca59] R.D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, Dover, New York, 1959 (reprint of the original 1914 and 1915 editions).

[Ch83] D. Chaum, ed., *Advances in Cryptology—Proceedings of Crypto 83*, Plenum, New York, 1984.

[ChRiSh83] D. Chaum, R.L. Rivest, A.T. Sherman, eds., *Advances in Cryptology—Proceedings of Crypto 82*, Plenum, New York, 1983.

[Ci88] B. Cipra, "PCs Factor a 'Most Wanted' Number," *Science*, Volume 242 (1988), 1634–1635.

[Ci90] B. Cipra, "Big Number Breakdown," *Science*, Volume 248 (1990), 1608.

[Co87] G.L. Cohen, "On the largest component of an odd perfect number," *Journal of the Australian Mathematical Society, (A)*, Volume 42 (1987), 280–286.

[CoWe91] W.N. Colquitt and L. Welsh, Jr., "A New Mersenne Prime," *Mathematics of Computation*, Volume 56 (1991), 867–870.

[CoGu96] R.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus Books, New York, 1996.

[Co97] D. Coppersmith, "Small solutions to polynomial equations, and low exponent RSA vulnerabilities," *Journals of Cryptology*, Volume 10 (1997), 233–260.

[CoLeRi01] T.H. Cormen, C.E. Leierson, R.L. Rivest, *Introduction to Algorithms*, 2nd ed., MIT Press, Cambridge, Massachusetts, 2001.

[CoSiSt97] G. Cornell, J.H. Silverman, and G. Stevens, *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, New York, 1997.

[Cr94] R.E. Crandall, *Projects in Scientific Computation*, Springer-Verlag, New York, 1994.

[CrPo01] R. Crandall and C. Pomerance, *Prime Numbers, A Computational Perspective*, Springer-Verlag, New York, 2001.

[Da99] H. Davenport, *The Higher Arithmetic*, 7th ed., Cambridge University Press, Cambridge, England, 1999.

[De82] D.E.R. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, Massachusetts, 1982.

[De03] J. Derbyshire, *Prime Obsession*, Joseph Henry Press, Washington, D.C., 2003.

[Di57] L.E. Dickson, *Introduction to the Theory of Numbers*, Dover, New York, 1957 (reprint of the original 1929 edition).

[Di71] L.E. Dickson, *History of the Theory of Numbers*, three volumes, Chelsea, New York, 1971 (reprint of the 1919 original).

[Di70] *Dictionary of Scientific Biography*, Scribners, New York, 1970.

[DiHe76] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Volume 22 (1976), 644–655.

[Di84] J.D. Dixon, "Factorization and primality tests," *American Mathematical Monthly*, Volume 91 (1984), 333–353.

[Du78] U. Dudley, *Elementary Number Theory*, 2nd ed., Freeman, New York, 1978.

[Ed96] H.M. Edwards, *Fermat's Last Theorem*, 5th ed., Springer-Verlag, New York, 1996.

[Ed01] H.M. Edwards, *Riemann's Zeta Function*, Dover, New York, 2001.

[ErSu03] P. Erdős and J. Surányi, *Topics in the History of Numbers*, Springer-Verlag, New York, 2003.

[Ev92] H. Eves, *An Introduction to the History of Mathematics*, 6th ed., Elsevier, New York, 1992.

[Ew83] J. Ewing, "$2^{86243} - 1$ is prime," *The Mathematical Intelligencer*, Volume 5 (1983), 60.

[Fl89] D. Flath, *Introduction to Number Theory*, Wiley, New York, 1989.

[Fl83] D.R. Floyd, "Annotated bibliographical in conventional and public key cryptography," *Cryptologia*, Volume 7 (1983), 12–24.

[Fr56] J.E. Freund, "Round robin mathematics," *American Mathematical Monthly*, Volume 63 (1956), 112–114.

[Fr78] W.F. Friedman, *Elements of Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1978.

[Ga91] J. Gallian, "The mathematics of identification numbers," *College Mathematics Journal*, Volume 22 (1991), 194–202.

[Ga92] J. Gallian, "Assigning drivers license numbers," *Mathematics Magazine*, Volume 64 (1992), 13–22.

[Ga96] J. Gallian, "Error Detection Methods," *ACM Computing Surveys*, Volume 28 (1996), 504–517.

[GaWi88] J. Gallian and S. Winters, "Modular arithmetic in the marketplace," *American Mathematical Monthly*, Volume 95 (1988), 584–551.

[Ga86] C.F. Gauss, *Disquisitiones Arithmeticae*, revised English translation by W.C. Waterhouse, Springer-Verlag, New York, 1986.

[Ge63] M. Gerstenhaber, "The 152nd proof of the law of quadratic reciprocity," *American Mathematical Monthly*, Volume 70 (1963), 397–398.

[Ge82] A. Gersho, ed., *Advances in Cryptography*, Department of Electrical and Computer Engineering, University of California, Santa Barbara, 1982.

[GeWaWi98] E. Gethner, S. Wagon, and B. Wick, "A stroll through the Gaussian primes," *American Mathematical Monthly*, Volume 104 (1998), 216–225.

[Gi70] A.A. Gioia, *The Theory of Numbers*, Markham, Chicago, 1970.

[Go98] J.R. Goldman, *The Queen of Mathematics: An Historically Motivated Guide to Number Theory*, A.K. Peters, Wellesley, Massachusetts, 1998.

[Go80] J. Gordon, "Use of intractable problems in cryptography," *Information Privacy*, Volume 2 (1980), 178–184.

[Gr04] A. Granville, "It is easy to determine whether a given integer is prime," *Current Events in Mathematics*, American Mathematical Society, 2004.

[GrTu02] A. Granville and T.J. Tucker, "It's as Easy as abc," *Notices of the American Mathematical Society*, Volume 49 (2002), 1224–1231.

[Gr82] E. Grosswald, *Topics from the Theory of Numbers*, 2nd ed., Birkhauser, Boston, 1982.

[GrKnPa94] R.L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1994.

[Gu80] H. Gupta, *Selected Topics in Number Theory*, Abacus Press, Kent, England, 1980.

[Gu75] R.K. Guy, "How to factor a number," *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics*, Utilitas, Winnepeg, Manitoba, 1975, 49–89.

[Gu94] R.K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer-Verlag, New York, 1994.

[Ha83] P. Hagis, Jr., "Sketch of a proof that an odd perfect number relatively prime to 3 has at least eleven prime factors," *Mathematics of Computations*, Volume 46 (1983), 399–404.

[HaWr79] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979.

[He80] A.K. Head, "Multiplication modulo n," *BIT*, Volume 20 (1980), 115–116.

[He79] M.E. Hellman, "The mathematics of public-key cryptography," *Scientific American*, Volume 241 (1979) 146–157.

[Hi31] L.S. Hill, "Concerning certain linear transformation apparatus of cryptography," *American Mathematical Monthly*, Volume 38 (1931), 135–154.

[Hu82] L. Hua, *Introduction to Number Theory*, Springer-Verlag, New York 1982.

[Hw79] K. Hwang, *Computer Arithmetic: Principles, Architecture and Design*, Wiley, New York, 1979.

[IrRo95] K.F. Ireland and M.I. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1995.

[Ka96] D. Kahn, *The Codebreakers, the Story of Secret Writing*, 2nd ed., Scribners, New York, 1996.

[Ka98] V. Katz, *A History of Mathematics: An Introduction*, 2nd ed., Addison-Wesley, Boston, 1998.

[Ki04] S.V. Kim, "An Elementary Proof of the Quadratic Reciprocity Law," *American Mathematical Monthly*, Volume 111, Number 1 (2004), 45–50.

[Ki74] A.M. Kirch, *Elementary Number Theory: A Computer Approach*, Intext, New York, 1974.

[Ki01] J. Kirtland, *Identification Numbers and Check Digit Schemes*, Mathematical Association of America, Washington, D.C., 2001.

[Kl72] M. Kline, *Mathematical Thought from Ancient to Modern Times*, Oxford University, New York, 1972.

[Kn97] D.E. Knuth, *Art of Computer Programming: Semi-Numerical Algorithms*, Volume 2, 3rd ed., Addison-Wesley, Reading, Massachusetts, 1997.

[Kn97a] D.E. Knuth, *Art of Computer Programming: Sorting and Searching*, Volume 3, 2nd ed., Addison-Wesley, Reading, Massachusetts, 1997.

[Ko96] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Springer-Verlag, New York, 1996.

[Ko94] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., Springer-Verlag, New York, 1994.

[Ko96a] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Advances in Cryptology—CRYPTO '96*, LNCS 1109, Springer-Verlag, New York, 1996, 104–113.

[Ko83] G. Kolata, "Factoring Gets Easier," *Science*, Volume 222 (1983), 999–1001.

[Ko81] A.G. Konheim, *Cryptography: A Primer*, Wiley, New York, 1981.

[Kr86] E. Kranakis, *Primality and Cryptography*, Wiley-Teubner, Stuttgart, Germany, 1986.

[Kr79] L.Kronsjo, *Algorithms: Their Complexity and Efficiency*, Wiley, New York, 1979.

[Ku76] S. Kullback, *Statistical Methods in Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1976.

[La90] J.C. Lagarias, "Pseudo-random number generators in cryptography and number theory," pages 115–143 in *Cryptology and Computational Number Theory*, Volume 42 of Proceedings of Symposia in Advanced Mathematics, American Mathematical Society, Providence, Rhode Island, 1990.

[LaOd82] J.C. Lagarias and A.M. Odlyzko, "New algorithms for computing $\pi(x)$," Bell Laboratories Technical Memorandum TM-82-11218-57.

[La58] E. Landau, *Elementary Number Theory*, Chelsea, New York, 1958.

[La60] E. Landau, *Foundations of Analysis*, 2nd ed., Chelsea, New York, 1960.

[La35] H.P. Lawther, Jr., "An application of number theory to the splicing of telephone cables," *American Mathematical Monthly*, Volume 42 (1935), 81–91.

[LePo31] D.H. Lehmer and R.E. Powers, "On factoring large numbers," *Bulletin of the American Mathematical Society*, Volume 37 (1931), 770–776.

[Le00] F. Lemmermeyer, *Reciprocity Laws I*, Springer-Verlag, Berlin, 2000.

[Le79] A. Lempel, "Cryptology in transition," *Computing Surveys*, Volume 11 (1979), 285–303.

[Le80] H.W. Lenstra, Jr., "Primality testing," *Studieweek Getaltheorie en Computers*, 1–5 September 1980, Stichting Mathematisch Centrum, Amsterdam, Holland.

[Le90] W.J. Leveque, *Elementary Theory of Numbers*, Dover, New York, 1990.

[Le96] W.J. LeVeque, *Fundamentals of Number Theory*, Dover, New York, 1996.

[Le74] W.J. LeVeque, editor, *Reviews in Number Theory* [1940–1972], and R.K. Guy, editor, *Reviews in Number Theory* [1973–1983], six volumes each, American Mathematical Society, Washington, D.C., 1974 and 1984, respectively.

[LiDu87] Y. Li and S. Du, *Chinese Mathematics: A Concise History*, translated by J. Crossley and A. Lun, Clarendon Press, Oxford, England, 1987.

[Li73] U. Libbrecht, *Chinese Mathematics in the Thirteenth Century, The Shu-shu chiu-chang of Ch'in Chiu-shao*, MIT Press, 1973.

[Li79] R.J. Lipton, "How to cheat at mental poker," and "An improved power encryption method," unpublished reports, Department of Computer Science, University of California, Berkeley, 1979.

[Lo95] C.T. Long, *Elementary Introduction to Number Theory*, 3rd ed., Waveland Press, Prospect Heights, Illinois, 1995.

[Lo90] J.H. Loxton, editor, *Number Theory and Cryptography*, Cambridge University Press, Cambridge, England, 1990.

[Ma79] D.G. Malm, *A Computer Laboratory Manual for Number Theory*, COMPress, Wentworth, New Hampshire, 1979.

[McRa79] J.H. McClellan and C.M. Rader, *Number Theory in Digital Signal Processing*, Prentice Hall, Englewood Cliffs, New Jersey, 1979.

[Ma--] G.B. Matthews, *Theory of Numbers*, Chelsea, New York (no publication date provided).

[Ma94] U. Maurer, "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms," *Advances in Cryptology—CRYPTO '94*, LNCS 839, 1994, 271–281.

[Ma95] U. Maurer, "Fast generation of prime numbers and secure public-key cryptographic parameters," *Journal of Cryptology*, Volume 8 (1995), 123–155.

[Ma00] B. Mazur, "Questions about powers of numbers," *Notices of the American Mathematical Society*, Volume 47 (2000), 195–202.

[MevaVa97] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, Florida, 1997.

[Me82] R.C. Merkle, *Secrecy, Authentication, and Public Key Systems*, UMI Research Press, Ann Arbor, Michigan, 1982.

[MeHe78] R.C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks," *IEEE Transactions in Information Theory*, Volume 24 (1978), 525–530.

[MeMa82] C.H. Meyer and S.M. Matyas, *Cryptography: A New Dimension in Computer Data Security*, Wiley, New York, 1982.

[Mi76] G.L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and Systems Science*, Volume 13 (1976), 300–317.

[Mi47] W.H. Mills, "A prime-representing function," *Bulletin of the American Mathematical Society*, Volume 53 (1947), 604.

[Mo96] R.A. Mollin, *Quadratics*, CRC Press, Boca Raton, Florida, 1996.

[Mo99] R.A. Mollin, *Algebraic Number Theory*, CRC Press, Boca Raton, Florida, 1999.

[Mo96] M.B. Monagan, K.O. Geddes, K.M. Heal, G. Labahn, and S.M. Vorkoetter, *Maple V Programming Guide*, Springer-Verlag, New York, 1996.

[Mo80] L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms, *Theoretical Computer Science*, Volume 11 (1980), 97–108.

[Mo69] L.J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[Na81] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1981.

[Ne69] O.E. Neugebauer, *The Exact Sciences in Antiquity*, Dover, New York, 1969.

[NeSc99] J. Neukirch and N. Schappacher, *Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[NiZuMo91] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.

[Odte85] A.M. Odlyzko and H.J.J. te Riele, "Disproof of the Mertens conjecture," *Journal für die reine und angewandte Mathematik*, Volume 357 (1985), 138–160.

[Od90] A.M. Odlyzko, "The rise and fall of knapsack cryptosystems," pages 75–88 in *Cryptology and Computational Number Theory*, Volume 42 of Proceedings of Symposia in Applied Mathematics, American Mathematical Society, Providence, Rhode Island, 1990.

[Od95] A.M. Odlyzko, "The future of integer factorization," *RSA CrytoBytes*, Volume 2, Number 1, 1995, 5–12.

[Or67] O. Ore, *An Invitation to Number Theory*, Random House, New York, 1967.

[Or88] O. Ore, *Number Theory and its History*, Dover, New York, 1988.

[PaMi88] S.K. Park and K.W. Miller, "Random Number Generators: Good Ones are Hard to Find," *Communications of the ACM*, Volume 31 (1988), 1192–1201.

[PeBy70] A.J. Pettofrezzo and D.R. Byrkit, *Elements of Number Theory*, Prentice Hall, Englewood Cliffs, New Jersey, 1970.

[Pf89] C.P. Pfleeger, *Security in Computing*, Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[Po14] H.C. Pocklington, "The determination of the prime or composite nature of large numbers by Fermat's theorem," *Proceedings of the Cambridge Philosophical Society*, Volume 18 (1914/6), 29–30.

[PoHe78] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, Volume 24 (1978), 106–110.

[Po99] H. Pollard and H. Diamond, *The Theory of Algebraic Numbers*, 3rd ed., Dover, New York, 1999.

[Po74] J.M. Pollard, "Theorems on Factorization and Primality Testing," *Proceedings of the Cambridge Philosophical Society*, Volume 76 (1974), 521–528.

[Po75] J.M. Pollard, "A Monte Carlo Method for Factorization," *Nordisk Tidskrift for Informationsbehandling (BIT)*, Volume 15 (1975), 331–334.

[Po81] C. Pomerance, "Recent developments in primality testing," *The Mathematical Intelligencer*, Volume 3 (1981), 97–105.

[Po82] C. Pomerance, "The search for prime numbers," *Scientific American*, Volume 247 (1982), 136–147.

[Po84] C. Pomerance, *Lecture Notes on Primality Testing and Factoring*, Mathematical Association of America, Washington, D.C., 1984.

[Po90] C. Pomerance, ed., *Cryptology and Computational Number Theory*, American Mathematical Society, Providence, Rhode Island, 1990.

[Po93] C. Pomerance, "Carmichael Numbers," *Nieuw Arch. v. Wiskunde*, Volume 4, number 11 (1993), 199–209.

[Ra79] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," M.I.T. Laboratory for Computer Science Technical Report LCS/TR-212, Cambridge, Massachusetts, 1979.

[Ra80] M.O. Rabin, "Probabilistic algorithms for testing primality," *Journal of Number Theory*, Volume 12 (1980), 128–138.

[Ra77] H. Rademacher, *Lectures on Elementary Number Theory*, Krieger, 1977.

[Re96] D. Redfern, *The Maple Handbook*, Springer-Verlag, New York, 1996.

[Re96] D. Redmond, *Number Theory: An Introduction*, Marcel Dekker, Inc., New York, 1996

[Ri79] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[Ri96] P. Ribenboim, *The New Book of Prime Number Record*, Springer-Verlag, New York, 1996.

[Ri01] P. Ribenboim, *Classical Theory of Algebraic Integers*, 2nd ed., Springer-Verlag, New York, 2001.

[Ri59] B. Riemann, "Uber die Anzahl der Primzahlen unter einer gegeben Grösse," *Monatsberichte der Berliner Akademie*, November, 1859.

[Ri85a] H. Riesel, "Modern factorization methods," *BIT*(1985), 205–222.

[Ri94] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhauser, Boston, 1994.

[Ri78] R.L. Rivest, "Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem," *Cryptologia*, Volume 2 (1978), 62–65.

[RiShAd78] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Volume 21 (1978), 120–126.

[RiShAd83] R.L. Rivest, A. Shamir, and L.M. Adleman, "Cryptographic communications system and method," United States Patent #4,405,8239, issued September 20, 1983.

[Ro77] J. Roberts, *Elementary Number Theory*, MIT Press, Cambridge, Massachusetts, 1977.

[Ro97] K. Rosen et. al., *Exploring Discrete Mathematics with Maple*, McGraw-Hill, New York, 1997.

[Ro99a] K.H. Rosen, *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Boca Raton, Florida, 1999.

[Ro03] K.H. Rosen, *Discrete Mathematics and its Applications*, 5th ed., McGraw-Hill, New York, 2003.

[Ru64] W. Rudin, *Principles of Mathematical Analysis*, 2nd ed., McGraw-Hill, New York, 1964.

[Ru83] R. Rumely, "Recent advances in primality testing," *Notices of the American Mathematical Society*, Volume 30 (1983), 475–477.

[Sa03a] K. Sabbagh, *The Riemann Hypothesis*, Farrar, Strauss, and Giroux, New York, 2003.

[Sa90] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, New York, 1990.

[Sa03b] M. du Sautoy, *The Music of the Primes*, Harper Collins, New York, 2003.

[ScOp85] W. Scharlau and H. Opolka, *From Fermat to Minkowski, Lectures on the Theory of Numbers and its Historical Development*, Springer-Verlag, New York, 1985.

[Sc86] M.R. Schroeder, *Number Theory in Science and Communication*, 2nd ed., Springer-Verlag, Berlin, 1986.

[SePi89] J. Seberry and J. Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall, New York, 1989.

[Sh79] A. Shamir, "How to share a secret," *Communications of the ACM*, Volume 22 (1979), 612–613.

[Sh83] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," in *Advances in Cryptology—Proceedings of Crypto 82*, 279–288.

[Sh84] A. Shamir, "A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem," *IEEE Transactions on Information Theory*, Volume 30 (1984), 699–704. (This is an improved version of [Sh83].)

[ShRiAd81] A. Shamir, R.L. Rivest, and L.M. Adleman, "Mental Poker," *The Mathematical Gardner*, ed. D.A. Klarner, Wadsworth International, Belmont, California, 1981, 37–43.

[Sh85] D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

[Sh83] H.S. Shapiro, *Introduction to the Theory of Numbers*, Wiley, New York, 1983.

[Sh67] J.E. Shockley, *Introduction to Number Theory*, Holt, Rinehart, and Winston, New York, 1967.

[Si64] W. Sierpinski, *A Selection of Problems in the Theory of Numbers*, Pergamon Press, New York, 1964.

[Si70] W. Sierpinski, *250 Problems in Elementary Number Theory*, Polish Scientific Publishers, Warsaw, 1970.

[Si87] W. Sierpinski, *Elementary Theory of Numbers*, 2nd ed., North-Holland, Amsterdam, 1987.

[Si82] G.J. Simmons, ed., *Secure Communications and Asymmetric Cryptosystems*, AAAS Selected Symposium Series Volume 69, Westview Press, Boulder, Colorado, 1982.

[Si97] S. Singh, *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*, Walker and Company, New York, 1997.

[Si66] A. Sinkov, *Elementary Cryptanalysis*, Mathematical Association of America, Washington, D.C., 1966.

[SlPl95] N.J.A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York, 1995.

[Sl78] D. Slowinski, "Searching for the 27th Mersenne prime," *Journal of Recreational Mathematics*, Volume 11 (1978/9), 258–261.

[SoSt77] R. Solovay and V. Strassen, "A fast Monte Carlo test for primality," *SIAM Journal for Computing*, Volume 6 (1977), 84–85 and erratum, Volume 7 (1978), 118.

[So86] M.A. Soderstrand et al., editors, *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing*, IEEE Press, New York, 1986.

[Sp82] D.D. Spencer, *Computers in Number Theory*, Computer Science Press, Rockville, Maryland, 1982.

[St78] H.M. Stark, *An Introduction to Number Theory*, Markham, Chicago, 1970; reprint MIT Press, Cambridge, Massachusetts, 1978.

[St64] B.M. Stewart, *The Theory of Numbers*, 2nd ed., Macmillan, New York, 1964.

[St02] D.R. Stinson, *Cryptography, Theory and Practice*, 2nd ed., Chapman & Hall/CRC, Boca Raton, Florida, 2002.

[SzTa67] N.S. Szabo and R.J. Tanaka, *Residue Arithmetic and its Applications to Computer Technology*, McGraw-Hill, 1967.

[TrWa02] W. Trappe and L. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, Upper Saddle River, New Jersey, 2002.

[UsHe39] J.V. Uspensky and M.A. Heaslet, *Elementary Number Theory*, McGraw-Hill, New York, 1939.

[Va89] S. Vajda, *Fibonacci & Lucas Numbers and the Golden Section: Theory and Applications*, Ellis Horwood, Chichester, England, 1989.

[Va96] A.J. van der Poorten, *Notes on Fermat's Last Theorem*, Wiley, New York, 1996.

[Va01] C. VandenEynden, *Elementary Number Theory*, McGraw-Hill, New York, 2001.

[Vi54] I.M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

[Wa86] S. Wagon, "Primality testing," *The Mathematical Intelligencer*, Volume 8, Number 3 (1986), 58–61.

[Wa99] S. Wagon, *Mathematica in Action*, 2nd ed. Telos, New York, 1999.

[Wa86] S.S. Wagstaff, "Using computers to teach number theory," *SIAM News*, Volume 19 (1986), 14 and 18.

[Wa90] S.S. Wagstaff, "Some uses of microcomputers in number theory research," *Computers and Mathematics with Applications*, Volume 19 (1990), 53–58.

[WaSm87] S.S. Wagstaff and J.W. Smith, "Methods of factoring large integers," in *Number Theory, New York, 1984–1985*, LNM, Volume 1240, Springer-Verlag, Berlin, 1987, 281–303.

[We84] A. Weil, *Number Theory: An approach through history from Hummurapi to Legendre*, Birkhauser, Boston, 1984.

[Wi90] M.J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, Volume 36 (1990), 553–558.

[Wi95] A. Wiles, "Modular elliptic-curves and Fermat's last theorem," *Annals of Mathematics*, Volume 141 (1995), 443–551.

[Wi86] H.C. Williams, ed., *Advances in Cryptology—CRYPTO '85*, Springer-Verlag, Berlin, 1986.

[Wi78] H.C. Williams, "Primality testing on a computer," *Ars Combinatorica*, Volume 5 (1978), 127–185.

[Wi82] H.C. Williams, "The influence of computers in the development of number theory," *Computers and Mathematics with Applications*, Volume 8 (1982), 75–93.

[Wi84] H.C. Williams, "An overview of factoring," in *Advances in Cryptology, Proceedings of Crypto 83*, Plenum, New York, 1984, 87–102.

[Wo03] S. Wolfram, *The Mathematica Book*, 5th ed., Cambridge University Press, New York, 2003.

[Wr39] H.N. Wright, *First Course in Theory of Numbers*, Wiley, New York, 1939.

[Wu85] M.C. Wunderlich, "Implementing the continued fraction algorithm on parallel machines," *Mathematics of Computation*, Volume 44 (1985), 251–260.

[WuKu90] M.C. Wunderlich and J.M. Kubina, "Extending Waring's conjecture to 471,600,000," *Mathematics of Computation*, Volume 55 (1990), 815–820.

Index of Biographies

Index

Photo Credits

Courtesy of The MacTutor History of Mathematics Archive, University of St. Andrews, Scotland: Stanislaw M. Ulam, Fibonacci, Francois-Edouard-Anatole Lucas, Paul Gustav Heinrich Bachmann, Edmund Landau, Pafnuty Lvovich Chebyshev, Jacques Hadamard, Alte Selberg, Joseph Louis François Bertrand, G. Lejeune Dirichlet, Gabriel Lamé, David Hilbert, Karl Friedrich Gauss, Kurt Hensel, Joseph Louis LaGrange, Georg Friedrich Bernhard Reimann, Leonhard Euler, Joesph Liouville, Srinivasa Ramanujan, Marin Mersenne, August Ferdinand Möbius, Adrien-Marie Legendre, Ferdinand Gotthold Max Eisenstein, Carl Gustav Jacob Jacobi, Leopold Kroneker, Georg Cantor, Pythagoras, Sophie Germain, Ernst Eduard Kummer, Andrew Wiles, Claude Bachet, Edward Waring, Axel Thue, and Blaise Pascal; Eratosthenes © Culver Pictures, Inc.; Paul Erdos © 1985 Wlodzimierz Kuperberg; Euclid © The Granger Collection; Pierre de Fermat © Giraudon/Art Resource, N.Y.; Derrick H. Lehmer © 1993 the American Mathematical Society; Gilbert S. Vernam © Worcester Polytechnic Institute, Class of 1914; Adi Shamir © the Weizmann Institute of Science, Israel; Ronald Rivest © 1999 Ronald Rivest; Leonard Adleman © 1999 Eric Mankin, University of Southern California; John Von Neumann © Corbis; Emil Artin © The Hall of Great Mathematicians, Southern Illinois University, Edwardsville; Eugène Catalan © Collections artistiques de l'Université de Liège.