Elementary Number Theory and Its Applications

Fifth Edition

Kenneth H. Rosen
AT&T Laboratories

PEARSON
Addison Wesley

Boston San Francisco New York
London Toronto Sydney Tokyo Singapore Madrid
Mexico City Munich Paris Cape Town Hong Kong Montreal

Publisher: Greg Tobin
Senior Acquisitions Editor: William Hoffman
Editorial Assistants: Emily Portwood and Mary Reynolds
Marketing Manager: Yolanda Cossio
Marketing Coordinator: Heather Peck
Managing Editor: Karen Wernholm
Senior Production Supervisors: Jeffrey Holcomb and Julie LaChance
Project Management: Barbara Pendergast
Composition and Art Illustration: Windfall Software, using ZzTEX
Senior Manufacturing Buyer: Evelyn Beaton
Photo Research: Beth Anderson
Interior Design: Barbara T. Atkinson
Cover Design: Suzin Purney Osborne
Cover Image: © Jasper Johns / Licensed by VAGA, New York, NY / SuperStock

Photo Credits: Grateful acknowledgment is made to the copyright holders of the biographical photos, listed on page 721, which is hereby made part of this copyright page.

ISBN 0-321-26314-6
1 2 3 4 5 6 7 8 9 10-PHT-07 06 05 04

Preface

In olden times (well, before 1975) number theory had the reputation of being the purest part of mathematics. It was studied for its long and rich history, its wealth of easily accessible and fascinating questions, and its intellectual appeal. But, in the past few years, people have looked at number theory in a new way. Today, people study number theory both for the traditional reasons and for the compelling reason that number theory has become essential for cryptography. The first edition of this book was the first text to integrate the modern applications of elementary number theory with traditional topics. This fifth edition builds on the basic approach of the original text. No other number theory text presents elementary number theory and its applications in as thoughtful a fashion as this book does. Instructors will be pleasantly surprised to see how modern applications can be seamlessly woven into their number theory course when they use this text.

This book is designed as a text for an undergraduate number theory course at any level. No formal prerequisites are needed for most of the material, other than some level of mathematical maturity. This book is also designed to be a useful supplement for computer science courses and as a number theory primer for people interested in learning about new developments in number theory and cryptography.

This fifth edition has been designed to preserve the strengths of previous editions while providing substantial enhancements and improvements. Instructors familiar with previous editions will be comfortable with this new edition. Those examining this book for the first time will see an up-to-date text, which integrates gems of number theory dating back thousands of years with developments less than ten years old. Those familiar with previous editions will find that this book has become more flexible, easier to teach from, and more interesting and compelling. They will also find that additional emphasis has also been placed on the historical context of results and on the experimental side of number theory.

Changes in the Fifth Edition

This new edition incorporates many improvements made at the request of users and reviewers. The new edition should be easier to teach from, easier to read, and more interesting and informative. This edition more effectively conveys both the beauty and the utility of number theory. Noteworthy changes include:

- ***More flexible organization***

The first section of the fourth edition has been divided into two shorter sections. The first covers types of numbers and sequences and introduces diophantine approximation. The second covers sums and products. Instructors can skip most of the material in these two sections if desired, although many will want to cover the material on diophantine approximation. Section 3.1 of the fourth edition has also been divided into two sections. The first of these sections introduces primes, establishes that there are infinitely many primes, and begins the discussion of how primes are found. The second section discusses the distribution of primes and introduces the prime number theorem and many conjectures about prime numbers.

- ***Expanded coverage of cryptography***

Cryptanalysis of Vigènere ciphers has been added with the introduction of the Kasiski test and the index of coincidence. Recent developments in cryptography are mentioned, including the AES encryption standard. Attacks that have been devised on implementations on RSA are now described. One such attack is now developed in Chapter 12 using ideas from diophantine approximation using continued fractions. The weakness in a proposed zero-knowledge proof method is now included in an exercise.

- ***Up-to-date discoveries***

The latest discoveries in number theory are reflected in the text, including a number of theoretical discoveries and discussions concerning the polynomial time algorithm for proving an integer in prime and the resolution of the Catalan conjecture. Computational discoveries, such as three new Mersenne primes, have been added. The Web site for the book will highlight the latest news in number theory and links will be provided that announce discoveries made subsequent to the publication of this book.

- ***New and expanded topic coverage***

Dirichlet's theorem on approximation of real numbers by rational numbers has been added, introducing the subject of diophantine approximation to the first section of the text. A proof using the pigeonhole principle is provided. Many important topics whose full treatment is beyond the scope of an elementary number theory text are now discussed; the goal is to give the student a fuller appreciation of number theory. In a similar vein, the coverage of diophantine equations has been expanded. This edition includes brief discussions of Beal's conjecture, the Catalan conjecture and its recent resolution, and the Fermat-Catalan conjecture. The abc conjecture is also discussed, and how it can be used to prove results on diophantine equations is illustrated.

A new chapter on the Gaussian integers has been added. This chapter introduces Gaussian primes, the greatest common divisor of Gaussian integers, the Euclidean algorithm for Gaussian integers, and the unique factorization of Gaussian integers into Gaussian primes. This new chapter also explains how Gaussian integers can be used to find the number of ways to express a positive integer into the sum of two squares.

- ***Improved examples and proofs***

Euclid's proof that there are infinitely many primes is now given in the text. A large number of other proofs of the infinitude of primes can be found in the exercises. Many proofs have been improved, either by simplification or by additional explanation.

- ***Enhanced exercise sets***

This book has long been noted for its exceptional exercises; in this edition the exercises are even better. All exercises in the text have been reviewed and solved; exercises from the fourth edition found to be ambiguous or lacking assumptions have been clarified.

Several hundred new exercises have been added. Additional exercises involving Fibonacci identities have been inserted. New exercises also outline different proofs that there are infinitely many primes. There are many new exercises on cryptography, including many relating to the Vigènere cipher and the RSA cryptosystem. The newest proof of the law of quadratic reciprocity is outlined in an exercise. More exercises on nonlinear diophantine equations have been added, including exercises on Bachet's equation, Markov's equation, and congruent numbers.

- ***Expanded historical context and biographies***

The history and status of the Riemann hypothesis are now covered. Skewes' constant, one of the largest numbers arising in a proof, is introduced. Also added is an account of the discovery by Thomas Nicely of the famous division flaw in the Pentium chip, found because two computations involving twin primes did not agree. This edition introduces many new biographies, including those of Bertrand, Farey, Waring, Bachet, Kronecker, Levi ben Gerson, and Catalan. Photographs have been also been added to many biographies.

- ***Enhanced ancillaries and enhanced support for Maple® and Mathematica®***

The *Student's Solutions Manual* and the *Instructor's Manual* have been enhanced. They both now contain a comprehensive guide explaining how to use Maple for computations in number theory. Suggested syllabi for different courses are now contained in the *Instructor's Manual.* The *Instructor's Manual* and the Web site now both contain migration guides for the exercises showing where exercises in the fourth edition can be found in the fifth edition, and conversely, where exercises in the fifth edition were located in the fourth edition, if they were included in this previous edition.

Commands for carrying out computations with the Gaussian integers have been added to the appendix that describes number theory commands in Maple and *Mathematica.*

- *Extra focus on accuracy*

This edition benefits from extra resources devoted to ensure the accuracy of the text, as well as the exercises and their answers and solutions. Three accuracy checkers have spent long hours making sure that this book is as error-free as possible.

- *Expanded Web site*

The Web site for this text has been expanded and enhanced in several key ways. "Number Theory News" is a new feature highlighting recent discoveries in number theory. The extensive list of number theory Web sites keyed to the text has been expanded and all links have been updated. These links will be periodically updated during the life of this edition. The Web site now also supports an extensive collection of number theory and cryptography applets which can be used for computations and exploration, as well as a tutorial on PARI/GP, a computational system for fast computation in number theory upon which these applets are built. A collection of suggested group or individual student projects can also be found on the Web site.

Features

A Development of Classical Number Theory

The core of this book presents classical elementary number theory in a comprehensive and compelling manner. The historical context and importance of key results are noted. The basic material on each topic is developed carefully, followed by more sophisticated results on the same topic.

Applications

A key strength of this book is how applications of number theory are covered. Once the requisite theory has been developed, applications are woven into the text in a flexible way. These applications are designed to motivate the coverage of the theory and illustrate the usefulness of different aspects of elementary number theory. Extensive coverage is devoted to applications of number theory to cryptography. Classical ciphers, block and stream ciphers, public key cryptosystems, and cryptographic protocols are all covered. Other applications to computer science include fast multiplication of integers, pseudorandom numbers, and check digits. Applications to many other areas, such as scheduling, telephony, entomology, and zoology can also be found in the text.

Unifying Themes

Many concepts from elementary number theory are used in primality testing and factoring. Furthermore, primality testing and factoring play a key role in applications of number theory to cryptography. As such, these topics are used as unifying themes and are returned to repeatedly. Almost every chapter includes material on these topics.

Accessibility

This book has been designed with a minimum of prerequisites. The book is almost entirely self-contained, with only a knowledge of what is generally known as "college algebra" required. There are several places where knowledge of some concepts from calculus is needed (such as in the discussions of the distribution of primes and big-O notation). Concepts from discrete mathematics and linear algebra are needed in a few places. All material that depends on topics more advanced than college algebra is explicitly noted and is optional.

Accuracy

Great effort has been made to ensure the accuracy of this edition. Input from many users of the fourth edition, reviewers, and proofreaders has helped achieve this goal.

Extensive Exercise Sets

The best (and maybe the only) way to learn mathematics is by doing exercises. This text contains an extremely extensive and diverse collection of exercises. Many routine exercises are included to develop basic skills, with care taken so that both odd-numbered and even-numbered exercises of this type are included. A large number of intermediate-level exercises help students put several concepts together to form new results. Many other exercises and blocks of exercises are designed to develop new concepts. Challenging exercises are in ample supply and are marked with one star (*) indicating a difficult exercise and two stars (**) indicating an extremely difficult exercise. There are some exercises that contain results used later in the text; these are marked with a pointing-hand symbol (☞). These exercises should be assigned by instructors whenever possible.

An extensive collection of computer projects is also provided. Each section includes computations and explorations designed to be done with a computational program such as Maple or *Mathematica*, or using programs written by instructors and/or students. There are some routine exercises of this sort that students should do to learn how to apply basic commands from Maple or *Mathematica* (as described in Appendix D), as well as more open-ended questions designed for experimentation and creativity. Each section also includes a set of programming projects designed to be done by students using a programming language of their choice, such as the programming languages included with Maple and *Mathematica*, or another programming language of their choice.

Exercise Answers

The answers to all odd-numbered exercises are provided at the end of the text. More complete solutions to these exercises can be found in the *Student's Solutions Manual* that accompanies this text. All solutions have been carefully checked and rechecked to ensure accuracy.

Discovery via Empirical Evidence

In many places in the text numerical evidence is examined to help motivate key results. This gives an opportunity to students to come up with a conjecture much as the people who originally developed many of the results of number theory did.

Extensive Examples

This book includes examples that illustrate each important concept. These examples are designed to illustrate the definitions, algorithms, and proofs in the text. They are also designed to help students work many of the exercises found at the end of sections.

Carefully Motivated Proofs

Many proofs in this book are motivated with examples that precede the formal proof and illustrate the key ideas of the proof. The proofs themselves are presented in a careful, rigorous, and fully explained manner. The proofs are designed so that students can understand each step and the flow of logic. Numerical examples illustrating the steps of the proof are often provided following the formal proof as well.

Algorithmic Reasoning

The algorithmic aspects of elementary number theory are thoroughly covered in this text. Not only are many algorithms described, but their complexity is also analyzed. Among the algorithms described in this book are those for computing greatest common divisors in many different ways and for primality testing and factoring. The coverage of the complexity of algorithms has been included so that instructors can choose whether they want to include this material in their course.

Biographies and Historical Notes

More than 60 biographies of contributors to number theory are included in this edition. Contributors included lived in ancient times, the Middle Ages, the sixteenth through eighteenth centuries, the nineteenth century, and the twentieth century, and lived in the East and in the West. These biographies are designed to give students an appreciation of contributors as unique individuals who often led (or are leading) interesting lives.

Open Questions

Many open questions in number theory are described throughout the book. Some are described in the text itself and others are found in exercise sets. These questions show that the subject of number theory is a work in progress. Readers should be aware that attempting to solve such problems can often be time-consuming and futile. However, it would be surprising if some of these questions were not settled in the next few years.

Up-to-Date Content

The latest discoveries in number theory are included in this book. The current status of many open questions is described, as are new theoretical results. Discoveries of new primes and factorizations made as late as September 2004 are included with the first printing of this edition. These discoveries will help readers understand that number theory is an extremely active area of study. They may even see how they may participate in the search for new primes.

Bibliography

An extensive bibliography is provided for this book. This bibliography lists key printed number theory resources, including both books and papers. Many useful number texts are listed, as are books dealing with the history of number theory and particular aspects of the subject. Many original sources are included, as is material covering cryptography.

Maple and *Mathematica* Support

An appendix has been provided which lists the commands in both Maple and *Mathematica* for carrying out computations in number theory. These commands are listed according to the chapter of the text relevant to these commands.

Web Resources

The Web site for this book includes a Web guide to number theory that is keyed to this text, as well as an extensive collection of other resources. To access this site go to `www.awlonline.com/rosen`. For convenience, the most important number theory Web sites are highlighted in Appendix D.

Tables

A set of five tables is included to help students with their computations and experimentation. Looking at these tables can help students search for patterns and formulate conjectures. The use of a computational software package, such as Maple or *Mathematica* is recommended when these tables are insufficient.

List of Symbols

A list of symbols used in the text and where they are defined is included on the inside front cover of this book.

Ancillaries

Student's Solutions Manual (ISBN 0-321-26840-7)

The *Student's Solutions Manual* contains worked solutions to all the odd-numbered exercises in the text and other helpful material, including some tips on using Maple and

Mathematica to explore number theory. A tutorial for using Maple to do computations in number theory is provided.

Instructor's Manual (ISBN 0-321-26842-3)

The *Instructor's Manual* contains solutions to all exercises in the text. It also contains advice on planning which sections to cover. Sample tests are also provided.

Web Site

The Web site for this book contains a guide providing annotated links to a large number of Web sites relevant to number theory. These sites are keyed to the page in the book where relevant material is discussed. These locations are marked with an icon (🕸) in the text. The Web site also contains a section highlighting the latest discoveries in number theory. An extensive collection of number theory and cryptography applets is also provided.

How to Use this Book

This text is designed to be extremely flexible. The essential, core material for a number theory course can be found in Section 1.4, which covers divisibility; Chapter 3, which covers primes, factoring, and greatest common divisors; Sections 4.1–4.3, which cover congruences; and Chapter 6, which covers important congruences including Fermat's little theorem. Instructors can design their own courses by supplementing core material with other content of their own choice. To help instructors decide which sections to cover, a brief description of the different parts of the book follows.

The material in Sections 1.1–1.4 is optional. Section 1.1 introduces different types of numbers, integer sequences, and countability. This section also introduces the notion of diophantine approximation. Section 1.2 reviews sums and products for students who need a review of these topics. Section 1.3 introduces mathematical induction, which students may already have studied elsewhere. (Material on integer axioms and the binomial theorem can be found in the appendices.) Section 1.4 introduces the Fibonacci numbers, a favorite topic of many instructors; students may have studied these numbers in a course in discrete mathematics. As stated previously, Section 1.5 presents core material on divisibility of integers and should be covered.

Chapter 2 is optional; it covers base b representations of integers, integer arithmetic, and the complexity of integer operations. Big-O notation is introduced in Section 2.3. This is important for students who have not seen this notation elsewhere, especially when the instructor wants to stress the complexity of computations in number theory.

As previously stated, Chapter 3 and Sections 4.1–4.3 present core material. Section 4.4, which deals with solving polynomial congruences modulo powers of primes is optional; it is important to development of p-adic number theory. Section 4.5 requires some background in linear algebra; the material in this section is used in Section 8.2; these sections may be omitted if desired. Section 4.6 introduces a particular factorization method (the Pollard rho method) and can be omitted.

Chapter 5 is optional. Instructors can pick and choose from a variety of applications of number theory. Section 5.1 introduces divisibility tests; Section 5.2 covers the perpetual calendar; Section 5.3 discusses scheduling round-robin tournaments; Section 5.4 shows how congruences can be used in hashing functions; and Section 5.5 describes how check digits are found and used. As mentioned previously, Chapter 6 presents core material.

Chapter 7 covers multiplicative functions. Section 7.1 should be covered; it introduces the basic concept of a multiplicative function and studies the Euler phi-function. The sum and number of divisors functions are studied in Section 7.2; this section is recommended for all instructors. All instructors will probably want to cover Section 7.3, which introduces the concept of a perfect number and describes the search for Mersenne primes.

Chapter 8 covers the applications of number theory to cryptology. It is highly recommended since this is such an important topic and one that students find extremely interesting. Section 8.1 introduces the basic terminology of this subject and some classical character ciphers; instructors who plan to cover cryptography in their course should be sure to include this section. Section 8.2 introduces block and stream ciphers, two important families of ciphers, and provides examples of these types of cipher that are based on number theory. Section 8.3 covers a particular type of block cipher based on modular exponentiation. Section 8.4 should be covered by all instructors. It introduces the fundamental concept of public key cryptography and illustrates this with the RSA cryptosystem. Section 8.5 discusses knapsack ciphers; it is an optional section. Section 8.6 provides an introduction to cryptographic protocols and is highly recommended for instructors interested in modern cryptographic applications. (Additional topics from cryptography are covered in Chapters 9, 10, and 11.)

Chapter 9 deals with the concept of the order of an integer, primitive roots, and index arithmetic. Sections 9.1–9.4 should be covered if possible. Section 9.5, which discusses how the concepts of this chapter are used in primality testing presents partial converses of Fermat's little theorem. Section 9.6, on universal exponents, is optional; it contains some interesting results about Carmichael numbers.

Chapter 10 introduces some applications that use the material from Chapter 9. The three sections that cover pseudorandom numbers, the ElGamal cryptosystem, and schemes for splicing telephone cable are optional. Instructors stressing cryptographic applications will especially want to cover Section 10.2.

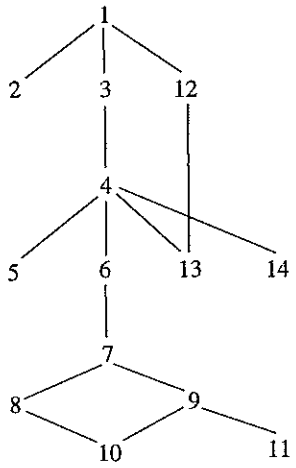
Sections 11.1 and 11.2, which cover quadratic residues and quadratic reciprocity, a key result of number theory, should be covered whenever possible. Sections 11.3 and 11.4 deal with Jacobi symbols and Euler pseudoprimes and are optional. Section 11.5 covers zero-knowledge proofs; instructors interested in cryptography will want to cover this section if possible.

Section 12.1, which covers decimal fractions, will be covered by many instructors. Instructors with an interest in continued fractions will want to cover Sections 12.2–12.4, which establish the basic results about finite and periodic continued fractions. Section 12.5, which deals with factoring using continued fractions, is optional.

Most instructors will want to cover Sections 13.1 and 13.2, which deal with Pythagorean triples and Fermat's last theorem, respectively. Section 13.3, which covers sums of squares, and Section 13.4, which discusses the solution of Pell's equation and which uses continued fractions, are optional sections.

Chapter 14 is an optional chapter covering the Gaussian integers. Many of their properties analogous to those of the integers are developed in this chapter. In particular, Gaussian primes are introduced and the unique factorization of Gaussian integers is established. Finally, the number of ways a positive integer can be expressed as the sum of two squares is found using Gaussian integers.

The following figure showing the dependency of chapters will help instructors plan their course. Suggested syllabi for courses with different emphases are provided in the *Instructor's Resource Guide.* Although Chapter 2 may be omitted if desired, it does explain the big-O notation used throughout the text to describe the complexity of algorithms. Chapter 12 only depends on Chapter 1 as shown, except for Theorem 12.4, which depends on material from Chapter 9. Section 13.4 is the only part of Chapter 13 that depends on Chapter 12. Chapter 11 can be covered without covering Chapter 9 if the optional comments involving primitive roots in Section 9.1 are omitted. Section 14.3 should also be covered in conjunction with Section 13.3.



Acknowledgments

I wish to thank my management at AT&T Laboratories for their support in the preparation of this edition and for providing a stimulating professional environment. Special thanks go to Bart Goddard who has prepared the ancillaries to this book and to Douglas Eubert, Tom Wegleitner, and Steve Whalen for their help reviewing the manuscript for accuracy and for their assistance with the solution of the exercises and for checking and rechecking the answers and solutions to these exercises.

Thanks go to Bill Hoffman, the editor of this edition, for his support, and to all the other editors of previous editions of this book at Addison-Wesley, going back to Wayne

Yuhasz and Jeff Pepper who endorsed the original concept and recognized the potential appeal of this book at a time when other publishers considered number theory a dead course not worthy of new books. My appreciation also goes to the editorial, production, marketing, and media team behind this book, including Mary Reynolds, Julie LaChance, Jeffrey Holcomb, Barbara Atkinson, Beth Anderson, Barbara Pendergast, Paul Anagnostopoulos, Emily Portwood, Lynne Blaszak, Greg Tobin, and Phyllis Hubbard. I would also like to thank David Wright for his many contributions to the Web site for this book, including material on PARI/GP, number theory and cryptography applets, and suggested projects.

I have benefited from the thoughtful reviews and suggestions from users of previous editions of this book. Many of their ideas have been incorporated in this edition. My profound thanks go the following reviewers who helped me prepare this edition:

Reviewers

Ruth Berger, *Luther College*
Joel Cohen, *University of Maryland*
Michael Cullinane, *Keene State College*
Mark Dickinson, *University of Michigan*
George Greaves, *Cardiff University*
Kerry Jones, *Ball State University*
Slawomir Klimek, *Indiana University-Purdue University Indianapolis*
Stephen Kudla, *University of Maryland*
Jennifer McNulty, *The University of Montana*
Stephen Miller, *Rutgers University*
Michael Mossinghoff, *Davidson College*
Michael E. O'Sullivan, *San Diego State University*
Gary Towsley, *SUNY Geneseo*
David Wright, *Oklahoma State University*

I also wish to thank again the reviewers of previous editions of this book who have helped improve this book from edition to edition. Their affiliations at the time they reviewed the book are noted.

David Bressoud, *Pennsylvania State University*
Sydney Bulman-Fleming, *Wilfred Laurier University*
Richard Bumby, *Rutgers University*
Charles Cook, *University of South Carolina, Sumter*
Christopher Cotter, *University of Northern Colorado*
Euda Dean, *Tarleton State University*
Daniel Drucker, *Wayne State University*
Bob Gold, *Ohio State University*
Fernando Gouvea, *Colby College*
Jennifer Johnson, *University of Utah*
Roy Jordan, *Monmouth College*
Herbert Kasube, *Bradley University*
Neil Koblitz, *University of Washington*
Steven Leonhardi, *Winona State University*

Charles Lewis, *Monmouth College*
James McKay, *Oakland University*
John Mairhuber, *University of Maine–Orono*
Alexsandrs Mihailovs, *University of Pennsylvania*
Rudolf Najar, *California State University, Fresno*
Carl Pomerance, *University of Georgia*
Sinai Robins, *Temple University*
Tom Shemanske, *Dartmouth College*
Leslie Vaaler, *University of Texas, Austin*
Evelyn Bender Vaskas, *Clark University*
Samuel Wagstaff, *Purdue University*
Edward Wang, *Wilfred Laurier University*
Betsey Whitman, *Framingham State University*
David Wright, *Oklahoma State*
Paul Zwier, *Calvin College*

Finally, I thank in advance all those who send me suggestions and corrections in the future. You may send such material to me care of Addison-Wesley at `math@awl.com`.

Kenneth H. Rosen
Middletown, New Jersey

Contents

What Is Number Theory?

There is a buzz about number theory: Thousands of people work on communal number theory problems over the Internet . . . the solution of a famous problem in number theory is reported on the PBS television series NOVA . . . people study number theory to understand systems for making messages secret . . . What is this subject, and why are so many people interested in it today?

Number theory is the branch of mathematics that studies the properties of, and the relationships between, particular types of numbers. Of the sets of numbers studied in number theory, the most important is the set of positive integers. More specifically, the *primes,* those positive integers with no positive proper factors other than 1, are of special importance. A key result of number theory shows that the primes are the multiplicative building blocks of the positive integers. This result, called the *fundamental theorem of arithmetic,* tells us that every positive integer can be uniquely written as the product of primes in nondecreasing order. Interest in prime numbers goes back at least 2500 years, to the studies of ancient Greek mathematicians. Perhaps the first question about primes that comes to mind is whether there are infinitely many. In *The Elements,* the ancient Greek mathematician Euclid provided a proof that there are infinitely many primes. Interest in primes was rekindled in the seventeenth and eighteenth centuries, when mathematicians such as Pierre de Fermat and Leonhard Euler proved many important results, and conjectured approaches for generating primes. The study of primes progressed substantially in the nineteenth century; results included the infinitude of primes in arithmetic progressions, and sharp estimates for the number of primes not exceeding a positive number x. The twentieth century has seen the development of many powerful techniques for the study of primes, but even with these powerful techniques, many questions remain unresolved. An example of a notorious unsolved question is whether there are infinitely many twin primes, which are primes that differ by 2. New results will certainly follow in the coming decades, as researchers continue working on the many open questions involving primes.

The development of modern number theory was made possible by the German mathematician Carl Friedrich Gauss, one of the greatest mathematicians in history, who developed the language of *congruences* in the early nineteenth century. We say that two integers a and b are congruent modulo m, where m is a positive integer, if m divides $a - b$. This language makes it easy to work with divisibility relationships in much the same way that we work with equations. Gauss developed many important concepts in number theory; for example, he proved one of its most subtle and beautiful results, the *law of quadratic reciprocity*. This law relates whether a prime p is a perfect square modulo a second prime q to whether q is a perfect square modulo p. Gauss developed many different proofs of this law, some of which have led to whole new areas of number theory.

Distinguishing primes from composite integers is a key problem of number theory. Work in this area has led to the development of an arsenal of *primality tests*. The simplest primality test is simply checking whether a positive integer is divisible by each prime not exceeding its square root. Unfortunately, this test is inefficient for extremely large positive integers. In the nineteenth century, Pierre de Fermat showed that p divides $2^p - 2$ whenever p is prime. Some mathematicians thought that the converse also was true (that is, that if n divides $2^n - 2$, then n must be prime). However, it is not; by the early nineteenth century, composite integers n, such as 341, were known for which n divides $2^n - 2$. Such integers are called *pseudoprimes*. Though pseudoprimes exist, primality tests based on the fact that most composite integers are not pseudoprimes are now used to quickly find extremely large primes.

Factoring a positive integer into primes is another central problem in number theory. The factorization of a positive integer can be found using trial division, but this method is extremely time-consuming. Fermat, Euler, and many other mathematicians devised imaginative factorization algorithms, which have been extended in the past 25 years into a wide array of factoring methods. Using the best-known techniques, we can easily find primes with hundreds of digits; factoring integers with the same number of digits, however, is beyond our most powerful computers.

The dichotomy between the time required to find large primes and the time required to factor large integers is the basis of an extremely important secrecy system, the *RSA cryptosystem*. The RSA system is a public-key cryptosystem, a security system in which each person has a public key and an associated private key. Messages can be encrypted by anyone using another person's public key, but these messages can be decrypted only by the owner of the private key. Concepts from number theory are essential to understanding the basic workings of the RSA cryptosystem, as well as many other parts of modern cryptography. The overwhelming importance of number theory in cryptography contradicts the earlier belief, held by many mathematicians, that number theory was unimportant for real-world applications. It is ironic that some famous mathematicians, such as G. H. Hardy, took pride in the notion that number theory would never be applied in the way that it is today.

The search for integer solutions of equations is another important part of number theory. An equation with the added proviso that only integer solutions are sought is called *diophantine*, after the ancient Greek mathematician Diophantus. Many different types of diophantine equations have been studied, but the most famous is the *Fermat equation*

$x^n + y^n = z^n$. *Fermat's last theorem* states that if n is an integer greater than 2, this equation has no solutions in integers x, y, and z, where $xyz \neq 0$. Fermat conjectured in the seventeenth century that this theorem was true, and mathematicians (and others) searched for proofs for more than three centuries, but it was not until 1995 that the first proof was given by Andrew Wiles.

As Wiles's proof shows, number theory is not a static subject! New discoveries continue steadily to be made, and researchers frequently establish significant theoretical results. The fantastic power available when today's computers are linked over the Internet yields a rapid pace of new computational discoveries in number theory. Everyone can participate in this quest; for instance, you can join the quest for the new *Mersenne primes,* primes of the form $2^p - 1$, where p itself is prime. In June 1999, the first prime with more than 1 million decimal digits was found: the Mersenne prime $2^{6,972,593} - 1$, and a concerted effort is under way to find a prime with more than 10 million digits. After learning about some of the topics covered in this text, you may decide to join the hunt yourself, putting your idle computing resources to good use.

What is elementary number theory? You may wonder why the word "elementary" is part of the title of this book. This book considers only that part of number theory called *elementary number theory,* which is the part not dependent on advanced mathematics, such as the theory of complex variables, abstract algebra, or algebraic geometry. Students who plan to continue the study of mathematics will learn about more advanced areas of number theory, such as analytic number theory (which takes advantage of the theory of complex variables), and algebraic number theory (which uses concepts from abstract algebra to prove interesting results about algebraic number fields).

Some words of advice. As you embark on your study, keep in mind that number theory is a classical subject with results dating back thousands of years, yet is also the most modern of subjects, with new discoveries being made at a rapid pace. It is pure mathematics with the greatest intellectual appeal, yet it is also applied mathematics, with crucial applications to cryptography and other aspects of computer science and electrical engineering. I hope that you find the many facets of number theory as captivating as aficionados who have preceded you, many of whom retained an interest in number theory long after their school days were over.

Experimentation and exploration form an indispensable part of the study of number theory. The results in this book were found by mathematicians who often examined large amounts of numerical evidence, looking for patterns and making conjectures. They worked diligently to prove their conjectures; some of these were proved and became theorems, others were rejected when counterexamples were found, and still others remain unresolved. As you study number theory, I recommend that you examine many examples, look for patterns, and formulate your own conjectures. This will help you to learn the subject—and you may even find some new results of your own!

1 The Integers

Introduction

In the most general sense, number theory deals with the properties of different sets of numbers. In this chapter, we will discuss some particularly important sets of numbers, including the integers, the rational numbers, and the algebraic numbers. We will briefly introduce the notion of approximating real numbers by rational numbers. We will also introduce the concept of a sequence, and particular sequences of integers, including some figurate numbers studied in ancient Greece. A common problem is the identification of a particular integer sequence from its initial terms; we will briefly discuss how to attack such problems.

Using the concept of a sequence, we will define countable sets and show that the set of rational numbers is countable. We will also introduce notations for sums and products, and establish some useful summation formulas.

One of the most important proof techniques in number theory (and in much of mathematics) is mathematical induction. We will discuss the two forms of mathematical induction, illustrate how they can be used to prove various results, and explain why mathematical induction is a valid proof technique.

Continuing, we will introduce the intriguing sequence of Fibonacci numbers, and describe the original problem from which they arose. We will establish some identities and inequalities involving the Fibonacci numbers, using mathematical induction for some of our proofs.

The final section of this chapter deals with a fundamental notion in number theory, that of divisibility. We will establish some of the basic properties of division of integers, including the "division algorithm." We will show how the quotient and remainder of a division of one integer by another can be expressed using values of the greatest integer function (we will describe a few of the many useful properties of this function, as well).

1.1 Numbers and Sequences

In this section, we introduce basic material that will be used throughout the text. In particular, we cover the important sets of numbers studied in number theory, the concept of integer sequences, and summations and products.

Numbers

To begin, we will introduce several different types of numbers. The *integers* are the numbers in the set

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

The integers play center stage in the study of number theory. One property of the positive integers deserves special mention.

The Well-Ordering Property Every nonempty set of positive integers has a least element.

The well-ordering property may seem obvious, but it is the basic principle that allows us to prove many results about sets of integers, as we will see in Section 1.3.

The well-ordering property can be taken as one of the axioms defining the set of positive integers or it may be derived from a set of axioms in which it is not included. (See Appendix A for axioms for the set of integers.) We say that the set of positive integers is *well ordered.* However, the set of all integers is not well ordered, as there are sets of integers without a smallest element, such as the set of negative integers, the set of even integers less than 100, and the set of all integers itself.

Another important class of numbers in the study of number theory is the set of numbers that can be written as a ratio of integers.

Definition. The real number r is *rational* if there are integers p and q, with $q \neq 0$, such that $r = p/q$. If r is not rational, it is said to be *irrational.*

Example 1.1. The numbers $-22/7, 0 = 0/1, 2/17$, and $1111/41$ are rational numbers. ◀

Note that every integer n is a rational number, because $n = n/1$. Examples of irrational numbers are $\sqrt{2}$, π, and e. We can use the well-ordering property of the set of positive integers to show that $\sqrt{2}$ is irrational. The proof that we provide, although quite clever, is not the simplest proof that $\sqrt{2}$ is irrational. You may prefer the proof that we will give in Chapter 4, which depends on concepts developed in that chapter. (The proof that e is irrational is left as Exercise 44. We refer the reader to [HaWr79] for a proof that π is irrational. It is not easy.)

Theorem 1.1. $\sqrt{2}$ is irrational.

Proof. Suppose that $\sqrt{2}$ were rational. Then there would exist positive integers a and b such that $\sqrt{2} = a/b$. Consequently, the set $S = \{k\sqrt{2} \mid k \text{ and } k\sqrt{2} \text{ are positive integers}\}$ is a nonempty set of positive integers (it is nonempty because $a = b\sqrt{2}$ is a member of S). Therefore, by the well-ordering property, S has a smallest element, say $s = t\sqrt{2}$.

We have $s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s - t)\sqrt{2}$. Because $s\sqrt{2} = 2t$ and s are both integers, $s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s - t)\sqrt{2}$ must also be an integer. Furthermore, it is positive, because $s\sqrt{2} - s = s(\sqrt{2} - 1)$ and $\sqrt{2} > 1$. It is less than s, because $s = t\sqrt{2}$, $s\sqrt{2} = 2t$ and $\sqrt{2} < 2$. This contradicts the choice of s as the smallest positive integer in S. It follows that $\sqrt{2}$ is irrational. ∎

The sets of integers, positive integers, rational numbers, and real numbers are traditionally denoted by $\mathbf{Z}$, $\mathbf{Z}^+$, $\mathbf{Q}$, and $\mathbf{R}$, respectively. Also, we write $x \in S$ to indicate that x belongs to the set S. Such notation will be used occasionally in this book.

We briefly mention several other types of numbers here, though we do not return to them until Chapter 12.

Definition. A number α is *algebraic* if it is the root of a polynomial with integer coefficients; that is, α is algebraic if there exist integers $a_0, a_1, \ldots, a_n$ such that $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$. The number α is called *transcendental* if it is not algebraic.

Example 1.2. The irrational number $\sqrt{2}$ is algebraic, because it is a root of the polynomial $x^2 - 2$. ◀

Note that every rational number is algebraic. This follows from the fact that the number a/b, where a and b are integers and $b \neq 0$, is the root of $bx - a$. In Chapter 12, we will give an example of a transcendental number. The numbers e and π are also transcendental, but the proofs of these facts (which can be found in [HaWr79]) are beyond the scope of this book.

The Greatest Integer Function

In number theory a special notation is used for the largest integer that is less than or equal to a particular real number.

Definition. The *greatest integer* in a real number x, denoted by $[x]$, is the largest integer less than or equal to x. That is, $[x]$ is the integer satisfying

$$[x] \leq x < [x] + 1.$$

Example 1.3. We have $[5/2] = 2$, $[-5/2] = -3$, $[\pi] = 3$, $[-2] = -2$, and $[0] = 0$. ◀

Remark. The greatest integer function is also known as the *floor function*. Instead of using the notation $[x]$ for this function, computer scientists usually use the notation $\lfloor x \rfloor$. The *ceiling function* is a related function often used by computer scientists. The ceiling function of a real number x, denoted by $\lceil x \rceil$, is the smallest integer greater than or equal to x. For example, $\lceil 5/2 \rceil = 3$ and $\lceil -5/2 \rceil = -2$.

The greatest integer function arises in many contexts. Besides being important in number theory, as we will see throughout this book, it plays an important role in the analysis of algorithms, a branch of computer science. The following example establishes a useful property of this function. Additional properties of the greatest integer function are found in the exercises at the end of this section and in [GrKnPa94].

Example 1.4. Show that if n is an integer, then $[x+n] = [x] + n$ whenever x is a real number. To show that this property holds, let $[x] = m$, so that m is an integer. This implies that $m \leq x < m+1$. We can add n to this inequality to obtain $m+n \leq x+n < m+n+1$. This shows that $m+n = [x]+n$ is the greatest integer less than or equal to $x+n$. Hence $[x+n] = [x]+n$. ◀

Definition. The *fractional part* of a real number x, denoted by $\{x\}$, is the difference between x and the largest integer less than or equal to x, namely $[x]$. That is, $\{x\} = x - [x]$.

Because $[x] \leq x < [x]+1$, it follows that $0 \leq \{x\} = x - [x] < 1$ for every real number x. The greatest integer in x is also called the *integral part* of x because $x = [x] + \{x\}$.

Example 1.5. We have $\{5/4\} = 5/4 - [5/4] = 5/4 - 1 = 1/4$ and $\{-2/3\} = -2/3 - [-2/3] = -2/3 - (-1) = 1/3$. ◀

Diophantine Approximation

We know that the distance of a real number to the integer closest to it is at most $1/2$. But can we show that one of the first k multiples of a real number must be much closer to an integer? An important part of number theory called *diophantine approximation* studies questions such as this. In particular, it concentrates on questions that involve the approximation of real numbers by rational numbers. (The adjective *diophantine* comes from the Greek mathematician Diophantus, whose biography can be found in Section 13.1.)

Here we will show that among the first n multiples of a real number α, there must be at least one at a distance less than $1/n$ from the integer nearest it. The proof will depend on the famous *pigeonhole principle,* introduced by the German mathematician Dirichlet.[1] Informally, this principle tells us if we have more objects than boxes, when these objects are placed in the boxes, at least two must end up in the same box. Although this seems like a particularly simple idea, it turns out to be extremely useful in number theory and combinatorics. We now state and prove this important fact, which is known as the pigeonhole principle because if you have more pigeons than roosts, two pigeons must end up in the same roost.

[1] Instead of calling Theorem 1.2 the pigeonhole principle, Dirichlet called it the *Schubfachprinzip* in German, which translates to the *drawer principle* in English. A biography of Dirichlet can be found in Section 3.1.

Theorem 1.2. ***The Pigeonhole Principle.*** If $k + 1$ or more objects are placed into k boxes, then at least one box contains two or more of the objects.

Proof. If none of the k boxes contains more than one object, then the total number of objects would be at most k. This contradiction shows that one of the boxes contains at least two or more of the objects. ∎

We now state and prove the approximation theorem, which guarantees that one of the first n multiples of a real number must be within $1/n$ of an integer. The proof we give illustrates the utility of the pigeonhole principle. (See [Ro03] for more applications of the pigeonhole principle.) (Note that in the proof we make use of the *absolute value function*. Recall that $|x|$, the absolute value of x, equals x if $x \geq 0$ and $-x$ if $x < 0$. Also recall that $|x - y|$ gives the distance between x and y.)

Theorem 1.3. ***Dirichlet's Approximation Theorem.*** If α is a real number and n is a positive integer, then there exist integers a and b with $1 \leq a \leq n$ such that $|a\alpha - b| < 1/n$.

Proof. Consider the $n + 1$ numbers $0, \{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$. These $n + 1$ numbers are the fractional parts of the numbers $j\alpha$, $j = 0, 1, \ldots, n$, so that $0 \leq \{j\alpha\} < 1$ for $j = 0, 1, \ldots, n$. Each of these $n + 1$ numbers lies in one of the n disjoint intervals $0 \leq x < 1/n, 1/n \leq x < 2/n, \ldots, (j-1)/n \leq x < j/n, \ldots, (n-1)/n \leq x < 1$. Because there are $n + 1$ numbers under consideration, but only n intervals, the pigeonhole principle tells us that at least two of these numbers lie in the same interval. Because each of these intervals has length $1/n$ and does not include its right endpoint, we know that the distance between two numbers that lie in the same interval is less than $1/n$. It follows that there exist integers j and k with $0 \leq j < k \leq n$ such that $|\{k\alpha\} - \{j\alpha\}| < 1/n$. Now let $a = k - j$ and $b = [k\alpha] - [j\alpha]$. Because $0 \leq j < k \leq n$, we see that $1 \leq a \leq n$. Moreover,

$$\begin{aligned} |a\alpha - b| &= |(k-j)\alpha - ([k\alpha] - [j\alpha])| \\ &= |(k\alpha - [k\alpha]) - (j\alpha - [j\alpha])| \\ &= |\{k\alpha\} - \{j\alpha\}| < 1/n. \end{aligned}$$

Consequently, we have found integers a and b with $1 \leq a \leq n$ and $|a\alpha - b| < 1/n$, as desired. ∎

Example 1.6. Suppose that $\alpha = \sqrt{2}$ and $n = 6$. We find that $1 \cdot \sqrt{2} \approx 1.414$, $2 \cdot \sqrt{2} \approx 2.828$, $3 \cdot \sqrt{2} \approx 4.243$, $4 \cdot \sqrt{2} \approx 5.657$, $5 \cdot \sqrt{2} \approx 7.071$, and $6 \cdot \sqrt{2} \approx 8.485$. Among these numbers $5 \cdot \sqrt{2}$ has the smallest fractional part. We see that $|5 \cdot \sqrt{2} - 7| \approx |7.071 - 7| = 0.071 \leq 1/6$. It follows that when $\alpha = \sqrt{2}$ and $n = 6$, we can take $a = 5$ and $b = 7$ to make $|a\alpha - b| < 1/n$. ◀

Our proof of Theorem 1.3 follows Dirichlet's original 1834 proof. Proving a stronger version of Theorem 1.3 with $1/(n + 1)$ replacing $1/n$ in the approximation is not difficult (see Exercise 32). Furthermore, in Exercise 34 we show how to use the Dirichlet approximation theorem to show that, given an irrational number α, there are infinitely many different rational numbers p/q such that $|\alpha - p/q| < 1/q^2$, and important result in the theory of diophantine approximation. We will return to this topic in Chapter 12.

Sequences

A *sequence* $\{a_n\}$ is a list of numbers $a_1, a_2, a_3, \ldots$. The terms of a sequence can be put into a one-to-one correspondence with the set of positive integers using the mapping $f(i) = a_i$. (Recall that a *one-to-one correspondence,* also called a *bijection,* is a function that is both one-to-one and onto.) We will consider many particular integer sequences in our study of number theory. We introduce several useful sequences in the following examples.

Example 1.7. The sequence $\{a_n\}$, where $a_n = n^2$, begins with the terms 1, 4, 9, 16, 25, 36, 49, 64, ... This is the sequence of the squares of integers. The sequence $\{b_n\}$, where $b_n = 2^n$, begins with the terms 2, 4, 8, 16, 32, 64, 128, 256, ... This is the sequence of powers of 2. The sequence $\{c_n\}$, where $c_n = 0$ if n is odd and $c_n = 1$ if n is even, begins with the terms 0, 1, 0, 1, 0, 1, 0, 1, ... ◀

There are many sequences in which each successive term is obtained from the previous term by multiplying by a common factor. For example, each term in the sequence of powers of 2 is 2 times the previous term. This leads to the following definition.

Definition. A *geometric progression* is a sequence of the form a, ar, ar^2, $ar^3, \ldots$, $ar^k, \ldots$, where a, the *initial term,* and r, the *common ratio,* are real numbers.

Example 1.8. The sequence $\{a_n\}$, where $a_n = 3 \cdot 5^n$, $n = 0, 1, 2, \ldots$, is a geometric sequence with initial term 3 and common ratio 5. (Note that we have started the sequence with the term a_0. We can start the index of the terms of a sequence with 0 or any other integer that we choose.) ◀

A common problem in number theory is finding a formula or rule for constructing the terms of a sequence, even when only a few terms are known (such as trying to find a formula for the nth triangular number $1 + 2 + 3 + \cdots + n$). Even though the initial terms of a sequence do not determine the sequence, knowing the first few terms can lead to a conjecture for a formula or rule for the terms. Consider the following examples.

Example 1.9. Conjecture a formula for a_n, where the first eight terms of $\{a_n\}$ are 4, 11, 18, 25, 32, 39, 46, 53. We note that each term, starting with the second, is obtained by adding 7 to the previous term. Consequently, the nth term could be the initial term plus $7(n - 1)$. A reasonable conjecture is that $a_n = 4 + 7(n - 1) = 7n - 3$. ◀

The sequence proposed in Example 1.9 is an *arithmetic progression,* that is, a sequence of the form $a, a + d, a + 2d, \ldots, a + nd, \ldots$. The particular sequence in Example 1.9 has $a = 4$ and $d = 7$.

Example 1.10. Conjecture a formula for a_n, where the first eight terms of the sequence $\{a_n\}$ are 5, 11, 29, 83, 245, 731, 2189, 6563. We note that each term is approximately 3 times the previous term, suggesting a formula for a_n in terms of 3^n. The integers 3^n for

$n = 1, 2, 3, \ldots$ are $3, 9, 27, 81, 243, 729, 2187, 6561$. Looking at these two sequences together, we find that the formula $a_n = 3^n + 2$ produces these terms. ◀

Example 1.11. Conjecture a formula for a_n, where the first ten terms of the sequence $\{a_n\}$ are $1, 1, 2, 3, 5, 8, 13, 21, 34, 55$. After examining this sequence from different perspectives, we notice that each term of this sequence, after the first two terms, is the sum of the two preceding terms. That is, we see that $a_n = a_{n-1} + a_{n-2}$ for $3 \leq n \leq 10$. This is an example of a recursive definition of a sequence, discussed in Section 1.3. The terms listed in this example are the initial terms of the Fibonacci sequence, which is discussed in Section 1.4. ◀

Integer sequences arise in many contexts in number theory. Among the sequences we will study are the Fibonacci numbers, the prime numbers (covered in Chapter 3), and the perfect numbers (introduced in Section 7.3). Integer sequences appear in an amazing range of subjects besides number theory. A fantastically diverse collection of more than 8000 integer sequences has been amassed by Neil Sloane, who created *The Encyclopedia of Integer Sequences* ([SlPl95]) with Simon Plouffe. An extended version of this list, and a program for finding sequences that match initial terms provided as input, can be found on the Web. You may find this a valuable resource as you continue your study of number theory (as well as other subjects).

We now define what it means for a set to be countable, and show that a set is countable if and only if its elements can be listed as the terms of a sequence.

Definition. A set is *countable* if it is finite or it is infinite and there exists a one-to-one correspondence between the set of positive integers and the set. A set that is not countable is called *uncountable*.

An infinite set is countable if and only if its elements can be listed as the terms of a sequence indexed by the set of positive integers. To see this, simply note that a one-to-one correspondence f from the set of positive integers to a set S is exactly the same as a listing of the elements of the set in a sequence $a_1, a_2, \ldots, a_n, \ldots$, where $a_i = f(i)$.

Example 1.12. The set of integers is countable, because the integers can be listed starting with 0, followed by 1 and -1, followed by 2 and -2, and so on. This produces the sequence $0, 1, -1, 2, -2, 3, -3, \ldots$, where $a_1 = 0$, $a_{2n} = n$, and $a_{2n+1} = -n$ for $n = 1, 2, \ldots$. ◀

Is the set of rational numbers countable? At first glance, it may seem unlikely that there would be a one-to-one correspondence between the set of positive integers and the set of all rational numbers. However, there is such a correspondence, as the following theorem shows.

Theorem 1.4. The set of rational numbers is countable.

Proof. We can list the rational numbers as the terms of a sequence, as follows. First, we arrange all the rational numbers in a two-dimensional array, as shown in Figure 1.1. We

put all fractions with a denominator of 1 in the first row. We arrange these by placing the fraction with a particular numerator in the position this numerator occupies in the list of all integers given in Example 1.12. Next, we list all fractions on successive diagonals, following the order shown in Figure 1.1. Finally, we delete from the list all fractions that represent rational numbers that have already been listed. (For example, we do not list 2/2, because we have already listed 1/1.)

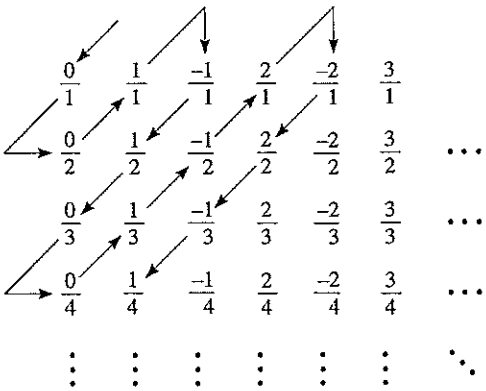


Figure 1.1 *Listing the rational numbers.*

The initial terms of the sequence are $0/1 = 0$, $1/1 = 1$, $-1/1 = -1$, $1/2$, $1/3$, $-1/2$, $2/1 = 2$, $-2/1 = -2$, $-1/3$, $1/4$, and so on.) We leave it to the reader to fill in the details, to see that this procedure lists all rational numbers as the terms of a sequence. ∎

1.1 Exercises

1. Determine whether each of the following sets is well ordered. Either give a proof using the well-ordering property of the set of positive integers, or give an example of a subset of the set that has no smallest element.
   a) the set of integers greater than 3
   b) the set of even positive integers
   c) the set of positive rational numbers
   d) the set of positive rational numbers that can be written in the form $a/2$, where a is a positive integer
   e) the set of nonnegative rational numbers

☞ 2. Show that if a and b are positive integers, then there is a smallest positive integer of the form $a - bk$, $k \in \mathbf{Z}$.

3. Prove that both the sum and the product of two rational numbers are rational.

4. Prove or disprove each of the following statements.
   a) The sum of a rational and an irrational number is irrational.
   b) The sum of two irrational numbers is irrational.
   c) The product of a rational number and an irrational number is irrational.
   d) The product of two irrational numbers is irrational.

* **5.** Use the well-ordering property to show that $\sqrt{3}$ is irrational.

6. Show that every nonempty set of negative integers has a greatest element.

7. Find the following values of the greatest integer function.

a) $[1/4]$ d) $[-2]$
b) $[-3/4]$ e) $[[1/2]+[1/2]]$
c) $[22/7]$ f) $[-3+[-1/2]]$

8. Find the following values of the greatest integer function.

a) $[-1/4]$ d) $[[1/2]]$
b) $[-22/7]$ e) $[[3/2]+[-3/2]]$
c) $[5/4]$ f) $[3-[1/2]]$

9. Find the fractional part of each of the following numbers.

a) 8/5 c) $-11/4$
b) 1/7 d) 7

10. Find the fractional part of each of the following numbers.

a) $-8/5$ c) -1
b) 22/7 d) $-1/3$

11. What is the value of $[x]+[-x]$ where x is a real number?

12. Show that $[x]+[x+1/2]=[2x]$ whenever x is a real number.

13. Show that $[x+y]\geq[x]+[y]$ for all real numbers x and y.

14. Show that $[2x]+[2y]\geq[x]+[y]+[x+y]$ whenever x and y are real numbers.

15. Show that if x and y are positive real numbers, then $[xy]\geq[x][y]$. What is the situation when both x and y are negative? When one of x and y is negative and the other positive?

16. Show that $-[-x]$ is the least integer greater than or equal to x when x is a real number.

17. Show that $[x+1/2]$ is the integer nearest to x (when there are two integers equidistant from x, it is the larger of the two).

18. Show that if m and n are integers, then $[(x+n)/m]=[([x]+n)/m]$ whenever x is a real number.

* **19.** Show that $\left[\sqrt{[x]}\right]=\left[\sqrt{x}\right]$ whenever x is a nonnegative real number.

* **20.** Show that if m is a positive integer, then

$$[mx]=[x]+[x+(1/m)]+[x+(2/m)]+\cdots+[x+(m-1)/m]$$

whenever x is a real number.

21. Conjecture a formula for the nth term of $\{a_n\}$, if the first ten terms of this sequence are as follows.

a) 3, 11, 19, 27, 35, 43, 51, 59, 67, 75
b) 5, 7, 11, 19, 35, 67, 131, 259, 515, 1027
c) 1, 0, 0, 1, 0, 0, 0, 0, 1, 0
d) 1, 3, 4, 7, 11, 18, 29, 47, 76, 123

22. Conjecture a formula for the nth term of $\{a_n\}$, if the first ten terms of this sequence are as follows.

a) 2, 6, 18, 54, 162, 486, 1458, 4374, 13122, 39366

b) 1, 1, 0, 1, 1, 0, 1, 1, 0, 1

c) 1, 2, 3, 5, 7, 10, 13, 17, 21, 26

d) 3, 5, 11, 21, 43, 85, 171, 341, 683, 1365

23. Find three different formulas or rules for the terms of a sequence $\{a_n\}$, if the first three terms of this sequence are 1, 2, 4.

24. Find three different formulas or rules for the terms of a sequence $\{a_n\}$, if the first three terms of this sequence are 2, 3, 6.

25. Show that the set of all integers greater than -100 is countable.

26. Show that the set of all rational numbers of the form $n/5$, where n is an integer, is countable.

27. Show that the set of all numbers of the form $a + b\sqrt{2}$, where a and b are integers, is countable.

* **28.** Show that the union of two countable sets is countable.

* **29.** Show that the union of a countable number of countable sets is countable.

30. Using a computational aid, if needed, find integers a and b such that $1 \leq a \leq 8$ and $|a\alpha - b| < 1/8$, where α is

a) $\sqrt{2}$. c) π.

b) $\sqrt[3]{2}$. d) e.

31. Using a computational aid, if needed, find integers a and b such that $1 \leq a \leq 10$ and $|a\alpha - b| < 1/10$, where α is

a) $\sqrt{3}$. c) π^2.

b) $\sqrt[3]{3}$. d) e^3.

32. Prove the following stronger version of Dirichlet's approximation. If α is a real number and n is a positive integer, there are integers a and b such that $1 \leq a \leq n$ and $|a\alpha - b| \leq 1/(n+1)$. (*Hint:* Consider the $n+2$ numbers $0, \ldots, \{j\alpha\}, \ldots, 1$ and the $n+1$ intervals $(k-1)/(n+1) \leq x < k/(n+1)$ for $k = 1, \ldots, n+1$.)

33. Show that if α is a real number and n is a positive integer, then there is an integer k such that $|\alpha - u/k| \leq 1/2k$.

34. Use Dirichlet's approximation theorem to show that if α is an irrational number, then there are infinitely many positive integers q for which there is an integer p such that $|\alpha - p/q| \leq 1/q^2$.

35. Find four rational numbers p/q with $|\sqrt{2} - p/q| \leq 1/q^2$.

36. Find five rational numbers p/q with $|\sqrt[3]{5} - p/q| \leq 1/q^2$.

37. Show that if $\alpha = a/b$ is a rational number, then there are only finitely many rational numbers p/q such that $|p/q - a/b| < 1/q^2$.

The *spectrum sequence* of a real number α is the sequence that has $[n\alpha]$ as its nth term.

38. Find the first ten terms of the spectrum sequence of each of the following numbers.

a) 2 c) $2+\sqrt{2}$ e) $(1+\sqrt{5})/2$
b) $\sqrt{2}$ d) e

39. Find the first ten terms of the spectrum sequence of each of the following numbers.

a) 3 c) $(3+\sqrt{3})/2$
b) $\sqrt{3}$ d) π

40. Prove that if $\alpha \neq \beta$, then the spectrum sequence of α is different from the spectrum sequence of β.

** **41.** Show that every positive integer occurs exactly once in the spectrum sequence of α or in the spectrum sequence of β if and only if α and β are positive irrational numbers such that $1/\alpha + 1/\beta = 1$.

The *Ulam numbers* $u_n, n = 1, 2, 3, \ldots$ are defined as follows. We specify that $u_1 = 1$ and $u_2 = 2$. For each successive integer m, $m > 2$, this integer is an Ulam number if and only if it can be written uniquely as the sum of two distinct Ulam numbers. These numbers are named for *Stanislaw Ulam,* who first described them in 1964.

STANISLAW M. ULAM (1909–1984) was born in Lvov, Poland. He became interested in astronomy and physics at age 12, after receiving a telescope from his uncle. He decided to learn the mathematics required to understand relativity theory, and at the age of 14 he used textbooks to learn calculus and other mathematics.

Ulam received his Ph.D. from the Polytechnic Institute in Lvov in 1933, completing his degree under the mathematician Banach, in the area of real analysis. In 1935, he was invited to spend several months at the Institute for Advanced Study; in 1936, he joined Harvard University as a member of the Society of Fellows, remaining in this position until 1940. During these years he returned each summer to Poland where he spent time in cafes, such as the Scottish Cafe, intensely doing mathematics with his fellow Polish mathematians.

Luckily for Ulam, he left Poland in 1939, just one month before the outbreak of World War II. In 1940, he was appointed to a position as an assistant professor at the University of Wisconsin, and in 1943, he was enlisted to work in Los Alamos on the development of the first atomic bomb, as part of the Manhattan Project. Ulam made several key contributions that led to the creation of thermonuclear bombs. At Los Alamos, Ulam also developed the Monte Carlo method, which uses a sampling technique with random numbers to find solutions of mathematical problems.

Ulam remained at Los Alamos after the war until 1965. He served on the faculties of the University of Southern California, the University of Colorado, and the University of Florida. Ulam had a fabulous memory and was an extremely verbal person. His mind was a repository of stories, jokes, puzzles, quotations, formulas, problems, and many other types of information. He wrote several books, including *Sets, Numbers, and Universes* and *Adventures of a Mathematician.* He was interested in and contributed to many areas of mathematics, including number theory, real analysis, probability theory, and mathematical biology.

42. Find the first ten Ulam numbers.

* 43. Show that there are infinitely many Ulam numbers.

* 44. Prove that e is irrational. (*Hint:* Use the fact that $e = 1 + 1/1! + 1/2! + 1/3! + \cdots$.)

1.1 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 10 rational numbers p/q such that $|\pi - p/q| \leq 1/q^2$.
2. Find 20 rational numbers p/q such that $|e - p/q| \leq 1/q^2$.
3. Find as many terms as you can of the spectrum sequence of $\sqrt{2}$. (See the preamble to Exercise 38 for the definition of spectrum.)
4. Find as many terms as you can of the spectrum sequence of π. (See the preamble to Exercise 38 for the definition of spectrum.)
5. Find the first 1000 Ulam numbers.
6. How many pairs of consecutive integers can you find, where both are Ulam numbers?
7. Can the sum of any two consecutive Ulam numbers, other than 1 and 2, be another Ulam number? If so, how many examples can you find?
8. How large are the gaps between consecutive Ulam numbers? Do you think that these gaps can be arbitrarily long?
9. What conjectures can you make about the number of Ulam numbers less than an integer n? Do your computations support these conjectures?

Programming Projects

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

1. Given a number α, find rational numbers p/q such that $|\alpha - p/q| \leq 1/q^2$.
2. Given a number α, find its spectrum sequence.
3. Find the first n Ulam numbers, where n is a positive integer.

1.2 Sums and Products

Because summations and products arise so often in the study of number theory, we now introduce notation for summations and products. The following notation represents the sum of the numbers $a_1, a_2, \ldots, a_n$:

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n.$$

The letter k, the *index of summation,* is a "dummy variable" and can be replaced by any letter. For instance,

$$\sum_{k=1}^{n} a_k = \sum_{j=1}^{n} a_j = \sum_{i=1}^{n} a_i, \text{ and so forth.}$$

Example 1.13. We see that $\sum_{j=1}^{5} j = 1+2+3+4+5 = 15$, $\sum_{j=1}^{5} 2 = 2+2+2+2+2 = 10$, and $\sum_{j=1}^{5} 2^j = 2+2^2+2^3+2^4+2^5 = 62$.

We also note that, in summation notation, the index of summation may range between any two integers, as long as the lower limit does not exceed the upper limit. If m and n are integers such that $m \le n$, then $\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \cdots + a_n$. For instance, we have $\sum_{k=3}^{5} k^2 = 3^2 + 4^2 + 5^2 = 50$, $\sum_{k=0}^{2} 3^k = 3^0 + 3^1 + 3^2 = 13$, and $\sum_{k=-2}^{1} k^3 = (-2)^3 + (-1)^3 + 0^3 + 1^3 = -8$. ◀

We will often need to consider sums in which the index of summation ranges over all those integers that possess a particular property. We can use summation notation to specify the particular property or properties the index must have for a term with that index to be included in the sum. This use of notation is illustrated in the following example.

Example 1.14. We see that

$$\sum_{\substack{j \le 10 \\ j \in \{n^2 \mid n \in \mathbf{Z}\}}} 1/(j+1) = 1/1 + 1/2 + 1/5 + 1/10 = 9/5,$$

because the terms in the sum are all those for which j is an integer not exceeding 10 that is a perfect square. ◀

The following three properties for summations are often useful. We leave their proofs to the reader.

$$\sum_{j=m}^{n} k a_j = k \sum_{j=m}^{n} a_j \tag{1.1}$$

$$\sum_{j=m}^{n} (a_j + b_j) = \sum_{j=m}^{n} a_j + \sum_{j=m}^{n} b_j \tag{1.2}$$

$$\sum_{i=m}^{n} \sum_{j=p}^{q} a_i b_j = \left(\sum_{i=m}^{n} a_i \right) \left(\sum_{j=p}^{q} b_j \right) = \sum_{j=p}^{q} \sum_{i=m}^{n} a_i b_j \tag{1.3}$$

Next, we develop several useful summation formulas. We often need to evaluate sums of consecutive terms of a geometric series. The following example shows how a formula for such sums can be derived.

Example 1.15. To evaluate

$$S = \sum_{j=0}^{n} ar^j,$$

the sum of the first $n+1$ terms of the geometric series $a, ar, \ldots, ar^k, \ldots$, we multiply both sides by r and manipulate the resulting sum to find:

$$\begin{aligned} rS &= r \sum_{j=0}^{n} ar^j \\ &= \sum_{j=0}^{n} ar^{j+1} \\ &= \sum_{k=1}^{n+1} ar^k && \textit{(shifting the index of summation)} \\ &= \sum_{k=0}^{n} ar^k + (ar^{n+1} - a) && \textit{(removing the term with } k = n+1 \\ & && \textit{from the set and adding the term with } k = 0) \\ &= S + (ar^{n+1} - a). \end{aligned}$$

It follows that

$$rS - S = (ar^{n+1} - a).$$

Solving for S shows that when $r \neq 1$,

$$S = \frac{ar^{n+1} - a}{r - 1}.$$

Note that when $r = 1$, we have $\sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} a = (n+1)a$. ◀

Example 1.16. Taking $a = 3$, $r = -5$, and $n = 6$ in the formula found in Example 1.15, we see that $\sum_{i=0}^{6} 3(-5)^j = \frac{3(-5)^7 - 3}{-5-1} = 39{,}063$. ◀

The following example shows that the sum of the first n consecutive powers of 2 is one less than the next power of 2.

Example 1.17. Let n be a positive integer. To find the sum

$$\sum_{k=0}^{n} 2^k = 1 + 2 + 2^2 + \cdots + 2^n,$$

we use Example 1.15, with $a = 1$ and $r = 2$, to obtain

$$1 + 2 + 2^2 + \cdots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$ ◀

A summation of the form $\sum_{j=1}^{n}(a_j - a_{j-1})$, where $a_0, a_1, a_2, \ldots, a_n$ is a sequence of numbers, is said to be *telescoping*. Telescoping sums are easily evaluated because

$$\begin{aligned}\sum_{j=1}^{n} a_j - a_{j-1} &= (a_1 - a_0) + (a_2 - a_1) + \cdots + (a_n - a_{n-1}) \\ &= a_n - a_0.\end{aligned}$$

The ancient Greeks were interested in sequences of numbers that can be represented by regular arrangements of equally spaced points. The following example illustrates one such sequence of numbers.

Example 1.18. The *triangular numbers* $t_1, t_2, t_3, \ldots, t_k, \ldots$ is the sequence where t_k is the number of dots in the triangular array of k rows with j dots in the jth row. ◀

Figure 1.2 illustrates that t_k counts the dots in successively larger regular triangles for $k = 1, 2, 3, 4$, and 5.

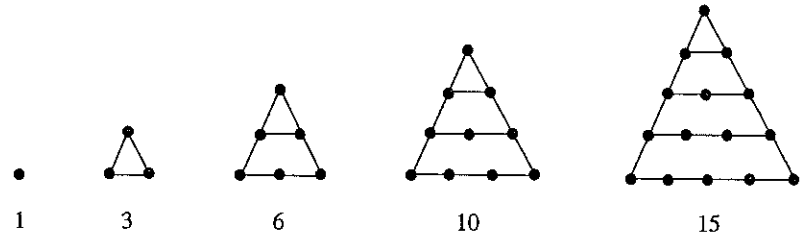


Figure 1.2 *The Triangular Numbers.*

Next, we will determine an explicit formula for the kth triangular number t_k.

Example 1.19. How can we find a formula for the nth triangular number? One approach is to use the identity $(k+1)^2 - k^2 = 2k + 1$. When we isolate the factor k, we find that $k = ((k+1)^2 - k^2)/2 - 1/2$. When we sum this expression for k over the values $k = 1, 2, \ldots, n$, we obtain

$$\begin{aligned}t_n &= \sum_{k=1}^{n} k \\ &= \left(\sum_{k=1}^{n}((k+1)^2 - k^2)/2\right) - \sum_{k=1}^{n} 1/2 \quad \textit{(replacing } k \textit{ with } ((k+1)^2 - k^2)/2) \\ &= ((n+1)^2/2 - 1/2) - n/2 \quad \textit{(simplifying a telescoping sum)} \\ &= (n^2 + 2n)/2 - n/2 \\ &= (n^2 + n)/2 \\ &= n(n+1)/2.\end{aligned}$$

The second equality here follows by the formula for the sum of a telescoping series with $a_k = (k+1)^2 - k^2$. We conclude that the nth triangular number $t_n = n(n+1)/2$. (See Exercise 7 for another way to find t_n.) ◀

We also define a notation for products, analogous to that for summations. The product of the numbers $a_1, a_2, \ldots, a_n$ is denoted by

$$\prod_{j=1}^{n} a_j = a_1 a_2 \cdots a_n.$$

The letter j above is a "dummy variable," and can be replaced arbitrarily.

Example 1.20. To illustrate the notation for products, we have

$$\prod_{j=1}^{5} j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120,$$

$$\prod_{j=1}^{5} 2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32, \text{ and}$$

$$\prod_{j=1}^{5} 2^j = 2 \cdot 2^2 \cdot 2^3 \cdot 2^4 \cdot 2^5 = 2^{15}.$$

◀

The *factorial function* arises throughout number theory.

Definition. Let n be a positive integer. Then $n!$ (read as "n factorial") is the product of the integers $1, 2, \ldots, n$. We also specify that $0! = 1$. In terms of product notation, we have $n! = \prod_{j=1}^{n} j$.

Example 1.21. We have $1! = 1$, $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$, and $12! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 = 479,001,600$. ◀

1.2 Exercises

1. Find each of the following sums.

   a) $\sum_{j=1}^{5} j^2$ b) $\sum_{j=1}^{5} (-3)$ c) $\sum_{j=1}^{5} 1/(j+1)$

2. Find each of the following sums.

   a) $\sum_{j=0}^{4} 3$ b) $\sum_{j=0}^{4} (j-3)$ c) $\sum_{j=0}^{4} (j+1)/(j+2)$

3. Find each of the following sums.

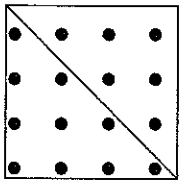
   a) $\sum_{j=1}^{8} 2^j$ b) $\sum_{j=1}^{8} 5(-3)^j$ c) $\sum_{j=1}^{8} 3(-1/2)^j$

4. Find each of the following sums.

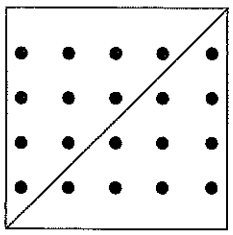
   a) $\sum_{j=0}^{10} 8 \cdot 3^j$ b) $\sum_{j=0}^{10} (-2)^{j+1}$ c) $\sum_{j=0}^{10} (1/3)^j$

* **5.** Find and prove a formula for $\sum_{k=1}^{n}[\sqrt{k}]$ in terms of n and $[\sqrt{n}]$.

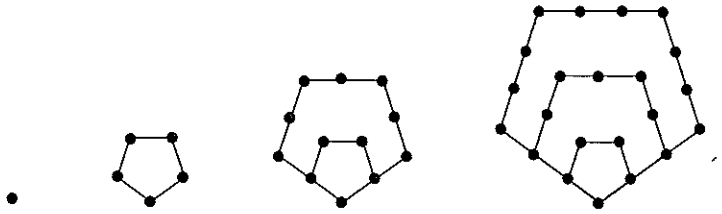
6. By putting together two triangular arrays, one with n rows and one with $n-1$ rows, to form a square (as illustrated for $n=4$), show that $t_{n-1}+t_n=n^2$, where t_n is the nth triangular number.



7. By putting together two triangular arrays, each with n rows, to form a rectangular array of dots of size n by $n+1$ (as illustrated for $n=4$), show that $2t_n=n(n+1)$. From this, conclude that $t_n=n(n+1)/2$.



The *pentagonal numbers* $p_1, p_2, p_3, \ldots, p_k, \ldots$, are the integers that count the number of dots in k nested pentagons, as shown in the following figure.



8. Show that $p_1=1$ and $p_k=p_{k-1}+(3k-2)$ for $k\geq 2$. Conclude that $p_n=\sum_{k=1}^{n}(3k-2)$.

9. Prove that the sum of the $(n-1)$st triangular number and the nth square number is the nth pentagonal number.

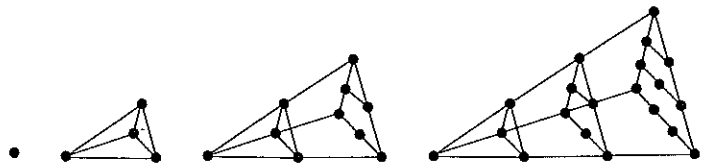
10. a) Define the hexagonal numbers in a manner analogous to the definitions of triangular, square, and pentagonal numbers. (Recall that a hexagon is a six-sided polygon.)

b) Find a closed formula for hexagonal numbers.

11. a) Define the heptagonal numbers in a manner analogous to the definitions of triangular, square, and pentagonal numbers. (Recall that a heptagon is a seven-sided polygon.)

b) Find a closed formula for heptagonal numbers.

The *tetrahedral numbers* $T_1, T_2, T_3, \ldots, T_k, \ldots$, are the integers that count the number of dots on the faces of k nested tetrahedra, as shown in the following figure.



12. Show that the nth tetrahedral number is the sum of the first n triangular numbers.

13. Find and prove a closed formula for the nth tetrahedral number.

14. Find $n!$ for n equal to each of the first ten positive integers.

15. List the integers $100!$, 100^{100}, 2^{100}, and $(50!)^2$ in order of increasing size. Justify your answer.

16. Express each of the following products in terms of $\prod_{i=1}^{n} a_i$, where k is a constant.

a) $\prod_{i=1}^{n} ka_i$ b) $\prod_{i=1}^{n} ia_i$ c) $\prod_{i=1}^{n} a_i^k$

17. Use the identity $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ to evaluate $\sum_{k=1}^{n} \frac{1}{k(k+1)}$.

18. Use the identity $\frac{1}{k^2-1} = \frac{1}{2}\left(\frac{1}{k-1} - \frac{1}{k+1}\right)$ to evaluate $\sum_{k=2}^{n} \frac{1}{k^2-1}$.

19. Find a formula for $\sum_{k=1}^{n} k^2$ using a technique analogous to that in Example 1.19 and the formula found there.

20. Find a formula for $\sum_{k=1}^{n} k^3$ using a technique analogous to that in Example 1.19, and the results of that example and Exercise 19.

21. Without multiplying all the terms, show that

a) $10! = 6!\,7!$. c) $16! = 14!\,5!\,2!$.
b) $10! = 7!\,5!\,3!$. d) $9! = 7!\,3!\,3!\,2!$.

22. Let $a_1, a_2, \ldots, a_n$ be positive integers. Let $b = (a_1!\ a_2! \ldots a_n!) - 1$, and $c = a_1!\,a_2! \ldots a_n!$. Show that $c! = a_1!\,a_2! \cdots a_n!b!$.

23. Find all positive integers x, y, and z such that $x! + y! = z!$.

24. Find the values of the following products.

a) $\prod_{j=2}^{n}(1 - 1/j)$ b) $\prod_{j=2}^{n}(1 - 1/j^2)$

1.2 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. What are the largest values of n for which $n!$ has fewer than 100 decimal digits, fewer than 1000 decimal digits, and fewer than 10,000 decimal digits?

Programming Projects

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

1. Given the terms of a sequence $a_1, a_2, \ldots, a_n$, compute $\sum_{j=1}^{n} a_j$ and $\prod_{j=1}^{n} a_j$.
2. Given the terms of a geometric progression, find the sum of its terms.

1.3 Mathematical Induction

By examining the sums of the first n odd positive integers for small values of n, we can conjecture a formula for this sum. We have

$$\begin{aligned} 1 &= 1, \\ 1+3 &= 4, \\ 1+3+5 &= 9, \\ 1+3+5+7 &= 16, \\ 1+3+5+7+9 &= 25, \\ 1+3+5+7+9+11 &= 36. \end{aligned}$$

From these values, we conjecture that $\sum_{j=1}^{n}(2j-1) = 1+3+5+7+\cdots+2n-1 = n^2$ for every positive integer n.

How can we prove that this formula holds for all positive integers n?

The *principle of mathematical induction* is a valuable tool for proving results about the integers—such as the formula just conjectured for the sum of the first n odd positive integers. First, we will state this principle, and then we will show how it is used. Subsequently, we will use the well-ordering principle to show that mathematical induction is a valid proof technique. We will use the principle of mathematical induction, and the well-ordering property, many times in our study of number theory.

We must accomplish two things to prove by mathematical induction that a particular statement holds for every positive integer. Letting S be the set of positive integers for which we claim the statement to be true, we must show that 1 belongs to S; that is, that the statement is true for the integer 1. This is called the *basis step*.

Second, we must show, for each positive integer n, that $n+1$ belongs to S if n does; that is, that the statement is true for $n+1$ if it is true for n. This is called the *inductive step*. Once these two steps are completed, we can conclude by the principle of mathematical induction that the statement is true for all positive integers.

Theorem 1.5. ***The Principle of Mathematical Induction.*** A set of positive integers that contains the integer 1, and that has the property that, if it contains the integer k, then it also contains $k+1$, must be the set of all positive integers.

We illustrate the use of mathematical induction by several examples; first, we prove the conjecture made at the start of this section.

Example 1.22. We will use mathematical induction to show that

$$\sum_{j=1}^{n}(2j-1) = 1+3+\cdots+(2n-1) = n^2$$

for every positive integer n. (By the way, if our conjecture for the value of this sum was incorrect, mathematical induction would fail to produce a proof!)

We begin with the basis step, which follows because

$$\sum_{j=1}^{1}(2j-1) = 2\cdot 1 - 1 = 1 = 1^2.$$

For the inductive step, we assume the inductive hypothesis that the formula holds for n; that is, we assume that $\sum_{j=1}^{n}(2j-1) = n^2$. Using the inductive hypothesis, we have

$$\begin{aligned}
\sum_{j=1}^{n+1}(2j-1) &= \sum_{j=1}^{n}(2j-1) + (2(n+1)-1) && \textit{(splitting off the term with } j = n+1\textit{)}\\
&= n^2 + 2(n+1) - 1 && \textit{(using the inductive hypothesis)}\\
&= n^2 + 2n + 1\\
&= (n+1)^2.
\end{aligned}$$

Because both the basis and the inductive steps have been completed, we know that the result holds. ◀

Next, we prove an inequality via mathematical induction.

Example 1.23. We can show by mathematical induction that $n! \leq n^n$ for every positive integer n. The basis step, namely the case where $n = 1$, holds since $1! = 1 \leq 1^1 = 1$. Now, assume that $n! \leq n^n$; this is the inductive hypothesis. To complete the proof, we must show, under the assumption that the inductive hypothesis is true, that

The Origin of Mathematical Induction

The first known use of mathematical induction appears in the work of the sixteenth-century mathematician Francesco Maurolico (1494–1575). In his book *Arithmeticorum Libri Duo*, Maurolico presented various properties of the integers, together with proofs. He devised the method of mathematical induction so that he could complete some of the proofs. The first use of mathematical induction in his book was in the proof that the sum of the first n odd positive integers equals n^2.

$(n+1)! \leq (n+1)^{n+1}$. Using the inductive hypothesis, we have

$$\begin{aligned}(n+1)! &= (n+1) \cdot n! \\ &\leq (n+1)n^n \\ &< (n+1)(n+1)^n \\ &\leq (n+1)^{n+1}.\end{aligned}$$

This completes both the inductive step and the proof. ◀

We now show that the principle of mathematical induction follows from the well-ordering principle.

Proof. Let S be a set of positive integers containing the integer 1, and the integer $n+1$ whenever it contains n. Assume (for the sake of contradiction) that S is not the set of all positive integers. Therefore, there are some positive integers not contained in S. By the well-ordering property, because the set of positive integers not contained in S is nonempty, there is a least positive integer n that is not in S. Note that $n \neq 1$, since 1 is in S.

Now, because $n > 1$ (as there is no positive integer n with $n < 1$), the integer $n-1$ is a positive integer smaller than n, and hence must be in S. But because S contains $n-1$, it must also contain $(n-1)+1 = n$, which is a contradiction, as n is supposedly the smallest positive integer not in S. This shows that S must be the set of all positive integers. ■

A slight variant of the principle of mathematical induction is also sometimes useful in proofs.

Theorem 1.6. ***The Second Principle of Mathematical Induction.*** A set of positive integers that contains the integer 1, and that has the property that, for every positive integer n, if it contains all the positive integers $1, 2, \ldots, n$, then it also contains the integer $n+1$, must be the set of all positive integers.

The second principle of mathematical induction is sometimes called *strong induction* to distinguish it from the principle of mathematical induction, which is also called *weak induction*.

Before proving that the second principle of mathematical induction is valid, we will give an example to illustrate its use.

Example 1.24. We will show that any amount of postage more than one cent can be formed using just two-cent and three-cent stamps. For the basis step, note that postage of two cents can be formed using one two-cent stamp and postage of three cents can be formed using one three-cent stamp.

For the inductive step, assume that every amount of postage not exceeding n cents, $n \geq 3$, can be formed using two-cent and three-cent stamps. Then a postage amount of $n+1$ cents can be formed by taking stamps of $n-1$ cents together with a two-cent stamp. This completes the proof. ◀

We will now show that the second principle of mathematical induction is a valid technique.

Proof. Let T be a set of integers containing 1 and such that for every positive integer n, if it contains $1, 2, \ldots, n$, it also contains $n + 1$. Let S be the set of all positive integers n such that all the positive integers less than or equal to n are in T. Then 1 is in S, and by the hypotheses, we see that if n is in S, then $n + 1$ is in S. Hence, by the principle of mathematical induction, S must be the set of all positive integers, so clearly T is also the set of all positive integers, since S is a subset of T. ∎

Recursive Definitions

The principle of mathematical induction provides a method for defining the values of functions at positive integers. Instead of explicitly specifying the value of the function at n, we give the value of the function at 1 and give a rule for finding, for each positive integer n, the value of the function at $n + 1$ from the value of the function at n.

Definition. We say that the function f is *defined recursively* if the value of f at 1 is specified and if for each positive integer n a rule is provided for determining $f(n + 1)$ from $f(n)$.

The principle of mathematical induction can be used to show that a function that is defined recursively is defined uniquely at each positive integer (see Exercise 25 at the end of this section). We illustrate how to define a function recursively with the following definition.

Example 1.25. We will recursively define the *factorial function* $f(n) = n!$. First, we specify that

$$f(1) = 1.$$

Then we give a rule for finding $f(n + 1)$ from $f(n)$ for each positive integer, namely

$$f(n + 1) = (n + 1) \cdot f(n).$$

These two statements uniquely define $n!$ for the set of positive integers.

To find the value of $f(6) = 6!$ from the recursive definition, use the second property successively, as follows:

$$f(6) = 6 \cdot f(5) = 6 \cdot 5 \cdot f(4) = 6 \cdot 5 \cdot 4 \cdot f(3) = 6 \cdot 5 \cdot 4 \cdot 3 \cdot f(2) = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot f(1).$$

Then use the first statement of the definition to replace $f(1)$ by its stated value 1, to conclude that

$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720.$$ ◀

The second principle of mathematical induction also serves as a basis for recursive definitions. We can define a function whose domain is the set of positive integers by specifying its value at 1 and giving a rule, for each positive integer n, for finding $f(n)$

from the values $f(j)$ for each integer j with $1 \leq j \leq n-1$. This will be the basis for the definition of the sequence of Fibonacci numbers discussed in Section 1.4.

1.3 Exercises

1. Use mathematical induction to prove that $n < 2^n$ whenever n is a positive integer.
2. Conjecture a formula for the sum of the first n even positive integers. Prove your result using mathematical induction.
3. Use mathematical induction to prove that $\sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ whenever n is a positive integer.
4. Conjecture a formula for $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}$ from the value of this sum for small integers n. Prove that your conjecture is correct using mathematical induction. (Compare this to Exercise 17 in Section 1.2.)
5. Conjecture a formula for $\mathbf{A}^n$ where $\mathbf{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Prove your conjecture using mathematical induction.
6. Use mathematical induction to prove that $\sum_{j=1}^{n} j = 1 + 2 + 3 + \cdots + n = n(n+1)/2$ for every positive integer n. (Compare this to Example 1.19 in Section 1.2.)
7. Use mathematical induction to prove that $\sum_{j=1}^{n} j^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ for every positive integer n.
8. Use mathematical induction to prove that $\sum_{j=1}^{n} j^3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = [n(n+1)/2]^2$ for every positive integer n.
9. Use mathematical induction to prove that $\sum_{j=1}^{n} j(j+1) = 1\cdot 2 + 2\cdot 3 + \cdots + n\cdot(n+1) = n(n+1)(n+2)/3$ for every positive integer n.
10. Use mathematical induction to prove that $\sum_{j=1}^{n} (-1)^{j-1} j^2 = 1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} n(n+1)/2$ for every positive integer n.
11. Find a formula for $\prod_{j=1}^{n} 2^j$.
12. Show that $\sum_{j=1}^{n} j \cdot j! = 1\cdot 1! + 2\cdot 2! + \cdots + n\cdot n! = (n+1)! - 1$ for every positive integer n.
13. Show that any amount of postage that is an integer number of cents greater than 11 cents can be formed using just 4-cent and 5-cent stamps.
14. Show that any amount of postage that is an integer number of cents greater than 53 cents can be formed using just 7-cent and 10-cent stamps.

Let H_n be the nth partial sum of the harmonic series, that is, $H_n = \sum_{j=1}^{n} 1/j$.

* 15. Use mathematical induction to show that $H_{2^n} \geq 1 + n/2$.

* 16. Use mathematical induction to show that $H_{2^n} \leq 1 + n$.

17. Show by mathematical induction that if n is a positive integer, then $(2n)! < 2^{2n}(n!)^2$.
18. Use mathematical induction to prove that $x - y$ is a factor of $x^n - y^n$, where x and y are variables.

☞ **19.** Use the principle of mathematical induction to show that a set of integers that contains the integer k, such that this set contains $n + 1$ whenever it contains n, contains the set of integers that are greater than or equal to k.

20. Use mathematical induction to prove that $2^n < n!$ for $n \geq 4$.

21. Use mathematical induction to prove that $n^2 < n!$ for $n \geq 4$.

22. Show by mathematical induction that if $h \geq -1$, then $1 + nh \leq (1 + h)^n$ for all nonnegative integers n.

23. A jigsaw puzzle is solved by putting its pieces together in the correct way. Show that exactly $n - 1$ moves are required to solve a jigsaw puzzle with n pieces, where a move consists of putting together two blocks of pieces, with a block consisting of one or more assembled pieces. (*Hint:* Use the second principle of mathematical induction.)

24. Explain what is wrong with the following proof by mathematical induction that all horses are the same color: Clearly all horses in any set of 1 horse are all the same color. This completes the basis step. Now assume that all horses in any set of n horses are the same color. Consider a set of $n + 1$ horses, labeled with the integers $1, 2, \ldots, n + 1$. By the induction hypothesis, horses $1, 2, \ldots, n$ are all the same color, as are horses $2, 3, \ldots, n, n + 1$. Because these two sets of horses have common members, namely horses $2, 3, 4, \ldots, n$, all $n + 1$ horses must be the same color. This completes the induction argument.

25. Use the principle of mathematical induction to show that the value at each positive integer of a function defined recursively is uniquely determined.

26. What function $f(n)$ is defined recursively by $f(1) = 2$ and $f(n + 1) = 2f(n)$ for $n \geq 1$? Prove your answer using mathematical induction.

27. If g is defined recursively by $g(1) = 2$ and $g(n) = 2^{g(n-1)}$ for $n \geq 2$, what is $g(4)$?

28. Use the second principle of mathematical induction to show that if $f(1)$ is specified and a rule for finding $f(n + 1)$ from the values of f at the first n positive integers is given, then $f(n)$ is uniquely determined for every positive integer n.

29. We define a function recursively for all positive integers n by $f(1) = 1$, $f(2) = 5$, and for $n > 2$, $f(n + 1) = f(n) + 2f(n - 1)$. Show that $f(n) = 2^n + (-1)^n$, using the second principle of mathematical induction.

30. Show that $2^n > n^2$ whenever n is an integer greater than 4.

31. Suppose that $a_0 = 1$, $a_1 = 3$, $a_2 = 9$, and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n \geq 3$. Show that $a_n \leq 3^n$ for every nonnegative integer n.

☠ **32.** The tower of Hanoi was a popular puzzle of the late nineteenth century. The puzzle includes three pegs and eight rings of different sizes placed in order of size, with the largest on the bottom, on one of the pegs. The goal of the puzzle is to move all of the rings, one at a time, without ever placing a larger ring on top of a smaller ring, from the first peg to the second, using the third as an auxiliary peg.

a) Use mathematical induction to show that the minimum number of moves to transfer n rings from one peg to another, with the rules we have described, is $2^n - 1$.

b) An ancient legend tells of the monks in a tower with 64 gold rings and 3 diamond pegs. They started moving the rings, one move per second, when the world was created. When they finish transferring the rings to the second peg, the world will end. How long will the world last?

* **33.** The *arithmetic mean* and the *geometric mean* of the positive real numbers $a_1, a_2, \ldots, a_n$ are $A = (a_1 + a_2 + \cdots + a_n)/n$ and $G = (a_1 a_2 \cdots a_n)^{1/n}$, respectively. Use mathematical induction to prove that $A \geq G$ for every finite sequence of positive real numbers. When does equality hold?

34. Use mathematical induction to show that a $2^n \times 2^n$ chessboard with one square missing can be covered with L-shaped pieces, where each L-shaped piece covers three squares.

* **35.** A *unit fraction* is a fraction of the form $1/n$, where n is a positive integer. Because the ancient Egyptians represented fractions as sums of distinct unit fractions, such sums are called *Egyptian fractions*. Show that every rational number p/q, where p and q are integers with $0 < p < q$, can be written as a sum of distinct unit fractions, that is, as an Egyptian fraction. (*Hint:* Use strong induction on the numerator p to show that the algorithm that adds the largest possible unit fraction at each stage always terminates. For example, running this algorithm shows that $5/7 = 1/2 + 1/5 + 1/70$.)

36. Using the algorithm in Exercise 35, write each of these numbers as Egyptian fractions.

a) 2/3 c) 11/17
b) 5/8 d) 44/101

1.3 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. Complete the basis and inductive steps, using both numerical and symbolic computation, to prove that $\sum_{j=1}^{n} j = n(n+1)/2$ for all positive integers n.

2. Complete the basis and inductive steps, using both numerical and symbolic computation, to prove that $\sum_{j=1}^{n} j^2 = n(n+1)(2n+1)/6$ for all positive integers n.

3. Complete the basis and inductive steps, using both numerical and symbolic computation, to prove that $\sum_{j=1}^{n} j^3 = (n(n+1)/2)^2$ for all positive integers n.

4. Use the values $\sum_{j=1}^{n} j^4$ for $n = 1, 2, 3, 4, 5, 6$ to conjecture a formula for this sum that is a polynomial of degree 5 in n. Attempt to prove your conjecture via mathematical induction using numerical and symbolic computation.

5. Paul Erdős and E. Strauss have conjectured that the fraction $4/n$ can be written as the sum of three unit fractions, that is, $4/n = 1/x + 1/y + 1/z$, where x, y, and z are distinct positive integers for all integers n with $n > 1$. Find such representation for as many positive integers n as you can.

6. It is conjectured that the rational number p/q, where p and q are integers with $0 < p < q$ and q is odd, can be expressed as an Egyptian fraction which is the sum of unit fractions with odd denominators. Explore this conjecture using the algorithm that successively adds the unit fraction with the least positive odd denominator q at each stage. (For example, $2/7 = 1/5 + 1/13 + 1/115 + 1/10{,}465$.)

Programming Projects

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

* 1. List the moves in the tower of Hanoi puzzle (see Exercise 32). If you can, animate these moves.

** 2. Cover a $2^n \times 2^n$ chessboard that is missing one square using L-shaped pieces (see Exercise 34).

3. Given a rational number p/q, express p/q as an Egyptian fraction using the algorithm described in Exercise 35.

1.4 The Fibonacci Numbers

In his book *Liber Abaci*, written in 1202, the mathematician *Fibonacci* posed a problem concerning the growth of the number of rabbits in a certain area. This problem can be phrased as follows: A young pair of rabbits, one of each sex, is placed on an island. Assuming that rabbits do not breed until they are two months old and after they are two months old, each pair of rabbits produces another pair each month, how many pairs are there after n months?

Let f_n be the number of pairs of rabbits after n months. We have $f_1 = 1$ because only the original pair is on the island after one month. As this pair does not breed during the second month, $f_2 = 1$. To find the number of pairs after n months, add the number on the island the previous month, f_{n-1}, to the number of newborn pairs, which equals f_{n-2}, because each newborn pair comes from a pair at least two months old. This leads to the following definition.

Definition. The *Fibonacci sequence* is defined recursively by $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. The terms of this sequence are called the *Fibonacci numbers*.

The mathematician Edouard Lucas named this sequence after Fibonacci in the nineteenth century when he established many of its properties. The answer to Fibonacci's question is that there are f_n rabbits on the island after n months.

FIBONACCI (c. 1180–1228) (short for *filus Bonacci*, son of Bonacci), also known as Leonardo of Pisa, was born in the Italian commercial center of Pisa. Fibonacci was a merchant who traveled extensively throughout the Mideast, where he came into contact with mathematical works from the Arabic world. In his *Liber Abaci* Fibonacci introduced Arabic notation for numerals and their algorithms for arithmetic into the European world. It was in this book that his famous rabbit problem appeared. Fibonacci also wrote *Practica geometriae*, a treatise on geometry and trigonometry, and *Liber quadratorum*, a book on diophantine equations.

Examining the initial terms of the Fibonacci sequence will be useful as we study their properties.

Example 1.26. We compute the first ten Fibonacci numbers as follows:

$$\begin{aligned} f_3 &= f_2 + f_1 = 1 + 1 = 2 \\ f_4 &= f_3 + f_2 = 2 + 1 = 3 \\ f_5 &= f_4 + f_3 = 3 + 2 = 5 \\ f_6 &= f_5 + f_4 = 5 + 3 = 8 \\ f_7 &= f_6 + f_5 = 8 + 5 = 13 \\ f_8 &= f_7 + f_6 = 13 + 8 = 21 \\ f_9 &= f_8 + f_7 = 21 + 13 = 34 \\ f_{10} &= f_9 + f_8 = 34 + 21 = 55. \end{aligned}$$

◀

We can define the value of $f_0 = 0$, so that $f_2 = f_1 + f_0$. We can also define f_n where n is a negative number so that the equality in the recursive definition is satisfied (see Exercise 37.)

The Fibonacci numbers occur in an amazing variety of applications. For example, in botany the number of spirals in plants with a pattern known as phyllotaxis is always a Fibonacci number. They occur in the solution of a tremendous variety of counting problems, such as counting the number of bit strings with no two consecutive 1s (see [Ro03]).

The Fibonacci numbers also satisfy an extremely large number of identities. For example, we can easily find an identity for the sum of the first n consecutive Fibonacci numbers.

Example 1.27. The sum of the first n Fibonacci numbers for $3 \leq n \leq 8$ equals 1, 2, 4, 7, 12, 20, 33, and 54. Looking at these numbers, we see that they are all just 1 less than the Fibonacci number f_{n+2}. This leads us to the conjecture that

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1.$$

Can we prove this identity for all positive integers n?

We will show, in two different ways, that this identity does hold for all integers n. We provide two different demonstrations, to show that there is often more than one way to prove that an identity is true.

First, we use the fact that $f_n = f_{n-1} + f_{n-2}$ for $n = 2, 3, \ldots$ to see that $f_k = f_{k+2} - f_{k+1}$ for $k = 1, 2, 3, \ldots$. This means that

$$\sum_{k=1}^{n} f_k = \sum_{k=1}^{n} (f_{k+2} - f_{k+1}).$$

We can easily evaluate this sum because it is telescoping. Using the formula for a telescoping sum found in Section 1.2, we have

$$\sum_{k=1}^{n} f_k = f_{n+2} - f_2 = f_{n+2} - 1.$$

This proves the result.

We can also prove this identity using mathematical induction. The basis step holds because $\sum_{k=1}^{1} f_k = 1$ and this equals $f_{1+2} - 1 = f_3 - 1 = 2 - 1 = 1$. The inductive hypothesis is

$$\sum_{k=1}^{n} f_k = f_{n+2} - 1.$$

We must show that, under this assumption,

$$\sum_{k=1}^{n+1} f_k = f_{n+3} - 1.$$

To prove this, note that by the inductive hypothesis we have

$$\begin{aligned}\sum_{k=1}^{n+1} f_k &= \left(\sum_{k=1}^{n} f_k\right) + f_{n+1} \\ &= (f_{n+2} - 1) + f_{n+1} \\ &= (f_{n+1} + f_{n+2}) - 1 \\ &= f_{n+3} - 1.\end{aligned}$$

◀

The exercise set at the end of this section asks you to prove many other identities of the Fibonacci numbers.

How Fast Do the Fibonacci Numbers Grow?

The following inequality, which shows that the Fibonacci numbers grow faster than a geometric series with common ratio $\alpha = (1 + \sqrt{5})/2$, will be used in Chapter 3.

Example 1.28. We can use the second principle of mathematical induction to prove that $f_n > \alpha^{n-2}$ for $n \geq 3$ where $\alpha = (1 + \sqrt{5})/2$. The basis step consists of verifying this inequality for $n = 3$ and $n = 4$. We have $\alpha < 2 = f_3$, so the theorem is true for $n = 3$. Since $\alpha^2 = (3 + \sqrt{5})/2 < 3 = f_4$, the theorem is true for $n = 4$.

The inductive hypothesis consists of assuming that $\alpha^{k-2} < f_k$ for all integers k with $k \leq n$. Because $\alpha = (1 + \sqrt{5})/2$ is a solution of $x^2 - x - 1 = 0$, we have $\alpha^2 = \alpha + 1$. Hence

$$\alpha^{n-1} = \alpha^2 \cdot \alpha^{n-3} = (\alpha + 1) \cdot \alpha^{n-3} = \alpha^{n-2} + \alpha^{n-3}.$$

By the inductive hypothesis, we have the inequalities

$$\alpha^{n-2} < f_n, \quad \alpha^{n-3} < f_{n-1}.$$

By adding these two inequalities, we conclude that

$$\alpha^{n-1} < f_n + f_{n-1} = f_{n+1}.$$

This finishes the proof. ◀

We conclude this section with an explicit formula for the nth Fibonacci number. We will not provide a proof in the text, but Exercises 41 and 42 at the end of this section outline how this formula can be found using linear homogeneous recurrence relations and generating functions, respectively. Furthermore, Exercise 40 asks that you prove this identity by showing that the terms satisfy the same recursive definition as the Fibonacci numbers do, and Exercise 45 asks for a proof via mathematical induction. The advantage of the first two approaches is that they can be used to find the formula, while the second two approaches cannot.

Theorem 1.7. Let n be a positive integer and let $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. Then the nth Fibonacci number f_n is given by

$$f_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n).$$

We have presented a few important results involving the Fibonacci numbers. There is a vast literature concerning these numbers and their many applications to botany, computer science, geography, physics, and other areas (see [Va89]). There is even a scholarly journal, *The Fibonacci Quarterly*, devoted to their study.

1.4 Exercises

1. Find the following Fibonacci numbers.
   a) f_{10} c) f_{15} e) f_{20}
   b) f_{13} d) f_{18} f) f_{25}
2. Find each of the following Fibonacci numbers.
   a) f_{12} c) f_{24} e) f_{32}
   b) f_{16} d) f_{30} f) f_{36}
3. Prove that $f_{n+3} + f_n = 2f_{n+2}$ whenever n is a positive integer.
4. Prove that $f_{n+3} - f_n = 2f_{n+1}$ whenever n is a positive integer.
5. Prove that $f_{2n} = f_n^2 + 2f_{n-1}f_n$ whenever n is a positive integer. (Recall that $f_0 = 0$.)
6. Prove that $f_{n-2} + f_{n+2} = 3f_n$ whenever n is an integer with $n \geq 2$. (Recall that $f_0 = 0$.)
7. Find and prove a simple formula for the sum of the first n Fibonacci numbers with odd indices when n is a positive integer. That is, find a simple formula for $f_1 + f_3 + \cdots + f_{2n-1}$.

8. Find and prove a simple formula for the sum of the first n Fibonacci numbers with even indices when n is a positive integer. That is, find a simple formula for $f_2 + f_4 + \cdots + f_{2n}$.
9. Find and prove a simple formula for the expression $f_n - f_{n-1} + f_{n-2} - \cdots + (-1)^{n+1} f_1$ when n is a positive integer.
10. Prove that $f_{2n+1} = f_{n+1}^2 + f_n^2$ whenever n is a positive integer.
11. Prove that $f_{2n} = f_{n+1}^2 - f_{n-1}^2$ whenever n is a positive integer. (Recall that $f_0 = 0$.)
12. Prove that $f_n + f_{n-1} + f_{n-2} + 2f_{n-3} + 4f_{n-4} + 8f_{n-5} + \cdots + 2^{n-3} = 2^{n-1}$ whenever n is an integer with $n \geq 3$.
13. Prove that $\sum_{j=1}^{n} f_j^2 = f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$ for every positive integer n.
14. Prove that $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ for every positive integer n.
15. Prove that $f_{n+1} f_n - f_{n-1} f_{n-2} = f_{2n-1}$ for every positive integer n, $n > 2$.
16. Prove that $f_1 f_2 + f_2 f_3 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2$ if n is a positive integer.
17. Prove that $f_{m+n} = f_m f_{n+1} + f_n f_{m-1}$ whenever m and n are positive integers.

The *Lucas numbers*, named after *François-Eduoard-Anatole Lucas* (see Chapter 7 for a biography), are defined recursively by

$$L_n = L_{n-1} + L_{n-2}, \quad n \geq 3$$

with $L_1 = 1$ and $L_2 = 3$. They satisfy the same recurrence relation as the Fibonacci numbers, but the two initial values are different.

18. Find the first 12 Lucas numbers.
19. Find and prove a formula for the sum of the first n Lucas numbers when n is a positive integer.
20. Find and prove a formula for the sum of the first n Lucas numbers with odd indices when n is a positive integer.
21. Find and prove a formula for the sum of the first n Lucas numbers with even indices when n is a positive integer.
22. Prove that $L_n^2 - L_{n+1} L_{n-1} = 5(-1)^n$ when n is an integer with $n \geq 2$.
23. Prove that $L_1^2 + L_2^2 + \cdots + L_n^2 = L_n L_{n+1} - 2$ when n is an integer with $n \geq 1$.
24. Show that the nth Lucas number L_n is the sum of the $(n+1)$st and $(n-1)$st Fibonacci numbers, f_{n+1} and f_{n-1}, respectively.
25. Show that $f_{2n} = f_n L_n$ for all integers n with $n \geq 1$, where f_n is the nth Fibonacci number and L_n is the nth Lucas number.
26. Prove that $5f_{n+1} = L_n + L_{n+2}$ whenever n is a positive integer, f_n is the nth Fibonacci number, and L_n is the nth Lucas number.
* 27. Prove that $L_{m+n} = f_{m+1} L_n + f_m L_{n-1}$ whenever m and n are positive integers with $n > 1$, f_n is the nth Fibonacci number, and L_n is the nth Lucas number.
28. Show that L_n, the nth Lucas number, is given by

$$L_n = \alpha^n + \beta^n,$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$.

The *Zeckendorf representation* of a positive integer is the unique expression of this integer as the sum of distinct Fibonacci numbers, where no two of these Fibonacci numbers are consecutive terms in the Fibonacci sequence and where the term $f_1 = 1$ is not used (but the term $f_2 = 1$ may be used.)

29. Find the Zeckendorf representation of each of the integers 50, 85, 110, and 200.

* **30.** Show that every positive integer has a unique Zeckendorf representation.

31. Show that $f_n \leq \alpha^{n-1}$ for every integer n with $n \geq 2$, where $\alpha = (1 + \sqrt{5})/2$.

32. Show that

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots = f_{n+1},$$

where n is a nonnegative integer and f_{n+1} is the $(n+1)$st Fibonacci number. (See Appendix B for a review of binomial coefficients. Here, the sum ends with the term $\binom{1}{n-1}$.)

33. Prove that whenever n is a nonegative integer, $\sum_{j=1}^{n} \binom{n}{j} f_j = f_{2n}$, where f_j is the jth Fibonacci number.

34. Let $\mathbf{F} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $\mathbf{F}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$ when $n \in \mathbf{Z}^+$.

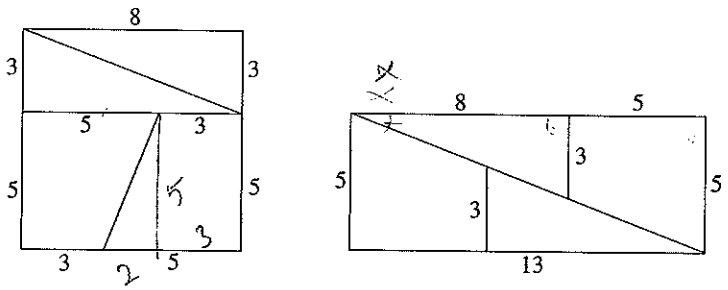
35. By taking determinants of both sides of the result of Exercise 34, prove the identity in Exercise 14.

36. Define the *generalized Fibonacci numbers* recursively by $g_1 = a$, $g_2 = b$, and $g_n = g_{n-1} + g_{n-2}$ for $n \geq 3$. Show that $g_n = af_{n-2} + bf_{n-1}$ for $n \geq 3$.

37. Give a recursive definition of the Fibonacci number f_n when n is a negative integer. Use your definition to find f_n for $n = -1, -2, -3, \ldots, -10$.

38. Use the results of Exercise 37 to formulate a conjecture that relates the values of f_{-n} and f_n when n is a positive integer. Prove this conjecture using mathematical induction.

39. What is wrong with the claim that an 8×8 square can be broken into pieces that can be reassembled to form a 5×13 rectangle as shown?



(*Hint:* Look at the identity in Exercise 14. Where is the extra square unit?)

40. Show that if $a_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$, where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$, then $a_n = a_{n-1} + a_{n-2}$ and $a_1 = a_2 = 1$. Conclude that $f_n = a_n$, where f_n is the nth Fibonacci number.

A *linear homogeneous recurrence relation of degree 2 with constant coefficients* is an equation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2},$$

where c_1 and c_2 are real numbers with $c_2 \neq 0$. It is not difficult to show (see [Ro03]) that if the equation $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2, then the sequence $\{a_n\}$ is a solution of the linear homogeneous recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if $a_n = C_1 r_1^n + C_2 r_2^n$ for $n = 0, 1, 2, \ldots$, where C_1 and C_2 are constants. The values of these constants can be found using the two initial terms of the sequence.

41. Find an explicit formula for f_n, proving Theorem 1.7, by solving the recurrence relation $f_n = f_{n-1} + f_{n-2}$ for $n = 2, 3, \ldots$ with initial conditions $f_0 = 0$ and $f_1 = 1$.

The *generating function* for the sequence $a_0, a_1, \ldots, a_k, \ldots$ is the infinite series

$$G(x) = \sum_{k=0}^{\infty} a_k x^k.$$

42. Use the generating function $G(x) = \sum_{k=0}^{\infty} f_k x^k$ where f_k is the kth Fibonacci number to find an explicit formula for f_k, proving Theorem 1.7. (*Hint:* Use the fact that $f_k = f_{k-1} + f_{k-2}$ for $k = 2, 3, \ldots$ to show that $G(x) - xG(x) - x^2 G(x) = x$. Solve this to show that $G(x) = x/(1 - x - x^2)$ and then write $G(x)$ in terms of partial fractions, as is done in calculus.) (See [Ro03] for information on using generating functions.)

43. Find an explicit formula for the Lucas numbers using the technique of Exercise 41.

44. Find an explicit formula for the Lucas numbers using the technique of Exercise 42.

45. Use mathematical induction to prove Theorem 1.7.

1.4 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 Fibonacci numbers f_{100}, f_{200}, and f_{500}.
2. Find the Lucas numbers L_{100}, L_{200}, and L_{500}.
3. A surprising theorem states that the Fibonacci numbers are the positive values of the polynomial $2xy^4 + x^2y^3 - 2x^3y^2 - y^5 - x^4y + 2y$ as x and y range over all nonnegative integers. Verify this conjecture for the values of x and y where x and y are nonnegative integers with $x + y \leq 100$.

Programming Projects

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

1. Given a positive integer n, find the first n terms of the Fibonacci sequence.
2. Given a positive integer n, find the first n terms of the Lucas sequence.

1.5 Divisibility

The concept of the divisibility of one integer by another is central in number theory.

Definition. If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$. If a divides b, we also say that a is a *divisor* or *factor* of b and that b is a *multiple* of a.

If a divides b we write $a \mid b$, and if a does not divide b we write $a \nmid b$. (Be careful not to confuse the notations $a \mid b$, which denotes that a divides b, and a/b, which is the quotient obtained when a is divided by b.)

Example 1.29. The following statements illustrate the concept of the divisibility of integers: $13 \mid 182$, $-5 \mid 30$, $17 \mid 289$, $6 \nmid 44$, $7 \nmid 50$, $-3 \mid 33$, and $17 \mid 0$. ◀

Example 1.30. The divisors of 6 are ± 1, ± 2, ± 3, ± 6. The divisors of 17 are ± 1, ± 17. The divisors of 100 are ± 1, ± 2, ± 4, ± 5, ± 10, ± 20, ± 25, ± 50, ± 100. ◀

In subsequent chapters, we will need some simple properties of divisibility, which we now state and prove.

Theorem 1.8. If a, b, and c are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Because $a \mid b$ and $b \mid c$, there are integers e and f such that $ae = b$ and $bf = c$. Hence, $c = bf = (ae)f = a(ef)$, and we conclude that $a \mid c$. ■

Example 1.31. Because $11 \mid 66$ and $66 \mid 198$, Theorem 1.8 tells us that $11 \mid 198$. ◀

Theorem 1.9. If a, b, m, and n are integers, and if $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$.

Proof. Because $c \mid a$ and $c \mid b$, there are integers e and f such that $a = ce$ and $b = cf$. Hence, $ma + nb = mce + ncf = c(me + nf)$. Consequently, we see that $c \mid (ma + nb)$. ■

Example 1.32. As $3 \mid 21$ and $3 \mid 33$, Theorem 1.9 tells us that 3 divides

$$5 \cdot 21 - 3 \cdot 33 = 105 - 99 = 6.$$ ◀

The following theorem states an important fact about division.

Theorem 1.10. ***The Division Algorithm.*** If a and b are integers such that $b > 0$, then there are unique integers q and r such that $a = bq + r$ with $0 \leq r < b$. ■

In the equation given in the division algorithm, we call q the *quotient* and r the *remainder*. We also call a the *dividend* and b the *divisor*. (*Note:* We use the traditional name for this theorem even though the division algorithm is not actually an algorithm. We discuss algorithms in Section 2.2.)

We note that a is divisible by b if and only if the remainder in the division algorithm is 0. Before we prove the division algorithm, consider the following examples.

Example 1.33. If $a = 133$ and $b = 21$, then $q = 6$ and $r = 7$, because $133 = 21 \cdot 6 + 7$. Likewise, if $a = -50$ and $b = 8$, then $q = -7$ and $r = 6$, because $-50 = 8(-7) + 6$. ◀

We now prove the division algorithm using the well-ordering property.

Proof. Consider the set S of all integers of the form $a - bk$ where k is an integer, that is, $S = \{a - bk \mid k \in \mathbf{Z}\}$. Let T be the set of all nonnegative integers in S. T is nonempty, because $a - bk$ is positive whenever k is an integer with $k < a/b$.

By the well-ordering property, T has a least element $r = a - bq$. (These are the values for q and r specified in the theorem.) We know that $r \geq 0$ by construction, and it is easy to see that $r < b$. If $r \geq b$ then $r > r - b = a - bq - b = a - b(q + 1) \geq 0$, which contradicts the choice of $r = a - bq$ as the least nonnegative integer of the form $a - bk$. Hence $0 \leq r < b$.

To show that these values for q and r are unique, assume that we have two equations $a = bq_1 + r_1$ and $a = bq_2 + r_2$, with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. By subtracting the second of these equations from the first, we find that

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Hence, we see that

$$r_2 - r_1 = b(q_1 - q_2).$$

This tells us that b divides $r_2 - r_1$. Because $0 \leq r_1 < b$ and $0 \leq r_2 < b$, we have $-b < r_2 - r_1 < b$. Hence, b can divide $r_2 - r_1$ only if $r_2 - r_1 = 0$ or, in other words, if $r_1 = r_2$. Because $bq_1 + r_1 = bq_2 + r_2$ and $r_1 = r_2$, we also see that $q_1 = q_2$. This shows that the quotient q and the remainder r are unique. ■

We now use the greatest integer function (defined in Section 1.1) to give explicit formulas for the quotient and remainder in the division algorithm. Because the quotient q is the largest integer such that $bq \leq a$, and $r = a - bq$, it follows that

$$q = [a/b], \quad r = a - b[a/b]. \tag{1.4}$$

The following examples display the quotient and remainder of a division.

Example 1.34. Let $a = 1028$ and $b = 34$. Then $a = bq + r$ with $0 \leq r < b$, where $q = [1028/34] = 30$ and $r = 1028 - [1028/34] \cdot 34 = 1028 - 30 \cdot 34 = 8$. ◀

Example 1.35. Let $a = -380$ and $b = 75$. Then $a = bq + r$ with $0 \leq r < b$, where $q = [-380/75] = -6$ and $r = -380 - [-380/75] \cdot 75 = -380 - (-6)75 = 70$. ◀

We can use Equation (1.4) to prove a useful property of the greatest integer function.

Example 1.36. Show that if n is a positive integer, then $[x/n] = [[x]/n]$ whenever x is a real number. To prove this identity, suppose that $[x] = m$. By the division algorithm,

we have integers q and r such that $m = nq + r$, where $0 \leq r \leq n - 1$. By Equation (1.4), we have $q = [[x]/n]$. Because $[x] \leq x < [x] + 1$, it follows that $x = [x] + \epsilon$, where $0 \leq \epsilon < 1$. We see that $[x/n] = [([x] + \epsilon)/n] = [(m + \epsilon)/n] = [((nq + r) + \epsilon)/n] = [q + (r + \epsilon)/n]$. Because $0 \leq \epsilon < 1$, we have $0 \leq r + \epsilon < (n - 1) + 1 = n$. It follows that $[x/n] = [q]$. ◀

Given a positive integer d, we can classify integers according to their remainders when divided by d. For example, with $d = 2$, we see from the division algorithm that every integer when divided by 2 leaves a remainder of either 0 or 1. This leads to the following definition of some common terminology.

Definition. If the remainder when n is divided by 2 is 0, then $n = 2k$ for some integer k, and we say that n is *even*, whereas if the remainder when n is divided by 2 is 1, then $n = 2k + 1$ for some integer k, and we say that n is *odd*.

Similarly, when $d = 4$, we see from the division algorithm that when an integer n is divided by 4, the remainder is either 0, 1, 2, or 3. Hence, every integer is of the form $4k$, $4k + 1$, $4k + 2$, or $4k + 3$, where k is a positive integer.

We will pursue these matters further in Chapter 4.

1.5 Exercises

1. Show that $3 \mid 99$, $5 \nmid 145$, $7 \mid 343$, and $888 \mid 0$.
2. Show that 1001 is divisible by 7, by 11, and by 13.
3. Decide which of the following integers are divisible by 7.

   a) 0 d) 123321
   b) 707 e) −285714
   c) 1717 f) −430597

4. Decide which of the following integers are divisible by 22.

   a) 0 d) 192544
   b) 444 e) −32516
   c) 1716 f) −195518

5. Find the quotient and remainder in the division algorithm, with divisor 17 and dividend

   a) 100. c) −44.
   b) 289. d) −100.

6. What can you conclude if a and b are nonzero integers such that $a \mid b$ and $b \mid a$?
7. Show that if a, b, c, and d are integers with a and c nonzero, such that $a \mid b$ and $c \mid d$, then $ac \mid bd$.
8. Are there integers a , b, and c such that $a \mid bc$, but $a \nmid b$ and $a \nmid c$?
9. Show that if a, b, and $c \neq 0$ are integers, then $a \mid b$ if and only if $ac \mid bc$.

10. Show that if a and b are positive integers and $a \mid b$, then $a \leq b$.

11. Show that if a and b are integers such that $a \mid b$, then $a^k \mid b^k$ for every positive integer k.

12. Show that the sum of two even or of two odd integers is even, whereas the sum of an odd and an even integer is odd.

13. Show that the product of two odd integers is odd, whereas the product of two integers is even if either of the integers is even.

14. Show that if a and b are odd positive integers and $b \nmid a$, then there are integers s and t such that $a = bs + t$, where t is odd and $|t| < b$.

15. When the integer a is divided by the integer b, where $b > 0$, the division algorithm gives a quotient of q and a remainder of r. Show that if $b \nmid a$, when $-a$ is divided by b, the division algorithm gives a quotient of $-(q+1)$ and a remainder of $b - r_j$, whereas if $b \mid a$, the quotient is $-q$ and the remainder is 0.

16. Show that if a, b, and c are integers with $b > 0$ and $c > 0$, such that when a is divided by b the quotient is q and the remainder is r, and when q is divided by c the quotient is t and the remainder is s, then when a is divided by bc, the quotient is t and the remainder is $bs + r$.

17. a) Extend the division algorithm by allowing negative divisors. In particular, show that whenever a and $b \neq 0$ are integers, there are unique integers q and r such that $a = bq + r$, where $0 \leq r < |b|$.

b) Find the remainder when 17 is divided by -7.

18. Show that if a and b are positive integers, then there are unique integers q and r such that $a = bq + r$, where $-b/2 < r \leq b/2$.

19. Show that if m and $n > 0$ are integers, then

$$\left\lceil \frac{m+1}{n} \right\rceil = \begin{cases} \left\lceil \frac{m}{n} \right\rceil & \text{if } m \neq kn - 1 \text{ for some integer } k; \\ \left\lceil \frac{m}{n} \right\rceil + 1 & \text{if } m = kn - 1 \text{ for some integer } k. \end{cases}$$

20. Show that the integer n is even if and only if $n - 2\lfloor n/2 \rfloor = 0$.

21. Show that the number of positive integers less than or equal to x, where x is a positive real number, that are divisible by the positive integer d equals $\lfloor x/d \rfloor$.

22. Find the number of positive integers not exceeding 1000 that are divisible by 5, by 25, by 125, and by 625.

23. How many integers between 100 and 1000 are divisible by 7? by 49?

24. Find the number of positive integers not exceeding 1000 that are not divisible by 3 or 5.

25. Find the number of positive integers not exceeding 1000 that are not divisible by 3, 5, or 7.

26. Find the number of positive integers not exceeding 1000 that are divisible by 3 but not by 4.

27. In 1999, to mail a first-class letter in the United States of America it cost 33 cents for the first ounce and 22 cents for each additional ounce or fraction thereof. Find a formula involving the greatest integer function for the cost of mailing a letter in 1999. Could it possibly have cost \$1.45 or \$2.31 to mail a first-class letter in the United States of America in 1999?

28. Show that if a is an integer, then 3 divides $a^3 - a$.

29. Show that the product of two integers of the form $4k + 1$ is again of this form, whereas the product of two integers of the form $4k + 3$ is of the form $4k + 1$.

30. Show that the square of every odd integer is of the form $8k + 1$.

31. Show that the fourth power of every odd integer is of the form $16k + 1$.

32. Show that the product of two integers of the form $6k + 5$ is of the form $6k + 1$.

33. Show that the product of any three consecutive integers is divisible by 6.

34. Use mathematical induction to show that $n^5 - n$ is divisible by 5 for every positive integer n.

35. Use mathematical induction to show that the sum of the cubes of three consecutive integers is divisible by 9.

In Exercises 36–40, let f_n denote the nth Fibonacci number.

36. Show that f_n is even if and only if n is divisible by 3.

37. Show that f_n is divisible by 3 if and only if n is divisible by 4.

38. Show that f_n is divisible by 4 if and only if n is divisible by 6.

39. Show that $f_n = 5f_{n-4} + 3f_{n-5}$ whenever n is a positive integer with $n > 5$. Use this result to show that f_n is divisible by 5 whenever n is divisible by 5.

* **40.** Show that $f_{n+m} = f_m f_{n+1} + f_{m-1} f_n$ whenever m and n are positive integers with $m > 1$. Use this result to show that $f_n \mid f_m$ when m and n are positive integers with $n \mid m$.

Let n be a positive integer. We define

$$T(n) = \begin{cases} n/2 & \text{if } n \text{ is even;} \\ (3n + 1)/2 & \text{if } n \text{ is odd.} \end{cases}$$

We then form the sequence obtained by iterating T: n, $T(n)$, $T(T(n))$, $T(T(T(n)))$, ... For instance, starting with $n = 7$, we have 7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, 2, 1, ... A well-known conjecture, sometimes called the *Collatz conjecture*, asserts that the sequence obtained by iterating T always reaches the integer 1 no matter which positive integer n begins the sequence.

41. Find the sequence obtained by iterating T starting with $n = 39$.

42. Show that the sequence obtained by iterating T starting with $n = (2^{2k} - 1)/3$, where k is a positive integer greater than 1, always reaches the integer 1.

43. Show that the Collatz conjecture is true if it can be shown that for every positive integer n with $n \geq 2$ there is a term in the sequence obtained by iterating T that is less than n.

44. Verify that there is a term in the sequence obtained by iterating T, starting with the positive integer n, that is less than n for all positive integers n with $2 \leq n \leq 100$. (*Hint:* Begin by considering sets of positive integers for which it is easy to show that this is true.)

* **45.** Show that $[(2 + \sqrt{3})^n]$ is odd whenever n is a nonnegative integer.

1.5 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. Verify the Collatz conjecture described in the preamble to Exercise 41 for all integers n not exceeding 10,000.
2. Using numerical evidence, what sort of conjectures can you make concerning the number of iterations needed before the sequence of iterations $T(n)$ reaches 1, where n is a given positive integer?
3. Using numerical evidence, make conjectures about the divisibility of Fibonacci numbers by 7, by 8, by 9, by 11, by 13, and so on.

Programming Projects

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

1. Decide whether an integer is divisible by a given integer.
2. Find the quotient and remainder in the division algorithm.
3. Find the quotient, remainder, and sign in the modified division algorithm given in Exercise 18.
4. Compute the terms of the sequence n, $T(n)$, $T(T(n))$, $T(T(T(n)))$, . . . for a given positive integer n, as defined in the preamble to Exercise 41.

2

Integer Representations and Operations

Introduction

The way in which integers are represented has a major impact on how easily people and computers can do arithmetic with these integers. The purpose of this chapter is to explain how integers are represented using base b expansions, and how basic arithmetic operations can be carried out using these expansions. In particular, we will show that when b is a positive integer, every positive integer has a unique base b expansion. For example, when b is 10, we have the decimal expansion of an integer; when b is 2, we have the binary expansion of this integer; and when b is 16, we have the hexadecimal expansion. We will describe a procedure for finding the base b expansion of an integer, and describe the basic algorithms used to carry out integer arithmetic with base b expansions. Finally, after introducing big-O notation, we will analyze the computational complexity of these basic operations in terms of big-O estimates of the number of bit operations that they use.

2.1 Representations of Integers

In daily life, we use decimal notation to represent integers. We write out numbers using digits to represent powers of ten. For instance, when we write out the integer 37465, we mean

$$3 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 5.$$

Decimal notation is an example of a *positional number system*, in which the position a digit occupies in a representation determines the quantity it represents. Throughout ancient and modern history, many other notations for integers have been used. For example, Babylonian mathematicians who lived more than 3000 years ago expressed integers using sixty as a base. The Romans employed Roman numerals, which are used

even today to represent years. The ancient Mayans used a positional notation with twenty as a base. Many other systems of integer notation have been invented and used over time.

There is no special reason for using ten as the base in a fixed positional number system, other than that we have ten fingers. As we will see, any positive integer can be used as a base. With the invention and proliferation of computers, bases other than ten have become increasingly important. In particular, base 2, base 8, and base 16 representations of integers are used extensively by computers for various purposes.

In this section, we will demonstrate that no matter which positive integer b is chosen as a base, every positive integer can be expressed uniquely in base b notation. In Section 2.2, we will show how these expansions can be used to do arithmetic with integers. (See the exercise set at the end of this section to learn about one's and two's complement notations, which are used by computers to represent both positive and negative integers.)

For more information about the fascinating history of positional number systems, the reader is referred to [Or88] or [Kn97], where extensive surveys and numerous references may be found.

We now show that every positive integer greater than 1 may be used as a base.

Theorem 2.1. Let b be a positive integer with $b > 1$. Then every positive integer n can be written uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, a_j is an integer with $0 \leq a_j \leq b-1$ for $j = 0, 1, \ldots, k$, and the initial coefficient $a_k \neq 0$.

Proof. We obtain an expression of the desired type by successively applying the division algorithm in the following way. We first divide n by b to obtain

$$n = bq_0 + a_0, \quad 0 \leq a_0 \leq b-1.$$

If $q_0 \neq 0$, we continue by dividing q_0 by b to find that

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 \leq b-1.$$

We continue this process to obtain

$$\begin{aligned}
q_1 &= bq_2 + a_2, \quad 0 \leq a_2 \leq b-1, \\
q_2 &= bq_3 + a_3, \quad 0 \leq a_3 \leq b-1, \\
&\vdots \\
q_{k-2} &= bq_{k-1} + a_{k-1}, \quad 0 \leq a_{k-1} \leq b-1, \\
q_{k-1} &= b \cdot 0 + a_k, \quad 0 \leq a_k \leq b-1.
\end{aligned}$$

The last step of the process occurs when a quotient of 0 is obtained. To see this, first note that the sequence of quotients satisfies

$$n > q_0 > q_1 > q_2 > \cdots \geq 0.$$

Because the sequence $q_0, q_1, q_2, \ldots$ is a decreasing sequence of nonnegative integers that continues as long as its terms are positive, there are at most q_0 terms in this sequence, and the last term equals 0.

From the first equation above, we find that

$$n = bq_0 + a_0.$$

We next replace q_0 using the second equation, to obtain

$$n = b(bq_1 + a_1) + a_0 = b^2q_1 + a_1b + a_0.$$

Successively substituting for $q_1, q_2, \ldots, q_{k-1}$, we have

$$\begin{aligned} n &= b^3q_2 + a_2b^2 + a_1b + a_0, \\ &\vdots \\ &= b^{k-1}q_{k-2} + a_{k-2}b^{k-2} + \cdots + a_1b + a_0, \\ &= b^kq_{k-1} + a_{k-1}b^{k-1} + \cdots + a_1b + a_0 \\ &= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0, \end{aligned}$$

where $0 \le a_j \le b - 1$ for $j = 0, 1, \ldots, k$ and $a_k \ne 0$, given that $a_k = q_{k-1}$ is the last nonzero quotient. Consequently, we have found an expansion of the desired type.

To see that the expansion is unique, assume that we have two such expansions equal to n, that is,

$$\begin{aligned} n &= a_kb^k + a_{k-1}b^{k-1} + \cdots + a_1b + a_0 \\ &= c_kb^k + c_{k-1}b^{k-1} + \cdots + c_1b + c_0, \end{aligned}$$

where $0 \le a_k < b$ and $0 \le c_k < b$ (and where, if necessary, we have added initial terms with zero coefficients to one of the expansions to have the number of terms agree). Subtracting one expansion from the other, we have

$$(a_k - c_k)b^k + (a_{k-1} - c_{k-1})b^{k-1} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

If the two expansions are different, there is a smallest integer j, $0 \le j \le k$, such that $a_j \ne c_j$. Hence,

$$b^j\big((a_k - c_k)b^{k-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)\big) = 0,$$

so that

$$(a_k - c_k)b^{k-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

Solving for $a_j - c_j$, we obtain

$$\begin{aligned} a_j - c_j &= (c_k - a_k)b^{k-j} + \cdots + (c_{j+1} - a_{j+1})b \\ &= b\big((c_k - a_k)b^{k-j-1} + \cdots + (c_{j+1} - a_{j+1})\big). \end{aligned}$$

Hence, we see that

$$b \mid (a_j - c_j).$$

But because $0 \leq a_j < b$ and $0 \leq c_j < b$, we know that $-b < a_j - c_j < b$. Consequently, $b \mid (a_j - c_j)$ implies that $a_j = c_j$. This contradicts the assumption that the two expansions are different. We conclude that our base b expansion of n is unique. ∎

For $b = 2$, we see by Theorem 2.1 that the following corollary holds.

Corollary 2.1.1. Every positive integer may be represented as the sum of distinct powers of 2. ∎

Proof. Let n be a positive integer. From Theorem 2.1 with $b = 2$, we know that $n = a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2 + a_0$, where each a_j is either 0 or 1. Hence, every positive integer is the sum of distinct powers of 2. ∎

In the expansions described in Theorem 2.1, b is called the *base* or *radix* of the expansion. We call base 10 notation, our conventional way of writing integers, *decimal* notation. Base 2 expansions are called *binary* expansions, base 8 expansions are called *octal* expansions, and base 16 expansions are called *hexadecimal*, or *hex* for short. The coefficients a_j are called the *digits* of the expansion. Binary digits are called *bits* (*b*inary dig*its*) in computer terminology.

To distinguish representations of integers with different bases, we use a special notation. We write $(a_k a_{k-1} \ldots a_1 a_0)_b$ to represent the number $a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$.

Example 2.1. To illustrate base b notation, note that $(236)_7 = 2 \cdot 7^2 + 3 \cdot 7 + 6 = 125$ and $(10010011)_2 = 1 \cdot 2^7 + 1 \cdot 2^4 + 1 \cdot 2^1 + 1 = 147$. ◀

The proof of Theorem 2.1 provides a method of finding the base b expansion $(a_k a_{k-1} \ldots a_1 a_0)_b$ of any positive integer n. Specifically, to find the base b expansion of n, we first divide n by b. The remainder is the digit a_0. Then, we divide the quotient $[n/b] = q_0$ by b. The remainder is the digit a_1. We continue this process, successively dividing the quotient obtained by b, to obtain the digits in the base b expansion of n. The process stops once a quotient of 0 is obtained. In other words, to find the base b expansion of n, we perform the division algorithm repeatedly, replacing the dividend each time with the quotient, and stop when we come to a quotient that is 0. We then read up the list of remainders to find the base b expansion. We illustrate this procedure in Example 2.2.

Example 2.2. To find the base 2 expansion of 1864, we use the division algorithm successively:

$$
\begin{aligned}
1864 &= 2 \cdot 932 + 0, \\
932 &= 2 \cdot 466 + 0, \\
466 &= 2 \cdot 233 + 0, \\
233 &= 2 \cdot 116 + 1, \\
116 &= 2 \cdot 58 + 0, \\
58 &= 2 \cdot 29 + 0, \\
29 &= 2 \cdot 14 + 1, \\
14 &= 2 \cdot 7 + 0, \\
7 &= 2 \cdot 3 + 1, \\
3 &= 2 \cdot 1 + 1, \\
1 &= 2 \cdot 0 + 1.
\end{aligned}
$$

To obtain the base 2 expansion of 1864, we simply take the remainders of these divisions. This shows that $(1864)_{10} = (11101001000)_2$. ◀

Computers represent numbers internally by using a series of "switches" that may be either "on" or "off." (This may be done mechanically, using magnetic tape, electrical switches, or by other means.) Hence, we have two possible states for each switch. We can use "on" to represent the digit 1 and "off" to represent the digit 0; this is why computers use binary expansions to represent integers internally.

Computers use base 8 or base 16 for display purposes. In base 16 (hexadecimal) notation there are 16 digits, usually denoted by 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. The letters A, B, C, D, E, and F are used to represent the digits that correspond to 10, 11, 12, 13, 14, and 15 (written in decimal notation). The following example demonstrates the conversion from hexadecimal to decimal notation.

Example 2.3. To convert $(\text{A35B0F})_{16}$ from hexadecimal to decimal notation, we write

$$
\begin{aligned}
(\text{A35B0F})_{16} &= 10 \cdot 16^5 + 3 \cdot 16^4 + 5 \cdot 16^3 + 11 \cdot 16^2 + 0 \cdot 16 + 15 \\
&= (10705679)_{10}.
\end{aligned}
$$

◀

A simple conversion is possible between binary and hexadecimal notation. We can write each hex digit as a block of four binary digits according to the correspondences given in Table 2.1.

Example 2.4. An example of conversion from hex to binary is $(\text{2FB3})_{16} = (10111110110011)_2$. Each hex digit is converted to a block of four binary digits (the initial zeros in the initial block $(0010)_2$ corresponding to the digit $(2)_{16}$ are omitted).

To convert from binary to hex, consider $(11110111101001)_2$. We break this into blocks of four, starting from the right. The blocks are, from right to left, 1001, 1110, 1101, and 0011 (with two initial zeros added). Translating each block to hex, we obtain $(\text{3DE9})_{16}$. ◀

Hex Digit	Binary Digits	Hex Digit	Binary Digits
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Table 2.1 *Conversion from hex digits to blocks of binary digits.*

We note that a conversion between two different bases is as easy as binary–hex conversion whenever one of the bases is a power of the other.

2.1 Exercises

1. Convert $(1999)_{10}$ from decimal to base 7 notation. Convert $(6105)_7$ from base 7 to decimal notation.
2. Convert $(89156)_{10}$ from decimal to base 8 notation. Convert $(706113)_8$ from base 8 to decimal notation.
3. Convert $(10101111)_2$ from binary to decimal notation and $(999)_{10}$ from decimal to binary notation.
4. Convert $(101001000)_2$ from binary to decimal notation and $(1984)_{10}$ from decimal to binary notation.
5. Convert $(100011110101)_2$ and $(11101001110)_2$ from binary to hexadecimal.
6. Convert $(\text{ABCDEF})_{16}$, $(\text{DEFACED})_{16}$, and $(\text{9A0B})_{16}$ from hexadecimal to binary.
7. Explain why we really are using base 1000 notation when we break large decimal integers into blocks of three digits, separated by commas.
8. Show that if b is a negative integer less than -1, then every nonzero integer n can be uniquely written in the form
$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$
where $a_k \neq 0$ and $0 \leq a_j < |\, b \,|$ for $j = 0, 1, 2, \ldots, k$. We write $n = (a_k a_{k-1} \ldots a_1 a_0)_b$, just as we do for positive bases.
9. Find the decimal representation of $(101001)_{-2}$ and $(12012)_{-3}$.
10. Find the base -2 representations of the decimal numbers -7, -17, and 61.
11. Show that any weight not exceeding $2^k - 1$ may be measured using weights of $1, 2, 2^2, \ldots, 2^{k-1}$, when all the weights are placed in one pan.

12. Show that every nonzero integer can be uniquely represented in the form

$$e_k 3^k + e_{k-1} 3^{k-1} + \cdots + e_1 3 + e_0,$$

where $e_j = -1, 0$, or 1 for $j = 0, 1, 2, \ldots, k$ and $e_k \neq 0$. This expansion is called a *balanced ternary expansion.*

13. Use Exercise 12 to show that any weight not exceeding $(3^k - 1)/2$ may be measured using weights of $1, 3, 3^2, \ldots, 3^{k-1}$, when the weights may be placed in either pan.

14. Explain how to convert from base 3 to base 9 notation, and from base 9 to base 3 notation.

15. Explain how to convert from base r to base r^n notation, and from base r^n to base r notation, when $r > 1$ and n are positive integers.

16. Show that if $n = (a_k a_{k-1} \ldots a_1 a_0)_b$, then the quotient and remainder when n is divided by b^j are $q = (a_k a_{k-1} \ldots a_j)_b$ and $r = (a_{j-1} \ldots a_1 a_0)_b$, respectively.

17. If the base b expansion of n is $n = (a_k a_{k-1} \ldots a_1 a_0)_b$, what is the base b expansion of $b^m n$?

One's complement representations of integers are used to simplify computer arithmetic. To represent positive and negative integers with absolute value less than 2^n, a total of $n + 1$ bits is used.

The leftmost bit is used to represent the sign. A 0 in this position is used for positive integers and a 1 in this position is used for negative integers.

For positive integers, the remaining bits are identical to the binary expansion of the integer. For negative integers, the remaining bits are obtained by first finding the binary expansion of the absolute value of the integer, and then taking the complement of each of these bits, where the complement of a 1 is a 0 and the complement of a 0 is a 1.

18. Find the one's complement representations, using bit strings of length six, of the following integers.

a) 22 c) -7
b) 31 d) -19

19. What integer does each of the following one's complement representations of length five represent?

a) 11001 c) 10001
b) 01101 d) 11111

20. How is the one's complement representation of $-m$ obtained from the one's complement of m, when bit strings of length n are used?

21. Show that if m is an integer with one's complement representation $a_{n-1} a_{n-2} \ldots a_1 a_0$, then $m = -a_{n-1}(2^{n-1} - 1) + \sum_{i=0}^{n-2} a_i 2^i$.

Two's complement representations of integers also are used to simplify computer arithmetic (in fact, they are used much more commonly than one's complement representations). To represent an integer x with $-2^{n-1} \leq x \leq 2^{n-1} - 1$, n bits are used.

The leftmost bit represents the sign, with a 0 used for positive integers and a 1 for negative integers.

For a positive integer, the remaining $n-1$ bits are identical to the binary expansion of the integer. For a negative integer, the remaining bits are the bits of the binary expansion of $2^{n-1} - |x|$.

22. Find the two's complement representations, using bit strings of length six, of the integers in Exercise 18.

23. What integers do the representations in Exercise 19 represent if each is the two's complement representation of an integer?

24. Show that if m is an integer with two's complement representation $a_{n-1}a_{n-2}\ldots a_1a_0$, then $m = -a_{n-1}\cdot 2^{n-1} + \sum_{i=0}^{n-2} a_i 2^i$.

25. How is the two's complement representation of $-m$ obtained from the two's complement representation of m, when bit strings of length n are used?

26. How can the two's complement representation of an integer be found from its one's complement representation?

27. Sometimes integers are encoded by using four-digit binary expansions to represent each decimal digit. This produces the *binary coded decimal* form of the integer. For instance, 791 is encoded in this way by 011110010001. How many bits are required to represent a number with n decimal digits using this type of encoding?

A *Cantor expansion* of a positive integer n is a sum

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1!,$$

where each a_j is an integer with $0 \leq a_j \leq j$ and $a_m \neq 0$.

28. Find Cantor expansions of 14, 56, and 384.

* **29.** Show that every positive integer has a unique Cantor expansion. (*Hint:* For each positive integer n there is a positive integer m such that $m! \leq n < (m+1)!$. For a_m, take the quotient from the division algorithm when n is divided by $m!$, then iterate.)

The Chinese game of *nim* is played as follows. There are several piles of matches, each containing an arbitrary number of matches at the start of the game. To make a move a player removes one or more matches from one of the piles. The players take turns, and the player who removes the last match wins the game.

A *winning position* is an arrangement of matches in piles such that if a player can move to this position, then (no matter what the second player does) the first player can continue to play in a way that will win the game. An example is the position where there are two piles, each containing one match; this is a winning position, because the second player must remove a match, leaving the first player the opportunity to win by removing the last match.

30. Show that the position in nim where there are two piles, each with two matches, is a winning position.

31. For each arrangement of matches into piles, write the number of matches in each pile in binary notation, and then line up the digits of these numbers into columns (adding initial zeros where necessary). Show that a position is a winning one if and only if the number of 1s in each column is even. (For example: Three piles of 3, 4, and 7 give

$$\begin{array}{ccc} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{array}$$

where each column has exactly two 1s.) (*Hint:* Show that any move from a winning position produces a nonwinning one. Show that there is a move from any nonwinning position to a winning one.)

Let a be an integer with a four-digit decimal expansion, where not all digits are the same. Let a' be the integer with a decimal expansion obtained by writing the digits of a in descending order, and let a'' be the integer with a decimal expansion obtained by writing the digits of a in ascending order. Define $T(a) = a' - a''$. For instance, $T(7318) = 8731 - 1378 = 7353$.

* **32.** Show that the only integer with a four-digit decimal expansion (where not all digits are the same) such that $T(a) = a$ is $a = 6174$. The integer 6174 is called *Kaprekar's constant,* after the Indian mathematician *D. R. Kaprekar*, because it is the only integer with this property.

** **33.** a) Show that if a is a positive integer with a four-digit decimal expansion where not all digits are the same, then the sequence $a, T(a), T(T(a)), T(T(T(a))), \ldots$, obtained by iterating T, eventually reaches the integer 6174.

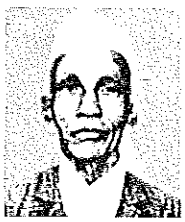
b) Determine the maximum number of steps required for the sequence defined in part (a) to reach 6174.

Let b be a positive integer and let a be an integer with a four-digit base b expansion, with not all digits the same. Define $T_b(a) = a' - a''$, where a' is the integer with base b expansion obtained by writing the base b digits of a in descending order, and a'' is the integer with base b expansion obtained by writing the base b digits of a in ascending order.

** **34.** Let $b = 5$. Find the unique integer a_0 with a four-digit base 5 expansion such that $T_5(a_0) = a_0$. Show that this integer a_0 is a Kaprekar constant for base 5; in other words, that $a, T(a), T(T(a)), T(T(T(a))), \ldots$ eventually reaches a_0, whenever a is an integer with a four-digit base 5 expansion where not all digits are the same.

* **35.** Show that no Kaprekar constant exists for four-digit numbers to the base 6.

* **36.** Determine whether there is a Kaprekar constant for three-digit integers to the base 10. Prove that your answer is correct.



D. R. KAPREKAR (1905–1986) was born in Dahanu, India, and was interested in numbers even as a small child. He received his secondary school education in Thana and studied at Ferguson College in Poona. Kaprekar attended the University of Bombay, receiving his bachelor's degree in 1929. From 1930 until his retirement in 1962, he worked as a schoolteacher in Devlali, India. Kaprekar discovered many interesting properties in recreational number theory. He published extensively, writing about such topics as recurring decimals, magic squares, and integers with special properties.

2.1 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 binary, octal, and hexadecimal expansions of each of the following integers.

   a) 9876543210 b) 1111111111 c) 10000000001

2. Find the decimal expansion of each of the following integers.

   a) $(1010101010101)_2$ b) $(765432101234567)_8$ c) $(\text{ABBAFADACABA})_{16}$

3. Evaluate each of the following sums, expressing your answer in the same base used to represent the summands.

   a) $(11011011011011011)_2 + (10010010010010010001)_2$

   b) $(12345670123456)_8 + (765432107654321)_8$

   c) $(123456789\text{ABCD})_{16} + (\text{BABACACADADA})_{16}$

4. Find the Cantor expansions of the integers 100,000, 10,000,000, and 1,000,000,000. (See the preamble to Exercise 28 for the definition of Cantor expansions.)

5. Verify the result described in Exercise 33 for several different four-digit integers, in which not all digits are the same.

6. Use numerical evidence to make conjectures about the behavior of the sequence $a, T(a), T(T(a)), \ldots$ where a is a five-digit integer in base 10 notation in which not all digits are the same, and $T(a)$ is defined as in the preamble to Exercise 32.

7. Explore the behavior for different bases b of the sequence $a, T(a), T(T(a)), \ldots$ where a is a three-digit integer in base b notation. What conjectures can you make? Repeat your exploration using four-digit and then five-digit integers in base b notation.

Programming Projects

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

1. Find the binary expansion of an integer from the decimal expansion of this integer, and vice versa.

2. Convert from base b_1 notation to base b_2 notation, where b_1 and b_2 are arbitrary positive integers greater than 1.

3. Convert from binary notation to hexadecimal notation, and vice versa.

4. Find the base (-2) notation of an integer from its decimal notation (see Exercise 8).

5. Find the balanced ternary expansion of an integer from its decimal expansion (see Exercise 12).

6. Find the Cantor expansion of an integer from its decimal expansion (see the preamble to Exercise 28).

7. Play a winning strategy in the game of nim (see the preamble to Exercise 30).

* 8. Investigate the sequence $a, T(a), T(T(a)), T(T(T(a))), \ldots$ (defined in the preamble to Exercise 32), where a is a positive integer, to discover the minimum number of iterations required to reach 6174.

2.2 Computer Operations with Integers

Before computers were invented, mathematicians did computations either by hand or by using mechanical devices. Either way, they were only able to work with integers of rather limited size. Many number theoretic problems, such as factoring and primality testing, require computations with integers of as many as 100 or even 200 digits. In this section, we will study some of the basic algorithms for doing computer arithmetic. In the following section, we will study the number of basic computer operations required to carry out these algorithms.

We have mentioned that computers internally represent numbers using bits, or binary digits. Computers have a built-in limit on the size of integers that can be used in machine arithmetic. This upper limit is called the *word size,* which we denote by w. The word size is usually a power of 2, such as 2^{32} for Pentium machines or 2^{35}, although sometimes the word size is a power of 10.

To do arithmetic with integers larger than the word size, it is necessary to devote more than one word to each integer. To store an integer $n > w$, we express n in base w notation, and for each digit of this expansion we use one computer word. For instance, if the word size is 2^{35}, using ten computer words we can store integers as large as $2^{350} - 1$, since integers less than 2^{350} have no more than ten digits in their base 2^{35} expansions. Also note that to find the base 2^{35} expansion of an integer, we need only group together blocks of 35 bits.

The first step in discussing computer arithmetic with large integers is to describe how the basic arithmetic operations are methodically performed.

We will describe the classical methods for performing the basic arithmetic operations with integers in base r notation, where $r > 1$ is an integer. These methods are examples of *algorithms.*

Definition. An *algorithm* is a finite set of precise instructions for performing a computation or for solving a problem.

We will describe algorithms for performing addition, subtraction, and multiplication of two n-digit integers $a = (a_{n-1}a_{n-2} \ldots a_1a_0)_r$ and $b = (b_{n-1}b_{n-2} \ldots b_1b_0)_r$, where initial digits of zero are added if necessary to make both expansions the same length. The algorithms described are used for both binary arithmetic with integers less than the word size of a computer, and *multiple precision* arithmetic with integers larger than the word size w, using w as the base.

Addition When we add a and b, we obtain the sum

$$a + b = \sum_{j=0}^{n-1} a_j r^j + \sum_{j=0}^{n-1} b_j r^j = \sum_{j=0}^{n-1} (a_j + b_j) r^j.$$

To find the base r expansion of $a + b$, first note that by the division algorithm, there are integers C_0 and s_0 such that

$$a_0 + b_0 = C_0 r + s_0, \quad 0 \leq s_0 < r.$$

Because a_0 and b_0 are positive integers not exceeding r, we know that $0 \leq a_0 + b_0 \leq 2r - 2$, so that $C_0 = 0$ or 1; here, C_0 is the *carry* to the next place. Next, we find that there are integers C_1 and s_1 such that

$$a_1 + b_1 + C_0 = C_1 r + s_1, \quad 0 \leq s_1 < r.$$

Since $0 \leq a_1 + b_1 + C_0 \leq 2r - 1$, we know that $C_1 = 0$ or 1. Proceeding inductively, we find integers C_i and s_i for $1 \leq i \leq n - 1$ by

$$a_i + b_i + C_{i-1} = C_i r + s_i, \quad 0 \leq s_i < r,$$

with $C_i = 0$ or 1. Finally, we let $s_n = C_{n-1}$, since the sum of two integers with n digits has $n + 1$ digits when there is a carry in the nth place. We conclude that the base r expansion for the sum is $a + b = (s_n s_{n-1} \ldots s_1 s_0)_r$.

When performing base r addition by hand, we can use the same familiar technique as is used in decimal addition.

Example 2.5. To add $(1101)_2$ and $(1001)_2$, we write

$$\begin{array}{cccccc} & \textit{1} & & \textit{1} & & \\ & 1 & 1 & 0 & 1 & \\ + & 1 & 0 & 0 & 1 & \\ \hline 1 & 0 & 1 & 1 & 0 & \end{array}$$

where we have indicated carries by 1s in italics written above the appropriate column. We found the binary digits of the sum by noting that $1 + 1 = 1 \cdot 2 + 0, 0 + 0 + 1 = 0 \cdot 2 + 1, 1 + 0 + 0 = 0 \cdot 2 + 1$, and $1 + 1 + 0 = 1 \cdot 2 + 0$. ◀

Subtraction Assume that $a > b$. Consider

$$a - b = \sum_{j=0}^{n-1} a_j r^j - \sum_{j=0}^{n-1} b_j r^j = \sum_{j=0}^{n-1} (a_j - b_j) r^j.$$

Note that by the division algorithm, there are integers B_0 and d_0 such that

$$a_0 - b_0 = B_0 r + d_0, \quad 0 \leq d_0 < r,$$

Where the Word "Algorithm" Comes from

"Algorithm" is a corruption of the original term "algorism," which originally comes from the name of the author of the ninth-century book *Kitab al-jabr w'al-muqabala (Rules of Restoration and Reduction), Abu Ja'far Mohammed ibn Mûsâ al-Khwârizmî* (see his biography included on the next page). The word "algorism" originally referred only to the rules of performing arithmetic using Hindu-Arabic numerals, but evolved into "algorithm" by the eighteenth century. With growing interest in computing machines, the concept of an algorithm became more general, to include all definite procedures for solving problems, not just the procedures for performing arithmetic with integers expressed in Arabic notation.

and because a_0 and b_0 are positive integers less than r, we have

$$-(r-1) \leq a_0 - b_0 \leq r - 1.$$

When $a_0 - b_0 \geq 0$, we have $B_0 = 0$. Otherwise, when $a_0 - b_0 < 0$, we have $B_0 = -1$; B_0 is the *borrow* from the next place of the base r expansion of a. We use the division algorithm again to find integers B_1 and d_1 such that

$$a_1 - b_1 + B_0 = B_1 r + d_1, \quad 0 \leq d_1 < r.$$

From this equation, we see that the borrow $B_1 = 0$ as long as $a_1 - b_1 + B_0 \geq 0$, and that $B_1 = -1$ otherwise, because $-r \leq a_1 - b_1 + B_0 \leq r - 1$. We proceed inductively to find integers B_i and d_i, such that

$$a_i - b_i + B_{i-1} = B_i r + d_i, \quad 0 \leq d_i < r$$

with $B_i = 0$ or -1, for $1 \leq i \leq n-1$. We see that $B_{n-1} = 0$, because $a > b$. We can conclude that

$$a - b = (d_{n-1} d_{n-2} \ldots d_1 d_0)_r.$$

When performing base r subtraction by hand, we use the familiar technique used in decimal subtraction.

Example 2.6. To subtract $(10110)_2$ from $(11011)_2$, we have

$$\begin{array}{cccccc} & & \textit{-1} & & & \\ 1 & 1 & 0 & 1 & 1 \\ -1 & 0 & 1 & 1 & 0 \\ \hline & & & 1 & 0 & 1 \end{array}$$

where the -1 in italics above a column indicates a borrow. We found the binary digits of the difference by noting that $1 - 0 = 0 \cdot 2 + 1$, $1 - 1 + 0 = 0 \cdot 2 + 0$, $0 - 1 + 0 = -1 \cdot 2 + 1$, $1 - 0 - 1 = 0 \cdot 2 + 0$, and $1 - 1 + 0 = 0 \cdot 2 + 0$. ◀

ABU JA'FAR MOHAMMED IBN MÛSÂ AL-KHWÂRIZMÎ (c. 780–c. 850), an astronomer and mathematician, was a member of the House of Wisdom, an academy of scientists in Baghdad. The name al-Khwârizmî means "from the town of Kowarzizm," now known as Khiva in modern Uzbekistan. Al-Khwârizmî was the author of books on mathematics, astronomy, and geography. People in the West first learned about algebra from his works; the word "algebra" comes from *al-jabr*, part of the title of his book *Kitab al-jabr w'al muqabala*, which was translated into Latin and widely used as a text. Another book describes procedures for arithmetic operations using Hindu-Arabic numerals.

Multiplication Before discussing multiplication, we describe *shifting*. To multiply $(a_{n-1} \dots a_1 a_0)_r$ by r^m, we need only shift the expansion left m places, appending the expansion with m zero digits.

Example 2.7. To multiply $(101101)_2$ by 2^5, we shift the digits to the left five places and append the expansion with five zeros, obtaining $(10110100000)_2$. ◀

We first discuss the multiplication of an n-place integer by a one-digit integer. To multiply $(a_{n-1} \dots a_1 a_0)_r$ by $(b)_r$, we first note that

$$a_0 b = q_0 r + p_0, \quad 0 \le p_0 < r,$$

and $0 \le q_0 \le r - 2$, because $0 \le a_0 b \le (r-1)^2$. Next, we have

$$a_1 b + q_0 = q_1 r + p_1, \quad 0 \le p_1 < r,$$

and $0 \le q_1 \le r - 1$. In general, we have

$$a_i b + q_{i-1} = q_i r + p_i, \quad 0 \le p_i < r,$$

and $0 \le q_i \le r - 1$. Furthermore, we have $p_n = q_{n-1}$. This yields $(a_{n-1} \dots a_1 a_0)_r (b)_r = (p_n p_{n-1} \cdots p_1 p_0)_r$.

To perform a multiplication of two n-place integers, we write

$$ab = a\left(\sum_{j=0}^{n-1} b_j r^j\right) = \sum_{j=0}^{n-1} (a b_j) r^j.$$

For each j, we first multiply a by the digit b_j, then shift j places to the left, and finally add all of the n integers we have obtained to find the product.

When multiplying two integers with base r expansions, we use the familiar method of multiplying decimal integers by hand.

Example 2.8. To multiply $(1101)_2$ and $(1110)_2$, we write

$$\begin{array}{r} 1\ 1\ 0\ 1 \\ \times\ 1\ 1\ 1\ 0 \\ \hline 0\ 0\ 0\ 0 \\ 1\ 1\ 0\ 1 \\ 1\ 1\ 0\ 1 \\ 1\ 1\ 0\ 1 \\ \hline 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0 \end{array}$$

Note that we first multiplied $(1101)_2$ by each digit of $(1110)_2$, shifting each time by the appropriate number of places, and then we added the appropriate integers to find our product. ◀

Division We wish to find the quotient q in the division algorithm

$$a = bq + R, \quad 0 \leq R < b.$$

If the base r expansion of q is $q = (q_{n-1}q_{n-2} \cdots q_1q_0)_r$, then we have

$$a = b\left(\sum_{j=0}^{n-1} q_j r^j\right) + R, \quad 0 \leq R < b.$$

To determine the first digit q_{n-1} of q, notice that

$$a - bq_{n-1}r^{n-1} = b\left(\sum_{j=0}^{n-2} q_j r^j\right) + R.$$

The right-hand side of this equation is not only positive, but also less than br^{n-1}, because $\sum_{j=0}^{n-2} q_j r^j \leq \sum_{j=0}^{n-2}(r-1)r^j = \sum_{j=1}^{n-1} r^j - \sum_{j=0}^{n-2} r^j = r^{n-1} - 1$. Therefore, we know that

$$0 \leq a - bq_{n-1}r^{n-1} < br^{n-1}.$$

This tells us that

$$q_{n-1} = \left\lfloor \frac{a}{br^{n-1}} \right\rfloor.$$

We can obtain q_{n-1} by successively subtracting br^{n-1} from a until we obtain a negative result; q_{n-1} is then one less than the number of subtractions.

To find the other digits of q, we define the sequence of *partial remainders* R_i by

$$R_0 = a$$

and

$$R_i = R_{i-1} - bq_{n-i}r^{n-i}$$

for $i = 1, 2, \ldots, n$. By mathematical induction, we show that

$$R_i = \left(\sum_{j=0}^{n-i-1} q_j r^j\right)b + R. \tag{2.1}$$

For $i = 0$, this is clearly correct, because $R_0 = a = qb + R$. Now, assume that

$$R_k = \left(\sum_{j=0}^{n-k-1} q_j r^j\right)b + R.$$

Then

$$\begin{aligned} R_{k+1} &= R_k - bq_{n-k-1}r^{n-k-1} \\ &= \left(\sum_{j=0}^{n-k-1} q_j r^j\right) b + R - bq_{n-k-1}r^{n-k-1} \\ &= \left(\sum_{j=0}^{n-(k+1)-1} q_j r^j\right) b + R, \end{aligned}$$

establishing (2.1).

By (2.1) we see that $0 \leq R_i < r^{n-i}b$, for $i = 1, 2, \ldots, n$, because $\sum_{j=0}^{n-i-1} q_j r^j \leq r_{n-i} - 1$. Consequently, because $R_i = R_{i-1} - bq_{n-i}r^{n-i}$ and $0 \leq R_i < r^{n-1}b$, we see that the digit q_{n-i} is given by $[R_{i-1}/(br^{n-i})]$ and can be obtained by successively subtracting br^{n-i} from R_{i-1} until a negative result is obtained, and then q_{n-i} is one less than the number of subtractions. This is how we find the digits of q.

Example 2.9. To divide $(11101)_2$ by $(111)_2$, we let $q = (q_2q_1q_0)_2$. We subtract $2^2(111)_2 = (11100)_2$ once from $(11101)_2$ to obtain $(1)_2$, and once more to obtain a negative result, so that $q_2 = 1$. Now, $R_1 = (11101)_2 - (11100)_2 = (1)_2$. We find that $q_1 = 0$, because $R_1 - 2(111)_2$ is less than zero, and likewise $q_0 = 0$. Hence, the quotient of the division is $(100)_2$ and the remainder is $(1)_2$. ◀

2.2 Exercises

1. Add $(101111011)_2$ and $(1100111011)_2$.
2. Add $(10001000111101)_2$ and $(11111101011111)_2$.
3. Subtract $(11010111)_2$ from $(1111000011)_2$.
4. Subtract $(101110101)_2$ from $(1101101100)_2$.
5. Multiply $(11101)_2$ and $(110001)_2$.
6. Multiply $(1110111)_2$ and $(10011011)_2$.
7. Find the quotient and remainder when $(110011111)_2$ is divided by $(1101)_2$.
8. Find the quotient and remainder when $(110100111)_2$ is divided by $(11101)_2$.
9. Add $(1234321)_5$ and $(2030104)_5$.
10. Subtract $(434421)_5$ from $(4434201)_5$.
11. Multiply $(1234)_5$ and $(3002)_5$.
12. Find the quotient and remainder when $(14321)_5$ is divided by $(334)_5$.
13. Add $(ABAB)_{16}$ and $(BABA)_{16}$.
14. Subtract $(CAFE)_{16}$ from $(FEED)_{16}$.
15. Multiply $(FACE)_{16}$ and $(BAD)_{16}$.
16. Find the quotient and remainder when $(BEADED)_{16}$ is divided by $(ABBA)_{16}$.

17. Explain how to add, subtract, and multiply the integers 18235187 and 22135674 on a computer with word size 1000.

18. Write algorithms for the basic operations with integers in base (-2) notation (see Exercise 8 of Section 2.1).

19. How is the one's complement representation of the sum of two integers obtained from the one's complement representations of those integers?

20. How is the one's complement representation of the difference of two integers obtained from the one's complement representations of those integers?

21. Give an algorithm for adding and an algorithm for subtracting Cantor expansions (see the preamble to Exercise 28 of Section 2.1).

22. A *dozen* equals 12, and a *gross* equals 12^2. Using base 12, or *duodecimal* arithmetic, answer the following questions.
    a) If 3 gross, 7 dozen, and 4 eggs are removed from a total of 11 gross and 3 dozen eggs, how many eggs are left?
    b) If 5 truckloads of 2 gross, 3 dozen, and 7 eggs each are delivered to the supermarket, how many eggs are delivered?
    c) If 11 gross, 10 dozen, and 6 eggs are divided in 3 groups of equal size, how many eggs are in each group?

23. A well-known rule used to find the square of an integer with decimal expansion $(a_n a_{n-1} \ldots a_1 a_0)_{10}$ and final digit $a_0 = 5$ is to find the decimal expansion of the product $(a_n a_{n-1} \ldots a_1)_{10}[(a_n a_{n-1} \ldots a_1)_{10} + 1]$, and append this with the digits $(25)_{10}$. For instance, we see that the decimal expansion of $(165)^2$ begins with $16 \cdot 17 = 272$, so that $(165)^2 = 27225$. Show that this rule is valid.

24. In this exercise, we generalize the rule given in Exercise 23 to find the squares of integers with final base $2B$ digit B, where B is a positive integer. Show that the base $2B$ expansion of the integer $(a_n a_{n-1} \ldots a_1 a_0)_{2B}$ starts with the digits of the base $2B$ expansion of the integer $(a_n a_{n-1} \ldots a_1)_{2B}\,[(a_n a_{n-1} \ldots a_1)_{2B} + 1]$ and ends with the digits $B/2$ and 0 when B is even, and the digits $(B-1)/2$ and B when B is odd.

2.2 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. Verify the rules given in Exercises 23 and 24 for examples of your choice.

Programming Projects

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

1. Perform addition with arbitrarily large integers.
2. Perform subtraction with arbitrarily large integers.
3. Multiply two arbitrarily large integers using the conventional algorithm.
4. Divide arbitrarily large integers, finding the quotient and remainder.

2.3 Complexity of Integer Operations

Once an algorithm has been specified for an operation, we can consider the amount of time required to perform this algorithm on a computer. We will measure the amount of time in terms of *bit operations*. By a bit operation we mean the addition, subtraction, or multiplication of two binary digits, the division of a two-bit by a one-bit integer (obtaining a quotient and a remainder), or the shifting of a binary integer one place. (The actual amount of time required to carry out a bit operation on a computer varies depending on the computer architecture and capacity.) When we describe the number of bit operations needed to perform an algorithm, we are describing the *computational complexity* of this algorithm.

In describing the number of bit operations needed to perform calculations, we will use *big-O* notation. Big-O notation provides an upper bound on the size of a function in terms of a particular well-known reference function whose size at large values is easily understood.

To motivate the definition of this notation, consider the following situation. Suppose that to perform a specified operation on an integer n requires at most $n^3 + 8n^2 \log n$ bit operations. Since $8n^2 \log n < 8n^3$ for every positive integer, less than $9n^3$ bit operations are required for this operation for every integer n. Since the number of bit operations required is always less than a constant times n^3, namely $9n^3$, we say that $O(n^3)$ bit operations are needed. In general, we have the following definition.

Definition. If f and g are functions taking positive values, defined for all $x \in S$, where S is a specified set of real numbers, then f is $O(g)$ on S if there is a positive constant K such that $f(x) < Kg(x)$ for all sufficiently large $x \in S$. (Normally, we take S to be the set of positive integers, and we drop all reference to S.)

Big-O notation is used extensively throughout number theory and in the analysis of algorithms. *Paul Bachmann* introduced big-O notation in 1892 ([Ba94]). The big-O notation is sometimes called a Landau symbol, after *Edmund Landau*, who used this notation throughout his work in the estimation of various functions in number theory. The use of big-O notation in the analysis of algorithms was popularized by renowned computer scientist *Donald Knuth*.

We illustrate this concept of big-O notation with several examples.

Example 2.10. We can show on the set of positive integers that $n^4 + 2n^3 + 5$ is $O(n^4)$. To do this, note that $n^4 + 2n^3 + 5 \leq n^4 + 2n^4 + 5n^4 = 8n^4$ for all positive integers. (We take $K = 8$ in the definition.) The reader should also note that n^4 is $O(n^4 + 2n^3 + 5)$. ◀

Example 2.11. We can easily give a big-O estimate for $\sum_{j=1}^{n} j$. Noting that each summand is less than n tells us that $\sum_{j=1}^{n} j \leq \sum_{j=1}^{n} n = n \cdot n = n^2$. Note that we could also derive this estimate easily from the formula $\sum_{j=1}^{n} j = n(n+1)/2$. ◀

We now will give some useful results for working with big-O estimates for combinations of functions.

Theorem 2.2. If f is $O(g)$ and c is a positive constant, then cf is $O(g)$.

Proof. If f is $O(g)$, then there is a constant K with $f(x) < Kg(x)$ for all x under consideration. Hence $cf(x) < (cK)g(x)$, so cf is $O(g)$. ∎

Theorem 2.3. If f_1 is $O(g_1)$ and f_2 is $O(g_2)$, then $f_1 + f_2$ is $O(g_1 + g_2)$, and $f_1 f_2$ is $O(g_1 g_2)$.

Proof. If f is $O(g_1)$ and f_2 is $O(g_2)$, then there are constants K_1 and K_2 such that $f_1(x) < K_1 g_1(x)$ and $f_2(x) < K_2 g_2(x)$ for all x under consideration. Hence,

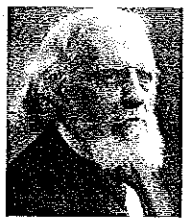
$$\begin{aligned} f_1(x) + f_2(x) &< K_1 g_1(x) + K_2 g_2(x) \\ &\leq K(g_1(x) + g_2(x)), \end{aligned}$$

where K is the maximum of K_1 and K_2. Hence, $f_1 + f_2$ is $O(g_1 + g_2)$.

Also,

$$\begin{aligned} f_1(x) f_2(x) &< K_1 g_1(x) K_2 g_2(x) \\ &= (K_1 K_2)(g_1(x) g_2(x)), \end{aligned}$$

so $f_1 f_2$ is $O(g_1 g_2)$. ∎



PAUL GUSTAV HEINRICH BACHMANN (1837–1920), the son of a pastor, shared his father's pious lifestyle, as well as his love of music. His talent for mathematics was discovered by one of his early teachers. After recovering from tuberculosis, he studied at the University of Berlin and later in Göttingen, where he attended lectures presented by Dirichlet. In 1862, he received his doctorate under the supervision of the number theorist Kummer. Bachmann became a professor at Breslau and later at Münster. After retiring, he continued mathematical research, played the piano, and served as a music critic for newspapers. His writings include a five-volume survey of number theory, a two-volume work on elementary number theory, a book on irrational numbers, and a book on Fermat's last theorem (this theorem is discussed in Chapter 13). Bachmann introduced big-O notation in 1892.

EDMUND LANDAU (1877–1938) was the son of a Berlin gynecologist, and attended high school in Berlin. He received his doctorate in 1899 under the direction of Frobenius. Landau first taught at the University of Berlin and then moved to Göttingen, where he was full professor until the Nazis forced him to stop teaching. His main contributions to mathematics were in the field of analytic number theory; he established several important results concerning the distribution of primes. He authored a three-volume work on number theory and many other books on mathematical analysis and analytic number theory.

Corollary 2.3.1. If f_1 and f_2 are $O(g)$, then $f_1 + f_2$ is $O(g)$.

Proof. Theorem 2.3 tells us that $f_1 + f_2$ is $O(2g)$. But if $f_1 + f_2 < K(2g)$, then $f_1 + f_2 < (2K)g$, so $f_1 + f_2$ is $O(g)$. ■

The goal in using big-O estimates is to give the best big-O estimate possible while using the simplest reference function possible. Well-known reference functions used in big-O estimates include 1, $\log n$, n, $n \log n$, $n \log n \log \log n$, n^2, and 2^n, as well as some other important functions. Calculus can be used to show that each function in this list is smaller than the next function in the list, in the sense that the ratio of the function and the next function tends to 0 as n grows without bound. Note that more complicated functions than these occur in big-O estimates, as you will see in later chapters.

We illustrate how to use theorems for working with big-O estimates with the following example.

Example 2.12. To give a big-O estimate for $(n + 8 \log n)\ (10n \log n + 17n^2)$, first note that $n + 8 \log n$ is $O(n)$ and $10n \log n + 17n^2$ is $O(n^2)$ (because $\log n$ is $O(n)$ and $n \log n$ is $O(n^2)$) by Theorems 2.2 and 2.3 and Corollary 2.3.1. By Theorem 2.3, we see that $(n + 8 \log n)(10n \log n + 17n^2)$ is $O(n^3)$. ◄

Using big-O notation, we can see that to add or subtract two n-bit integers takes $O(n)$ bit operations, whereas to multiply two n-bit integers in the conventional way takes $O(n^2)$ bit operations (see Exercises 12 and 13 at the end of this section). Surprisingly,

DONALD KNUTH (b. 1938) grew up in Milwaukee where his father owned a small printing business and taught bookkeeping. He was an excellent student who also applied his intelligence in unconventional ways, such as finding more than 4500 words that could be spelled from the letters in "Ziegler's Giant Bar," winning a television set for his school and candy bars for everyone in his class.

Knuth graduated from Case Institute of Technology in 1960 with B.S. and M.S. degrees in mathematics, by special award of the faculty who considered his work outstanding. At Case he managed the basketball team and applied his mathematical talents by evaluating each player using a formula he developed (receiving coverage on CBS television and in *Newsweek*). Knuth received his doctorate in 1963 from the California Institute of Technology.

Knuth taught at the California Institute of Technology and Stanford University, retiring in 1992 to concentrate on writing. He is especially interested in updating and adding to his famous series, *The Art of Computer Programming*. This series has had a profound influence on the development of computer science. Knuth is the founder of the modern study of computational complexity and has made fundamental contributions to the theory of compilers. Knuth has also invented the widely used TeX and Metafont systems used for mathematical (and general) typography. TeX played an important role in the development of HTML and the Internet. He popularized the big-O notation in his work on the analysis of algorithms.

Knuth has written for a wide range of professional journals in computer science and mathematics. However, his first publication, in 1957, when he was a college freshman, was the "The Potrzebie System of Weights and Measures," a parody of the metric system, which appeared in *MAD Magazine*.

there are faster algorithms for multiplying large integers. To develop one such algorithm, we first consider the multiplication of two $2n$-bit integers, say $a = (a_{2n-1}a_{2n-2}\ldots a_1a_0)_2$ and $b = (b_{2n-1}b_{2n-2}\ldots b_1b_0)_2$. We write

$$a = 2^nA_1 + A_0 \quad b = 2^nB_1 + B_0,$$

where

$$A_1 = (a_{2n-1}a_{2n-2}\ldots a_{n+1}a_n)_2 \quad A_0 = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$$
$$B_1 = (b_{2n-1}b_{2n-2}\ldots b_{n+1}b_n)_2 \quad B_0 = (b_{n-1}b_{n-2}\ldots b_1b_0)_2.$$

We will use the identity

$$ab = (2^{2n} + 2^n)A_1B_1 + 2^n(A_1 - A_0)(B_0 - B_1) + (2^n + 1)A_0B_0. \tag{2.2}$$

To find the product of a and b using (2.2) requires that we perform three multiplications of n-bit integers (namely, A_1B_1, $(A_1 - A_0)(B_0 - B_1)$, and A_0B_0), as well as a number of additions and shifts. This is illustrated by the following example.

Example 2.13. We can use (2.2) to multiply $(1101)_2$ and $(1011)_2$. We have $(1101)_2 = 2^2(11)_2 + (01)_2$ and $(1011)_2 = 2^2(10)_2 + (11)_2$. Using (2.2), we find that

$$\begin{aligned}(1101)_2(1011)_2 &= (2^4 + 2^2)(11)_2(10)_2 + 2^2((11)_2 - (01)_2)\cdot((11)_2 - (10)_2) + \\ &\qquad (2^2 + 1)(01)_2(11)_2 \\ &= (2^4 + 2^2)(110)_2 + 2^2(10)_2(01)_2 + (2^2 + 1)(11)_2 \\ &= (1100000)_2 + (11000)_2 + (1000)_2 + (1100)_2 + (11)_2 \\ &= (10001111)_2.\end{aligned}$$

◀

We will now estimate the number of bit operations required to multiply two n-bit integers by using (2.2) repeatedly. If we let $M(n)$ denote the number of bit operations needed to multiply two n-bit integers, we find from (2.2) that

$$M(2n) \leq 3M(n) + Cn, \tag{2.3}$$

where C is a constant, because each of the three multiplications of n-bit integers takes $M(n)$ bit operations, whereas the number of additions and shifts needed to compute ab via (2.2) does not depend on n, and each of these operations takes $O(n)$ bit operations.

From (2.3), using mathematical induction, we can show that

$$M(2^k) \leq c(3^k - 2^k), \tag{2.4}$$

where c is the maximum of the quantities $M(2)$ and C (the constant in (2.3)). To carry out the induction argument, we first note that with $k = 1$, we have $M(2) \leq c(3^1 - 2^1) = c$, because c is the maximum of $M(2)$ and C.

As the induction hypothesis, we assume that

$$M(2^k) \leq c(3^k - 2^k).$$

Then, using (2.3), we have

$$\begin{aligned} M(2^{k+1}) &\leq 3M(2^k) + C2^k \\ &\leq 3c(3^k - 2^k) + C2^k \\ &\leq c3^{k+1} - c \cdot 3 \cdot 2^k + c2^k \\ &\leq c(3^{k+1} - 2^{k+1}). \end{aligned}$$

This establishes that (2.4) is valid for all positive integers k.

Using inequality (2.4), we can prove the following theorem.

Theorem 2.4. Multiplication of two n-bit integers can be performed using $O(n^{\log_2 3})$ bit operations. (*Note:* $\log_2 3$ is approximately 1.585, which is considerably less than the exponent 2 that occurs in the estimate of the number of bit operations needed for the conventional multiplication algorithm.)

Proof. From (2.4), we have

$$\begin{aligned} M(n) = M(2^{\log_2 n}) &\leq M(2^{[\log_2 n]+1}) \\ &\leq c(3^{[\log_2 n]+1} - 2^{[\log_2 n]+1}) \\ &\leq 3c \cdot 3^{[\log_2 n]} \leq 3c \cdot 3^{\log_2 n} = 3cn^{\log_2 3} \quad (\textit{because } 3^{\log_2 n} = n^{\log_2 3}). \end{aligned}$$

Hence, $M(n)$ is $O(n^{\log_2 3})$. ∎

We now state, without proof, two pertinent theorems. Proofs may be found in [Kn97] or [Kr79].

Theorem 2.5. Given a positive number $\epsilon > 0$, there is an algorithm for multiplication of two n-bit integers using $O(n^{1+\epsilon})$ bit operations.

Note that Theorem 2.4 is a special case of Theorem 2.5 with $\epsilon = \log_2 3 - 1$, which is approximately 0.585.

Theorem 2.6. There is an algorithm to multiply two n-bit integers using $O(n \log_2 n \log_2 \log_2 n)$ bit operations.

Since $\log_2 n$ and $\log_2 \log_2 n$ are much smaller than n^ϵ for large numbers n, Theorem 2.6 is an improvement over Theorem 2.5. Although we know that $M(n)$ is $O(n \log_2 n \log_2 \log_2 n)$, for simplicity we will use the obvious fact that $M(n)$ is $O(n^2)$ in our subsequent discussions.

The conventional algorithm described in Section 2.2 performs a division of a $2n$-bit integer by an n-bit integer with $O(n^2)$ bit operations. However, the number of bit operations needed for integer division can be related to the number of bit operations needed for integer multiplication. We state the following theorem, which is based on an algorithm discussed in [Kn97].

Theorem 2.7. There is an algorithm to find the quotient $q = [a/b]$, when the $2n$-bit integer a is divided by the integer b (having no more than n bits), using $O(M(n))$ bit operations, where $M(n)$ is the number of bit operations needed to multiply two n-bit integers.

2.3 Exercises

1. Determine whether each of the following functions is $O(n)$ on the set of positive integers.
   a) $2n + 7$
   b) $n^2/3$
   c) 10
   d) $\log(n^2 + 1)$
   e) $\sqrt{n^2 + 1}$
   f) $(n^2 + 1)/(n + 1)$
2. Show that $2n^4 + 3n^3 + 17$ is $O(n^4)$ on the set of positive integers.
3. Show that $(n^3 + 4n^2 \log n + 101n^2)(14n \log n + 8n)$ is $O(n^4 \log n)$.
4. Show that $n!$ is $O(n^n)$ on the set of positive integers.
5. Show that $(n! + 1)(n + \log n) + (n^3 + n^n)((\log n)^3 + n + 7)$ is $O(n^{n+1})$.
6. Suppose that m is a positive real number. Show that $\sum_{j=1}^{n} j^m$ is $O(n^{m+1})$.
* 7. Show that $n \log n$ is $O(\log n!)$ on the set of positive integers.
8. Show that if f_1 and f_2 are $O(g_1)$ and $O(g_2)$, respectively, and c_1 and c_2 are constants, then $c_1 f_1 + c_2 f_2$ is $O(g_1 + g_2)$.
9. Show that if f is $O(g)$, then f^k is $O(g^k)$ for all positive integers k.
10. Let r be a positive real number greater than 1. Show that a function f is $O(\log_2 n)$ if and only if f is $O(\log_r n)$. (*Hint:* Recall that $\log_a n / \log_b n = \log_a b$.)
11. Show that the base b expansion of a positive integer n has $[\log_b n] + 1$ digits.
12. Analyzing the conventional algorithms for subtraction and addition, show that these operations require $O(n)$ bit operations with n-bit integers.
13. Show that to multiply an n-bit and an m-bit integer in the conventional manner requires $O(nm)$ bit operations.
14. Estimate the number of bit operations needed to find $1 + 2 + \cdots + n$,
    a) by performing all the additions;
    b) by using the identity $1 + 2 + \cdots + n = n(n + 1)/2$, and multiplying and shifting.
15. Give an estimate for the number of bit operations needed to find each of the following quantities.
    a) $n!$
    b) $\binom{n}{k}$
16. Give an estimate of the number of bit operations needed to find the binary expansion of an integer from its decimal expansion.
17. Use identity (2.2) with $n = 2$ to multiply $(1001)_2$ and $(1011)_2$.
18. Use identity (2.2) with $n = 4$, and then with $n = 2$, to multiply $(10010011)_2$ and $(11001001)_2$.

19. a) Show there is an identity analogous to (2.2) for decimal expansions.

b) Using part (a), multiply 73 and 87 performing only three multiplications of one-digit integers, plus shifts and additions.

c) Using part (a), reduce the multiplication of 4216 and 2733 to three multiplications of two-digit integers, plus shifts and additions; then, using part (a) again, reduce each of the multiplications of two-digit integers into three multiplications of one-digit integers, plus shifts and additions. Complete the multiplication using only nine multiplications of one-digit integers, and shifts and additions.

20. If **A** and **B** are $n \times n$ matrices, with entries a_{ij} and b_{ij} for $1 \leq i \leq n$, $1 \leq j \leq n$, then **AB** is the $n \times n$ matrix with entries $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$. Show that n^3 multiplications of integers are used to find **AB** directly from its definition.

21. Show that it is possible to multiply two 2×2 matrices using only seven multiplications of integers, by using the identity

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & x + (a_{21} + a_{22})(b_{12} - b_{11}) \\ & \quad + (a_{11} + a_{12} - a_{21} - a_{22})b_{22} \\ x + (a_{11} - a_{21})(b_{22} - b_{12}) & x + (a_{11} - a_{21})(b_{22} - b_{12}) \\ \quad - a_{22}(b_{11} - b_{21} - b_{12} + b_{22}) & \quad + (a_{21} + a_{22})(b_{12} - b_{11} \end{pmatrix},$$

where $x = a_{11}b_{11} - (a_{11} - a_{21} - a_{22})(b_{11} - b_{12} + b_{22})$.

* **22.** Using an inductive argument, and splitting $(2n) \times (2n)$ matrices into four $n \times n$ matrices, use Exercise 21 to show that it is possible to multiply two $2^k \times 2^k$ matrices using only 7^k multiplications, and less than 7^{k+1} additions.

23. Conclude from Exercise 22 that two $n \times n$ matrices can be multiplied using $O(n^{\log_2 7})$ bit operations when all entries of the matrices have less than c bits, where c is a constant.

2.3 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. Multiply 81,873,569 and 41,458,892 by using identity (2.2) with these eight-digit integers, with the resulting four-digit integers, and with the resulting two-digit integers.

2. Multiply two 8×8 matrices of your choice, by using the identity in Exercise 21 with these matrices and then again for the multiplication of the resulting 4×4 matrices.

Programming Projects

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

* **1.** Multiply two arbitrarily large integers using identity (2.2).

** **2.** Multiply two $n \times n$ matrices using the algorithm discussed in Exercises 21–23.

3

Primes and Greatest Common Divisors

Introduction

This chapter introduces a central concept of number theory, namely that of a prime number. A prime is an integer with precisely two positive integer divisors. Prime numbers were studied extensively by the ancient Greeks, who discovered many of their basic properties. In the past three centuries, mathematicians have devoted countless hours to exploring the world of primes. They have discovered many fascinating properties, formulated diverse conjectures, and proved interesting and surprising results. Research into questions involving primes continues today, partly driven by the importance of primes in modern cryptography. Open questions about primes stimulate new research. There are also hordes of people trying to enter the record books by finding the largest prime yet known.

In this chapter, we will show that there are infinitely many primes. The proof we will give dates back to ancient times. We will also show how to find all the primes not exceeding a given integer, using the sieve of Eratosthenes, also dating back to antiquity. We will discuss the distribution of primes, and state the famous prime number theorem that was proved at the end of the nineteenth century. This theorem provides an accurate estimate for the number of primes not exceeding a given integer. Many questions about primes remain open despite attention from mathematicians over hundreds of years; we will discuss two of the best known, the twin prime conjecture and Goldbach's conjecture.

This chapter also shows that every positive integer can be written uniquely as the product of primes (when the primes are written in increasing order of size). This result is known as the *fundamental theorem of arithmetic*. To prove this theorem, we will use the concept of the greatest common divisor of two integers. We will establish many important properties of the greatest common divisor in this chapter, such as the fact that it is the smallest linear combination of these integers. We will describe the Euclidean algorithm that can be used for finding the greatest common divisor of two integers, and analyze its computational complexity. We will discuss methods used to find the factorization of

integers into products of primes, and discuss the complexity of these methods. Numbers of special form are often studied in number theory; in this chapter, we will introduce the Fermat numbers, which are integers of the form $2^{2^n} + 1$. (Fermat conjectured that they are all prime but this turns out not to be true.)

Finally, we will introduce the concept of a diophantine equation, which is an equation where only solutions in integers are sought. We will show how greatest common divisors can be used to help solve linear diophantine equations. Unlike many other diophantine equations, linear diophantine equations can be solved easily and systematically.

3.1 Prime Numbers

The positive integer 1 has just one positive divisor. Every other positive integer has at least two positive divisors, because it is divisible by 1 and by itself. Integers with exactly two positive divisors are of great importance in number theory; they are called *primes.*

Definition. A *prime* is a positive integer greater than 1 that is divisible by no positive integers other than 1 and itself.

Example 3.1. The integers 2, 3, 5, 13, 101, and 163 are primes. ◀

Definition. A positive integer greater than 1 that is not prime is called *composite.*

Example 3.2. The integers $4 = 2 \cdot 2$, $8 = 4 \cdot 2$, $33 = 3 \cdot 11$, $111 = 3 \cdot 37$, and $1001 = 7 \cdot 11 \cdot 13$ are composite. ◀

The primes are the multiplicative building blocks of the integers. Later, we will show that every positive integer can be written uniquely as the product of primes.

In this section, we will discuss the distribution of prime numbers among the set of positive integers, and prove some elementary properties about this distribution. We will also discuss more powerful results about the distribution of primes. The theorems we will introduce include some of the most famous results in number theory.

You can find all primes less than 10,000 in Table E.1 at the end of the book.

The Infinitude of Primes We start by showing that there are infinitely many primes, for which the following lemma is needed.

Lemma 3.1. Every positive integer greater than 1 has a prime divisor.

Proof. We prove the lemma by contradiction; we assume that there is a positive integer greater than 1 having no prime divisors. Then, since the set of positive integers greater than 1 with no prime divisors is nonempty, the well-ordering property tells us that there is a least positive integer n greater than 1 with no prime divisors. Since n has no prime divisors and n divides n, we see that n is not prime. Hence, we can write $n = ab$ with $1 < a < n$ and $1 < b < n$. Because $a < n$, a must have a prime divisor. By Theorem 1.8, any divisor of a is also a divisor of n, so n must have a prime divisor, contradicting the

fact that n has no prime divisors. We can conclude that every positive integer greater than 1 has at least one prime divisor. ∎

We now show that there are infinitely many primes, a wondrous result known by the ancient Greeks. This is one of the key theorems in number theory that can be proved in a variety of ways. The proof we will provide was presented by Euclid in his book the *Elements* (Book IX, 20). This simple, yet elegant proof is considered by many to be particularly beautiful. It is not surprising that the very first proof found in the book *Proofs from THE BOOK* [AiZi03], a collection of particularly insightful and clever proofs, begins with this proof found in Euclid. Moreover, this book presents six quite different proofs of the infinitude of primes. (Here, *THE BOOK* refers to the imagined collection of perfect proofs that Paul Erdős claimed is maintained by God.) We will introduce a variety of different proofs that there are infinitely many primes later in this chapter. (See Exercise 8 at the end of this section, the exercise sets in Sections 3.3 and 3.5, and Section 3.6.)

Theorem 3.1. There are infinitely many primes.

Proof. Suppose that there are only finitely many primes, $p_1, p_2, \ldots p_n$, where n is a positive integer. Consider the integer Q_n, obtained by multiplying these primes together and adding one, that is,

$$Q_n = p_1 p_2 \cdots p_n + 1.$$

By Lemma 3.1, Q has at least one prime divisor, say q. We obtain a contradiction by showing that q is not one of the primes listed. (These supposedly formed a complete list of all primes.) If $q = p_j$ for some integer j with $1 \leq j \leq n$, then since $Q_n - p_1 p_2 \cdots p_n = 1$, because q divides both terms on the left-hand side of this equation, by Theorem 1.9 it follows that $q|1$. This is impossible because no prime divides 1. Consequently, q must be a prime we have not listed. This contradiction shows that there are infinity many primes. ∎

The proof of Theorem 3.1 is nonconstructive because the integer we have constructed in the proof, Q_n, which is one more than the product of the first n primes, may or may not be prime (see Exercise 11). Consequently, in the proof we have not found a new prime, but we know that one exists.

Finding Primes In later chapters, we will be interested in finding and using extremely large primes. Tests distinguishing between primes and composite integers will be crucial; such tests are called *primality tests*. The most basic primality test is *trial division*, which tells us that the integer n is prime if and only if it is not divisible by any prime not exceeding $\sqrt{n}$. We now prove that this test can be used to determine whether n is prime.

Theorem 3.2. If n is a composite integer, then n has a prime factor not exceeding $\sqrt{n}$.

Proof. Since n is composite, we can write $n = ab$, where a and b are integers with $1 < a \leq b < n$. We must have $a \leq \sqrt{n}$, since otherwise $b \geq a > \sqrt{n}$ and $ab > \sqrt{n} \cdot \sqrt{n} = n$. Now, by Lemma 3.1, a must have a prime divisor, which by Theorem 1.8 is also a divisor of n and which is clearly less than or equal to $\sqrt{n}$. ∎

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figure 3.1 *Using the sieve of Eratosthenes to find the primes less than 100.*

We can use Theorem 3.2 to find all the primes less than or equal to a given positive integer n. This procedure is called the *sieve of Eratosthenes,* since it was invented by the ancient Greek mathematician *Eratosthenes*. We illustrate its use in Figure 3.1 by finding all primes less than 100. We first note that every composite integer less than 100 must have a prime factor less than $\sqrt{100} = 10$. Since the only primes less than 10 are 2, 3, 5, and 7, we only need to check each integer less than 100 for divisibility by these primes. We first cross out, with a horizontal slash (—), all multiples of 2 greater than 2. Next, we cross out with a slash (/) those integers remaining that are multiples of 3, other than 3 itself. Then all multiples of 5, other than 5, that remain are crossed out with a backslash (\). Finally, all multiples of 7, other than 7, that are left are crossed out with a vertical slash (|). All remaining integers (other than 1) must be prime.

Although the sieve of Eratosthenes produces all primes less than or equal to a fixed integer, to determine in this manner whether a particular integer n is prime it is necessary to check n for divisibility by all primes not exceeding $\sqrt{n}$. This is quite inefficient; later, we will give better methods for deciding whether or not an integer is prime.

ERATOSTHENES (c. 276–194 B.C.E.) was born in Cyrene, which was a Greek colony west of Egypt. It is known that he spent some time studying at Plato's school in Athens. King Ptolemy II invited Eratosthenes to Alexandria to tutor his son. Later, Eratosthenes became the chief librarian of the famous library at Alexandria, which was a central repository of ancient works of literature, art, and science. He was an extremely versatile scholar, having written on mathematics, geography, astronomy, history, philosophy, and literature. Besides his work in mathematics, Eratosthenes was most noted for his chronology of ancient history and for his geographical measurements, including his famous measurement of the size of the earth.

We now introduce a function that counts the primes not exceeding a specified number.

Definition. The function $\pi(x)$, where x is a positive real number, denotes the number of primes not exceeding x.

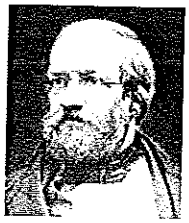
Example 3.3. From our illustration of the sieve of Eratosthenes, we see that $\pi(10) = 4$ and $\pi(100) = 25$. ◀

Primes in Arithmetic Progressions Every odd integer is either of the form $4n + 1$ or the form $4n + 3$. Are there infinitely many primes in both these forms? The primes $5, 13, 17, 29, 37, 41, \ldots$ are of the form $4n + 1$ and the primes $3, 7, 11, 19, 23, 31, 43, \ldots$ are of the form $4n + 3$. Looking at this evidence hints that there are infinitely many primes in both these progressions. What about other arithmetic progressions such as $3n + 1$, $7n + 4$, $8n + 7$, and so on? Does each of these contain infinitely many primes? German mathematician *G. Lejeune Dirichlet* settled this question in 1837, when he used methods from complex analysis to prove the following theorem.

Theorem 3.3. ***Dirichlet's Theorem on Primes in Arithmetic Progressions.*** Suppose that a and b are positive integers not divisible by the same prime. Then the arithmetic progression $an + b$, $n = 1, 2, 3, \ldots$, contains infinitely many primes.

No simple proof of Dirichlet's theorem on primes in arithmetic progressions is known. (Dirichlet's original proof used complex variables. In the 1950s an elementary but complicated proof was found by Selberg.) However, special cases of Dirichlet's theorem can be proved quite easily. We will illustrate this in Section 3.5, by showing that there are infinitely many primes of the form $4n + 3$.

The Largest Known Primes For hundreds if not thousands of years, professional and amateur mathematicians have been motivated to find a prime larger than any currently known. The person who discovers such a prime becomes famous, at least for a time,



G. LEJEUNE DIRICHLET (1805–1859) was born into a French family living in the vicinity of Cologne, Germany. He studied at the University of Paris when this was an important world center of mathematics. He held positions at the University of Breslau and the University of Berlin, and in 1855 was chosen to succeed Gauss at the University of Göttingen. Dirichlet is said to be the first person to master Gauss's *Disquisitiones Arithmeticae,* which had appeared 20 years earlier. He is said to have kept a copy of this book at his side even when he traveled. His book on number theory, *Vorlesungen über Zahlentheorie,* helped make Gauss's discoveries accessible to other mathematicians. Besides his fundamental work in number theory, Dirichlet made many important contributions to analysis. His famous "drawer principle," also called the pigeonhole principle, is used extensively in combinatorics and in number theory.

and has his or her name entered into the record books. Because there are infinitely many prime numbers, there is always a prime larger than the current record. Looking for new primes is done somewhat systematically; rather than checking randomly, people examine numbers that have a special form. For example, in Chapter 7 we will discuss primes of the form $2^p - 1$, where p is prime; such numbers are called *Mersenne primes*. We will see that there is a special test that makes it possible to determine whether $2^p - 1$ is prime, without performing trial divisions. The largest known prime number has been a Mersenne prime for most of the past hundred years. Currently, the world record for the largest prime known is $2^{24,036,583} - 1$.

Formulas for Primes Is there a formula that generates only primes? This is another question that has interested mathematicians for many years. No polynomial in one variable has this property, as Exercise 23 demonstrates. It is also the case that no polynomial in n variables, where n is a positive integer, generates only primes (a result that is beyond the scope of this book). There are several impractical formulas that generate only primes. For example, Mills has shown that there is a constant Θ such that the function $f(n) = [\Theta^{3^n}]$ generates only primes. Here the value of Θ is known only approximately, with $\Theta \approx 1.3064$. This formula is impractical for generating primes not only because the exact value of Θ is not known, but also because to compute Θ you must know the primes that $f(n)$ generates (see [Mi47] for details).

If no useful formula can be used to generate large primes, how can they be generated? In Chapter 6, we will learn how to generate large primes using what are known as probabilistic primality tests.

Primality Proofs

If someone presents you with a positive integer n and claims that n is prime, how can you be sure that n really is prime? We already know that we can determine whether n is prime by performing trial divisions of n by the primes not exceeding $\sqrt{n}$. If n is not divisible by any of these primes, it itself is prime. Consequently, once we have determined that n is not divisible by any prime not exceeding its square root, we have produced a proof that n is prime. Such a proof is also known as a *certificate of primality*.

Unfortunately, using trial division to produce a certificate of primality is extremely inefficient. To see this, we estimate the number of bit operations used by this test. Using the prime number theorem, we can estimate the number of bit operations needed to show that an integer n is prime by trial divisions of n by all primes not exceeding $\sqrt{n}$. The prime number theorem tells us that there are approximately $\sqrt{n}/\log \sqrt{n} = 2\sqrt{n}/\log n$ primes not exceeding $\sqrt{n}$. To divide n by an integer m takes $O(\log_2 n \cdot \log_2 m)$ bit operations. Therefore, the number of bit operations needed to show that n is prime by this method is at least $(2\sqrt{n}/\log n)(c \log_2 n) = c\sqrt{n}$ (where we have ignored the $\log_2 m$ term because it is at least 1, even though it sometimes is as large as $(\log_2 n)/2$). This method of showing that an integer n is prime is very inefficient, for it is necessary not only to know all the primes not larger than $\sqrt{n}$, but to do at least a constant multiple of $\sqrt{n}$ bit operations.

To input an integer into a computer program, we input the binary digits of the integer. Consequently, the computational complexity of algorithms for determining whether an integer is prime is measured in terms of the number of binary digits in the integer. By Exercise 11 in Section 2.3 we know that a positive integer n has $[\log_2 n] + 1$ binary digits. Consequently, a big-O estimate for the computational complexity of an algorithm in terms of number of binary digits of n translates to the same big-O estimate in terms of $\log_2 n$, and vice versa. Note that the algorithm using trial divisions to determine whether an integer n is prime is exponential in terms of the number of binary digits of n, or in terms of $\log_2 n$, because $\sqrt{n} = 2^{\log_2 n/2}$. That is, this algorithm has exponential time complexity, measured in terms of the number of binary digits in n. As n gets large, an algorithm with exponential complexity quickly becomes impractical. Determining whether a number with 200 digits is prime using trial division still takes billions of years on the fastest computers.

Mathematicians have looked for efficient primality tests for many years. In particular, they have searched for an algorithm that produces a certificate of primality in polynomial time, measured in terms of the number of binary digits of the integer input. In 1975, G. L. Miller developed an algorithm that can prove that an integer is prime using $O((\log n)^5)$ bit operations, assuming the validity of a hypothesis called the generalized Riemann hypothesis. Unfortunately, the generalized Riemann hypothesis remains an open conjecture. In 1983, Leonard Adleman, Carl Pomerance, and Robert Rumely developed an algorithm that can prove an integer is prime using $(\log n)^{c \log\log\log n}$ bit operations, where c is a constant. Although their algorithm does not run in polynomial time, it runs in close to polynomial time because the function $\log\log\log n$ grows so slowly. To use their algorithm with an up-to-date PC to determine whether a 100-digit integer is prime requires just a few milliseconds, determining whether a 400-digit integer is prime requires less than a second, and determining whether a 1000-digit integer is prime takes less than an hour. (For more information about their test, see [AdPoRu83] and [Ru83].)

Until 2002, no one was able to find a polynomial time algorithm for proving that a positive integer is prime. In 2002, M. Agrawal, N. Kayal, and N. Saxena, an Indian computer science professor and two of his undergraduate students, announced that they had found an algorithm that can produce a certificate of primality for an integer n using $O((\log n)^{12})$ bit operations. Their discovery of a polynomial time algorithm for proving that a positive integer is prime surprised the mathematical community. Their announcement stated that "*PRIMES* is in *P*." Here, computer scientists denote by *PRIMES* the problem of determining whether a given integer n is prime, and P denotes the class of problems that can be solved in polynomial time. Consequently, *PRIMES* is in P means that one can determine whether n is prime using an algorithm that has computational complexity bounded by a polynomial in the number of binary digits in n, or equivalently, in $\log n$. Their proof can be found in [AgKaSa02] and can be understood by undergraduate students who have studied number theory and abstract algebra. In this paper, they also show that under the assumption of a widely believed conjecture about the density of Sophie Germain primes (primes p for which $2p + 1$ is also prime), their algorithm uses only $O((\log n)^6)$ bit operations. Other mathematicians have also improved on Agrawal, Kayal, and Saxena's result. In particular, H. Lenstra

and C. Pomerance have reduced the exponent 12 in the original estimate to $6 + \epsilon$, where ϵ is any positive real number.

It is important to note that in our discussion of primality tests, we have only addressed *deterministic* algorithms, that is, algorithms that decide with certainty whether an integer is prime. In Chapter 6, we will introduce the notion of probabilistic primality tests, that is, tests that tell us that there is a high probability, but not a certainty, that an integer is prime.

3.1 Exercises

1. Determine which of the following integers are primes.

   a) 101 c) 107 e) 113
   b) 103 d) 111 f) 121

2. Determine which of the following integers are primes.

   a) 201 c) 207 e) 213
   b) 203 d) 211 f) 221

3. Use the sieve of Eratosthenes to find all primes less than 150.

4. Use the sieve of Eratosthenes to find all primes less than 200.

5. Find all primes that are the difference of the fourth powers of two integers.

6. Show that no integer of the form $n^3 + 1$ is a prime, other than $2 = 1^3 + 1$.

7. Show that if a and n are positive integers with $n > 1$ and $a^n - 1$ is prime, then $a = 2$ and n is prime. (*Hint:* Use the identity $a^{kl} - 1 = (a^k - 1)(a^{k(l-1)} + a^{k(l-2)} + \cdots + a^k + 1)$.)

8. (This exercise constructs another proof of the infinitude of primes.) Show that the integer $Q_n = n! + 1$, where n is a positive integer, has a prime divisor greater than n. Conclude that there are infinitely many primes.

9. Can you show that there are infinitely many primes by looking at the integers $S_n = n! - 1$, where n is a positive integer?

10. Using Euclid's proof that there are infinitely many primes, show that the nth prime p_n does not exceed $2^{2^{n-1}}$ whenever n is a positive integer. Conclude that when n is a positive integer, there are at least $n + 1$ primes less than 2^{2^n}.

11. Let $Q_n = p_1 p_2 \cdots p_n + 1$, where $p_1, p_2, \ldots, p_n$ are the n smallest primes. Determine the smallest prime factor of Q_n for $n = 1, 2, 3, 4, 5$, and 6. Do you think that Q_n is prime infinitely often? (*Note:* This is an unresolved question.)

12. Show that if p_k is the kth prime, where k is a positive integer, then $p_n \leq p_1 p_2 \cdots p_{n-1} + 1$ for all integers n with $n \geq 3$.

13. Show that if the smallest prime factor p of the positive integer n exceeds $\sqrt[3]{n}$, then n/p must be prime or 1.

14. Show that if p is a prime in the arithmetic progression $3n + 1, n = 1, 2, 3, \ldots$, then it is also in the arithmetic progression $6n + 1, n = 1, 2, 3, \ldots$.

15. Find the smallest prime in the arithmetic progression $an + b$, where

a) $a = 3, b = 1$. b) $a = 5, b = 4$. c) $a = 11, b = 16$.

16. Find the smallest prime in the arithmetic progression $an + b$, where

a) $a = 5, b = 1$. b) $a = 7, b = 2$. c) $a = 23, b = 13$.

17. Use the second principle of mathematical induction to prove that every integer greater than 1 is either prime or the product of two or more primes.

* **18.** Use the principle of inclusion-exclusion (Exercise 16 of Appendix B) to show that

$$\pi(n) = (\pi(\sqrt{n}) - 1) + n - \left(\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_r} \right\rfloor\right) + \left(\left\lfloor \frac{n}{p_1 p_2} \right\rfloor + \left\lfloor \frac{n}{p_1 p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{r-1} p_r} \right\rfloor\right) - \left(\left\lfloor \frac{n}{p_1 p_2 p_3} \right\rfloor + \left\lfloor \frac{n}{p_1 p_2 p_4} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{r-2} p_{r-1} p_r} \right\rfloor\right) + \cdots,$$

where $p_1, p_2, \ldots, p_r$ are the primes less than or equal to $\sqrt{n}$ (with $r = \pi(\sqrt{n})$). (*Hint:* Let property P_i be the property that an integer is divisible by p_i.)

19. Use Exercise 18 to find $\pi(250)$.

20. Show that $x^2 - x + 41$ is prime for all integers x with $0 \leq x \leq 40$. Show, however, that it is composite for $x = 41$.

21. Show that $2n^2 + 11$ is prime for all integers n with $0 \leq n \leq 10$, but is composite for $n = 11$.

22. Show that $2n^2 + 29$ is prime for all integers n with $0 \leq n \leq 28$, but is composite for $n = 29$.

* **23.** Show that if $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where the coefficients are integers, then there is an integer y such that $f(y)$ is composite. (*Hint:* Assume that $f(x) = p$ is prime, and show that p divides $f(x + kp)$ for all integers k. Conclude that there is an integer y such that $f(y)$ is composite from the fact that a polynomial of degree $n, n > 1$, takes on each value at most n times.)

The *lucky numbers* are generated by the following sieving process: Start with the positive integers. Begin the process by crossing out every second integer in the list, starting your count with the integer 1. Other than 1, the smallest integer not crossed out is 3, so we continue by crossing out every third integer left, starting the count with the integer 1. The next integer left is 7, so we cross out every seventh integer left. Continue this process, where at each stage we cross out every kth integer left, where k is the smallest integer not crossed out, other than 1, not yet used in the sieving process. The integers that remain are the lucky numbers.

24. Find all lucky numbers less than 100.

25. Show that there are infinitely many lucky numbers.

26. Suppose that t_k is the smallest prime greater than $Q_k = p_1 p_2 \cdots p_k + 1$, where p_j is the jth prime number.
    a) Show that $t_k - Q_k + 1$ is not divisible by p_j for $j = 1, 2, \ldots, k$.
    b) R. F. Fortune conjectured that $t_k - Q_k + 1$ is prime for all positive integers k. Show that this conjecture is true for all positive integers k with $k \leq 5$.

3.1 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 nth prime, where n is each of the following integers.
   a) 1,000,000 b) 333,333,333 c) 1,000,000,000
2. Find the smallest prime greater than each of the following integers.
   a) 1,000,000 b) 100,000,000 c) 100,000,000,000
3. Plot the nth prime as a function of n for $1 \leq n \leq 100$.
4. Plot $\pi(x)$ for $1 \leq x \leq 500$.
5. Find the smallest prime factor of $n! + 1$ for all positive integers n not exceeding 20.
6. Find the smallest prime factor of $p_1 p_2 \cdots p_k + 1$, where $p_1, p_2, \ldots, p_k$ are the kth smallest primes for all positive integers k not exceeding 50.
7. Use the sieve of Eratosthenes to find all primes less than 10,000.
8. Use the result given in Exercise 18 to find $\pi(10{,}000)$, the number of primes not exceeding 10,000.
9. Verify R. F. Fortune's conjecture that $t_k - Q_k + 1$ is prime for all positive integers k, where t_k is the smallest prime greater than $Q_k = \prod_{j=1}^{k} p_j + 1$ for as many k as you can.
10. Find all lucky numbers (as defined in the preamble to Exercise 24) not exceeding 10,000.

Programming Projects

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

1. Decide whether a given positive integer is prime, using trial division of the integer by all primes not exceeding its square root.

* 2. Use the sieve of Eratosthenes to find all primes less than n, where n is a given positive integer.

** 3. Find $\pi(n)$, the number of primes less than or equal to n, using Exercise 18.

4. Given positive integers a and b not divisible by the same prime, find the smallest prime number in the arithmetic progression $an + b$, where n is a positive integer.

* 5. Find the lucky numbers less than n, where n is a given integer (see the preamble to Exercise 24).

3.2 The Distribution of Primes

We know that there are infinitely many primes, but can we estimate how many primes there are less than a positive real number x? One of the most famous theorems of number theory, and of all mathematics, is the *prime number theorem*, which answers this question.

Mathematicians in the late eighteenth century examined tables of prime numbers created using hand calculations. Using these values, they looked for functions that estimated $\pi(x)$. In 1798, French mathematician Adrien-Marie Legendre (see Chapter 11 for a biography) used tables of primes up to 400,031, computed by Jurij Vega, to note that $\pi(x)$ could be approximated by the function

$$\frac{x}{\log x - 1.08366}.$$

The great German mathematician Karl Friedrich Gauss (see Chapter 4 for a biography) conjectured that $\pi(x)$ increases at the same rate as the functions

$$x/\log x \quad \text{and} \quad \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

(where $\int_2^x \frac{dt}{\log t}$ represents the area under the curve $y = 1/\log t$ and above the t-axis from $t = 2$ to $t = x$). (The name *Li* is an abbreviation of *logarithmic integral*.)

Neither Legendre nor Gauss managed to prove that these functions approximated $\pi(x)$ closely for large values of x. By 1811, a table of all primes up to 1,020,000 had been produced (by Chernac), which could be used to provide evidence for these conjectures.

The first substantial result showing that $\pi(x)$ could be approximated by $x/\log x$ was established in 1850 by Russian mathematician *Pafnuty Lvovich Chebyshev*. He showed that there are positive real numbers C_1 and C_2, with $C_1 < 1 < C_2$, such that

$$C_1(x/\log x) < \pi(x) < C_2(x/\log x)$$

PAFNUTY LVOVICH CHEBYSHEV (1821–1894) was born on the estate of his parents in Okatovo, Russia. His father was a retired army officer. In 1832, Chebyshev's family moved to Moscow, where he completed his secondary education with study at home. In 1837, Chebyshev entered Moscow University, graduating in 1841. While still an undergraduate, he made his first original contribution, a new method for approximating roots of equations. Chebyshev joined the faculty of St. Petersburg University in 1843, where he remained until 1882. His doctoral thesis, written in 1849, was long used as a number theory textbook at Russian universities. Chebyshev made contributions to many areas of mathematics besides number theory, including probability theory, numerical analysis, and real analysis. He worked in theoretical and applied mechanics, and had a bent for constructing mechanisms, including linkages and hinges. He was a popular teacher, and had a strong influence on the development of Russian mathematics.

for sufficiently large values of x. (In particular, he showed that this result holds with $C_1 = 0.929$ and $C_2 = 1.1$.) He also demonstrated that if the ratio of $\pi(x)$ and $x/\log x$ approaches a limit as x increases, then this limit must be 1.

The prime number theorem, which states that the ratio of $\pi(x)$ and $x/\log x$ approaches 1 as x grows without bound, was finally proved in 1896, when French mathematician *Jacques Hadamard* and Belgian mathematician *Charles-Jean-Gustave-Nicholas de la Vallée-Poussin* produced independent proofs. Their proofs were based on results from the theory of complex analysis. They used ideas developed in 1859 by German mathematician Bernhard Riemann, which related $\pi(x)$ to the behavior of the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

in the complex plane. (The function $\zeta(s)$ is known as the *Riemann zeta function.*) The connection between the Riemann zeta function and the prime numbers comes from the identity

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} (1 - \frac{1}{p^s})^{-1},$$

JACQUES HADAMARD (1865–1963) was born in Versailles, France. His father was a Latin teacher and his mother a distinguished piano teacher. After completing his undergraduate studies, he taught at a Paris secondary school. After receiving his doctorate in 1892, he became lecturer at the Faculté des Sciences of Bordeaux. He subsequently served on the faculties of the Sorbonne, the Collège de France, the École Polytechnique, and the École Centrale des Arts et Manufactures. Hadamard made important contributions to complex analysis, functional analysis, and mathematical physics. His proof of the prime number theorem was based on his work in complex analysis. Hadamard was a famous teacher; he wrote numerous articles about elementary mathematics that were used in French schools, and his text on elementary geometry was used for many years.

CHARLES-JEAN-GUSTAVE-NICHOLAS DE LA VALLEÉ-POUSSIN (1866–1962), the son of a geology professor, was born at Louvain, Belgium. He studied at the Jesuit College at Mons, first studying philosophy, later turning to engineering. After receiving his degree, instead of pursuing a career in engineering, he devoted himself to mathematics. De la Valleé-Poussin's most significant contribution to mathematics was his proof of the prime number theorem. Extending this work, he established results about the distribution of primes in arithmetic progression and the distribution of primes represented by quadratic forms. Furthermore, he refined the prime number theorem to include error estimates. He made important contributions to differential equations, approximation theory, and analysis. His textbook, *Cours d'analyse,* had a strong impact on mathematical thought in the first half of the twentieth century.

where the product on the right-hand side of the equation extends over all primes p. We will explain why this identity is true in Section 3.5.

In addition to proving the prime number theorem, de la Vallée-Poussin showed that the function $\mathrm{Li}(x)$ is a closer approximation to $\pi(x)$ than $x/(\log x - a)$ for all values of the constant a.

The proofs of the prime number theorem found by Hadamard and de la Valleé-Poussin depend on complex analysis, though the theorem itself does not involve complex numbers. This left open the challenge of finding a proof that did not use the theory of complex variables. It surprised the mathematical community when, in 1949, Norwegian mathematician *Atle Selberg* and Hungarian mathematician *Paul Erdős* independently found elementary proofs of the prime number theorem. Their proofs, though elementary (meaning that they do not use the theory of complex variables), are quite complicated and difficult.

We now formally state the prime number theorem.

Theorem 3.4. ***The Prime Number Theorem.*** The ratio of $\pi(x)$ to $x/\log x$ approaches 1 as x grows without bound. (Here, $\log x$ denotes the natural logarithm of x and in the language of limits, we have $\lim_{x\to\infty} \pi(x)/(x/\log x) = 1$.)

Remark. A concise way to state the prime number theorem is to write $\pi(x) \sim x/\log x$. Here the symbol $\sim$ denotes "is asymptotic to." We write $a(x) \sim b(x)$ to denote that $\lim_{x\to\infty} a(x)/b(x) = 1$, and we say that $a(x)$ is asymptotic to $b(x)$.

The prime number theorem tells us that the ratio between $x/\log x$ and $\pi(x)$ is close to 1 when x is large. However, there are functions for which the ratio between these functions and $\pi(x)$ approaches 1 more rapidly than it does for $x/\log x$. In particular, it

ATLE SELBERG (b. 1917), born in Langesund, Norway, became interested in mathematics as a schoolboy. He was inspired by Ramanujan's writing, both by the mathematics and the "air of mystery" surrounding Ramanujan's personality. Selberg received his doctorate in 1943 from the University of Oslo. He remained at the university until 1947, when he married and took a position at the Institute for Advanced Study in Princeton. After a brief stay at Syracuse University, he returned to the Institute for Advanced Study, where he was appointed a permanent member in 1949; he became a professor at Princeton University in 1951. Selberg received the Fields Medal, the most prestigious award in mathematics, for his work on sieve methods and on the properties of the set of zeros of the Riemann zeta function. He is also well known for his elementary proofs of the prime number theorem (also done by Paul Erdős), Dirichlet's theorem on primes in arithmetic progressions, and the generalization of the prime number theorem for primes in arithmetic progressions.

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$Li(x)$	$\pi(x)/Li(x)$
10^3	168	144.8	1.160	178	0.9438202
10^4	1229	1085.7	1.132	1246	0.9863563
10^5	9592	8685.9	1.104	9630	0.9960540
10^6	78498	72382.4	1.085	78628	0.9983466
10^7	664579	620420.7	1.071	664918	0.9998944
10^8	5761455	5428681.0	1.061	5762209	0.9998691
10^9	50847534	48254942.4	1.054	50849235	0.9999665
10^{10}	455052512	434294481.9	1.048	455055614	0.9999932
10^{11}	4118054813	3948131663.7	1.043	4118165401	0.9999731
10^{12}	37607912018	36191206825.3	1.039	37607950281	0.9999990
10^{13}	346065536839	334072678387.1	1.036	346065645810	0.9999997
10^{14}	3204941750802	3102103442166.0	1.033	3204942065692	0.9999999

Table 3.1 *Approximations to* $\pi(x)$.

has been shown that $\mathrm{Li}(x)$ is an even better approximation. In Table 3.1, we see evidence for the prime number theorem and that $\mathrm{Li}(x)$ is an excellent approximation of $\pi(x)$. (Note that the values of $\mathrm{Li}(x)$ have been rounded to the nearest integer.)

It is not necessary to find all primes not exceeding x to compute $\pi(x)$. One way to evaluate $\pi(x)$ without finding all the primes less than x is to use a counting ar-

PAUL ERDŐS (1913-1996), born in Budapest, Hungary, was the son of high-school mathematics teachers. When he was three years old, he could multiply three-digit numbers in his head, and when he was four, he discovered negative numbers on his own. At 17 he entered Eötvös University, graduating in four years with a Ph.D. in mathematics. After graduating, he spent four years at Manchester University, England, as a postdoctoral fellow. In 1938 he came to the United States because of the difficult political situation in Hungary, especially for Jews.

Erdős made many significant contributions to combinatorics and to number theory. One of the discoveries of which he was most proud was his elementary proof of the prime number theorem. He also participated in the modern development of Ramsey theory, a part of combinatorics. Erdős traveled extensively throughout the world to work with other mathematicians. He traveled from one mathematician or group of mathematicians to the next, proclaiming, "My brain is open." Erdős wrote more than 1500 papers, with almost 500 coauthors. Erdős offered monetary rewards for the solutions of problems he found particularly interesting. Two recently published biographies ([Sc98] and [Ho99]) give further details on his life and work.

gument based on the sieve of Eratosthenes (see Exercise 18 in Section 3.1). Efficient ways of computing $\pi(x)$ requiring only $O(x^{(3/5)+\epsilon})$ bit operations have been devised by Lagarias and Odlyzko [LaOd82]. The current world record is $\pi(4 \cdot 10^{22}) = 783{,}964{,}159{,}847{,}056{,}303{,}858$, found as part of a distributed computing effort on the Internet. (Efforts to extend these computations to larger values of x have temporarily hit a snag.)

The Riemann Hypothesis

Many mathematicians consider the *Riemann hypothesis*, a conjecture about the zeros of the zeta function, the most important open problem in pure mathematics. For more than 100 years, number theorists have struggled to solve this problem. Interest in it has spread, perhaps because a prize of one million dollars for a proof (if it is indeed true) has been offered by the Clay Mathematics Institute. Recently, many general-interest books about the Riemann hypothesis, such as [De03], [Sa03a], and [Sa03b], have appeared, even though the hypothesis involves sophisticated notions from complex analysis. We will briefly describe the Riemann hypothesis for the benefit of readers familiar with complex analysis, as well as for the general appreciation of others.

We have defined the Riemann zeta function as $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. This definition is valid for all complex numbers s with $Re(s) > 1$, where $Re(s)$ is the real part of the complex number s. Riemann was able to extend the function defined by the infinite series to a function in the entire complex plane with a pole at $s = 1$. In his famous 1859 paper [Ri59], Riemann connected the zeta function with the distribution of prime numbers. He derived a formula for $\pi(x)$ in terms of the zeros of $\zeta(s)$. The more we understand about the location of the zeros of the zeta function, the more we know about the distribution of the primes. The Riemann hypothesis is a statement about the location of the zeros of this function. Before stating the hypothesis, we first note that the zeta function has zeros at the negative even integers $-2, -4, -6, \ldots$, called the *trivial zeros*. The Riemann hypothesis is the assertion that the nontrivial zeros of $\zeta(s)$ all have real part equal to 1/2. Note that there is an equivalent formulation of the Riemann hypothesis in terms of the error introduced when $\mathrm{Li}(x)$ is used to estimate $\pi(x)$; this alternative formulation does not involve complex variables. In 1901, von Koch showed that the Riemann hypothesis is equivalent to the statement that the error that occurs when $\pi(x)$ is estimated by $\mathrm{Li}(x)$ is $O(x^{1/2} \log x)$.

Many mathematicians believe the Riemann hypothesis is true, particularly because of the wealth of evidence supporting it. First, a vast amount of numerical evidence has been found. We now know that the first 2.5×10^{11} zeros (in order of increasing imaginary parts) have real part equal to 1/2. (These computations were done by Sebastian Wedeniwski, who has set up a distributed computing project to carry them out called ZetaGrid). Second, we know that at least 40% of the nontrivial zeros of the zeta function are simple and have real part equal to 1/2. Third, we know that if there are exceptions to the Riemann hypothesis, they must be rare as we move away from the line $Re(s) = 1/2$. Of course, it is still possible that this evidence is misleading us and that the Riemann hypothesis is not true. Perhaps this famous problem will be resolved in the next few years, or maybe it will resist all attacks for hundreds of years into the future. For more technical information about the Riemann hypothesis, consult the article by Enrico Bomberi on the Web and [Ed01].

How big is the nth prime? The prime number theorem has the following corollary, which can be proved using calculus (see page 10 of [HaWr79]).

Corollary 3.4.1. Let p_n be the nth prime, where n is a positive integer. Then $p_n \sim n \log n$.

What is the probability that a randomly selected positive integer is prime? Given that there are approximately $x/\log x$ primes not exceeding x, the probability that x is prime is approximately $(x/\log x)/x = 1/\log x$. For example, the probability that an integer near 10^{1000} is prime is approximately $1/\log 10^{1000} \approx 1/2302$. Suppose that you want to find a prime with 1000 digits; what is the expected number of integers you must select before you find a prime? The answer is that you must select roughly $1/(1/2302) = 2302$ integers of this size before one of them will be a prime. Of course, you will need to check each one to determine whether it is prime. In Chapter 6, we will discuss how this can be done efficiently.

Gaps in the Distribution of Primes We have shown that there are infinitely many primes and we have discussed the abundance of primes below a given bound x, but we have yet to discuss how regularly primes are distributed throughout the positive integers. We first give a result that shows that there are arbitrarily long runs of integers containing no primes.

Theorem 3.5. For any positive integer n, there are at least n consecutive composite positive integers.

Proof. Consider the n consecutive positive integers

$$(n+1)!+2, \quad (n+1)!+3, \quad \ldots, \quad (n+1)!+n+1.$$

When $2 \leq j \leq n+1$, we know that $j \mid (n+1)!$. By Theorem 1.9 it follows that $j \mid (n+1)!+j$. Hence, these n consecutive integers are all composite. ∎

One of the Largest Numbers Ever Appearing Naturally in a Mathematical Proof Using the data in Table 3.1, we can show that for all x in the table, the difference $\mathrm{Li}(x) - \pi(x)$ is positive and increases as x grows. Gauss, who only had access to the data in the first few rows of this table, believed this trend held for all positive integers x. However, in 1914, the English mathematician J. E. Littlewood showed that $\mathrm{Li}(x) - \pi(x)$ changes sign infinitely many times. In his proof, Littlewood did not establish a lower bound for the first time that $\mathrm{Li}(x) - \pi(x)$ changes from positive to negative. This was done in 1933 by Samuel Skewes, a student of Littlewood's, who managed to show that $\mathrm{Li}(x) - \pi(x)$ changes signs for at least one x with $x < 10^{10^{10^{34}}}$, a humongous number. This number, known as *Skewes' constant*, became famous as the largest number to appear naturally in a mathematical proof. Fortunately, in the past seven decades, considerable progress has been made in reducing this bound. The best current results show that $\mathrm{Li}(x) - \pi(x)$ changes sign near $x = 1.39822 \times 10^{316}$.

Example 3.4. The seven consecutive integers beginning with $8! + 2 = 40{,}322$ are all composite. (However, these are much larger than the smallest seven consecutive composites, 90, 91, 92, 93, 94, 95, and 96.) ◀

Conjectures About Primes

Professional and amateur mathematicians alike find the prime numbers fascinating. It is not surprising that a tremendous variety of conjectures have been formulated concerning prime numbers. Some of these conjectures have been settled, but many still elude resolution. We will describe some of the best known of these conjectures here.

Looking at tables of primes led mathematicians in the first half of the nineteenth century to make conjectures that the distribution of primes satisfies some basic properties, such as this following conjecture.

Bertrand's Conjecture. In 1845, the French mathematician Joseph Bertrand conjectured that for every positive integer n with $n > 1$, there is a prime p such that $n < p < 2n$. Bertrand verified this conjecture for all n not exceeding 3,000,000, but he could not produce a proof. The first proof of this conjecture was found by Pafnuty Lvovich Chebyshev in 1852. Because this conjecture has been proved, it is often called *Bertrand's postulate*. (See Exercises 22–24 for an outline of a proof.)

Theorem 3.5 shows that the gap between consecutive primes is arbitrarily long. On the other hand, primes may often be close together. The only consecutive primes are 2 and 3, because 2 is the only even prime. However, many pairs of primes differ by two; these pairs of primes are called *twin primes*. Examples are the pairs 3, 5 and 7, 11 and 13, 101 and 103, and 4967 and 4969.

Evidence seems to indicate that there are infinitely many pairs of twin primes. There are 35 pairs of twin primes less than 10^3; 8169 pairs less than 10^6; 3,424,506 pairs less than 10^9; and 1,870,585,220 pairs less than 10^{12}. This leads to the following conjecture.

Twin Prime Conjecture. There are infinitely many pairs of primes p and $p + 2$.

JOSEPH LOUIS FRANÇOIS BERTRAND (1822–1900) was born in Paris. He studied at the École Polytechnique from 1839 until 1841 and at the École des Mines from 1841 to 1844. Instead of becoming a mining engineer, he decided to become a mathematician. Bertrand was appointed to a position at the École Polytechnique in 1856 and, in 1862, he also became professor at the Collège de France. In 1845, on the basis of extensive numerical evidence in tables of primes, Bertrand conjectured that there is at least one prime between n and $2n$ for every integer n with $n > 1$. This result was first proved by Chebyshev in 1852. Besides working in number theory, Bertrand worked on probability theory and differential geometry. He wrote several brief volumes on the theory of probability and on analyzing data from observations. His book *Calcul des probabilitiés*, written in 1888, contains a paradox on continuous probabilities now known as Bertrand's paradox. Bertrand was considered to be kind at heart, extremely clever, and full of spirit.

In 1966, Chinese mathematician J. R. Chen showed, using sophisticated sieve methods, that there are infinitely many primes p such that $p + 2$ has at most two prime factors. An active competition is under way to produce new largest pairs of twin primes. The current record for the largest pair of twin primes is $33{,}218{,}925 \cdot 2^{169{,}690} \pm 1$, a pair of primes with 51,090 digits each, discovered by Daniel Papp and Yves Gallot in 2002.

Viggo Brun showed that the sum $\sum_{\text{primes } p \text{ with } p+2 \text{ prime}} \frac{1}{p} = (1/3 + 1/5) + (1/5 + 1/7) + (1/11 + 1/13) + \cdots$ converges to a constant called *Brun's constant*, which is approximately equal to 1.9021605824. Surprisingly, the computation of Brun's constant has played a role in discovering flaws in Intel's original Pentium chip. In 1994, Thomas Nicely at Lynchburg College in Virginia computed Brun's constant in two different ways using different methods on a Pentium PC and came up with different answers. He traced the error back to a flaw in the Pentium chip and he alerted Intel to this problem. (See page 85 for more information about Nicely's discovery.)

We now discuss perhaps the most notorious conjecture about primes.

Goldbach's Conjecture. Every even positive integer greater than 2 can be written as the sum of two primes.

Example 3.5. The integers 10, 24, and 100 can be written as the sum of two primes in the following ways:

$$\begin{aligned} 10 &= 3 + 7 = 5 + 5, \\ 24 &= 5 + 19 = 7 + 17 = 11 + 13, \\ 100 &= 3 + 97 = 11 + 89 = 17 + 83 \\ &= 29 + 71 = 41 + 59 = 47 + 53. \end{aligned}$$

◀

This conjecture was stated by *Christian Goldbach* in a letter to Leonhard Euler in 1742. It has been verified for all even integers less than $4 \cdot 10^{14}$, with this limit increasing as computers become more powerful. Usually, there are many ways to write a particular even integer as the sum of primes, as Example 3.5 illustrates. However, a proof that there is always at least one way has not yet been found. The best result known to date is due to J. R. Chen, who showed (in 1966), using powerful sieve methods, that all sufficiently large integers are the sum of a prime and the product of at most two primes.

Goldbach's conjecture asserts that infinitely many primes occur as pairs of consecutive odd numbers. However, consecutive primes may be far apart. A consequence of

JING RUN CHEN (1933–1996) was a student of the prominent Chinese number theorist Loo Keng Hua. Chen was almost entirely devoted to mathematical research. During the Cultural Revolution in China, he continued his research, working almost all day and night in a tiny room with no electric lights, no table or chairs, only a small bed and his books and papers. It was during this period that he made his most important discoveries concerning twin primes and Goldbach's conjecture. Although he was a mathematical prodigy, Chen was considered to be next to hopeless in other aspects of life. He died in 1996 after a long illness.

the prime number theorem is that as n grows, the average gap between the consecutive primes p_n and p_{n+1} is $\log n$. Number theorists have worked hard to prove results that show that the gaps between consecutive primes are much smaller than average for infinitely many primes. For example, it has been shown that $p_{n+1} - p_n < 0.2486 \log n$ for infinitely many positive integers n. Showing that for every positive real number ϵ, there are infinitely many positive integers n such that $(p_{n+1} - p_n)/\log n < \epsilon$ remains an elusive goal on the way toward the proof of Goldbach's conjecture.

There are many conjectures concerning the number of primes of various forms, such as the following conjecture.

The $n^2 + 1$ Conjecture. There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer.

The smallest primes of the form $n^2 + 1$ are $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, $101 = 10^2 + 1$, $197 = 14^2 + 1$, $257 = 16^2 + 1$, and $401 = 20^2 + 1$. The best result known

Pentium Chip Flaw

The story behind the Pentium chip flaw encountered by Thomas Nicely shows that answers produced by computers should not always be trusted. A surprising number of hardware and software problems arise that lead to incorrect computational results. This story also shows that companies risk serious problems when they hide errors in their products. In June 1994, testers at Intel discovered that Pentium chips did not always carry out computations correctly. However, Intel decided not to make public information about this problem. Instead, they concluded that because the error would not affect many users, it was unnecessary to alert the millions of owners of Pentium computers. The Pentium flaw involved an incorrect implementation of an algorithm for floating-point division. Although the probability is low that divisions of numbers affected by this error come up in a computation, such divisions arise in many computations in mathematics, science, and engineering, and even in spreadsheets running business applications.

Later in that same month, Nicely came up with two different results when he used a Pentium computer to compute Brun's constant in different ways. In October 1994, after checking all possible sources of computational error, Nicely contacted Intel customer support. They duplicated his computations and verified the existence of an error. Furthermore, they told him that this error had not been previously reported. After not hearing any additional information from Intel, Nicely sent e-mail to a few people telling them about this. These people forwarded the message to other interested parties, and within a few days, information about the bug was posted on an Internet newsgroup. By late November, this story was reported by CNN, the *New York Times*, and the Associated Press.

Surprised by the bad publicity, Intel offered to replace Pentium chips, but only for users running applications determined by Intel to be vulnerable to the Pentium division flaw. This offer did not mollify the Pentium user community. All the bad publicity drove Intel stock down several dollars a share and Intel became the object of many jokes, such as: "At Intel, quality is job 0.999999998." Finally, in December 1994, Intel decided to offer a replacement Pentium chip upon request. They set aside almost half a billion dollars to cover costs, and they hired hundreds of extra employees to handle customer requests. Nevertheless, this story does have a happy ending for Intel. Their corrected and improved version of the Pentium chip was extremely successful.

to date is that there are infinitely many integers n for which $n^2 + 1$ is either a prime or the product of two primes. This was shown by Henryk Iwaniec in 1973. Conjectures such as the $n^2 + 1$ conjecture may be easy to state, but are sometimes extremely difficult to resolve (see [Ri96] for more information).

3.2 Exercises

1. Find the smallest five consecutive composite integers.
2. Find one million consecutive composite integers.
3. Show that there are no "prime triplets," that is, primes p, $p + 2$, and $p + 4$, other than 3, 5 , and 7.
4. Find the smallest four sets of prime triplets of the form p, $p + 2$, $p + 6$.
5. Find the smallest four sets of prime triplets of the form p, $p + 4$, $p + 6$.
6. Find the smallest prime between n and $2n$ when n is

   a) 3. c) 19.
   b) 5. d) 31.

7. Find the smallest prime between n and $2n$ when n is

   a) 4. c) 23.
   b) 6. d) 47.

An unsettled conjecture asserts that for every positive integer n there is a prime between n^2 and $(n + 1)^2$.

8. Find the smallest prime between n^2 and $(n + 1)^2$ for all positive integers n with $n \leq 10$.
9. Find the smallest prime between n^2 and $(n + 1)^2$ for all positive integers n with $11 \leq n \leq 20$.
10. Verify Goldbach's conjecture for each of the following values of n.

    a) 50 c) 102 e) 200
    b) 98 d) 144 f) 222

CHRISTIAN GOLDBACH (1690–1764) was born in Königsberg, Prussia (the city noted in mathematical circles for its famous bridge problem). He became professor of mathematics at the Imperial Academy of St. Petersburg in 1725. In 1728, Goldbach went to Moscow to tutor Tsarevich Peter II. In 1742, he entered the Russian Ministry of Foreign Affairs as a staff member. Goldbach is most noted for his correspondence with eminent mathematicians, in particular Leonhard Euler and Daniel Bernoulli. Besides his well-known conjectures that every even positive integer greater than 2 is the sum of two primes and that every odd positive integer greater than 5 is the sum of three primes, Goldbach made several notable contributions to analysis.

11. Goldbach also conjectured that every odd positive integer greater than 5 is the sum of three primes. Verify this conjecture for each of the following odd integers.

a) 7 c) 27 e) 101
b) 17 d) 97 f) 199

12. Show that every integer greater than 11 is the sum of two composite integers.

13. Show that Goldbach's conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the conjecture that every integer greater than 5 is the sum of three primes.

14. Let $G(n)$ denote the number of ways to write the even integer n as the sum $p + q$, where p and q are primes with $p \leq q$. Goldbach's conjecture asserts that $G(n) \geq 1$ for all even integers n with $n > 2$. A stronger conjecture asserts that $G(n)$ tends to infinity as the even integer n grows without bound.

a) Find $G(n)$ for all even integers n with $4 \leq n \leq 30$.
b) Find $G(158)$.
c) Find $G(188)$.

* **15.** Show that if n and k are positive integers with $n > 1$ and all n positive integers $a, a + k, \ldots, a + (n-1)k$ are odd primes, then k is divisible by every prime less than n.

Use Exercise 15 to help you solve Exercises 16–19.

16. Find an arithmetic progression of length six that begins with the integer 7 and where every term is a prime.

17. Find the smallest possible minimum difference for an arithmetic progression that contains four terms and where every term is a prime.

18. Find the smallest possible minimum difference for an arithmetic progression that contains five terms and where every term is a prime.

* **19.** Find the smallest possible minimum difference for an arithmetic progression that contains six terms and where every term is a prime.

20. a) In 1848, A. de Polignac conjectured that every odd positive integer is the sum of a prime and a power of two. Show that this conjecture is false by showing that 509 is a counterexample.

b) Find the next smallest counterexample after 509.

* **21.** A *prime power* is an integer of the form p^n, where p is prime and n is a positive integer greater than 1. Find all pairs of prime powers that differ by 1. Prove that your answer is correct.

22. Let n be a positive integer greater than 1 and let $p_1, p_2, \ldots, p_t$ be the primes not exceeding n. Show that $p_1 p_2 \cdots p_t < 4^n$.

* **23.** Let n be a positive integer greater than 3 and let p be a prime such that $2n/3 < p \leq n$. Show that p does not divide the binomial coefficient $\binom{2n}{n}$.

** **24.** Use Exercises 22 and 23 to show that if n is a positive integer, then there exists a prime p such that $n < p < 2n$. (This is *Bertrand's conjecture.*)

25. Use Exercise 24 to show that if p_n is the nth prime, then $p_n \leq 2^n$.

26. Use Bertrand's conjecture to show that every positive integer n with $n \geq 7$ is the sum of distinct primes.

27. Use Bertrand's postulate to show that $\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+m}$ does not equal an integer when n and m are positive integers.

* **28.** In this exercise, we show that if n is an integer with $n \geq 4$, then $p_{n+1} < p_1 p_2 \cdots p_n$, where p_k is the kth prime. This result is known as *Bonse's inequality.*

a) Let k be a positive integer. Show that none of the integers $p_1 p_2 \cdots p_{k-1} \cdot 1 - 1$, $p_1 p_2 \cdots p_{k-1} \cdot 2 - 1$, $\ldots$, $p_1 p_2 \cdots p_{k-1} \cdot p_k - 1$ is divisible by one of the first $k-1$ primes and that if a prime p divides one of these integers, it cannot divide another of these integers.

b) Conclude from part (a) that if $n - k + 1 < p_k$, then there is an integer among those listed in part (a) not divisible by p_j for $j = 1, \ldots, n$. (*Hint:* Use the pigeonhole principle.)

c) Use part (b) to show that if $n - k + 1 < p_k$, then $p_{n+1} < p_1 p_2 \cdots p_k$. Fix n and suppose that k is the least positive integer such that $n - k + 1 < p_k$. Show that $n - k \geq p_{k-1} - 2$ and that $p_{k-1} - 2 \geq k$ when $k \geq 5$ and that if $n \geq 10$, then $k \geq 5$. Conclude that if $n \geq 20$, then $p_{(n+1)} < p_2 p_2 \cdots p_k$ for some k with $n - k \geq k$. Use this to derive Bonse's inequality when $n \geq 10$.

d) Check the cases when $4 \leq n < 10$ to finish the proof.

29. Show that 30 is the largest integer n with the property that if $k < n$ and there is no prime p that divides both k and n, then k is prime. (*Hint:* Show that if n has this property and $n \geq p^2$ where p is prime, then $p \mid n$. Conclude that if $n \geq 7^2$, then n must be divisible by 2, 3, 5, and 7. Apply Bonse's inequality to show that such an n must be divisible by every prime, a contradiction. Show that 30 has the desired property, but no n with $30 < n < 49$ does.)

* **30.** Show that $p_{n+1} p_{n+2} < p_1 \cdot p_2 \cdots p_n$, where p_k is the kth prime whenever n is an integer with $n \geq 4$. (*Hint:* Use Bertrand's postulate and the work done in part (c) of the proof of Bonse's inequality.

31. Show that $p_n^2 < p_{n-1} p_{n-2} p_{n-3}$, where p_k is the kth prime number and $n \geq 6$. Also, show that inequality does not hold when $n = 3, 4$, or 5. (*Hint:* Use Bertrand's postulate to obtain $p_n < 2p_{n-1}$ and $p_{n-1} < 2p_{n-2}$.)

32. Show that for every positive integer N there is an even number K so that there are more than N pairs of successive primes such that K is the difference between these successive primes. (*Hint:* Use the prime number theorem.)

3.2 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. Verify as much of the information given in Table 3.1 as you can.

2. Find as many tuples of primes of the form p, $p + 2$, and $p + 6$ as you can.

3. Verify Goldbach's conjecture for all even positive integers less than 10,000.

4. Find all twin primes less than 10,000.
5. Find the first pair of twin primes greater than each of the integers in Computation 1.
6. Plot $\pi_2(x)$, the number of twin primes not exceeding x, for $1 \le x \le 1000$ and $1 \le x \le 10,000$.
7. Hardy and Littlewood conjectured that $\pi_2(x)$, the number of twin primes not exceeding x, is asymptotic to $2C_2 x/(\log x)^2$ where $C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right)$. The constant C_2 is approximately equal to 0.66016. Determine how accurate this asymptotic formula for $\pi_2(x)$ is for values of x as large as you can compute.
8. Compute Brun's constant with as much accuracy as possible.
9. Explore the conjecture that $G(n)$, the number of ways to write the even integer n as the sum $p + q$, where p and q are primes with $p \le q$, satisfies $G(n) \ge 10$ for all even integers n with $n \ge 188$.
10. An unsettled conjecture asserts that for every positive integer n, there is an arithmetic progression of length n comprised of n consecutive prime numbers. The longest such arithmetic progression currently known consists of 22 consecutive primes. Find arithmetic progressions consisting of three consecutive primes with all primes less than 100 and four consecutive primes with all primes less than 500.
11. Show that all terms of the arithmetic progression of length five that begins with 1464481 and has common difference 210 are prime.
12. Show that all terms of the arithmetic progression of length twelve that begins with 23143 and has common difference 30030 are prime.
13. Find an arithmetic progression containing ten primes that begins with 199.
14. An unsettled conjecture asserts that for all positive integers n, there is a prime p such that $n^2 < p < (n+1)^2$. Verify this conjecture for as many positive integers n as you can.
15. Explore the conjecture that every even integer is the sum of two, not necessarily distinct, lucky numbers. Continue by exploring the conjecture that given a positive integer k, there is a positive integer n that can be expressed as the sum of two lucky numbers in exactly k ways.

Programming Projects

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

1. Verify Goldbach's conjecture for all even integers less than n, where n is a given positive integer.
2. Find all twin primes less than n, where n is a given positive integer.
3. Find the first m primes of the form $n^2 + 1$, where n is a positive integer and m is a given positive integer.
4. Find $G(n)$, the number of ways to write the even integer n as the sum $p + q$, where p and q are primes with $p \le q$.
5. Given a positive integer n, find as many arithmetic progressions of length n, where every term is a prime.

3.3 Greatest Common Divisors

If a and b are integers, not both 0, then the set of common divisors of a and b is a finite set of integers, always containing the integers $+1$ and -1. We are interested in the largest integer among the common divisors of the two integers.

Definition. The *greatest common divisor* of two integers a and b, which are not both 0, is the largest integer that divides both a and b.

The greatest common divisor of a and b is written as (a, b). (Note that the notation $\gcd(a, b)$ is also used, especially outside of number theory. We will use the traditional notation (a, b) here, even though it is the same notation used for ordered pairs.) We also define $(0, 0) = 0$.

Even though every positive integer divides 0, we define $(0, 0) = 0$. This is done to ensure that the results we prove about greatest common divisors hold in all cases.

Example 3.6. The common divisors of 24 and 84 are ± 1, ± 2, ± 3, ± 4, ± 6, and ± 12. Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that $(15, 81) = 3$, $(100, 5) = 5$, $(17, 25) = 1$, $(0, 44) = 44$, $(-6, -15) = 3$, and $(-17, 289) = 17$. ◀

We are particularly interested in pairs of integers sharing no common divisors greater than 1. Such pairs of integers are called *relatively prime.*

Definition. The integers a and b are *relatively prime* if a and b have greatest common divisor $(a, b) = 1$.

Example 3.7. Since $(25, 42) = 1$, 25 and 42 are relatively prime. ◀

Note that since the divisors of $-a$ are the same as the divisors of a, it follows that $(a, b) = (|a|, |b|)$ (where $|a|$ denotes the absolute value of a, which equals a if $a \geq 0$ and $-a$ if $a < 0$). Hence, we can restrict our attention to the greatest common divisors of pairs of positive integers.

In Example 3.6, we noted that $(15, 81) = 3$. If we divide 15 and 81 by $(15, 81) = 3$, we obtain two relatively prime integers, 5 and 27. This is no surprise, because we have removed all common factors. This illustrates the following theorem, which tells us that we obtain two relatively prime integers when we divide each of two original integers by their greatest common divisor.

Theorem 3.6. Let a and b be integers with $(a, b) = d$. Then $(a/d, b/d) = 1$.

Proof. Let a and b be integers with $(a, b) = d$. We will show that a/d and b/d have no common positive divisors other than 1. Assume that e is a positive integer such that $e \mid (a/d)$ and $e \mid (b/d)$. Then, there are integers k and l with $a/d = ke$ and $b/d = le$, so that $a = dek$ and $b = del$. Hence, de is a common divisor of a and b. Since d is

the greatest common divisor of a and b, $de \leq d$, so that e must be 1. Consequently, $(a/d, b/d) = 1$. ∎

We do not change the greatest common divisor of two integers when we add a multiple of one of the integers to the other. In Example 3.6, we showed that $(24, 84) = 12$. When we add any multiple of 24 to 84, the greatest common divisor of 24 and the resulting number is still 12. For example, since $2 \cdot 24 = 48$ and $(-3) \cdot 24 = -72$, we see that $(24, 84 + 48) = (24, 132) = 12$ and $(24, 84 + (-72)) = (24, 12) = 12$. The reason for this is that the common divisors of 24 and 84 are the same as the common divisors of 24 and the integer that results when a multiple of 24 is added to 84. The proof of the following theorem justifies this reasoning.

Theorem 3.7. Let a, b, and c be integers. Then $(a + cb, b) = (a, b)$.

Proof. Let a, b, and c be integers. We will show that the common divisors of a and b are exactly the same as the common divisors of $a + cb$ and b. This will show that $(a + cb, b) = (a, b)$. Let e be a common divisor of a and b. By Theorem 1.9, we see that $e \mid (a + cb)$, so that e is a common divisor of $a + cb$ and b. If f is a common divisor of $a + cb$ and b, then by Theorem 1.9, we see that f divides $(a + cb) - cb = a$, so that f is a common divisor of a and b. Hence, $(a + cb, b) = (a, b)$. ∎

We will show that the greatest common divisor of the integers a and b, not both 0, can be written as a sum of multiples of a and b. To phrase this more succinctly, we use the following definition.

Definition. If a and b are integers, then a *linear combination* of a and b is a sum of the form $ma + nb$, where both m and n are integers.

Example 3.8. What are the linear combinations $9m + 15n$, where m and n are both integers? Among these combinations are $-6 = 1 \cdot 9 + (-1) \cdot 15$; $-3 = (-2)9 + 1 \cdot 15$; $0 = 0 \cdot 9 + 0 \cdot 15$; $3 = 2 \cdot 9 + (-1) \cdot 15$; $6 = (-1) \cdot 9 + 1 \cdot 15$; and so on. It can be shown that the set of all linear combinations of 9 and 15 is the set $\{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$, as the reader should verify after reading the proofs of the following two theorems. ◀

In Example 3.8, we found that $(9, 15) = 3$ appears as the smallest positive linear combination with integer coefficients of 9 and 15. This is no accident, as the following theorem demonstrates.

Theorem 3.8. The greatest common divisor of the integers a and b, not both 0, is the least positive integer that is a linear combination of a and b.

Proof. Let d be the least positive integer that is a linear combination of a and b. (There is a *least* such positive integer, using the well-ordering property, since at least one of two linear combinations $1 \cdot a + 0 \cdot b$ and $(-1)a + 0 \cdot b$, where $a \neq 0$, is positive.) We write

$$d = ma + nb, \tag{3.1}$$

where m and n are integers. We will show that $d \mid a$ and $d \mid b$.

By the division algorithm, we have

$$a = dq + r, \quad 0 \leq r < d.$$

From this equation and (3.1), we see that

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

This shows that the integer r is a linear combination of a and b. Since $0 \leq r < d$, and d is the least positive linear combination of a and b, we conclude that $r = 0$, and hence $d \mid a$. In a similar manner, we can show that $d \mid b$.

We have shown that d, the least positive integer that is a linear combination of a and b, is a common divisor of a and b. What remains to be shown is that it is the *greatest common divisor* of a and b. To show this, all we need show is that any common divisor c of a and b must divide d, since any proper positive divisor of d is less than d. Since $d = ma + nb$, if $c \mid a$ and $c \mid b$, Theorem 1.9 tells us that $c \mid d$, so that $d \geq c$. This concludes the proof. ∎

Because we will often need to apply Theorem 3.8 in the case where a and b are relatively prime integers, we state the following corollary.

Corollary 3.8.1. If a and b are relatively prime integers, then there are integers m and n such that $ma + nb = 1$.

Proof. To prove this corollary, we note that if a and b are relatively prime, then $(a, b) = 1$. Consequently, by Theorem 3.8, 1 is the least positive integer that is a linear combination of a and b. It follows that there are integers m and n such that $ma + nb = 1$. ∎

Theorem 3.8 is valuable: We can obtain results about the greatest common divisor of two integers using the fact that the greatest common divisor is the least positive linear combination of these integers. Having different representations of the greatest common divisor of two integers allows us to choose the one that is most useful for a particular purpose. This is illustrated in the proof of the following theorem.

Theorem 3.9. If a and b are positive integers, then the set of linear combinations of a and b is the set of integer multiples of (a, b).

Proof. Suppose that $d = (a, b)$. We first show that every linear combination of a and b must also be a multiple of d. First note that by the definition of greatest common divisor, we know that $d \mid a$ and $d \mid b$. Now every linear combination of a and b is of the form $ma + nb$, where m and n are integers. By Theorem 1.9, it follows that whenever m and m are integers, d divides $ma + nb$. That is, $ma + nb$ is a multiple of d.

We now show that every multiple of d is also a linear combination of a and b. By Theorem 3.8 we know that there are integers r and s such that $(a, b) = ra + sb$. The multiples of d are the integers of the form jd, where j is an integer. Multiplying both sides of the equation $d = ra + sb$ by j, we see that $jd = (jr)a + (js)b$. Consequently, every multiple of d is a linear combination of a and b. This completes the proof. ∎

We have defined greatest common divisors using the notion that the integers are ordered. That is, given two distinct integers, one is larger than the other. However, we can define the greatest common divisor of two integers without relying on this notion of order, as we do in Theorem 3.10. This characterization of the greatest common divisor of two integers not depending on ordering is generalized in the study of algebraic number theory to apply to what are known as algebraic number fields.

Theorem 3.10. If a and b are integers, not both 0, then a positive integer d is the greatest common divisor of a and b if and only if:

(i) $d \mid a$ and $d \mid b$

(ii) if c is an integer with $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. We will first show that the greatest common divisor of a and b has these two properties. Suppose that $d = (a, b)$. By the definition of common divisor, we know that $d \mid a$ and $d \mid b$. By Theorem 3.8, we know that $d = ma + nb$, where m and n are integers. Consequently, if $c \mid a$ and $c \mid b$, then by Theorem 1.9, $c \mid d = ma + nb$. We have now shown that if $d = (a, b)$, then properties (i) and (ii) hold.

Now assume that properties (i) and (ii) hold. Then we know that d is a common divisor of a and b. Furthermore, by property (ii), we know that if c is a common divisor of a and b, then $c \mid d$, so that $d = ck$ for some integer k. Hence, $c = d/k \leq d$. (We have used the fact that a positive integer divided by any nonzero integer is less than that integer.) This shows that a positive integer satisfying (i) and (ii) must be the greatest common divisor of a and b. ∎

We have shown that the greatest common divisor of a and b, not both 0, is a linear combination of a and b. However, we have not explained how to find a particular linear combination of a and b that equals (a, b). In the next section, we will provide an algorithm that finds a particular linear combination of a and b that equals (a, b).

We can also define the greatest common divisor of more than two integers.

Definition. Let $a_1, a_2, \ldots, a_n$ be integers, not all 0. The *greatest common divisor* of these integers is the largest integer that is a divisor of all of the integers in the set. The greatest common divisor of $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$. (Note that the order in which the a_i's appear does affect the result.)

Example 3.9. We easily see that $(12, 18, 30) = 6$ and $(10, 15, 25) = 5$. ◀

We can use the following lemma to find the greatest common divisor of a set of more than two integers.

Lemma 3.2. If $a_1, a_2, \ldots, a_n$ are integers, not all 0, then $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$.

Proof. Any common divisor of the n integers $a_1, a_2, \ldots, a_{n-1}, a_n$ is, in particular, a divisor of a_{n-1} and a_n, and therefore a divisor of (a_{n-1}, a_n). Also, any common divisor

of the $n-1$ integers $a_1, a_2, \ldots, a_{n-2}$, and (a_{n-1}, a_n) must be a common divisor of all n integers, for if it divides (a_{n-1}, a_n), it must divide both a_{n-1} and a_n. Since the set of n integers and the set of the first $n-2$ integers together with the greatest common divisor of the last two integers have exactly the same divisors, their greatest common divisors are equal. ∎

Example 3.10. To find the greatest common divisor of the three integers 105, 140, and 350, we use Lemma 3.2 to see that $(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35$. ◀

Example 3.11. Consider the integers 15, 21, and 35. We find that the greatest common divisor of these three integers is 1 using the following steps:

$$(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1.$$

Each pair among these integers has a common factor greater than 1, since $(15, 21) = 3$, $(15, 35) = 5$, and $(21, 35) = 7$. ◀

Example 3.11 motivates the following definition.

Definition. We say that the integers $a_1, a_2, \ldots, a_n$ are *mutually relatively prime* if $(a_1, a_2, \ldots, a_n) = 1$. These integers are called *pairwise relatively prime* if, for each pair of integers a_i and a_j with $i \neq j$ from the set, $(a_i, a_j) = 1$; that is, if each pair of integers from the set is relatively prime.

The concept of pairwise relatively prime is used much more often than the concept of mutually relatively prime. Also, note that pairwise relatively prime integers must be mutually relatively prime, but that the converse is false (as the integers 15, 21, and 35 in Example 3.11 show).

3.3 Exercises

1. Find the greatest common divisor of each of the following pairs of integers.

   a) 15, 35
   b) 0, 111
   c) −12, 18
   d) 99, 100
   e) 11, 121
   f) 100, 102

2. Find the greatest common divisor of each of the following pairs of integers.

   a) 5, 15
   b) 0, 100
   c) −27, −45
   d) −90, 100
   e) 100, 121
   f) 1001, 289

3. Let a be a positive integer. What is the greatest common divisor of a and $2a$?

4. Let a be a positive integer. What is the greatest common divisor of a and a^2?

5. Let a be a positive integer. What is the greatest common divisor of a and $a + 1$?

6. Let a be a positive integer. What is the greatest common divisor of a and $a + 2$?

7. Show that if a and b are integers, not both 0, and c is a nonzero integer, then $(ca, cb) = |c|(a, b)$.

8. Show that if a and b are integers with $(a, b) = 1$, then $(a + b, a - b) = 1$ or 2.

9. What is $(a^2 + b^2, a + b)$, where a and b are relatively prime integers that are not both 0?

10. Show that if a and b are both even integers that are not both 0, then $(a, b) = 2(a/2, b/2)$.

11. Show that if a is an even integer and b is an odd integer, then $(a, b) = (a/2, b)$.

12. Show that if a, b, and c are integers such that $(a, b) = 1$ and $c \mid (a + b)$, then $(c, a) = (c, b) = 1$.

13. Show that if a, b, and c are mutually relatively prime nonzero integers, then $(a, bc) = (a, b)(a, c)$.

☞ 14. a) Show that if a, b, and c are integers with $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.
b) Use mathematical induction to show that if $a_1, a_2, \ldots, a_n$ are integers, and b is another integer such that $(a_1, b) = (a_2, b) = \cdots = (a_n, b) = 1$, then $(a_1 a_2 \cdots a_n, b) = 1$.

15. Find a set of three integers that are mutually relatively prime, but any two of which are not relatively prime. Do not use examples from the text.

16. Find four integers that are mutually relatively prime such that any three of these integers are not mutually relatively prime.

17. Find the greatest common divisor of each of the following sets of integers.

a) 8, 10, 12
b) 5, 25, 75
c) 99, 9999, 0
d) 6, 15, 21
e) -7, 28, -35
f) 0, 0, 1001

18. Find three mutually relatively prime integers from among the integers 66, 105, 42, 70, and 165.

19. Show that if $a_1, a_2, \ldots, a_n$ are integers that are not all 0 and c is a positive integer, then $(ca_1, ca_2, \ldots, ca_n) = c(a_1, a_2 \ldots, a_n)$.

20. Show that the greatest common divisor of the integers $a_1, a_2, \ldots, a_n$, not all 0, is the least positive integer that is a linear combination of $a_1, a_2, \ldots, a_n$.

21. Show that if k is an integer, then the integers $6k - 1$, $6k + 1$, $6k + 2$, $6k + 3$, and $6k + 5$ are pairwise relatively prime.

22. Show that if k is a positive integer, then $3k + 2$ and $5k + 3$ are relatively prime.

23. Show that $8a + 3$ and $5a + 2$ are relatively prime for all integers a.

24. Show that if a and b are relatively prime integers, then $(a + 2b, 2a + b) = 1$ or 3.

25. Show that every positive integer greater than 6 is the sum of two relatively prime integers greater than 1.

The *Farey series* $\mathcal{F}_n$ *of order* n is the set of fractions h/k, where h and k are integers, $0 \le h \le k \le n$, and $(h, k) = 1$, in ascending order. We include 0 and 1 in the forms $0/1$ and $1/1$, respectively. For instance, the Farey series of order 4 is

$$\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}.$$

Exercises 26–29 deal with Farey series.

26. Find the Farey series of order 7.

* **27.** Show that if a/b, c/d, and e/f are successive terms of a Farey series, then

$$\frac{c}{d} = \frac{a+e}{b+f}.$$

* **28.** Show that if a/b and c/d are successive terms of a Farey series, then $ad - bc = -1$.

* **29.** Show that if a/b and c/d are successive terms of the Farey series of order n, then $b + d > n$.

JOHN FAREY (1766–1826) attended school in Woburn, England, until the age of 16. In 1782, he entered a school in Halifax, Yorkshire, where he studied mathematics, drawing, and surveying. In 1790, he married and his first son was born the following year. In 1792, the Duke of Bedford appointed Farey as land steward for his Woburn estates. Farey held this post until 1802, developing expertise in geology. When the duke died suddenly, the duke's brother dismissed Farey, who went to London and established an extensive practice as a surveyor and geologist.

Farey's geologic work included studies of soils and strata in Derbyshire. He also produced a map of the strata visible between London and Brighton. Farey also produced extensive scientific writings, publishing around 60 articles in philosophical and scientific magazines. These articles address a wide range of topics, including geology, forestry, physics, and many other areas.

Although he achieved moderate fame as a geologist, ironically Farey is remembered for a contribution to mathematics. In his four-paragraph 1816 article, "On a curious property of vulgar fractions," Farey noted that a reduced fraction p/q with $0 < p/q < 1$ and $q < n$ equals the fraction whose numerator and denominator are the sum of the numerators and the sum of the denominators, respectively, of the fractions on either side of p/q when all reduced fractions between 0 and 1 with denominators not exceeding n are written in increasing order (see Exercise 27). Farey said he was unaware whether this property was already known. He also wrote that he did not have a proof. The French mathematician Cauchy read Farey's article and proved this property in the book *Exercises de mathématique*, published in 1816. It was Cauchy who coined the name *Farey series* because he thought Farey was the first person to notice this property.

Not surprisingly, Farey was not the first person to notice the property for which he became famous. In 1802, C. Haros wrote an article in which he approximates decimal fractions using common fractions, constructing the Farey sequence for $n = 99$ employing this curious property in his construction.

* **30.** a) Show that if a and b are positive integers, then $((a^n - b^n)/(a - b), a - b) = (n(a, b)^{n-1}, a - b)$.

b) Show that if a and b are relatively prime positive integers, then $((a^n - b^n)/(a - b), a - b) = (n, a - b)$.

31. Show that if a, b, c, and d are integers such that b and d are positive, $(a, b) = (c, d) = 1$, and $\frac{a}{b} + \frac{c}{d}$ is an integer, then $b = d$.

32. What can you conclude if a, b, and c are positive integers such that $(a, b) = (b, c) = 1$ and $\frac{1}{a} + \frac{1}{b} + \frac{1}{c}$ is an integer?

33. Show that if a and b are positive integers, then $(a, b) = 2\sum_{i=1}^{a-1}[bi/a] + a + b - ab$. (*Hint:* Count the number of lattice points, that is, points with integer coordinates, inside or on the triangle with vertices $(0, 0)$, $(0, b)$, and $(a, 0)$ in two different ways.)

34. Show that if n is a positive integer and i and j are integers with $1 \leq i < j \leq n$, then $(n! \cdot i + 1, n! \cdot j + 1) = 1$.

35. Use Exercise 34 to show that there are infinitely many primes. (*Hint:* Assume that there are exactly r primes and consider the $r + 1$ numbers $(r + 1)! \cdot i + 1$. This proof was discovered by P. Schorn.)

36. Show that if c and d are relatively prime positive integers, then the integers a_j, $j = 0, 1, 2, \ldots$, defined by $a_0 = c$ and $a_n = a_0 a_1 \cdots a_{n-1} + d$ for $n = 1, 2, \ldots$, are pairwise relatively prime.

3.3 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. Construct the Farey series of order 100.

2. Verify the properties of the Farey series given in Exercises 27, 28, and 29 for successive terms of your choice in the Farey series of order 100.

Programming Projects

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

1. Find the greatest common divisor of two integers from the lists of their divisors.

2. Print out the Farey series of order n for a given positive integer n.

3.4 The Euclidean Algorithm

We are going to develop a systematic method, or algorithm, to find the greatest common divisor of two positive integers. This method is called the *Euclidean algorithm.* It is named after the ancient Greek mathematician *Euclid,* who describes this algorithm in his *Elements.* (The same method for finding greatest common divisors was also described in the sixth century by the Indian mathematician *Aryabhata,* who called it "the pulverizer.")

Before we discuss the algorithm in general, we demonstrate its use with an example. We find the greatest common divisor of 30 and 72. First, we use the division algorithm to write $72 = 30 \cdot 2 + 12$, and we use Theorem 3.7 to note that $(30, 72) = (30, 72 - 2 \cdot 30) = (30, 12)$. Note that we have replaced 72 by the smaller number 12 in our computations because $(72, 30) = (30, 12)$. Next, we use the division algorithm again to write $30 = 2 \cdot 12 + 6$. Using the same reasoning as before, we see that $(30, 12) = (12, 6)$. Because $12 = 6 \cdot 2 + 0$, we now see that $(12, 6) = (6, 0) = 6$. Consequently, we can conclude that $(72, 30) = 6$, without finding all the common divisors of 30 and 72.

We now present the general form of the Euclidean algorithm for computing the greatest common divisor of two positive integers.

Theorem 3.11. ***The Euclidean Algorithm.*** Let $r_0 = a$ and $r_1 = b$ be integers such that $a \geq b > 0$. If the division algorithm is successively applied to obtain $r_j = r_{j+1}q_{j+1} + r_{j+2}$, with $0 < r_{j+2} < r_{j+1}$ for $j = 0, 1, 2, \ldots, n-2$ and $r_{n+1} = 0$, then $(a, b) = r_n$, the last nonzero remainder. ∎

From this theorem, we see that the greatest common divisor of a and b is the last nonzero remainder in the sequence of equations generated by successively applying the division algorithm and continuing until a remainder is 0—where, at each step, the dividend and divisor are replaced by smaller numbers, namely the divisor and remainder.

To prove that the Euclidean algorithm produces greatest common divisors, the following lemma will be helpful.

Lemma 3.3. If e and d are integers and $e = dq + r$, where q and r are integers, then $(e, d) = (d, r)$.

Proof. This lemma follows directly from Theorem 3.7, taking $a = r$, $b = d$, and $c = q$. ∎

We now prove that the Euclidean algorithm produces the greatest common divisor of two integers.

EUCLID (c. 350 B.C.E) was the author of the most successful mathematics textbook ever written, namely his *Elements*, which has appeared in over a thousand editions from ancient to modern times. Very little is known about Euclid's life, other than that he taught at the famed academy at Alexandria. Evidently he did not stress the applications of mathematics, for it is reputed that when asked by a student for the use of geometry, Euclid had his slave give the student some coins, "since he must needs make gain of what he learns." Euclid's *Elements* provides an introduction to plane and solid geometry, and to number theory. The Euclidean algorithm is found in Book VII of the thirteen books in the *Elements*, and his proof of the infinitude of primes is found in Book IX. Euclid also wrote books on a variety of other topics, including astronomy, optics, music, and mechanics.

Proof. Let $r_0 = a$ and $r_1 = b$ be positive integers with $a \geq b$. By successively applying the division algorithm, we find that

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2,\\
&\vdots\\
r_{j-2} &= r_{j-1} q_{j-1} + r_j && 0 \leq r_j < r_{j-1},\\
&\vdots\\
r_{n-4} &= r_{n-3} q_{n-3} + r_{n-2} && 0 \leq r_{n-2} < r_{n-3},\\
r_{n-3} &= r_{n-2} q_{n-2} + r_{n-1} && 0 \leq r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_n q_n.
\end{aligned}$$

We can assume that we eventually obtain a remainder of zero, because the sequence of remainders $a = r_0 \geq r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms (because each remainder is an integer). By Lemma 3.3, we see that $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Hence, $(a, b) = r_n$, the last nonzero remainder. ∎

We illustrate the use of the Euclidean algorithm with the following example.

Example 3.12. The steps used by the Euclidean algorithm to find (252, 198) are

$$\begin{aligned}
252 &= 1 \cdot 198 + 54\\
198 &= 3 \cdot 54 + 36\\
54 &= 1 \cdot 36 + 18\\
36 &= 2 \cdot 18.
\end{aligned}$$

ARYABHATA (476–550) was born in Kusumapura (now Patna), India. He is the author of the *Aryabhatiya*, a summary of Hindu mathematics written entirely in verse. This book covers astronomy, geometry, plane and spherical trigonometry, arithmetic, and algebra. Topics studied include formulas for areas and volumes, continued fractions, sums of power series, an approximation for π, and tables of sines. Aryabhata also described a method for finding greatest common divisors which is the same as the method described by Euclid. His formulas for the areas of triangles and circles are correct, but those for the volumes of spheres and pyramids are wrong. Aryabhata also produced an astronomy text, *Siddhanta*, which includes a number of remarkably accurate statements (as well as other statements that are not correct). For example, he states that the orbits of the planets are ellipses, and he correctly describes the causes of solar and lunar eclipses. India named its first satellite, launched in 1975 by the Russians, *Aryabhata*, in recognition of his fundamental contributions to astronomy and mathematics.

We summarize these steps in the following table:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

The last nonzero remainder (found in the next-to-last row in the last column) is the greatest common divisor of 252 and 198. Hence, $(252, 198) = 18$. ◀

The Euclidean algorithm is an extremely fast way to find greatest common divisors.

Later, we will see this when we estimate the maximum number of divisions used by the Euclidean algorithm to find the greatest common divisor of two positive integers. However, we first show that, given any positive integer n, there are integers a and b such that exactly n divisions are required to find (a, b) using the Euclidean algorithm. We can find such numbers by taking successive terms of the Fibonacci sequence.

The reason that the Euclidean algorithm operates so slowly when it finds the greatest common divisor of successive Fibonacci numbers is that the quotient in all but the last step is 1, as illustrated in the following example.

Example 3.13. We apply the Euclidean algorithm to find (34, 55). Note that $f_9 = 34$ and $f_{10} = 55$. We have

$$\begin{aligned}
55 &= 34 \cdot 1 + 21 \\
34 &= 21 \cdot 1 + 13 \\
21 &= 13 \cdot 1 + 8 \\
13 &= 8 \cdot 1 + 5 \\
8 &= 5 \cdot 1 + 3 \\
5 &= 3 \cdot 1 + 2 \\
3 &= 2 \cdot 1 + 1 \\
2 &= 1 \cdot 2.
\end{aligned}$$

Observe that when the Euclidean algorithm is used to find the greatest common divisor of $f_9 = 34$ and $f_{10} = 55$, a total of eight divisions are required. Furthermore, $(34, 55) = 1$, since 1 is the last nonzero remainder. ◀

The following theorem tells us how many divisions are used by the Euclidean algorithm to find the greatest common divisor of successive Fibonacci numbers.

Theorem 3.12. Let f_{n+1} and f_{n+2} be successive terms of the Fibonacci sequence, with $n > 1$. Then the Euclidean algorithm takes exactly n divisions to show that $(f_{n+1}, f_{n+2}) = 1$.

Proof. Applying the Euclidean algorithm, and using the defining relation for the Fibonacci numbers $f_j = f_{j-1} + f_{j-2}$ in each step, we see that

$$\begin{aligned} f_{n+2} &= f_{n+1} \cdot 1 + f_n, \\ f_{n+1} &= f_n \cdot 1 + f_{n-1}, \\ &\vdots \\ f_4 &= f_3 \cdot 1 + f_2, \\ f_3 &= f_2 \cdot 2. \end{aligned}$$

Hence, the Euclidean algorithm takes exactly n divisions, to show that $(f_{n+2}, f_{n+1}) = f_2 = 1$. ∎

The Complexity of the Euclidean Algorithm We can now prove a theorem first proved by *Gabriel Lamé*, a French mathematician of the nineteenth century, which gives an estimate for the number of divisions needed to find the greatest common divisor using the Euclidean algorithm.

Theorem 3.13. ***Lamé's Theorem.*** The number of divisions needed to find the greatest common divisor of two positive integers using the Euclidean algorithm does not exceed five times the number of decimal digits in the smaller of the two integers.

Proof. When we apply the Euclidean algorithm to find the greatest common divisor of $a = r_0$ and $b = r_1$ with $a > b$, we obtain the following sequence of equations:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 \le r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, && 0 \le r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

We have used n divisions. We note that each of the quotients $q_1, q_2, \ldots, q_{n-1} \ge 1$, and $q_n \ge 2$, because $r_n < r_{n-1}$. Therefore,

GABRIEL LAMÉ (1795–1870) was a graduate of the École Polytechnique. A civil and railway engineer, he advanced the mathematical theory of elasticity and invented curvilinear coordinates. Although his main contributions were to mathematical physics, he made several discoveries in number theory, including the estimate of the number of steps required by the Euclidean algorithm, and the proof that Fermat's last theorem holds for $n = 7$ (see Section 13.2). It is interesting to note that Gauss considered Lamé to be the foremost French mathematician of his time.

$$\begin{aligned}
r_n &\geq 1 = f_2,\\
r_{n-1} &\geq 2r_n \geq 2f_2 = f_3,\\
r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4,\\
r_{n-3} &\geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5,\\
&\vdots\\
r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n,\\
b &= r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.
\end{aligned}$$

Thus, for there to be n divisions used in the Euclidean algorithm, we must have $b \geq f_{n+1}$. By Example 1.28, we know that $f_{n+1} > \alpha^{n-1}$ for $n > 2$, where $\alpha = (1 + \sqrt{5})/2$. Hence, $b > \alpha^{n-1}$. Now, since $\log_{10} \alpha > 1/5$, we see that

$$\log_{10} b > (n-1) \log_{10} \alpha > (n-1)/5.$$

Consequently,

$$n - 1 < 5 \cdot \log_{10} b.$$

Let b have k decimal digits, so that $b < 10^k$ and $\log_{10} b < k$. Hence, we see that $n - 1 < 5k$, and because k is an integer, we can conclude that $n \leq 5k$. This establishes Lamé's theorem. ∎

The following result is a consequence of Lamé's theorem. It tells us that the Euclidean algorithm is very efficient.

Corollary 3.13.1. The greatest common divisor of two positive integers a and b with $a > b$ can be found using $O((\log_2 a)^3)$ bit operations.

Proof. We know from Lamé's theorem that $O(\log_2 a)$ divisions, each taking $O((\log_2 a)^2)$ bit operations, are needed to find (a, b). Hence, by Theorem 2.3, (a, b) may be found using a total of $O((\log_2 a)^3)$ bit operations. ∎

Expressing Greatest Common Divisors—As Linear Combinations The Euclidean algorithm can be used to express the greatest common divisor of two integers as a linear combination of these integers. We illustrate this by expressing $(252, 198) = 18$ as a linear combination of 252 and 198. Referring to the steps of the Euclidean algorithm used to find (252, 198), by the next to the last step we see that

$$18 = 54 - 1 \cdot 36.$$

By the preceding step, it follows that

$$36 = 198 - 3 \cdot 54,$$

which implies that

$$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

Likewise, by the first step, we have

$$54 = 252 - 1 \cdot 198,$$

so that

$$18 = 4(252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

This last equation exhibits $18 = (252, 198)$ as a linear combination of 252 and 198.

In general, to see how $d = (a, b)$ may be expressed as a linear combination of a and b, refer to the series of equations that is generated by the Euclidean algorithm. By the penultimate equation, we have

$$r_n = (a, b) = r_{n-2} - r_{n-1}q_{n-1}.$$

This expresses (a, b) as a linear combination of r_{n-2} and r_{n-1}. The second to the last equation can be used to express r_{n-1} as $r_{n-3} - r_{n-2}q_{n-2}$. Using this last equation to eliminate r_{n-1} in the previous expression for (a, b), we find that

$$r_n = r_{n-3} - r_{n-2}q_{n-2},$$

so that

$$\begin{aligned}(a, b) &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1} \\ &= (1 + q_{n-1}q_{n-2})r_{n-2} - q_{n-1}r_{n-3},\end{aligned}$$

which expresses (a, b) as a linear combination of r_{n-2} and r_{n-3}. We continue working backward through the steps of the Euclidean algorithm to express (a, b) as a linear combination of each preceding pair of remainders, until we have found (a, b) as a linear combination of $r_0 = a$ and $r_1 = b$. Specifically, if we have found at a particular stage that

$$(a, b) = sr_j + tr_{j-1},$$

then, since

$$r_j = r_{j-2} - r_{j-1}q_{j-1},$$

we have

$$\begin{aligned}(a, b) &= s(r_{j-2} - r_{j-1}q_{j-1}) + tr_{j-1} \\ &= (t - sq_{j-1})r_{j-1} + sr_{j-2}.\end{aligned}$$

This shows how to move up through the equations that are generated by the Euclidean algorithm so that, at each step, the greatest common divisor of a and b may be expressed as a linear combination of a and b.

This method for expressing (a, b) as a linear combination of a and b is somewhat inconvenient for calculation, because it is necessary to work out the steps of the Euclidean algorithm, save all these steps, and then proceed backward through the steps to write (a, b) as a linear combination of each successive pair of remainders. There is another method for finding (a, b) which requires working through the steps of the Euclidean algorithm only once. The following theorem gives this method, which is called the *extended Euclidean algorithm.*

Theorem 3.14. Let a and b be positive integers. Then

$$(a, b) = s_n a + t_n b,$$

where s_n and t_n are the nth terms of the sequences defined recursively by

$$s_0 = 1, \quad t_0 = 0,$$
$$s_1 = 0, \quad t_1 = 1,$$

and

$$s_j = s_{j-2} - q_{j-1}s_{j-1}, \quad t_j = t_{j-2} - q_{j-1}t_{j-1}$$

for $j = 2, 3, \ldots, n$, where the q_j are the quotients in the divisions of the Euclidean algorithm when it is used to find (a, b).

Proof. We will prove that

$$r_j = s_j a + t_j b \tag{3.2}$$

for $j = 0, 1, \ldots, n$. Since $(a, b) = r_n$, once we have established (3.2), we will know that

$$(a, b) = s_n a + t_n b.$$

We prove (3.2) using the second principle of mathematical induction. For $j = 0$, we have $a = r_0 = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b$. Hence, (3.2) is valid for $j = 0$. Likewise, $b = r_1 = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b$, so that (3.2) is valid for $j = 1$.

Now, we assume that

$$r_j = s_j a + t_j b$$

for $j = 1, 2, \ldots, k - 1$. Then, from the kth step of the Euclidean algorithm, we have

$$r_k = r_{k-2} - r_{k-1}q_{k-1}.$$

Using the induction hypothesis, we find that

$$\begin{aligned} r_k &= (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1} \\ &= (s_{k-2} - s_{k-1}q_{k-1})a + (t_{k-2} - t_{k-1}q_{k-1})b \\ &= s_k a + t_k b. \end{aligned}$$

This finishes the proof. ∎

The following example illustrates the use of this algorithm for expressing (a, b) as a linear combination of a and b.

Example 3.14. We summarize the steps used by the extended Euclidean algorithm to express (252, 198) as a linear combination of 252 and 198 in the following table.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	−1
3	36	18	2	0	−3	4
4					4	−5

The values of s_j and t_j, $j = 0, 1, 2, 3, 4$, are computed as follows:

$$s_0 = 1, \qquad t_0 = 0,$$
$$s_1 = 0, \qquad t_1 = 1,$$
$$s_2 = s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1, \qquad t_2 = t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1,$$
$$s_3 = s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3, \qquad t_3 = t_1 - t_2q_2 = 1 - (-1)3 = 4,$$
$$s_4 = s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4, \qquad t_4 = t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5.$$

Because $r_4 = 18 = (252, 198)$ and $r_4 = s_4a + t_4b$, we have

$$18 = (252, 198) = 4 \cdot 252 - 5 \cdot 198. \quad \blacktriangleleft$$

Note that the greatest common divisor of two integers may be expressed as a linear combination of these integers in an infinite number of ways. To see this, let $d = (a, b)$ and let $d = sa + tb$ be one way to write d as a linear combination of a and b, guaranteed to exist by the previous discussion. Then for all integers k,

$$d = (s + k(b/d))a + (t - k(a/d))b.$$

Example 3.15. With $a = 252$ and $b = 198$, we have $18 = (252, 198) = (4 + 11k)252 + (-5 - 14k)198$ for any integer k. $\blacktriangleleft$

3.4 Exercises

1. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) (45, 75) c) (666, 1414)
   b) (102, 222) d) (20785, 44350)

2. Use the Euclidean algorithm to find each of the following greatest common divisors.

   a) (51, 87) c) (981, 1234)
   b) (105, 300) d) (34709, 100313)

3. For each pair of integers in Exercise 1, express the greatest common divisor of the integers as a linear combination of these integers.

4. For each pair of integers in Exercise 2, express the greatest common divisor of the integers as a linear combination of these integers.

5. Find the greatest common divisor of each of the following sets of integers.

   a) 6, 10, 15 b) 70, 98, 105 c) 280, 330, 405, 490

6. Find the greatest common divisor of each of the following sets of integers.

a) 15, 35, 90 b) 300, 2160, 5040 c) 1240, 6660, 15540, 19980

The greatest common divisor of the n integers $a_1, a_2, \ldots, a_n$ can be expressed as a linear combination of these integers. To do this, first express (a_1, a_2) as a linear combination of a_1 and a_2. Then express $(a_1, a_2, a_3) = ((a_1, a_2), a_3)$ as a linear combination of a_1, a_2, and a_3. Repeat this until $(a_1, a_2, \ldots, a_n)$ is expressed as a linear combination of $a_1, a_2, \ldots, a_n$. Use this procedure in Exercises 7 and 8.

7. Express the greatest common divisor of each set of numbers in Exercise 5 as a linear combination of the numbers in that set.

8. Express the greatest common divisor of each set of numbers in Exercise 6 as a linear combination of the numbers in that set.

The greatest common divisor of two positive integers can be found by an algorithm that uses only subtractions, parity checks, and shifts of binary expansions, without using any divisions. The algorithm proceeds recursively using the following reduction:

$$(a, b) = \begin{cases} a & \text{if } a = b; \\ 2(a/2, b/2) & \text{if } a \text{ and } b \text{ are even;} \\ (a/2, b) & \text{if } a \text{ is even and } b \text{ is odd;} \\ (a - b, b) & \text{if } a \text{ and } b \text{ are odd, where } a > b. \end{cases}$$

(*Note:* Reverse the roles of a and b when necessary.) Exercises 9–13 refer to this algorithm.

9. Find (2106, 8318) using this algorithm.

10. Show that this algorithm always produces the greatest common divisor of a pair of positive integers.

* **11.** How many steps does this algorithm use to find (a, b) if $a = (2^n - (-1)^n)/3$ and $b = 2(2^{n-1} - (-1)^{n-1})/3$, when n is a positive integer?

* **12.** Show that to find (a, b) this algorithm uses the subtraction step in the reduction no more than $1 + [\log_2 \max(a, b)]$ times.

* **13.** Devise an algorithm for finding the greatest common divisor of two positive integers using their balanced ternary expansions.

In Exercise 18 of Section 1.5, a modified division algorithm is given, which states that if a and $b > 0$ are integers, then there exist unique integers q, r, and e such that $a = bq + er$, where $e = \pm 1$, $r \geq 0$, and $-b/2 < er \leq b/2$. We can set up an algorithm, analogous to the Euclidean algorithm, based on this modified division algorithm, called the *least-remainder algorithm.* It works as follows: Let $r_0 = a$ and $r_1 = b$, where $a > b > 0$. Using the modified division algorithm repeatedly, obtain the greatest common divisor of a and b as the last nonzero remainder r_n in the sequence of divisions

$$\begin{aligned} r_0 &= r_1 q_1 + e_2 r_2, && -r_1/2 < e_2 r_2 \leq r_1/2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + e_n r_n, && -r_{n-1}/2 < e_n r_n \leq r_{n-1}/2 \\ r_{n-1} &= r_n q_n. \end{aligned}$$

14. Use the least-remainder algorithm to find (384, 226).

15. Show that the least-remainder algorithm always produces the greatest common divisor of two integers.

** **16.** Show that the least-remainder algorithm is always at least as fast as the Euclidean algorithm. (*Hint:* First show that if a and b are positive integers with $2b < a$, then the least-remainder algorithm can find (a, b) with no more steps than it uses to find $(a, a - b)$.)

* **17.** Find a sequence of integers $v_0, v_1, v_2, \ldots$, such that the least-remainder algorithm takes exactly n divisions to find (v_{n+1}, v_{n+2}).

* **18.** Show that the number of divisions needed to find the greatest common divisor of two positive integers using the least-remainder algorithm is less than 8/3 times the number of digits in the smaller of the two numbers, plus 4/3.

* **19.** Let m and n be positive integers and let a be an integer greater than 1. Show that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

* **20.** Show that if m and n are positive integers, then $(f_m, f_n) = f_{(m,n)}$.

The next two exercises deal with the *game of Euclid*. Two players begin with a pair of positive integers and take turns making moves of the following type. A player can move from the pair of positive integers $\{x, y\}$ with $x \geq y$, to any of the pairs $\{x - ty, y\}$, where t is a positive integer and $x - ty \geq 0$. A *winning move* consists of moving to a pair with one element equal to 0.

21. Show that every sequence of moves starting with the pair $\{a, b\}$ must eventually end with the pair $\{0, (a, b)\}$.

* **22.** Show that in a game beginning with the pair $\{a, b\}$, the first player may play a winning strategy if $a = b$ or if $a > b(1 + \sqrt{5})/2$; otherwise, the second player may play a winning strategy. (*Hint:* First show that if $y < x \leq y(1 + \sqrt{5})/2$, then there is a unique move from $\{x, y\}$ that goes to a pair $\{z, y\}$ with $y > z(1 + \sqrt{5})/2$.)

* **23.** Show that the number of bit operations needed to use the Euclidean algorithm to find the greatest common divisor of two positive integers a and b with $a > b$ is $O((\log_2 a)^2)$. (*Hint:* First show that the complexity of division of the positive integer q by the positive integer d is $O(\log d \log q)$.)

* **24.** Let a and b be positive integers and let r_j and q_j, $j = 1, 2, \ldots, n$ be the remainders and quotients of the steps of the Euclidean algorithm as defined in this section.

a) Find the value of $\sum_{j=1}^{n} r_j q_j$.

b) Find the value of $\sum_{j=1}^{n} r_j^2 q_j$.

25. Suppose that a and b are positive integers with $a \geq b$. Let q_i and r_i be the quotients and remainders in the steps of the Euclidean algorithm for $i = 1, 2, \ldots, n$, where r_n is the last nonzero remainder. Let $Q_i = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ and $Q = \prod_{i=0}^{n} Q_i$. Show that $\begin{pmatrix} a \\ b \end{pmatrix} = Q \begin{pmatrix} r_n \\ 0 \end{pmatrix}$.

3.4 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 (9876543210, 123456789), (11111111111, 1000000001) and (45666020043321, 73433510078091009).
2. Verify Lamé's theorem for several different pairs of large positive integers of your choice.
3. Compare the number of steps required to find the greatest common divisor of different pairs of large positive integers of your choice using the Euclidean algorithm, the algorithm described in the preamble to Exercise 9, and the least-remainder algorithm described in the preamble to Exercise 14.
4. Estimate the proportion of pairs of positive integers (a, b) that are relatively prime, where a and b are positive integers not exceeding 1000, not exceeding 10,000, not exceeding 100,000, and not exceeding 1,000,000. To do so, you may want to test a random selection of a small number of such pairs (see Section 10.1 for material on pseudorandom numbers). Can you make any conjectures from this evidence?

Programming Projects

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

1. Find the greatest common divisor of two integers using the Euclidean algorithm.
2. Find the greatest common divisor of two integers using the modified Euclidean algorithm given in the preamble to Exercise 14.
3. Find the greatest common divisor of two integers using no divisions (see the preamble to Exercise 9).
4. Find the greatest common divisor of a set of more than two integers.
5. Express the greatest common divisor of two integers as a linear combination of these integers.
6. Express the greatest common divisor of a set of more than two integers as a linear combination of these integers.

* 7. Play the game of Euclid described in the preamble to Exercise 21.

3.5 The Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic is an important result that shows that the primes are the multiplicative building blocks of the integers.

Theorem 3.15. ***The Fundamental Theorem of Arithmetic.*** Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in nondecreasing order.

Sometimes, the fundamental theorem of arithmetic is extended to apply to the integer 1. That is, 1 is considered to be written uniquely as the empty product of primes.

Example 3.16. The factorizations of some positive integers are given by

$$240 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^4 \cdot 3 \cdot 5, \quad 289 = 17 \cdot 17 = 17^2, \quad 1001 = 7 \cdot 11 \cdot 13. \quad \blacktriangleleft$$

Note that it is convenient to combine all the factors of a particular prime into a power of this prime, such as in the previous example: For the factorization of 240, all the factors of 2 were combined to form 2^4. Factorizations of integers in which the factors of primes are combined to form powers are called *prime-power factorizations.*

To prove the fundamental theorem of arithmetic, we need the following lemma concerning divisibility. This lemma turns out to be a crucial part of the proof.

Lemma 3.4. If a, b, and c are positive integers such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof. Since $(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Multiplying both sides of this equation by c, we have $acx + bcy = c$. By Theorem 1.9, a divides $acx + bcy$, because this is a linear combination of a and bc, both of which are divisible by a. Hence, $a \mid c$. ∎

The following consequence of this lemma will be needed in the proof of the fundamental theorem of arithmetic.

Lemma 3.5. If p divides $a_1 a_2 \cdots a_n$, where p is a prime and $a_1, a_2, \ldots, a_n$ are positive integers, then there is an integer i with $1 \leq i \leq n$ such that p divides a_i.

Proof. We prove this result by induction. The case where $n = 1$ is trivial. Assume that the result is true for n. Consider a product of $n + 1$ integers $a_1 a_2 \cdots a_{n+1}$ that is divisible by the prime p. We know that either $(p, a_1 a_2 \cdots a_n) = 1$ or $(p, a_1 a_2 \cdots a_n) = p$. If $(p, a_1 a_2 \cdots a_n) = 1$, then by Lemma 3.4, $p | a_{n+1}$. On the other hand, if $p | a_1 a_2 \cdots a_n$, using the induction hypothesis, there is an integer i with $1 \leq i \leq n$ such that $p | a_i$. Consequently, $p | a_i$ for some i with $1 \leq i \leq n + 1$. This proves the result. ∎

We now begin the proof of the fundamental theorem of arithmetic. First, we will show that every positive integer greater than 1 can be written as the product of primes in at least one way. Then we will show that this product is unique up to the order of primes that appear.

Proof. We use proof by contradiction. Assume that some positive integer cannot be written as the product of primes. Let n be the smallest such integer (such an integer must exist, from the well-ordering property). If n is prime, it is obviously the product of a set of primes, namely the one prime n. So n must be composite. Let $n = ab$, with $1 < a < n$ and $1 < b < n$. But since a and b are smaller than n, they must be the product of primes. Then, since $n = ab$, we conclude that n is also a product of primes. This contradiction shows that every positive integer can be written as the product of primes.

We now finish the proof of the fundamental theorem of arithmetic by showing that the factorization is unique. Suppose that there is an integer n that has two different factorizations into primes:

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t,$$

where $p_1, p_2, \ldots, p_s$, and $q_1, q_2, \ldots, q_t$ are all primes, with $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$.

Remove all common primes from the two factorizations to obtain

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

where the primes on the left-hand side of this equation differ from those on the right-hand side, $u \geq 1$, and $v \geq 1$ (because the two original factorizations were presumed to differ). However, this leads to a contradiction of Lemma 3.5; by this lemma, p_{i_1} must divide q_{j_k} for some k, which is impossible, since each q_{j_k} is prime and is different from p_{i_1}. Hence, the prime factorization of a positive integer n is unique. ∎

Where Unique Factorization Fails The fact that every positive integer has a unique factorization into primes is a special property of the set of integers that is shared by some, but not all, systems of numbers. In Chapter 13, we will study the diophantine equation $x^n + y^n = z^n$. In the nineteenth century, mathematicians thought they could prove that this equation has no solutions in nonzero integers when n is an integer with $n \geq 3$ (a result known as Fermat's last theorem), using a form of unique factorization for certain types of algebraic numbers. It turned out that these numbers do not enjoy the property of unique factorization. The supposed proofs were incorrect, a problem that escaped the notice of many eminent mathematicians.

Although we do not want to go too far afield (by introducing algebraic number theory, for instance), we can provide an example showing that unique factorization fails for certain types of numbers. Consider the set of numbers of the form $a + b\sqrt{-5}$, where a and b are integers. This set contains every integer (taking $b = 0$), as well as other numbers such as $3\sqrt{-5}$, $-1 + 4\sqrt{-5}$, $7 - 5\sqrt{-5}$, and so on. A number of this form is prime (in this context) if it cannot be written as the product of two other numbers of this form both different than ± 1. Note that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Each of the numbers 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ is a prime (see Exercises 19–22 at the end of this section to see how this can be established). It follows that the set of numbers of the form $a + b\sqrt{-5}$ does not enjoy the property of unique factorization into primes. On the other hand, numbers of the form $a + b\sqrt{-1}$, where a and b are integers, do have unique factorization, as we will show in Chapter 14.

Using Prime Factorizations

The prime-power factorization of a positive integer n encodes essential information about n. Given this factorization, we can immediately deduce whether a prime p divides n since p divides n if and only if it appears in this factorization. (We can obtain a contradiction of the uniqueness of the prime-power factorization of n if a prime q divided n, but did not appear in the prime-power factorization of n. The reader should fill in the other parts

of the proof.) For instance, since $168 = 2^3 \cdot 3 \cdot 7$, each of the primes 2, 3, and 7 divides 120, but none of the primes 5, 11, and 13 do. Furthermore, the highest power of a prime p that divides n is the power of this prime in the prime-power factorization of n. For instance, each of 2^3, 3, and 7 divides 168, but none of 2^4, 3^2, and 7^2 do. Moreover, an integer d divides n if and only if all the primes in the prime-power factorization of d appear in the prime-power factorization of n to powers at least as large as they do in the prime-power factorization of d. (The reader should also verify that this follows from the fundamental theorem of arithmetic.) The following example illustrates how we can find all the positive divisors of a positive integer using this observation.

Example 3.17. The positive divisors of $120 = 2^3 \cdot 3 \cdot 5$ are those positive integers with prime-power factorizations containing only the primes 2, 3, and 5, to powers less than or equal to 3, 1, and 1, respectively. These divisors are

1	3	5	$3 \cdot 5 = 15$
2	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 3 \cdot 5 = 30$
$2^2 = 4$	$2^2 \cdot 3 = 12$	$2^2 \cdot 5 = 20$	$2^2 \cdot 3 \cdot 5 = 60$
$2^3 = 8$	$2^3 \cdot 3 = 24$	$2^3 \cdot 5 = 40$	$2^3 \cdot 3 \cdot 5 = 120.$ ◀

Another way in which we can use prime factorizations is to find greatest common divisors, as illustrated in the following example.

Example 3.18. To be a common divisor of $720 = 2^4 \cdot 3^2 \cdot 5$ and $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$, a positive integer can contain only the primes 2, 3, and 5 in its prime-power factorization, and the power to which one of these primes appears cannot be larger than either of the powers of that prime in the factorizations of 720 and 2100. Consequently, to be a common divisor of 720 and 2100, a positive integer can contain only the primes 2, 3, and 5 to powers no larger than 2, 1, and 1, respectively. Therefore, the greatest common divisor of 720 and 2100 is $2^2 \cdot 3 \cdot 5 = 60$. ◀

To describe, in general, how prime factorizations can be used to find greatest common divisors, let $\min(a, b)$ denote the smaller, or minimum, of the two numbers a and b. Now, let the prime factorizations of a and b be

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorizations of a and of b are included in both products, perhaps with 0 exponents. We note that

$$(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

because for each prime p_i, a and b share exactly $\min(a_i, b_i)$ factors of p_i.

Prime factorizations can also be used to find the smallest integer that is a multiple of each of two positive integers. The problem of finding this integer arises when fractions are added.

Definition. The *least common multiple* of two nonzero integers a and b is the smallest positive integer that is divisible by a and b.

The least common multiple of a and b is denoted by $[a, b]$. (*Note:* The notation $\text{lcm}(a, b)$ is also commonly used to denote the least common multiple of a and b.)

Example 3.19. We have the following least common multiples: $[15, 21] = 105$, $[24, 36] = 72$, $[2, 20] = 20$, and $[7, 11] = 77$. ◀

Once the prime factorizations of a and b are known, it is easy to find $[a, b]$. If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, where $p_1, p_2, \ldots, p_n$ are the primes occurring in the prime-power factorizations of a and b (where we might have $a_i = 0$ or $b_i = 0$ for some i), then for an integer to be divisible by both a and b, it is necessary that in the factorization of the integer, each p_j occurs with a power at least as large as a_j and b_j. Hence, $[a, b]$, the smallest positive integer divisible by both a and b, is

$$[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

where $\max(x, y)$ denotes the larger, or maximum, of x and y.

Finding the prime factorization of large integers is time-consuming. Therefore, we would prefer a method for finding the least common multiple of two integers without using the prime factorizations of these integers. We will show that we can find the least common multiple of two positive integers once we know the greatest common divisor of these integers. The latter can be found via the Euclidean algorithm. First, we prove the following lemma.

Lemma 3.6. If x and y are real numbers, then $\max(x, y) + \min(x, y) = x + y$.

Proof. If $x \geq y$, then $\min(x, y) = y$ and $\max(x, y) = x$, so that $\max(x, y) + \min(x, y) = x + y$. If $x < y$, then $\min(x, y) = x$ and $\max(x, y) = y$, and again we find that $\max(x, y) + \min(x, y) = x + y$. ■

We use the following theorem to find $[a, b]$ once (a, b) is known.

Theorem 3.16. If a and b are positive integers, then $[a, b] = ab/(a, b)$, where $[a, b]$ and (a, b) are the least common multiple and greatest common divisor of a and b, respectively.

Proof. Let a and b have prime-power factorizations $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, where the exponents are nonnegative integers and all primes occurring in either factorization occur in both, perhaps with 0 exponents. Now let $M_j = \max(a_j, b_j)$

and $m_j = \min(a_j, b_j)$. Then, we have

$$\begin{aligned}[a, b](a, b) &= p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n} p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} \\ &= p_1^{M_1+m_1} p_2^{M_2+m_2} \cdots p_n^{M_n+m_n} \\ &= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n} \\ &= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} p_1^{b_1} \cdots p_n^{b_n} \\ &= ab,\end{aligned}$$

since $M_j + m_j = \max(a_j, b_j) + \min(a_j, b_j) = a_j + b_j$ by Lemma 3.6. ∎

The following consequence of the fundamental theorem of arithmetic will be needed later.

Lemma 3.7. Let m and n be relatively prime positive integers. Then, if d is a positive divisor of mn, there is a unique pair of positive divisors d_1 of m and d_2 of n such that $d = d_1 d_2$. Conversely, if d_1 and d_2 are positive divisors of m and n, respectively, then $d = d_1 d_2$ is a positive divisor of mn.

Proof. Let the prime-power factorizations of m and n be $m = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ and $n = q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t}$. Since $(m, n) = 1$, the set of primes $p_1, p_2, \ldots p_s$ and the set of primes $q_1, q_2, \ldots, q_t$ have no common elements. Therefore, the prime-power factorization of mn is

$$mn = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t}.$$

Hence, if d is a positive divisor of mn, then

$$d = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t},$$

where $0 \le e_i \le m_i$ for $i = 1, 2, \ldots, s$ and $0 \le f_j \le n_j$ for $j = 1, 2, \ldots, t$. Now, let $d_1 = (d, m)$ and $d_2 = (d, n)$, so that

$$d_1 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \quad \text{and} \quad d_2 = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}.$$

Clearly, $d = d_1 d_2$ and $(d_1, d_2) = 1$. This is the decomposition of d that we desire. Furthermore, this decomposition is unique. To see this, note that every prime power in the factorization of d must occur in either d_1 or d_2, that prime powers in the factorization of d that are powers of primes dividing m must appear in d_1, and that prime powers in the factorization of d that are powers of primes dividing n must appear in d_2. It follows that d_1 must be (d, m) and d_2 must be (d, n).

Conversely, let d_1 and d_2 be positive divisors of m and n, respectively. Then

$$d_1 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s},$$

where $0 \le e_i \le m_i$ for $i = 1, 2, \ldots, s$, and

$$d_2 = q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t},$$

where $0 \leq f_j \leq n_j$ for $j = 1, 2, \ldots, t$. The integer

$$d = d_1 d_2 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}$$

is clearly a divisor of

$$mn = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t},$$

because the power of each prime occurring in the prime-power factorization of d is less than or equal to the power of that prime in the prime-power factorization of mn. ∎

A Proof of a Special Case of Dirichlet's Theorem Unique factorization can be used to prove special cases of Dirichlet's theorem, which states that the arithmetic progression $an + b$ contains infinitely many primes whenever a and b are relatively prime positive integers. We will illustrate this with a proof of Dirichlet's theorem for the progression $4n + 3$.

Theorem 3.17. There are infinitely many primes of the form $4n + 3$, where n is a positive integer.

Before we prove this result, we prove a useful lemma.

Lemma 3.8. If a and b are integers, both of the form $4n + 1$, then the product ab is also of this form.

Proof. Since a and b are both of the form $4n + 1$, there exist integers r and s such that $a = 4r + 1$ and $b = 4s + 1$. Hence,

$$ab = (4r + 1)(4s + 1) = 16rs + 4r + 4s + 1 = 4(4rs + r + s) + 1,$$

which is again of the form $4n + 1$. ∎

We now prove the desired result.

Proof. Let us assume that there are only a finite number of primes of the form $4n + 3$, say $p_0 = 3, p_1, p_2, \ldots, p_r$. Let

$$Q = 4p_1 p_2 \cdots p_r + 3.$$

Then, there is at least one prime in the factorization of Q of the form $4n + 3$. Otherwise, all of these primes would be of the form $4n + 1$, and by Lemma 3.8, this would imply that Q would also be of this form, which is a contradiction. However, none of the primes $p_0, p_1, \ldots, p_n$ divides Q. The prime 3 does not divide Q, for if $3 \mid Q$, then $3 \mid (Q - 3) = 4p_1 p_2 \cdots p_r$, which is a contradiction. Likewise, none of the primes p_j can divide Q, because $p_j \mid Q$ implies $p_j \mid (Q - 4p_1 p_2 \cdots p_r) = 3$, which is absurd. Hence, there are infinitely many primes of the form $4n + 3$. ∎

Results About Irrational Numbers We conclude this section by proving some results about irrational numbers. If α is a rational number, then we may write α as the

quotient of two integers in infinitely many ways, for if $\alpha = a/b$, where a and b are integers with $b \neq 0$, then $\alpha = ka/kb$ whenever k is a nonzero integer. It is easy to see that a positive rational number may be written uniquely as the quotient of two relatively prime positive integers; when this is done we say that the rational number is in *lowest terms*. We note that the rational number 11/21 is in lowest terms. We also see that

$$\cdots = -33/-63 = -22/-42 = -11/-21 = 11/21 = 22/42 = 33/63 = \cdots.$$

The next two results show that certain numbers are irrational. We start by giving another proof that $\sqrt{2}$ is irrational (we proved this originally in Section 1.1).

Example 3.20. Suppose that $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$, where a and b are relatively prime integers with $b \neq 0$. It follows that $2 = a^2/b^2$, so that $2b^2 = a^2$. Since $2 \mid a^2$, it follows (see Exercise 40 at the end of this section) that $2 \mid a$. Let $a = 2c$, so that $b^2 = 2c^2$. Hence, $2 \mid b^2$, and by Exercise 40, 2 also divides b. However, since $(a, b) = 1$, we know that 2 cannot divide both a and b. This contradiction shows that $\sqrt{2}$ is irrational. ◀

We can also use the following more general result to show that $\sqrt{2}$ is irrational.

Theorem 3.18. Let α be a root of the polynomial $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, where the coefficients $c_0, c_1, \ldots, c_{n-1}$ are integers. Then α is either an integer or an irrational number.

Proof. Suppose that α is rational. Then we can write $\alpha = a/b$, where a and b are relatively prime integers with $b \neq 0$. Because α is a root of $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$, we have

$$(a/b)^n + c_{n-1}(a/b)^{n-1} + \cdots + c_1(a/b) + c_0 = 0.$$

Multiplying by b^n, we find that

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n = 0.$$

Since

$$a^n = b(-c_{n-1}a^{n-1} - \cdots - c_1ab^{n-2} - c_0b^{n-1}),$$

we see that $b \mid a^n$. Assume that $b \neq \pm 1$. Then, b has a prime divisor p. Since $p \mid b$ and $b \mid a^n$, we know that $p \mid a^n$. Hence, by Exercise 41, we see that $p \mid a$. However, since $(a, b) = 1$, this is a contradiction, which shows that $b = \pm 1$. Consequently, if α is rational then $\alpha = \pm a$, so that α must be an integer. ■

We illustrate the use of Theorem 3.18 with the following example.

Example 3.21. Let a be a positive integer that is not the mth power of an integer, so that $\sqrt[m]{a}$ is not an integer. Then $\sqrt[m]{a}$ is irrational by Theorem 3.18, since $\sqrt[m]{a}$ is a root of $x^m - a$. Consequently, such numbers as $\sqrt{2}$, $\sqrt[3]{5}$, $\sqrt[10]{17}$, etc., are irrational. ◀

The fundamental theorem of arithmetic can be used to prove the following result, which relates the famous Riemann zeta function to the prime numbers.

Theorem 3.19. If s is a real number with $s > 1$, then

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Not surprisingly, we will not prove Theorem 3.19 because its proof depends on results from analysis. We note here that the proof uses the fundamental theorem of arithmetic to show that the term $1/n^s$, where n is a positive integer, appears exactly once when the terms of the product on the right-hand side are expanded. To see this, we use the fact that

$$\frac{1}{1 - p_j^{-s}} = \sum_{k=0}^{\infty} \frac{1}{p_j^{k_s}}$$

and then we multiply these sums together, obtaining the term

$$\frac{1}{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

when the denominator is the prime-power factorization of n exactly once. The details of the proof can be found in [HaWr79].

3.5 Exercises

1. Find the prime factorizations of each of the following integers.

   a) 36 e) 222 i) 5040
   b) 39 f) 256 j) 8000
   c) 100 g) 515 k) 9555
   d) 289 h) 989 l) 9999

2. Find the prime factorization of 111,111.
3. Find the prime factorization of 4,849,845.
4. Find all of the prime factors of each of the following integers.

   a) 100,000 b) 10,500,000 c) 10! d) $\binom{30}{10}$

5. Find all of the prime factors of each of the following integers.

   a) 196,608 b) 7,290,000 c) 20! d) $\binom{50}{25}$

6. Show that all of the powers in the prime-power factorization of an integer n are even if and only if n is a perfect square.
7. Which positive integers have exactly three positive divisors? Which have exactly four positive divisors?

8. Show that every positive integer can be written as the product of possibly a square and a square-free integer. A *square-free integer* is an integer that is not divisible by any perfect squares other than 1.

9. An integer n is called *powerful* if, whenever a prime p divides n, p^2 divides n. Show that every powerful number can be written as the product of a perfect square and a perfect cube.

10. Show that if a and b are positive integers and $a^3 \mid b^2$, then $a \mid b$.

Let p be a prime and n a positive integer. If $p^a \mid n$, but $p^{a+1} \nmid n$, we say that p^a *exactly divides* n, and we write $p^a \,||\, n$.

11. Show that if $p^a \,||\, m$ and $p^b \,||\, n$, then $p^{a+b} \,||\, mn$.

12. Show that if $p^a \,||\, m$, then $p^{ka} \,||\, m^k$.

13. Show that if $p^a \,||\, m$ and $p^b \,||\, n$ with $a \neq b$, then $p^{\min(a,b)} \,||\, (m+n)$.

14. Let n be a positive integer. Show that the power of the prime p occurring in the prime-power factorization of $n!$ is

$$[n/p] + [n/p^2] + [n/p^3] + \cdots.$$

15. Use Exercise 14 to find the prime-power factorization of 20!.

16. How many zeros are there at the end of 1000! in decimal notation? How many in base 8 notation?

17. Find all positive integers n such that $n!$ ends with exactly 74 zeros in decimal notation.

18. Show that if n is a positive integer, it is impossible for $n!$ to end with exactly 153, 154, or 155 zeros when it is written in decimal notation.

Let $\alpha = a + b\sqrt{-5}$, where a and b are integers. Define the *norm* of α, denoted by $N(\alpha)$, as $N(\alpha) = a^2 + 5b^2$.

19. Show that if $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$, where a, b, c, and d are integers, then $N(\alpha\beta) = N(\alpha)N(\beta)$.

20. A number of the form $a + b\sqrt{-5}$ is *prime* if it cannot be written as the product of numbers α and β, where neither α nor β equals ± 1. Show that the number 2 is a prime number of the form $a + b\sqrt{-5}$. (*Hint:* Start with $N(2) = N(\alpha\beta)$, and use Exercise 19.)

21. Use an argument similar to that in Exercise 20 to show that 3 is a prime number of the form $a + b\sqrt{-5}$.

22. Use arguments similar to that in Exercise 20 to show that both $1 \pm \sqrt{-5}$ are prime numbers of the form $a + b\sqrt{-5}$.

23. Find two different factorizations of the number 21 into primes of the form $a + b\sqrt{-5}$, where a and b are integers.

* 24. Show that the set of all numbers of the form $a + b\sqrt{-6}$, where a and b are integers, does not enjoy the property of unique factorization.

The next four exercises present another example of a system where unique factorization into primes fails. Let H be the set of all positive integers of the form $4k + 1$, where k is a nonnegative integer.

25. Show that the product of two elements of H is also in H.

26. An element $h \neq 1$ in H is called a *Hilbert prime* (named after famous German mathematician *David Hilbert*) if the only way it can be written as the product of two integers in H is $h = h \cdot 1 = 1 \cdot h$. Find the 20 smallest Hilbert primes.

27. Show that every element of H can be factored into Hilbert primes.

28. Show that factorization of elements of H into Hilbert primes is not necessarily unique, by finding two different factorizations of 693 into Hilbert primes.

29. Which positive integers n are divisible by all integers not exceeding $\sqrt{n}$?

30. Find the least common multiple of each of the following pairs of integers.

a) 8, 12
b) 14, 15
c) 28, 35
d) 111, 303
e) 256, 5040
f) 343, 999

31. Find the least common multiple of each of the following pairs of integers.

a) 7, 11
b) 12, 18
c) 25, 30
d) 101, 333
e) 1331, 5005
f) 5040, 7700

32. Find the greatest common divisor and least common multiple of the following pairs of integers.

a) $2 \cdot 3^2 5^3$, $2^2 3^3 7^2$
b) $2 \cdot 3 \cdot 5 \cdot 7$, $7 \cdot 11 \cdot 13$
c) $2^8 3^6 5^4 11^{13}$, $2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$
d) $41^{101} 47^{43} 103^{1001}$, $41^{11} 43^{47} 83^{111}$

DAVID HILBERT (1862–1943), born in Königsberg, the city famous in mathematics for its seven bridges, was the son of a judge. During his tenure at Göttingen University, from 1892 to 1930, Hilbert made many fundamental contributions to a wide range of mathematical subjects. He almost always worked on one area of mathematics at a time, making important contributions, then moving to a new mathematical subject. Some areas in which Hilbert worked are the calculus of variations, geometry, algebra, number theory, logic, and mathematical physics. Besides his many outstanding original contributions, Hilbert is remembered for his famous list of 23 difficult problems. He described these problems at the 1900 International Congress of Mathematicians, as a challenge to mathematicians at the birth of the twentieth century. Since that time, they have spurred a tremendous amount and variety of research. Although many of these problems have now been solved, several remain open, including the Riemann hypothesis, which is part of Problem 8 on Hilbert's list. Hilbert was also the author of several important textbooks in number theory and geometry.

33. Find the greatest common divisor and least common multiple of the following pairs of integers.

a) $2^2 3^3 5^5 7^7$, $2^7 3^5 5^3 7^2$

b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $17 \cdot 19 \cdot 23 \cdot 29$

c) $2^3 5^7 11^{13}$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

d) $47^{11} 79^{111} 101^{1001}$, $41^{11} 83^{111} 101^{1000}$

34. Show that every common multiple of the positive integers a and b is divisible by the least common multiple of a and b.

35. Periodical cicadas are insects with very long larval periods and brief adult lives. For each species of periodical cicada with a larval period of 17 years, there is a similar species with a larval period of 13 years. If both the 17-year and 13-year species emerged in a particular location in 1900, when will they next both emerge in that location?

36. Which pairs of integers a and b have greatest common divisor 18 and least common multiple 540?

37. Show that if a and b are positive integers, then $(a, b) \mid [a, b]$. When does $(a, b) = [a, b]$?

38. Show that if a and b are positive integers, then there are divisors c of a and d of b with $(c, d) = 1$ and $cd = [a, b]$.

☞ **39.** Show that if a, b, and c are integers, then $[a, b] \mid c$ if and only if $a \mid c$ and $b \mid c$.

☞ **40.** Use Lemma 3.4 to show that if p is a prime and a is an integer with $p \mid a^2$, then $p \mid a$.

☞ **41.** Show that if p is a prime, a is an integer, and n is a positive integer such that $p \mid a^n$, then $p \mid a$.

42. Show that if a, b, and c are integers with $c \mid ab$, then $c \mid (a, c)(b, c)$.

43. a) Show that if a and b are positive integers with $(a, b) = 1$, then $(a^n, b^n) = 1$ for all positive integers n.

b) Use part (a) to prove that if a and b are integers such that $a^n \mid b^n$, where n is a positive integer, then $a \mid b$.

44. Show that $\sqrt[3]{5}$ is irrational:

a) by an argument similar to that given in Example 3.20;

b) using Theorem 3.18.

45. Show that $\sqrt{2} + \sqrt{3}$ is irrational.

46. Show that $\log_2 3$ is irrational.

47. Show that $\log_p b$ is irrational, where p is a prime and b is a positive integer that is not the second or higher power of p.

* **48.** Let n be a positive integer greater than 1. Show that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.

49. Show that if a and b are positive integers, then $(a, b) = (a + b, [a, b])$.

50. Find the two positive integers with sum 798 and least common multiple 10,780. (*Hint:* Use Exercise 49.)

51. Show that if a, b, and c are positive integers, then $([a, b], c) = [(a, c), (b, c)]$ and $[(a, b), c] = ([a, c], [b, c])$.

The *least common multiple* of the integers $a_1, a_2, \ldots, a_n$, which are not all zero, is the smallest positive integer that is divisible by all the integers $a_1, a_2, \ldots, a_n$; it is denoted by $[a_1, a_2, \ldots, a_n]$.

52. Find [6, 10, 15] and [7, 11, 13].

53. Show that $[a_1, a_2, \ldots, a_{n-1}, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n]$.

54. Let n be a positive integer. How many pairs of positive integers satisfy $[a, b] = n$? (*Hint:* Consider the prime factorization of n.)

55. a) Show that if a, b, and c are positive integers, then

$$\max(a, b, c) = a + b + c - \min(a, b) - \min(a, c) - \min(b, c) + \min(a, b, c).$$

b) Use part (a) to show that

$$[a, b, c] = \frac{abc(a, b, c)}{(a, b)(a, c)(b, c)}.$$

56. Generalize Exercise 55 to find a formula relating $(a_1, a_2, \ldots, a_n)$ and $[a_1, a_2, \ldots, a_n]$, where $a_1, a_2, \ldots, a_n$ are positive integers.

57. Show that if a, b, and c are positive integers, then $(a, b, c)[ab, ac, bc] = abc$.

58. Show that if a, b, and c are positive integers, then $[a, b, c](ab, ac, bc) = abc$.

59. Show that if a, b, and c are positive integers, then $([a, b], [a, c], [b, c]) = [(a, b), (a, c), (b, c)]$.

60. Prove that there are infinitely many primes of the form $6k + 5$, where k is a positive integer.

* **61.** Show that if a and b are positive integers, then the arithmetic progression a, $a + b$, $a + 2b, \ldots$, contains an arbitrary number of consecutive composite terms.

62. Find the prime factorizations of each of the following integers.

a) $10^6 - 1$ d) $2^{24} - 1$
b) $10^8 - 1$ e) $2^{30} - 1$
c) $2^{15} - 1$ f) $2^{36} - 1$

63. A discount store sells a camera at a price less than its usual retail price of \$99 but more than \$1. If they sell \$8137 worth of this camera and the discounted dollar price is an integer, how many cameras did they sell?

64. A publishing company sells \$375,961 worth of a particular book. How many copies of the book did they sell if their price is an exact dollar amount which is more than \$1?

65. If a store sells \$139,499 worth of electronic organizers at a sale price which is an exact dollar amount less than \$300 and more than \$1, how many electronic organizers did they sell?

66. Show that if a and b are positive integers, then $a^2 \mid b^2$ implies that $a \mid b$.

67. Show that if a, b, and c are positive integers with $(a, b) = 1$ and $ab = c^n$, then there are positive integers d and e such that $a = d^n$ and $b = e^n$.

☞ **68.** Show that if $a_1, a_2, \ldots, a_n$ are pairwise relatively prime integers, then $[a_1, a_2, \ldots, a_n] = a_1 a_2 \cdots a_n$.

69. Show that among any set of $n + 1$ positive integers not exceeding $2n$, there is an integer that divides a different integer in the set.

70. Show that $(m + n)!/m!n!$ is an integer whenever m and n are positive integers.

*** 71.** Find all solutions of the equation $m^n = n^m$, where m and n are integers.

72. Let $p_1, p_2, \ldots, p_n$ be the first n primes and let m be an integer with $1 < m < n$. Let Q be the product of a set of m primes in the list and let R be the product of the remaining primes. Show that $Q + R$ is not divisible by any primes in the list, and hence must have a prime factor not in the list. Conclude that there are infinitely many primes.

73. This exercise presents another proof that there are infinitely many primes. Assume that there are exactly r primes $p_1, p_2, \ldots, p_r$. Let $Q_k = \left(\prod_{j=1}^{r} p_j\right)/p_k$ for $k = 1, 2, \ldots, r$. Let $S = \sum_{j=1}^{r} Q_j$. Show that S must have a prime factor not among the r primes listed. Conclude that there are infinitely many primes. (This proof was published by G. Métrod in 1917.)

74. Show that if p is prime and $1 \leq k < p$, then the binomial coefficient $\binom{p}{k}$ is divisible by p.

75. Prove that in the prime factorization of $n!$, where n is an integer with $n > 1$, there is at least one prime factor with 1 as its exponent. (*Hint:* Use Bertrand's postulate.)

Exercises 76 and 77 outline two additional proofs that there are infinitely many primes.

76. Suppose that $p_1, \ldots, p_j$ are the first j primes, listed in increasing order. Denote by $N(x)$ the number of integers n not exceeding the integer x that are not divisible by any prime exceeding p_j.

a) Show that every integer n not divisible by any prime exceeding p_j can be written in the form $n = r^2 s$, where s is square-free.

b) Show there are only 2^j possible values of s in part (a) by looking at the prime factorization of such an integer n, which is a product of terms $p_k^{e_k}$, where $0 \leq k \leq j$ and e_k is 0 or 1.

c) Show that if $n \leq x$, then $r \leq \sqrt{n} \leq \sqrt{x}$, where r is in part (a). Conclude that there are no more than $\sqrt{x}$ different values possible for r. Conclude that $N(x) \leq 2^j \sqrt{x}$.

d) Show that if the number of primes is finite and p_j is the largest prime, then $N(x) = x$ for all integers x.

e) Show from parts (c) and (d) that $x \leq 2^j \sqrt{x}$, so that $x \leq 2^{2j}$ for all x, leading to a contradiction. Conclude that there must be infinitely many primes.

*** 77.** This exercise develops a proof that there are infinitely many primes based on the fundamental theorem of arithmetic published by A. Auric in 1915. Assume that there are exactly r primes, $p_1 < p_2 < \cdots < p_r$. Suppose that n is a positive integer and let $Q = p_r^n$.

a) Show that an integer m with $1 \leq m \leq Q$ can be written uniquely as $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $e_i \geq 0$ for $i = 1, 2, \ldots, r$. Furthermore, show that for the integer m with this factorization, $p_1^{e_1} \leq m \leq Q = p_r^n$.

b) Let $C = (\log p_r)/(\log p_1)$. Show that $e_i \leq nC$ for $i = 1, 2, \ldots, r$ and that Q does not exceed the number of r-tuples $(e_1, e_2, \ldots, e_r)$ of exponents in the prime-power factorizations of integers m with $1 \leq m \leq Q$.

c) Conclude from part (b) that $Q = p_r^n \leq (Cn+1)^r \leq n^r(C+1)^r$.

d) Show that the inequality in part (c) cannot hold for sufficiently large values of n. Conclude that there must be infinitely many primes.

Suppose that n is a positive integer. We define the *Smarandache function* $S(n)$ by specifying that $S(n)$ is the least positive integer for which n divides $S(n)!$. For example, $S(8) = 4$ since 8 does not divide $1! = 1$, $2! = 2$, and $3! = 6$, but it does divide $4! = 24$.

78. Find $S(n)$ for all positive integers n not exceeding 12.

79. Find $S(n)$ for $n = 40, 41$, and 43.

80. Show that $S(p) = p$ whenever p is prime.

Let $a(n)$ be the least inverse of the Smarandache function, that is, the least positive integer for m for which $S(m) = n$. In other words, $a(n)$ is the position of the first occurrence of the integer n in the sequence $S(1), S(2), \ldots, S(k), \ldots$.

81. Find $a(n)$ for all positive integers n not exceeding 11.

* **82.** Find $a(12)$.

83. Show that $a(p) = p$ whenever p is prime.

Let $\text{rad}(n)$ be the product of the primes that occur in the prime-power factorization of n. For example, $\text{rad}(360) = \text{rad}(2^3 \cdot 3^2 \cdot 5) = 2 \cdot 3 \cdot 5 = 60$.

84. Find $\text{rad}(n)$ for each of these values of n.

a) 300 c) 44004

b) 44 d) 128128

85. Show that $\text{rad}(n) = n$ when n is a positive integer if and only if n is square-free.

86. What is the value of $\text{rad}(n!)$ when n is a positive integer?

87. Show that $\text{rad}(nm) \leq \text{rad}(n)\text{rad}(m)$ for all positive integers m and n. For which positive integers m and n does equality hold?

The next six exercises establish some estimates for the size of $\pi(x)$, the number of primes less than or equal to x. These results were originally proved in the nineteenth century by Chebyshev.

88. Let p be a prime and let n be a positive integer. Show that p divides $\binom{2n}{n}$ exactly

$$([2n/p] - 2[n/p]) + ([2n/p^2] - 2[n/p^2]) + \cdots + ([2n/p^t] - 2[n/p^t])$$

times, where $t = [\log_p 2n]$. Conclude that if p^r divides $\binom{2n}{n}$, then $p^r \leq 2n$.

89. Use Exercise 88 to show that

$$\binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

90. Show that the product of all primes between n and $2n$ is between $\binom{2n}{n}$ and $n^{\pi(2n)-\pi(n)}$. (*Hint:* Use the fact that every prime between n and $2n$ divides $(2n)!$ but not $(n!)^2$.)

91. Use Exercises 89 and 90 to show that

$$\pi(2n) - \pi(n) < n \log 4 / \log n.$$

* **92.** Use Exercise 91 to show that

$$\pi(2n) = (\pi(2n) - \pi(n)) + (\pi(n) - \pi(n/2)) + (\pi(n/2) - \pi(n/4)) + \cdots \leq n \log 64 / \log n.$$

* **93.** Use Exercises 89 and 92 to show that there are positive constants c_1 and c_2 such that

$$c_1 x / \log x < \pi(x) < c_2 x / \log x$$

for all $x \geq 2$. (Compare this to the strong statement given in the prime number theorem, stated as Theorem 3.4 in Section 3.2.)

3.5 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. Find the prime factorizations of 8,616,460,799; 1,234,567,890; 111,111,111,111; and 43,854,532,213,873.
2. Compare the number of primes of the form $4n + 1$ and the number of primes of the form $4n + 3$ for a range of values of n. Can you make any conjectures about the relationship between these numbers?
3. Find the smallest prime of the form $an + b$, given integers a and b, for a range of values of a and b. Can you make any conjectures about such primes?

Programming Projects

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

1. Find all of the positive divisors of a positive integer from its prime factorization.
2. Find the greatest common divisor of two positive integers from their prime factorizations.
3. Find the least common multiple of two positive integers from their prime factorizations.
4. Find the number of zeros at the end of the decimal expansion of $n!$, where n is a positive integer.
5. Find the prime factorization of $n!$, where n is a positive integer.

3.6 Factorization Methods and the Fermat Numbers

By the fundamental theorem of arithmetic, we know that every positive integer can be written uniquely as the product of primes. In this section, we discuss the problem of determining this factorization, and we introduce several simple factoring methods. Factoring integers is an extremely active area of mathematical research, especially because it is important in cryptography, as we will see in Chapter 8. In that chapter,

we will learn that the security of the RSA public-key cryptosystem is based on the observation that factoring integers is much, much harder than finding large primes.

Before we discuss the current status of factoring algorithms, we will consider the most direct way to factor integers, called *trial division*. We will explain why it is not very efficient. Recall from Theorem 3.2 that n either is prime, or has a prime factor not exceeding $\sqrt{n}$. Consequently, when we divide n successively by the primes $2, 3, 5, \ldots$, not exceeding $\sqrt{n}$, either we find a prime factor p_1 of n or we conclude that n is prime. If we have located a prime factor p_1 of n, we next look for a prime factor of $n_1 = n/p_1$, beginning our search with the prime p_1, as n_1 has no prime factor less than p_1, and any factor of n_1 is also a factor of n. We continue, if necessary, determining whether any of the primes not exceeding $\sqrt{n_1}$ divide n_1. We continue in this manner, proceeding iteratively, to find the prime factorization of n.

Example 3.22. Let $n = 42{,}833$. We note that n is not divisible by 2, 3, or 5, but that $7 \mid n$. We have

$$42{,}833 = 7 \cdot 6119.$$

Trial divisions show that 6119 is not divisible by any of the primes 7, 11, 13, 17, 19, or 23. However, we see that

$$6119 = 29 \cdot 211.$$

Since $29 > \sqrt{211}$, we know that 211 is prime. We conclude that the prime factorization of 42,833 is $42{,}833 = 7 \cdot 29 \cdot 211$. ◀

Unfortunately, this method for finding the prime factorization of an integer is quite inefficient. To factor an integer N, it may be necessary to perform as many as $\pi(\sqrt{N})$ divisions (assuming that we already have a list of the primes not exceeding $\sqrt{N}$), altogether requiring on the order of $\sqrt{N} \log N$ bit operations because, from the prime number theorem, $\pi(\sqrt{N})$ is approximately $\sqrt{N}/\log \sqrt{N} = 2\sqrt{N}/\log N$, and from Theorem 2.7, these divisions take $O(\log^2 N)$ bit operations each.

Modern Factorization Methods

Mathematicians have long been fascinated with the problem of factoring integers. In the seventeenth century, *Pierre de Fermat* invented a factorization method based on the idea of representing a composite integer as the difference of two squares. This method is of theoretical and some practical importance, but is not very efficient in itself. We will discuss Fermat's factorization method later in this section.

Since 1970, many new factorization methods have been invented that make it possible, using powerful modern computers, to factor integers that had previously seemed impervious. We will describe several of the simplest of these newer methods. However, the most powerful factorization methods currently known are extremely complicated. Their description is beyond the scope of this book, but we will discuss the size of the integers that they can factor.

Among recent factorization methods (developed in the past twenty-five years) are several invented by J. M. Pollard, including the Pollard rho method (discussed in Section 4.6) and the Pollard $p-1$ method (discussed in Section 6.1). These two methods are generally too slow for difficult factoring problems, unless the numbers being factored have special properties. In Section 12.5, we will introduce another method for factoring that uses continued fractions. A variation of this method, introduced by Morrison and Brillhart, was the major method used to factor large integers during the 1970s. This algorithm was the first factoring algorithm to run in *subexponential time,* which means that the number of bit operations required to factor an integer n could be written in the form $n^{\alpha(n)}$ where $\alpha(n)$ decreases as n increases. A useful notation for describing the number of bit operations required to factor a number by an algorithm running in subexponential time is $L(a, b)$, which implies that the number of bit operations used by the algorithm is $O(\exp(b(\log n)^a(\log\log n)^{1-a}))$. (The precise definition of $L(a, b)$ is somewhat more complicated.) The variation of the continued fraction algorithm invented by Morrison and Brillhart uses $L(1/2, \sqrt{3/2})$ bit operations. Its greatest success was the factorization of a 63-digit number in 1970.

The *quadratic sieve,* described by Carl Pomerance in 1981, made it possible for the first time to factor numbers having more than one hundred digits not of a special form. This method, with many enhancements added after its original invention, uses $L(1/2, 1)$ bit operations. Its great success was in factoring a 129-digit integer known as RSA-129, whose factorization was posed as a challenge by the inventors of the RSA cryptosystem discussed in Chapter 8. Currently, the best general-purpose factoring algorithm for integers with more than 115 digits is the *number field sieve,* originally suggested by Pollard and improved by Buhler, Lenstra, and Pomerance, which uses $L(1/3, (64/9)^{1/3})$ bit operations. Its greatest success has been the factorization of a 160-digit integer known as RSA-160 in early 2003. For factoring numbers with fewer than 115 digits, the quadratic sieve still seems to be quicker than the number field sieve.

An important feature of the number field and quadratic sieves (as well as other methods) is that these algorithms can be run in parallel on many computers (or processors) at the same time. This makes it possible for large teams of people to work on factoring the

PIERRE DE FERMAT (1601–1665) was a lawyer by profession. He was a noted jurist at the provincial parliament in the French city of Toulouse. Fermat was probably the most famous amateur mathematician in history. He published almost none of his mathematical discoveries, but did correspond with contemporary mathematicians about them. From his correspondents, especially the French monk Mersenne (discussed in Chapter 6), the world learned about his many contributions to mathematics. Fermat was one of the inventors of analytic geometry. Furthermore, he laid the foundations of calculus. Fermat, along with Pascal, gave a mathematical basis to the concept of probability. Some of Fermat's discoveries come to us only because he made notes in the margins of his copy of the work of Diophantus. His son found his copy with these notes, and published them so that other mathematicians would be aware of Fermat's results and claims.

Number of Decimal Digits	Approximate MIPS–Years Required
150	10^4
225	10^8
300	10^{11}
450	10^{16}
600	10^{20}

Table 3.2 *Computing power required to factor integers using the number field sieve.*

same integer. (See the historical note on factoring RSA-129 and other RSA challenge numbers, at the end of this subsection.)

How big will the numbers be that can be factored in the future? The answer depends on whether (or, more likely, how soon) more efficient algorithms are invented, as well as how quickly computing power advances. A useful and commonly used measure for estimating the amount of computing required to factor integers of a certain size is millions of instructions per second–years, or MIPS–years. (One MIPS–year represents the computing power of the classical DEC VAX 11/780 during one year. It is still used as a reference point even though this computer is obsolete. Pentium PCs operate at hundreds of MIPS.) Table 3.2 (adapted from information in [Od95]) displays the computing power (in terms of MIPS–years, rounded to the nearest power of ten) required to factor integers of a given size using the number field sieve. Teams of people can work together, dedicating thousands or even millions of MIPS–years to factor particular numbers. Consequently, even without the development of new algorithms, it might not be surprising to see the factorization, within the next ten years, of integers (not of a special form) with 200, or perhaps as many as 250 decimal digits.

For further information on factoring algorithms, we refer the reader to [Br89], [Br00], [Di84], [Gu75], [Od95], [Po84], [Po90], [Ri94], [Ru83], [WaSm87], and [Wi84].

Fermat Factorization We now describe a factorization technique that is interesting, although it is not always efficient. This technique, discovered by Fermat, is known as *Fermat factorization,* and is based on the following lemma.

Lemma 3.9. If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers and differences of two squares that equal n.

Proof. Let n be an odd positive integer and let $n = ab$ be a factorization of n into two positive integers. Then n can be written as the difference of two squares, because

$$n = ab = s^2 - t^2,$$

where $s = (a + b)/2$ and $t = (a - b)/2$ are both integers because a and b are both odd.

Conversely, if n is the difference of two squares, say $n = s^2 - t^2$, then we can factor n by noting that $n = (s - t)(s + t)$.

We leave it to the reader to show that this is a one-to-one correspondence. ■

To carry out the method of Fermat factorization, we look for solutions of the equation $n = x^2 - y^2$ by searching for perfect squares of the form $x^2 - n$. Hence, to find factorizations of n, we search for a square among the sequence of integers

$$t^2 - n, (t + 1)^2 - n, (t + 2)^2 - n, \ldots$$

where t is the smallest integer greater than $\sqrt{n}$. This procedure is guaranteed to terminate, since the trivial factorization $n = n \cdot 1$ leads to the equation

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2.$$

Example 3.23. We factor 6077 using the method of Fermat factorization. Since $77 < \sqrt{6077} < 78$, we look for a perfect square in the sequence

$$78^2 - 6077 = 7$$
$$79^2 - 6077 = 164$$
$$80^2 - 6077 = 323$$
$$81^2 - 6077 = 484 = 22^2.$$

Since $6077 = 81^2 - 22^2$, we see that $6077 = (81 - 22)(81 + 22) = 59 \cdot 103$. ◀

Unfortunately, Fermat factorization can be very inefficient. To factor n using this technique, it may be necessary to check as many as $(n + 1)/2 - [\sqrt{n}]$ integers to

The RSA Factoring Challenge

The RSA Factoring Challenge is an ongoing contest that challenges mathematicians to factor certain large integers. The first RSA challenge, posed in 1977 in Martin Gardner's column in *Scientific American,* was to factor a 129-digit integer, known as RSA-129. A $100 prize was offered for the decryption of a message; the message could be decrypted easily when this 129-digit number was factored, but not otherwise. Seventeen years passed before this challenge was met in 1994. The factorization of RSA-129 using the quadratic sieve method took approximately 5000 MIPS–years, and was carried out in eight months by more than 600 people working together. RSA Labs, a part of RSA Data Security (the company that holds the patents for the RSA cryptosystem discussed in Chapter 8), sponsors the challenge, offering cash prizes for the factorization of integers on challenge lists. So far, they have awarded more than $40,000 for successful factorizations. Factorizations of numbers on their list have led to world records. For example, in 1996, a team led by Arjen Lenstra used the number field sieve to factor RSA-130. This took approximately 750 MIPS–years. In 1999, the number field sieve was used to factor RSA-140 and RSA-155, using 2000 and 8000 MIPS–years, respectively. The factorization of RSA-160 in April 2003 is the current world record for the factorization of a number not of a special form.

determine whether they are perfect squares. Fermat factorization works best when it is used to factor integers having two factors of similar size. Although Fermat factorization is rarely used to factor large integers, its basic idea is the basis for many more powerful factorization algorithms used extensively in computer calculations.

The Fermat Numbers

The integers $F_n = 2^{2^n} + 1$ are called the *Fermat numbers*. Fermat conjectured that these integers are all primes. Indeed, the first few are primes, namely $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65{,}537$. Unfortunately, $F_5 = 2^{2^5} + 1$ is composite, as we will now demonstrate.

Example 3.24. The Fermat number $F_5 = 2^{2^5} + 1$ is divisible by 641. We can show that $641 \mid F_5$ without actually performing the division, using several not-so-obvious observations. Note that

$$641 = 5 \cdot 2^7 + 1 = 2^4 + 5^4.$$

Hence,

$$\begin{aligned} 2^{2^5} + 1 = 2^{32} + 1 &= 2^4 \cdot 2^{28} + 1 = (641 - 5^4)2^{28} + 1 \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 + 1 = 641 \cdot 2^{28} - (641 - 1)^4 + 1 \\ &= 641(2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4). \end{aligned}$$

Therefore, we see that $641 \mid F_5$. ◀

The following result is a valuable aid in the factorization of Fermat numbers.

Theorem 3.20. Every prime divisor of the Fermat number $F_n = 2^{2^n} + 1$ is of the form $2^{n+2}k + 1$.

The proof of Theorem 3.20 is presented as an exercise in Chapter 11. Here, we indicate how Theorem 3.20 is useful in determining the factorization of Fermat numbers.

Example 3.25. From Theorem 3.20, we know that every prime divisor of $F_3 = 2^{2^3} + 1 = 257$ must be of the form $2^5k + 1 = 32 \cdot k + 1$. Because there are no primes of this form less than or equal to $\sqrt{257}$, we can conclude that $F_3 = 257$ is prime. ◀

Example 3.26. When factoring $F_6 = 2^{2^6} + 1$, we use Theorem 3.20 to see that all of its prime factors are of the form $2^8k + 1 = 256 \cdot k + 1$. Hence, we need only perform trial divisions of F_6 by primes of the form $256 \cdot k + 1$ that do not exceed $\sqrt{F_6}$. After considerable computation, we find that a prime divisor is obtained with $k = 1071$, that is, $274{,}177 = (256 \cdot 1071 + 1) \mid F_6$. ◀

The Factorization of Fermat Numbers A tremendous amount of effort has been devoted to the factorization of Fermat numbers. As yet, no new Fermat primes (beyond

F_4) have been found. Many mathematicians believe that no additional Fermat primes exist. We will develop a primality test for Fermat numbers in Chapter 11, which has been used to show that many Fermat numbers are composite. (When such a test is used, it is not necessary to use trial division to show that a number is not divisible by a prime not exceeding its square root.)

As of this writing (2004), a total of 214 Fermat numbers are known to be composite, but the complete factorizations are known for only seven composite Fermat numbers: F_5, F_6, F_7, F_8, F_9, F_{10}, and F_{11}. The Fermat number F_9, a number with 155 decimal digits, was factored in 1990 by Mark Manasse and Arjen Lenstra, using the number field sieve, which breaks the problem of factoring an integer into a large number of smaller factoring problems that can be done in parallel. Though Manasse and Lenstra farmed out computations for the factorization of F_9 to hundreds of mathematicians and computer scientists, it still took about two months to complete the computations. (For details of the factorization of F_9, see [Ci90].)

The prime factorization of F_{11} was discovered by Richard Brent in 1989, using a factorization algorithm known as the elliptic curve method (described in detail in [Br89]). There are 617 decimal digits in F_{11}, and $F_{11} = 319{,}489 \cdot 974{,}849 \cdot P_{21} \cdot P_{22} \cdot P_{564}$, where P_{21}, P_{22}, and P_{564} are primes with 21, 22, and 564 digits, respectively. It took until 1995 for Brent to completely factor F_{10}. He discovered, using elliptic curve factorization, that $F_{10} = 45{,}592{,}577 \cdot 6{,}487{,}031{,}809 \cdot P_{40} \cdot P_{252}$, where P_{40} and P_{252} are primes with 40 and 252 digits, respectively.

Many Fermat numbers are known to be composite because at least one prime factor of these numbers has been found, using results such as Theorem 3.20. It is also known that F_n is composite for $n = 14$, 20, 22, and 24, but no factors of these numbers have yet been found. The largest n for which it is known that F_n is composite is $n = 2{,}478{,}782$. ($F_{382{,}447}$ was the first Fermat number with more than 100,000 digits shown to be composite; it was shown to be composite in July 1999.) F_{33} is the smallest Fermat number that has not yet been shown to be composite, if it is indeed composite. Because of steady advances in computer software and hardware, we can expect new results on the nature of Fermat numbers and their factorizations to be found at a healthy rate.

The factorization of Fermat numbers is part of the *Cunningham project*, sponsored by the American Mathematical Society. Devoted to building tables of all the known factors of integers of the form $b^n \pm 1$, where $b = 2$, 3, 5, 6, 7, 10, 11, and 12, the project's name refers to A. J. Cunningham, a colonel in the British army, who compiled a table of factors of integers of the sort in the early years of the twentieth century. The factor tables as of 1988 are contained in [Br88]; the current state of affairs is available over the Internet. Numbers of the form $b^n \pm 1$ are of special interest because of their importance in generating pseudorandom numbers (see Chapter 10), their importance in abstract algebra, and their significance in number theory.

In conjunction with the Cunningham project, a list of the "ten most wanted" integers to be factored is kept by Samuel Wagstaff of Purdue University. For example, until it was factored in 1990, F_9 was on this list. With advances in factoring techniques and computer power, increasingly larger numbers are included on the list. In the early 1980s, the largest

had between 50 and 70 decimal digits, in the early 1990s between 90 and 130 decimal digits, and today they have between 190 and 200 decimal digits.

Using the Fermat Numbers to Prove the Infinitude of Primes It is possible to prove that there are infinitely many primes using Fermat numbers. We begin by showing that any two distinct Fermat numbers are relatively prime. The following lemma will be used.

Lemma 3.10. Let $F_k = 2^{2^k} + 1$ denote the kth Fermat number, where k is a nonnegative integer. Then for all positive integers n, we have

$$F_0F_1F_2 \cdots F_{n-1} = F_n - 2.$$

Proof. We will prove the lemma using mathematical induction. For $n = 1$, the identity reads

$$F_0 = F_1 - 2.$$

This is obviously true, because $F_0 = 3$ and $F_1 = 5$. Now, let us assume that the identity holds for the positive integer n, so that

$$F_0F_1F_2 \cdots F_{n-1} = F_n - 2.$$

With this assumption, we can easily show that the identity holds for the integer $n + 1$, because

$$\begin{aligned} F_0F_1F_2 \cdots F_{n-1}F_n &= (F_0F_1F_2 \cdots F_{n-1})F_n \\ &= (F_n - 2)F_n = (2^{2^n} - 1)(2^{2^n} + 1) \\ &= (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \end{aligned}$$

■

This leads to the following theorem.

Theorem 3.21. Let m and n be distinct nonnegative integers. Then the Fermat numbers F_m and F_n are relatively prime.

Proof. Let us assume that $m < n$. By Lemma 3.10, we know that

$$F_0F_1F_2 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

Assume that d is a common divisor of F_m and F_n. Then, Theorem 1.8 tells us that

$$d \mid (F_n - F_0F_1F_2 \cdots F_m \cdots F_{n-1}) = 2.$$

Hence, either $d = 1$ or $d = 2$. However, since F_m and F_n are odd, d cannot be 2. Consequently, $d = 1$ and $(F_m, F_n) = 1$. ■

Using Fermat numbers, we now give another proof that there are infinitely many primes. First, we note that by Lemma 3.1 in Section 3.1, every Fermat number F_n has a prime divisor p_n. Because $(F_m, F_n) = 1$, we know that $p_m \neq p_n$ whenever $m \neq n$. Hence, we can conclude that there are infinitely many primes.

The Fermat Primes and Geometry The Fermat primes are important in geometry. The proof of the following famous theorem of Gauss may be found in [Or88].

Theorem 3.22. A regular polygon of n sides can be constructed using a ruler and compass if and only if n is the product of a nonnegative power of 2 and a nonnegative number of distinct Fermat primes.

3.6 Exercises

1. Find the prime factorization of each of the following positive integers.

   a) 33,776,925 b) 210,733,237 c) 1,359,170,111

2. Find the prime factorization of each of the following positive integers.

   a) 33,108,075 b) 7,300,977,607 c) 4,165,073,376,607

3. Using the Fermat factorization method, factor each of the following positive integers.

   a) 143
   b) 2279
   c) 43
   d) 11,413

4. Using the Fermat factorization method, factor each of the following positive integers.

   a) 8051
   b) 73
   c) 46,009
   d) 11,021
   e) 3,200,399
   f) 24,681,023

5. Show that the last two decimal digits of a perfect square must be one of the following pairs: 00, $e1$, $e4$, 25, $o6$, $e9$, where e stands for any even digit and o stands for any odd digit. (*Hint:* Show that n^2, $(50+n)^2$, and $(50-n)^2$ all have the same final decimal digits, and then consider those integers n with $0 \le n \le 25$.)

6. Explain how the result of Exercise 5 can be used to speed up Fermat's factorization method.

7. Show that if the smallest prime factor of n is p, then $x^2 - n$ will not be a perfect square for $x > (n + p^2)/(2p)$, with the single exception $x = (n+1)/2$.

Exercises 8–10 involve the method of *Draim factorization.* To use this technique to search for a factor of the positive integer $n = n_1$, we start by using the division algorithm, to obtain

$$n_1 = 3q_1 + r_1, \quad 0 \le r_1 < 3.$$

Setting $m_1 = n_1$, we let

$$m_2 = m_1 - 2q_1, \quad n_2 = m_2 + r_1.$$

We use the division algorithm again, to obtain

$$n_2 = 5q_2 + r_2, \quad 0 \le r_2 < 5,$$

and we let

$$m_3 = m_2 - 2q_2, \quad n_3 = m_3 + r_2.$$

We proceed recursively, using the division algorithm, to write

$$n_k = (2k+1)q_k + r_k, \quad 0 \le r_k < 2k+1,$$

and we define

$$m_k = m_{k-1} - 2q_{k-1}, \quad n_k = m_k + r_{k-1}.$$

We stop when we obtain a remainder $r_k = 0$.

8. Show that $n_k = kn_1 - (2k+1)(q_1 + q_2 + \cdots + q_{k-1})$ and that $m_k = n_1 - 2 \cdot (q_1 + q_2 + \cdots + q_{k-1})$.

9. Show that if $(2k+1) \mid n$, then $(2k+1) \mid n_k$ and $n = (2k+1)m_{k+1}$.

10. Factor 5899 using Draim factorization.

In Exercises 11–13, we develop a factorization technique known as *Euler's method.* It is applicable when the integer being factored is odd and can be written as the sum of two squares in two different ways. Let n be odd and let $n = a^2 + b^2 = c^2 + d^2$, where a and c are odd positive integers, and b and d are even positive integers.

11. Let $u = (a-c, b-d)$. Show that u is even, and that if $r = (a-c)/u$ and $s = (d-b)/u$, then $(r,s) = 1$, $r(a+c) = s(d+b)$, and $s \mid (a+c)$.

12. Let $sv = a + c$. Show that $rv = d + b$, $v = (a+c, d+b)$, and v is even.

13. Conclude that n may be factored as $n = [(u/2)^2 + (v/2)^2][(r^2 + s^2)$.

14. Use Euler's method to factor each of the following integers.

a) $221 = 10^2 + 11^2 = 5^2 + 14^2$

b) $2501 = 50^2 + 1^2 = 49^2 + 10^2$

c) $1{,}000{,}009 = 1000^2 + 3^2 = 972^2 + 235^2$

15. Show that any number of the form $2^{4n+2} + 1$ can be factored easily by the use of the identity $4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$. Factor $2^{18} + 1$ using this identity.

16. Show that if a is a positive integer and $a^m + 1$ is an odd prime, then $m = 2^n$ for some positive integer n. (*Hint:* Recall the identity $a^m + 1 = (a^k + 1)(a^{k(l-1)} - a^{k(l-2)} + \cdots - a^k + 1)$, where $m = kl$ and l is odd).

17. Show that the last digit in the decimal expansion of $F_n = 2^{2^n} + 1$ is 7 if $n \ge 2$. (*Hint:* Using mathematical induction, show that the last decimal digit of 2^{2^n} is 6.)

18. Use the fact that every prime divisor of $F_4 = 2^{2^4} + 1 = 65{,}537$ is of the form $2^6k + 1 = 64k + 1$ to verify that F_4 is prime. (You should need only one trial division.)

19. Use the fact that every prime divisor of $F_5 = 2^{2^5} + 1$ is of the form $2^7k + 1 = 128k + 1$ to demonstrate that the prime factorization of F_5 is $F_5 = 641 \cdot 6{,}700{,}417$.

20. Find all primes of the form $2^{2^n} + 5$, where n is a nonnegative integer.

21. Estimate the number of decimal digits in the Fermat number F_n.

* **22.** What is the greatest common divisor of n and F_n, where n is a positive integer? Prove that your answer is correct.

23. Show that the only integer of the form $2^m + 1$, where m is a positive integer, that is a power of a positive integer (i.e., is of the form n^k, where n and k are positive integers with $k \ge 2$) occurs when $m = 3$.

24. Factoring kn by the Fermat factorization method, where k is a small positive integer, is sometimes easier than factoring n by this method. Show that to factor 901 by the Fermat factorization method, it is easier to factor $3 \cdot 901 = 2703$ than to factor 901.

3.6 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. Using trial division, find the prime factorization of several integers of your choice exceeding 10,000.
2. Factor several integers of your choice exceeding 10,000, using Fermat factorization.
3. Factor the Fermat numbers F_6 and F_7 using Theorem 3.20.

Programming Projects

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

1. Given a positive integer n, find the prime factorization of n.
2. Given a positive integer n, perform the Fermat factorization method on n.
3. Given a positive integer n, perform Draim factorization on n (see the preamble to Exercise 8).
4. Check the Fermat number F_n, where n is a positive integer, for prime factors, using Theorem 3.20.

3.7 Linear Diophantine Equations

Consider the following problem: A man wishes to purchase \$510 of travelers' checks. The checks are available only in denominations of \$20 and \$50. How many of each denomination should he buy? If we let x denote the number of \$20 checks and y the number of \$50 checks that he should buy, then the equation $20x + 50y = 510$ must be satisfied. To solve this problem, we need to find all solutions of this equation, where both x and y are nonnegative integers.

A related problem arises when a woman wishes to mail a package. The postal clerk determines the cost of postage to be 83 cents, but only 6-cent and 15-cent stamps are available. Can some combination of these stamps be used to mail the package? To answer this, we first let x denote the number of 6-cent stamps and y the number of 15-cent stamps to be used. Then we must have $6x + 15y = 83$, where both x and y are nonnegative integers.

When we require that solutions of a particular equation come from the set of integers, we have a *diophantine equation.* These equations get their name from the ancient Greek mathematician *Diophantus*, who wrote on equations where solutions are restricted to

rational numbers. The equation $ax + by = c$, where a, b, and c are integers, is called a *linear diophantine equation in two variables.*

Note that the pair of integers (x, y) is a solution of the linear diophantine equation $ax + by = c$ if and only if the (x, y) is a lattice point in the plane that lies on the line $ax + by = c$. We illustrate this in Figure 3.2 for the linear diophantine equation $2x + 3y = 5$.

The first person to describe a general solution of linear diophantine equations was the Indian mathematician *Brahmagupta*, who included it in a book he wrote in the seventh century. We now develop the theory for solving such equations. The following theorem tells us when such an equation has solutions, and when there are solutions, explicitly describes them.

Theorem 3.23. Let a and b be integers with $d = (a, b)$. The equation $ax + by = c$ has no integral solutions if $d \nmid c$. If $d \mid c$, then there are infinitely many integral solutions. Moreover, if $x = x_0$, $y = y_0$ is a particular solution of the equation, then all solutions are given by

$$x = x_0 + (b/d)n, \qquad y = y_0 - (a/d)n,$$

where n is an integer.

Proof. Assume that x and y are integers such that $ax + by = c$. Then, because $d \mid a$ and $d \mid b$, by Theorem 1.9, $d \mid c$ as well. Hence, if $d \nmid c$, there are no integral solutions of the equation.

Now assume that $d \mid c$. By Theorem 3.8, there are integers s and t with

$$d = as + bt. \tag{3.3}$$

Since $d \mid c$, there is an integer e with $de = c$. Multiplying both sides of (3.3) by e, we have

$$c = de = (as + bt)e = a(se) + b(te).$$

Hence, one solution of the equation is given by $x = x_0$ and $y = y_0$, where $x_0 = se$ and $y_0 = te$.

DIOPHANTUS (c. 250) wrote the *Arithmetica,* which is the earliest known book on algebra; it contains the first systematic use of mathematical notation to represent unknowns in equations and powers of these unknowns. Almost nothing is known about Diophantus, other than that he lived in Alexandria around 250 C.E. The only source of details about his life comes from an epigram found in a collection called the *Greek Anthology:* "Diophantus passed one sixth of his life in childhood, one twelfth in youth, and one seventh as a bachelor. Five years after his marriage was born a son who died four years before his father, at half his father's age." From this the reader can infer that Diophantus lived to the age of 84.

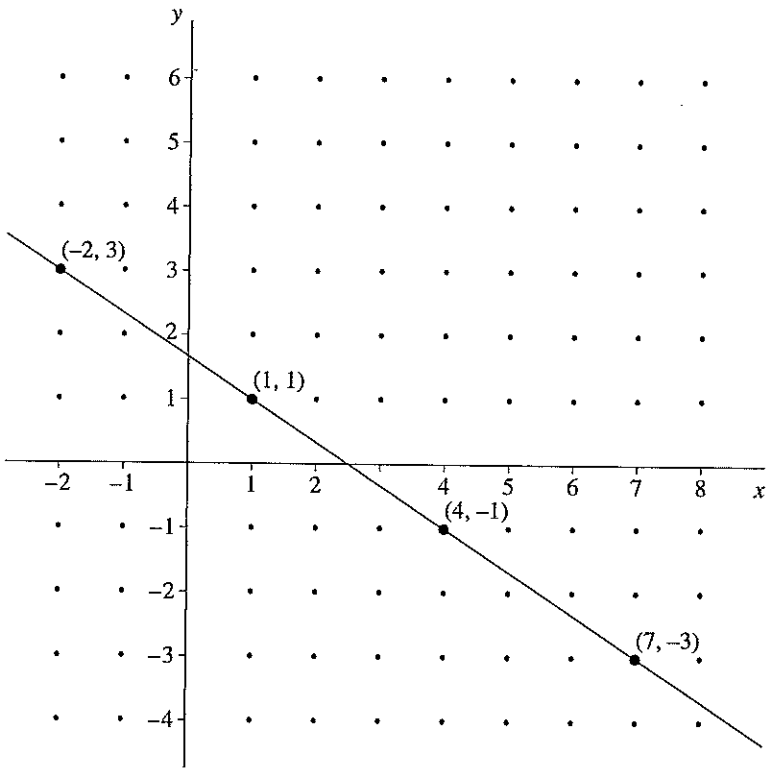


Figure 3.2 *Solutions of* $2x + 3y = 5$ *in integers* x *and* y *correspond to the lattice points on the line* $2x + 3y = 5$.

To show that there are infinitely many solutions, let $x = x_0 + (b/d)n$ and $y = y_0 - (a/d)n$, where n is an integer. We will first show that any pair (x, y), with $x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$, where n is an integer, is a solution; then we will show that every solution must have this form. We see that this pair (x, y) is a solution, because

$$ax + by = ax_0 + a(b/d)n + by_0 - b(a/d)n = ax_0 + by_0 = c.$$

BRAHMAGUPTA (598–670), thought to have been born in Ujjain, India, became the head of the astronomical observatory there; this observatory was the center of Indian mathematical studies at that time. Brahmagupta wrote two important books on mathematics and astronomy, *Brahma-sphuta-siddhanta* ("The Opening of the Universe") and *Khandakhadyaka*, written in 628 and 665, respectively. He developed many interesting formulas and theorems in planar geometry, and studied arithmetic progressions and quadratic equations. Brahmagupta developed new algebraic notation, and his understanding of the number system was advanced for his time. He is considered to be the first person to describe a general solution of linear diophantine equations. In astronomy, he studied eclipses, positions of the planets, and the length of the year.

We now show that every solution of the equation $ax + by = c$ must be of the form described in the theorem. Suppose that x and y are integers with $ax + by = c$. Because

$$ax_0 + by_0 = c,$$

by subtraction we find that

$$(ax + by) - (ax_0 + by_0) = 0,$$

which implies that

$$a(x - x_0) + b(y - y_0) = 0.$$

Hence,

$$a(x - x_0) = b(y_0 - y).$$

Dividing both sides of this last equation by d, we see that

$$(a/d)(x - x_0) = (b/d)(y_0 - y).$$

By Theorem 3.6, we know that $(a/d, b/d) = 1$. Using Lemma 3.4, it follows that $(a/d) \mid (y_0 - y)$. Hence, there is an integer n with $(a/d)n = y_0 - y$; this means that $y = y_0 - (a/d)n$. Now, putting this value of y into the equation $a(x - x_0) = b(y_0 - y)$, we find that $a(x - x_0) = b(a/d)n$, which implies that $x = x_0 + (b/d)n$. ■

The following examples illustrate the use of Theorem 3.23.

Example 3.27. By Theorem 3.23, there are no integral solutions of the diophantine equation $15x + 6y = 7$, because $(15, 6) = 3$ but $3 \nmid 7$. ◀

Example 3.28. By Theorem 3.23, there are infinitely many solutions of the diophantine equation $21x + 14y = 70$, because $(21, 14) = 7$ and $7 \mid 70$. To find these solutions, note that by the Euclidean algorithm, $1 \cdot 21 + (-1) \cdot 14 = 7$, so that $10 \cdot 21 + (-10) \cdot 14 = 70$. Hence, $x_0 = 10$, $y_0 = -10$ is a particular solution. All solutions are given by $x = 10 + 2n$, $y = -10 - 3n$, where n is an integer. ◀

We will now use Theorem 3.23 to solve the two problems described at the beginning of the section.

Example 3.29. Consider the problem of forming 83 cents in postage using only 6- and 15-cent stamps. If x denotes the number of 6-cent stamps and y denotes the number of 15-cent stamps, we have $6x + 15y = 83$. Since $(6, 15) = 3$ does not divide 83, by Theorem 3.23 we know that there are no integral solutions. Hence, no combination of 6- and 15-cent stamps gives the correct postage. ◀

Example 3.30. Consider the problem of purchasing \$510 of travelers' checks, using only \$20 and \$50 checks. How many of each type of check should be used?

Let x be the number of \$20 checks and let y be the number of \$50 checks. We have the equation $20x + 50y = 510$. Note that the greatest common divisor of 20 and 50 is $(20, 50) = 10$. Because $10 \mid 510$, there are infinitely many integral solutions of this linear diophantine equation. Using the Euclidean algorithm, we find that $20(-2) + 50 = 10$. Multiplying both sides by 51, we obtain $20(-102) + 50(51) = 510$. Hence, a particular solution is given by $x_0 = -102$ and $y_0 = 51$. Theorem 3.23 tells us that all integral solutions are of the form $x = -102 + 5n$ and $y = 51 - 2n$. Because we want both x and y to be nonnegative, we must have $-102 + 5n \geq 0$ and $51 - 2n \geq 0$; thus, $n \geq 20\ 2/5$ and $n \leq 25\ 1/2$. Because n is an integer, it follows that $n = 21,\ 22,\ 23,\ 24$, or 25. Hence, we have the following five solutions: $(x, y) = (3, 9), (8, 7), (13, 5), (18, 3)$, and $(23, 1)$. So the teller can give the customer 3 \$20 checks and 9 \$50 checks, 8 \$20 checks and 7 \$50 checks, 13 \$20 checks and 5 \$50 checks, 18 \$20 checks and 3 \$50 checks, or 23 \$20 checks and 1 \$50 check. ◀

We can extend Theorem 3.23 to cover linear diophantine equations with more than two variables as the following theorem demonstrates.

Theorem 3.24. If $a_1, a_2, \ldots, a_n$ are nonzero positive integers, then the equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$ has an integral solution if and only if $d = (a_1, a_2, \ldots, a_n)$ divides c. Furthermore, when there is a solution, there are infinitely many solutions.

Proof. If there are integers $x_1, x_2, \ldots, x_n$ such that $a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$, then because d divides a_i for $i = 1, 2, \ldots, n$, by Theorem 1.9, d also divides c. Hence, if $d \nmid c$ there are no integral solutions of the equation.

We will use mathematical induction to prove that there are infinitely many integral solutions when $d \mid c$. Note that by Theorem 3.23 this is true when $n = 2$.

Now, suppose that there are infinitely many solutions for all equations in n variables satisfying the hypotheses. By Theorem 3.9, the set of linear combinations $a_nx_n + a_{n+1}x_{n+1}$ is the same as the set of multiples of (a_n, a_{n+1}). Hence, for every integer y there are infinitely many solutions of the linear diophantine equation $a_nx_n + a_{n+1}x_{n+1} = (a_n, a_{n+1})y$. It follows that the original equation in $n + 1$ variables can be reduced to a linear diophantine equation in n variables:

$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + (a_n, a_{n+1})y = c.$$

Note that c is divisible by $(a_1, a_2, \ldots, a_{n-1}, (a_n, a_{n+1}))$ because, by Lemma 3.2, this greatest common divisor equals $(a_1, a_2, \ldots, a_n, a_{n+1})$. By the inductive hypothesis, this equation has infinitely many integer solutions, as it is a linear diophantine equation in n variables where the greatest common divisor of the coefficients divides the constant c. It follows that there are infinitely many solutions to the original equation. ■

A method for solving linear diophantine equations in more than two variables can be found using the reduction in the proof of Theorem 3.24. We leave an application of Theorem 3.24 to the exercises.

3.7 Exercises

1. For each of the following linear diophantine equations, either find all solutions, or show that there are no integral solutions.
   a) $2x + 5y = 11$
   b) $17x + 13y = 100$
   c) $21x + 14y = 147$
   d) $60x + 18y = 97$
   e) $1402x + 1969y = 1$

2. For each of the following linear diophantine equations, either find all solutions, or show that there are no integral solutions.
   a) $3x + 4y = 7$
   b) $12x + 18y = 50$
   c) $30x + 47y = -11$
   d) $25x + 95y = 970$
   e) $102x + 1001y = 1$

3. A Japanese businessman returning home from a trip to North America exchanges his U.S. and Canadian dollars for yen. If he receives 15,286 yen, and received 122 yen for each U.S. and 112 yen for each Canadian dollar, how many of each type of currency did he exchange?

4. A student returning from Europe changes his euros and Swiss francs into U.S. money. If she receives \$46.26, and received \$1.11 for each euro and 83¢ for each Swiss franc, how much of each type of currency did she exchange?

5. A professor returning home from conferences in Paris and London changes his euros and pounds into U.S. money. If he receives \$117.98, and received \$1.11 for each euro and \$1.69 for each pound, how much of each type of currency did he exchange?

6. The Indian astronomer and mathematician Mahavira, who lived in the ninth century, posed this puzzle: A band of 23 weary travelers entered a lush forest where they found 63 piles each containing the same number of plantains and a remaining pile containing seven plantains. They divided the plantains equally. How many plantains were in each of the 63 piles? Solve this puzzle.

7. A grocer orders apples and oranges at a total cost of \$8.39. If apples cost him 25¢ each and oranges cost him 18¢ each, how many of each type of fruit did he order?

8. A shopper spends a total of \$5.49 for oranges, which cost 18¢ each, and grapefruit, which cost 33¢ each. What is the minimum number of pieces of fruit the shopper could have bought?

9. A postal clerk has only 14- and 21-cent stamps to sell. What combinations of these may be used to mail a package requiring postage of exactly each of the following amounts?

   a) \$3.50 b) \$4.00 c) \$7.77

10. At a clambake, the total cost of a lobster dinner is \$11 and of a chicken dinner is \$8. What can you conclude if the total bill is each of the following amounts?

    a) \$777 b) \$96 c) \$69

* **11.** Find all integer solutions of each of the following linear diophantine equations.
  a) $2x + 3y + 4z = 5$
  b) $7x + 21y + 35z = 8$
  c) $101x + 102y + 103z = 1$

* **12.** Find all integer solutions of each of the following linear diophantine equations.
  a) $2x_1 + 5x_2 + 4x_3 + 3x_4 = 5$
  b) $12x_1 + 21x_2 + 9x_3 + 15x_4 = 9$
  c) $15x_1 + 6x_2 + 10x_3 + 21x_4 + 35x_5 = 1$

13. Which combinations of pennies, dimes, and quarters have a total value of $99¢$?

14. How many ways can change be made for one dollar, using each of the following coins?
  a) dimes and quarters
  b) nickels, dimes, and quarters
  c) pennies, nickels, dimes, and quarters

In Exercises 15–17, we consider simultaneous linear diophantine equations. To solve these, first eliminate all but two variables and then solve the resulting equation in two variables.

15. Find all integer solutions of the following systems of linear diophantine equations.

a) $x + y + z = 100$
$x + 8y + 50z = 156$

b) $x + y + z = 100$
$x + 6y + 21z = 121$

c) $x + y + z + w = 100$
$x + 2y + 3z + 4w = 300$
$x + 4y + 9z + 16w = 1000$

16. A piggy bank contains 24 coins, all of which are nickels, dimes, or quarters. If the total value of the coins is two dollars, what combinations of coins are possible?

17. Nadir Airways offers three types of tickets on their Boston–New York flights. First-class tickets are \$140, second-class tickets are \$110, and standby tickets are \$78. If 69 passengers pay a total of \$6548 for their tickets on a particular flight, how many of each type of ticket were sold?

18. Is it possible to have 50 coins, all of which are pennies, dimes, or quarters, with a total worth \$3?

Let a and b be relatively prime positive integers, and let n be a positive integer. A solution (x, y) of the linear diophantine equation $ax + by = n$ is *nonnegative* when both x and y are nonnegative.

* **19.** Show that whenever $n \geq (a-1)(b-1)$, there is a nonnegative solution of $ax + by = n$.

* **20.** Show that if $n = ab - a - b$, then there are no nonnegative solutions of $ax + by = n$.

* **21.** Show that there are exactly $(a-1)(b-1)/2$ nonnegative integers $n < ab - a - b$ such that the equation has a nonnegative solution.

22. The post office in a small Maine town is left with stamps of only two values. They discover that there are exactly 33 postage amounts that cannot be made up using these stamps, including 46¢. What are the values of the remaining stamps?

* 23. A Chinese puzzle found in the sixth-century work of mathematician Chang Ch'iu-chien, called the "hundred fowls" problem, asks: If a cock is worth five coins, a hen three coins, and three chickens together are worth one coin, how many cocks, hens, and chickens, totaling 100, can be bought for 100 coins? Solve this problem.

* 24. Find all solutions where x and y are integers to the diophantine equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

3.7 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. Determine which positive integers are of the form $ax + by$, where x and y are nonnegative integers and a and b are relatively prime positive integers of your choice. Use your evidence to confirm the results of Exercises 19–21.

Programming Projects

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

1. Find the solutions of a linear diophantine equation in two variables.
2. Find the positive solutions of a linear diophantine equation in two variables.
3. Find the solutions of a linear diophantine equation in three variables.

* 4. Find all positive integers n for which the linear diophantine equation $ax + by = n$ has no positive solutions (see the preamble to Exercise 19).

4 Congruences

Introduction

The language of congruences was invented by the great German mathematician Gauss. It allows us to work with divisibility relationships in much the same way as we work with equalities. We will develop the basic properties of congruences in this chapter, describe how to do arithmetic with congruences, and study congruences involving unknowns, such as linear congruences. An example leading to a linear congruence is the problem of finding all integers x such that when $7x$ is divided by 11, the remainder is 3. We will also study systems of linear congruences that arise from such problems as the ancient Chinese puzzle that asks for a number that leaves a remainder of 2, 3, and 2, when divided by 3, 5, and 7, respectively. We will learn how to solve systems of linear congruences in one unknown, such as the system that results from this puzzle, using a famous method known as the Chinese remainder theorem. We will also learn how to solve polynomial congruences. Finally, we will introduce a factoring method, known as the Pollard rho method, which we use congruences to specify.

4.1 Introduction to Congruences

The special language of congruences that we introduce in this chapter, which is extremely useful in number theory, was developed at the beginning of the nineteenth century by *Karl Friedrich Gauss*, one of the most famous mathematicians in history.

The language of congruences makes it possible to work with divisibility relationships much as we work with equalities. Prior to the introduction of congruences, the notation used for divisibility relationships was awkward and difficult to work with. The introduction of a convenient notation helped accelerate the development of number theory.

Definition. Let m be a positive integer. If a and b are integers, we say that a is *congruent to b modulo m* if $m \mid (a - b)$.

If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$. If $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$, and say that a and b are *incongruent modulo m*. The integer m is called the *modulus* of the congruence. The plural of modulus is *moduli*.

Example 4.1. We have $22 \equiv 4 \pmod{9}$, since $9 \mid (22 - 4) = 18$. Likewise $3 \equiv -6 \pmod{9}$ and $200 \equiv 2 \pmod{9}$. On the other hand, $13 \not\equiv 5 \pmod{9}$ since $9 \nmid (13 - 5) = 8$. ◀

Congruences often arise in everyday life. For instance, clocks work either modulo 12 or 24 for hours and modulo 60 for minutes and seconds; calendars work modulo 7 for days of the week and modulo 12 for months. Utility meters often operate modulo 1000, and odometers usually work modulo 100,000.

In working with congruences, we will sometimes need to translate them into equalities. The following theorem helps us to do this.

Theorem 4.1. If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Proof. If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. This means that there is an integer k with $km = a - b$, so that $a = b + km$.

KARL FRIEDRICH GAUSS (1777–1855) was the son of a bricklayer. It was quickly apparent that he was a prodigy. In fact, at the age of 3, he corrected an error in his father's payroll. In his first arithmetic class, the teacher gave an assignment designed to keep the class busy, namely to find the sum of the first 100 positive integers. Gauss, who was 8 at the time, realized that this sum is $50 \cdot 101 = 5050$, because the terms can be grouped as $1 + 100 = 101$, $2 + 99 = 101$, . . . , $49 + 52 = 101$, and $50 + 51 = 101$. In 1796, Gauss made an important discovery in an area of geometry that had not progressed since ancient times. In particular, he showed that a regular heptadecagon (17-sided polygon) could be drawn using just a ruler and a compass. In 1799, he presented the first rigorous proof of the fundamental theorem of algebra, which states that a polynomial of degree n with real coefficients has exactly n roots. Gauss made fundamental contributions to astronomy, including calculating the orbit of the asteroid Ceres. On the basis of this calculation, Gauss was appointed director of the Göttingen Observatory. He laid the foundations of modern number theory with his book *Disquisitiones Arithmeticae* in 1801. Gauss was called "Princeps Mathematicorum" (the Prince of Mathematicians) by his contemporaries. Although Gauss is noted for his many discoveries in geometry, algebra, analysis, astronomy, and mathematical physics, he had a special interest in number theory. This can be seen from his statement: "Mathematics is the queen of sciences, and the theory of numbers is the queen of mathematics." Gauss made most of his important discoveries early in his life, and spent his later years refining them. Gauss made several fundamental discoveries that he did not reveal. Mathematicians making the same discoveries were often surprised to find that Gauss had described the results years earlier in his unpublished notes.

Conversely, if there is an integer k with $a = b + km$, then $km = a - b$. Hence $m \mid (a - b)$, and consequently, $a \equiv b \pmod{m}$. ∎

Example 4.2. We have $19 \equiv -2 \pmod{7}$ and $19 = -2 + 3 \cdot 7$. ◀

The following proposition establishes some important properties of congruences.

Theorem 4.2. Let m be a positive integer. Congruences modulo m satisfy the following properties:

(i) *Reflexive property.* If a is an integer, then $a \equiv a \pmod{m}$.

(ii) *Symmetric property.* If a and b are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) *Transitive property.* If a, b, and c are integers with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof.

(i) We see that $a \equiv a \pmod{m}$, since $m \mid (a - a) = 0$.

(ii) If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. Hence, there is an integer k such that $km = a - b$. This shows that $(-k)m = b - a$, so that $m \mid (b - a)$. Consequently, $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Hence, there are integers k and l such that $km = a - b$ and $lm = b - c$. Therefore, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. It follows that $m \mid (a - c)$ and $a \equiv c \pmod{m}$. ∎

By Theorem 4.2, we see that the set of integers is divided into m different sets called *congruence classes modulo m,* each containing integers that are mutually congruent modulo m.

Example 4.3. The four congruence classes modulo 4 are given by

$$\ldots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \ldots \pmod{4}$$
$$\ldots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \ldots \pmod{4}$$
$$\ldots \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots \pmod{4}$$
$$\ldots \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv \ldots \pmod{4}.$$ ◀

Suppose that m is a positive integer. Given an integer a, by the division algorithm we have $a = bm + r$, where $0 \leq r \leq m - 1$. We call r the *least nonnegative residue* of a modulo m. We say that r is the result of *reducing a modulo m.* Similarly, when we know that a is not divisible by m, we call r the *least positive residue* of a modulo m.

Another commonly used notation, especially in computer science applications, is a **mod** $m = r$, which denotes that r is the remainder obtained when a is divided by m. For example, 17 **mod** $5 = 2$ and -8 **mod** $7 = 6$. Although we do not use such notation in this book, it is commonly used in other contexts.

Now note that from the equation $a = bm + r$, it follows that $a \equiv r \pmod{m}$. Hence, every integer is congruent modulo m to one of the integers of the set $0, 1, \ldots, m-1$, namely the remainder when it is divided by m. Since no two of the integers $0, 1, \ldots, m-1$ are congruent modulo m, we have m integers such that every integer is congruent to exactly one of these m integers.

Definition. A *complete system of residues modulo m* is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.

Example 4.4. The division algorithm shows that the set of integers $0, 1, 2, \ldots, m-1$ is a complete system of residues modulo m. This is called the set of *least nonnegative residues modulo m.* ◀

Example 4.5. Let m be an odd positive integer. Then the set of integers

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2},$$

the set of *absolute least residues modulo m,* is a complete system of residues. ◀

We will often do arithmetic with congruences, which is called *modular arithmetic.* Congruences have many of the same properties that equalities do. First, we show that an addition, subtraction, or multiplication to both sides of a congruence preserves the congruence.

Theorem 4.3. If a, b, c, and m are integers, with $m > 0$, such that $a \equiv b \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Proof. Because $a \equiv b \pmod{m}$, we know that $m \mid (a - b)$. From the identity $(a + c) - (b + c) = a - b$, we see that $m \mid ((a + c) - (b + c))$, so that (i) follows. Likewise, (ii) follows from the fact that $(a - c) - (b - c) = a - b$. To show that (iii) holds, note that $ac - bc = c(a - b)$. Because $m \mid (a - b)$, it follows that $m \mid c(a - b)$, and hence, $ac \equiv bc \pmod{m}$. ■

Example 4.6. Because $19 \equiv 3 \pmod{8}$, it follows from Theorem 4.3 that $26 = 19 + 7 \equiv 3 + 7 = 10 \pmod{8}$, $15 = 19 - 4 \equiv 3 - 4 = -1 \pmod{8}$, and $38 = 19 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod{8}$. ◀

What happens when both sides of a congruence are divided by an integer? Consider the following example.

Example 4.7. We have $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8 \pmod{6}$. But we cannot cancel the common factor of 2, because $7 \not\equiv 4 \pmod{6}$. ◀

This example shows that it is not necessarily true that we preserve a congruence when we divide both sides by an integer. However, the following theorem gives a valid congruence when both sides of a congruence are divided by the same integer.

Theorem 4.4. If a, b, c, and m are integers such that $m > 0, d = (c, m)$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/d}$.

Proof. If $ac \equiv bc \pmod{m}$, we know that $m \mid (ac - bc) = c(a - b)$. Hence, there is an integer k with $c(a - b) = km$. By dividing both sides by d, we have $(c/d)(a - b) = k(m/d)$. Because $(m/d, c/d) = 1$, by Lemma 3.4 it follows that $m/d \mid (a - b)$. Hence, $a \equiv b \pmod{m/d}$. ∎

Example 4.8. Because $50 \equiv 20 \pmod{15}$ and $(10, 15) = 5$, we see that $50/10 \equiv 20/10 \pmod{15/5}$, or $5 \equiv 2 \pmod{3}$. ◀

The following corollary, which is a special case of Theorem 4.4, is used often; it allows us to cancel numbers that are relatively prime to the modulus m in congruences modulo m.

Corollary 4.4.1. If a, b, c, and m are integers such that $m > 0, (c, m) = 1$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

Example 4.9. Since $42 \equiv 7 \pmod{5}$ and $(5, 7) = 1$, we can conclude that $42/7 \equiv 7/7 \pmod{5}$, or that $6 \equiv 1 \pmod{5}$. ◀

The following theorem, which is more general than Theorem 4.3, is also useful. Its proof is similar to the proof of Theorem 4.3.

Theorem 4.5. If a, b, c, d, and m are integers such that $m > 0$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

Proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we know that $m \mid (a - b)$ and $m \mid (c - d)$. Hence, there are integers k and l with $km = a - b$ and $lm = c - d$.

To prove (i), note that $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$. Hence, $m \mid [(a + c) - (b + d)]$. Therefore, $a + c \equiv b + d \pmod{m}$.

To prove (ii), note that $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$. Hence, $m|[(a - c) - (b - d)]$, so that $a - c \equiv b - d \pmod{m}$.

To prove (iii), note that $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$. Hence, $m \mid (ac - bd)$. Therefore, $ac \equiv bd \pmod{m}$. ∎

Example 4.10. Because $13 \equiv 3 \pmod 5$ and $7 \equiv 2 \pmod 5$, using Theorem 3.5 we see that $20 = 13 + 7 \equiv 3 + 2 = 5 \pmod 5$, $6 = 13 - 7 \equiv 3 - 2 = 1 \pmod 5$, and $91 = 13 \cdot 7 \equiv 3 \cdot 2 = 6 \pmod 5$. ◀

The following lemma helps us to determine whether a set of m numbers forms a complete set of residues modulo m.

Lemma 4.1. A set of m incongruent integers modulo m forms a complete set of residues modulo m.

Proof. Suppose that a set of m incongruent integers modulo m does not form a complete set of residues modulo m. This implies that at least one integer a is not congruent to any of the integers in the set. Hence, there is no integer in the set congruent modulo m to the remainder of a when it is divided by m. Hence, there can be at most $m - 1$ different remainders of the integers when they are divided by m. It follows (by the pigeonhole principle, which says that if more than n objects are distributed into n boxes, at least two objects are in the same box) that at least two integers in the set have the same remainder modulo m. This is impossible, because these integers are incongruent modulo m. Hence, any m incongruent integers modulo m form a complete system of residues modulo m. ■

Theorem 4.6. If $r_1, r_2, \ldots, r_m$ is a complete system of residues modulo m, and if a is a positive integer with $(a, m) = 1$, then

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

is a complete system of residues modulo m for any integer b.

Proof. First, we show that no two of the integers

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

are congruent modulo m. To see this, note that if

$$ar_j + b \equiv ar_k + b \pmod m,$$

then, by (ii) of Theorem 4.3, we know that

$$ar_j \equiv ar_k \pmod m.$$

Because $(a, m) = 1$, Corollary 4.4.1 shows that

$$r_j \equiv r_k \pmod m.$$

Given that $r_j \not\equiv r_k \pmod m$ if $j \neq k$, we conclude that $j = k$.

By Lemma 4.1, because the set of integers in question consists of m incongruent integers modulo m, these integers form a complete system of residues modulo m. ■

The following theorem shows that a congruence is preserved when both sides are raised to the same positive integral power.

Theorem 4.7. If a, b, k, and m are integers such that $k > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Proof. Because $a \equiv b \pmod{m}$, we have $m \mid (a - b)$, and because

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

we see that $(a - b) \mid (a^k - b^k)$. Therefore, by Theorem 1.8 it follows that $m \mid (a^k - b^k)$. Hence, $a^k \equiv b^k \pmod{m}$. ∎

Example 4.11. Since $7 \equiv 2 \pmod{5}$, Theorem 4.7 tells us that $343 = 7^3 \equiv 2^3 = 8 \pmod{5}$. ◀

The following result shows how to combine congruences of two numbers to different moduli.

Theorem 4.8. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, where a, b, $m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, m_2, \ldots, m_k]$ is the least common multiple of $m_1, m_2, \ldots, m_k$.

Proof. Because $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, we know that $m_1 \mid (a - b), m_2 \mid (a - b), \ldots, m_k \mid (a - b)$. By Exercise 39 of Section 3.5 we see that

$$[m_1, m_2, \ldots, m_k] \mid (a - b).$$

Consequently,

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$ ∎

The following result is an immediate and useful consequence of this theorem.

Corollary 4.8.1. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $\ldots$, $a \equiv b \pmod{m_k}$, where a and b are integers and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, then

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Proof. Since $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, Exercise 68 of Section 3.5 tells us that

$$[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k.$$

Hence, by Theorem 4.8, we know that

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$ ∎

Modular Exponentiation

In our subsequent studies, we will be working with congruences involving large powers of integers. For example, we will want to find the least positive residue of 2^{644}

modulo 645. If we attempt to find this least positive residue by first computing 2^{644}, we would have an integer with 194 decimal digits, a most undesirable thought. Instead, to find 2^{644} modulo 645 we first express the exponent 644 in binary notation:

$$(644)_{10} = (1010000100)_2.$$

Next, we compute the least positive residues of $2, 2^2, 2^4, 2^8, \ldots, 2^{512}$ by successively squaring and reducing modulo 645. This gives us the congruences

$$\begin{aligned}
2 &\equiv 2 \pmod{645},\\
2^2 &\equiv 4 \pmod{645},\\
2^4 &\equiv 16 \pmod{645},\\
2^8 &\equiv 256 \pmod{645},\\
2^{16} &\equiv 391 \pmod{645},\\
2^{32} &\equiv 16 \pmod{645},\\
2^{64} &\equiv 256 \pmod{645},\\
2^{128} &\equiv 391 \pmod{645},\\
2^{256} &\equiv 16 \pmod{645},\\
2^{512} &\equiv 256 \pmod{645}.
\end{aligned}$$

We can now compute 2^{644} modulo 645 by multiplying the least positive residues of the appropriate powers of 2. This gives

$$2^{644} = 2^{512+128+4} = 2^{512}2^{128}2^4 \equiv 256 \cdot 391 \cdot 16 = 1{,}601{,}536 \equiv 1 \pmod{645}.$$

We have just illustrated a general procedure for *modular exponentiation,* that is, for computing b^N modulo m, where b, m, and N are positive integers. We first express the exponent N in binary notation, as $N = (a_k a_{k-1} \ldots a_1 a_0)_2$. We then find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, by successively squaring and reducing modulo m. Finally, we multiply the least positive residues modulo m of b^{2^j} for those j with $a_j = 1$, reducing modulo m after each multiplication.

In our subsequent discussions, we will need an estimate for the number of bit operations needed for modular exponentiation. This is provided by the following proposition.

Theorem 4.9. Let b, m, and N be positive integers such that $b < m$. Then the least positive residue of b^N modulo m can be computed using $O((\log_2 m)^2 \log_2 N)$ bit operations.

Proof. To find the least positive residue of b^N modulo m, we can use the algorithm just described. First, we find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, where $2^k \leq N < 2^{k+1}$, by successively squaring and reducing modulo m. This requires a total of $O((\log_2 m)^2 \log_2 N)$ bit operations, because we perform $[\log_2 N]$ squarings modulo m, each requiring $O((\log_2 m)^2)$ bit operations. Next, we multiply together the least positive residues of the integers b^{2^j} corresponding to the binary digits of N that are equal to one, and we reduce modulo m after each multiplication. This also requires $O((\log_2 m)^2 \log_2 N)$ bit operations, because there are at most $\log_2 N$ multiplications,

each requiring $O((\log_2 m)^2)$ bit operations. Therefore, a total of $O((\log_2 m)^2 \log_2 N)$ bit operations is needed. ■

4.1 Exercises

1. Show that each of the following congruences holds.

   a) $13 \equiv 1 \pmod 2$
   b) $22 \equiv 7 \pmod 5$
   c) $91 \equiv 0 \pmod{13}$
   d) $69 \equiv 62 \pmod 7$
   e) $-2 \equiv 1 \pmod 3$
   f) $-3 \equiv 30 \pmod{11}$
   g) $111 \equiv -9 \pmod{40}$
   h) $666 \equiv 0 \pmod{37}$

2. Determine whether each of the following pairs of integers is congruent modulo 7.

   a) 1,15
   b) 0,42
   c) 2,99
   d) -1,8
   e) -9,5
   f) -1,699

3. For which positive integers m is each of the following statements true?

   a) $27 \equiv 5 \pmod m$
   b) $1000 \equiv 1 \pmod m$
   c) $1331 \equiv 0 \pmod m$

4. Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$, and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

☞ 5. Show that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

6. Find the least nonnegative residue modulo 13 of each of the following integers.

   a) 22
   b) 100
   c) 1001
   d) -1
   e) -100
   f) -1000

7. Find the least positive residue of $1! + 2! + 3! + \cdots + 100!$ modulo each of the following integers.

   a) 2
   b) 7
   c) 12
   d) 25

8. Show that if a, b, m, and n are integers such that $m > 0$, $n > 0$, $n \mid m$, and $a \equiv b \pmod m$, then $a \equiv b \pmod n$.

9. Show that if a, b, c, and m are integers such that $c > 0$, $m > 0$, and $a \equiv b \pmod m$, then $ac \equiv bc \pmod{mc}$.

10. Show that if a, b, and c are integers with $c > 0$ such that $a \equiv b \pmod c$, then $(a, c) = (b, c)$.

11. Show that if $a_j \equiv b_j \pmod m$ for $j = 1, 2, \ldots, n$, where m is a positive integer and a_j, b_j, $j = 1, 2, \ldots, n$, are integers, then

a) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m}$.

b) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod{m}$.

In Exercises 12–14, construct tables for arithmetic modulo 6 using the least nonnegative residues modulo 6 to represent the congruence classes.

12. Construct a table for addition modulo 6.

13. Construct a table for subtraction modulo 6.

14. Construct a table for multiplication modulo 6.

15. What time does a clock read

a) 29 hours after it reads 11 o'clock?

b) 100 hours after it reads 2 o'clock?

c) 50 hours before it reads 6 o'clock?

16. Which decimal digits occur as the final digit of a fourth power of an integer?

17. What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where a and b are integers and p is prime?

18. Show that if $a^k \equiv b^k \pmod{m}$ and $a^{k+1} \equiv b^{k+1} \pmod{m}$, where a, b, k, and m are integers with $k > 0$ and $m > 0$ such that $(a, m) = 1$, then $a \equiv b \pmod{m}$. If the condition $(a, m) = 1$ is dropped, is the conclusion that $a \equiv b \pmod{m}$ still valid?

19. Show that if n is an odd positive integer, then

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}.$$

Is this statement true if n is even?

20. Show that if n is an odd positive integer or if n is a positive integer divisible by 4, then

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

Is this statement true if n is even but not divisible by 4?

21. For which positive integers n is it true that

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}?$$

22. Show by mathematical induction that if n is a positive integer, then $4^n \equiv 1 + 3n \pmod{9}$.

23. Show by mathematical induction that if n is a positive integer, then $5^n \equiv 1 + 4n \pmod{16}$.

24. Give a complete system of residues modulo 13 consisting entirely of odd integers.

25. Show that if $n \equiv 3 \pmod{4}$, then n cannot be the sum of the squares of two integers.

26. Show that if p is prime, then the only solutions of the congruence $x^2 \equiv x \pmod{p}$ are those integers x such that $x \equiv 0$ or $1 \pmod{p}$.

27. Show that if p is prime and k is a positive integer, then the only solutions of $x^2 \equiv x \pmod{p^k}$ are those integers x such that $x \equiv 0$ or $1 \pmod{p^k}$.

28. Find the least positive residues modulo 47 of each of the following integers.

a) 2^{32} b) 2^{47} c) 2^{200}

29. Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers. Let $M = m_1 m_2 \cdots m_k$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, k$. Show that

$$M_1 a_1 + M_2 a_2 + \cdots + M_k a_k$$

runs through a complete system of residues modulo M when $a_1, a_2, \ldots, a_k$ run through complete systems of residues modulo $m_1, m_2, \ldots, m_k$, respectively.

30. Explain how to find the sum $u + v$ from the least positive residue of $u + v$ modulo m, where u and v are positive integers less than m. (*Hint:* Assume that $u \leq v$, and consider separately the cases where the least positive residue of $u + v$ is less than u, and where it is greater than v.)

31. On a computer with word size w, multiplication modulo n where $n < w/2$ can be performed as outlined. Let $T = [\sqrt{n} + 1/2]$, and $t = T^2 - n$. For each computation, show that all the required computer arithmetic can be done without exceeding the word size. (This method was described by Head [He80]).

a) Show that $|t| \leq T$.

b) Show that if x and y are nonnegative integers less than n, then

$$x = aT + b, \quad y = cT + d,$$

where a, b, c, and d are integers such that $0 \leq a \leq T$, $0 \leq b < T$, $0 \leq c \leq T$, and $0 \leq d < T$.

c) Let $z \equiv ad + bc \pmod{n}$, such that $0 \leq z < n$. Show that

$$xy \equiv act + zT + bd \pmod{n}.$$

d) Let $ac = eT + f$, where e and f are integers with $0 \leq e \leq T$ and $0 \leq f < T$. Show that

$$xy \equiv (z + et)T + ft + bd \pmod{n}.$$

e) Let $v \equiv z + et \pmod{n}$, such that $0 \leq v < n$. Show that we can write

$$v = gT + h,$$

where g and h are integers with $0 \leq g \leq T$, $0 \leq h < T$, and such that

$$xy \equiv hT + (f + g)t + bd \pmod{n}.$$

f) Show that the right-hand side of the congruence of part (e) can be computed without exceeding the word size, by first finding j such that

$$j \equiv (f + g)t \pmod{n}$$

and $0 \leq j < n$, and then finding k such that

$$k \equiv j + bd \pmod{n}$$

and $0 \leq k < n$, so that

$$xy \equiv hT + k \pmod{n}.$$

This gives the desired result.

32. Develop an algorithm for modular exponentiation from the base 3 expansion of the exponent.

33. Find the least positive residue of each of the following.
   a) 3^{10} modulo 11
   b) 2^{12} modulo 13
   c) 5^{16} modulo 17
   d) 3^{22} modulo 23
   e) Can you propose a theorem from the above congruences?

34. Find the least positive residues of each of the following.
   a) 6! modulo 7
   b) 10! modulo 11
   c) 12! modulo 13
   d) 16! modulo 17
   e) Can you propose a theorem from the above congruences?

* **35.** Show that for every positive integer m there are infinitely many Fibonacci numbers f_n such that m divides f_n. (*Hint:* Show that the sequence of least positive residues modulo m of the Fibonacci numbers is a repeating sequence.)

36. Prove Theorem 4.7 using mathematical induction.

37. Show that the least nonnegative residue modulo m of the product of two positive integers less than m can be computed using $O(\log^2 m)$ bit operations.

* **38.** Five men and a monkey are shipwrecked on an island. The men have collected a pile of coconuts which they plan to divide equally among themselves the next morning. Not trusting the other men, one of the group wakes up during the night and divides the coconuts into five equal parts with one left over, which he gives to the monkey. He then hides his portion of the pile. During the night, each of the other four men does exactly the same thing by dividing the pile he finds into five equal parts leaving one coconut for the monkey and hiding his portion. In the morning, the men gather and split the remaining pile of coconuts into five parts and one is left over for the monkey. What is the minimum number of coconuts the men could have collected for their original pile?

* **39.** Answer the question in Exercise 38, where instead of five men and one monkey, there are n men and k monkeys, and at each stage the monkeys receive one coconut each.

We say that the polynomials $f(x)$ and $g(x)$ are *congruent modulo n as polynomials* if for each power of x the coefficients of that power in $f(x)$ and $g(x)$ are congruent modulo n. For example, $11x^3 + x^2 + 2$ and $x^3 - 4x^2 + 5x + 22$ are congruent as polynomials modulo 5. The notation $f(x) \equiv g(x) \pmod{n}$ is often used to denote that $f(x)$ and $g(x)$ are congruent as polynomials modulo n. In Exercises 40–44 assume that n is a positive integer with $n > 1$ and that all polynomials have integer coefficients.

40. a) Show that if $f(x)$ and $g(x)$ are congruent as polynomials modulo n, then for every integer a, $f(a) \equiv g(a) \pmod{n}$.
   b) Show that it is not necessarily true that $f(x)$ and $g(x)$ are congruent as polynomials modulo n if $f(a) \equiv g(a) \pmod{n}$ for every integer a.

41. Show that if $f_1(x)$ and $g_1(x)$ are congruent as polynomials modulo n and $f_2(x)$ and $g_2(x)$ are congruent as polynomials modulo n, then
   a) $(f_1 + f_2)(x)$ and $(g_1 + g_2)(x)$ are congruent as polynomials modulo n.
   b) $(f_1 f_2)(x)$ and $(g_1 g_2)(x)$ are congruent as polynomials modulo n.

42. Show that if $f(x)$ is a polynomial with integer coefficients and $f(a) \equiv 0 \pmod{n}$, then there is a polynomial $g(x)$ with integer coefficients such that $f(x)$ and $(x-a)g(x)$ are congruent as polynomials modulo n.

43. Suppose that p is prime, $f(x)$ is a polynomial with integer coefficients, $a_1, a_2, \ldots, a_k$ are incongruent integers modulo p, and $f(a_j) \equiv 0 \pmod{p}$ for $j = 1, 2, \ldots, k$. Show that there exists a polynomial $g(x)$ with integer coefficients such that $f(x)$ and $(x-a_1)(x-a_2)\cdots(x-a_k)g(x)$ are congruent as polynomials modulo p.

44. Use Exercise 43 to show that if p is a prime, $f(x)$ is a polynomial with integer coefficients, and x^n is the largest power of x with a coefficient divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most p incongruent solutions modulo p.

4.1 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. Compute the least positive residue modulo 10,403 of 7651^{891}.
2. Compute the least positive residue modulo 10,403 of $7651^{20!}$.

Programming Projects

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

1. Find the least nonnegative residue of an integer with respect to a fixed modulus.
2. Perform modular addition and subtraction when the modulus is less than half of the word size of the computer.
3. Perform modular multiplication when the modulus is less than half of the word size of the computer, using Exercise 31.
4. Perform modular exponentiation using the algorithm described in the text.

4.2 Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

where x is an unknown integer, is called a *linear congruence in one variable*. In this section, we will see that the study of such congruences is similar to the study of linear diophantine equations in two variables.

We first note that if $x = x_0$ is a solution of the congruence $ax \equiv b \pmod{m}$, and if $x_1 \equiv x_0 \pmod{m}$, then $ax_1 \equiv ax_0 \equiv b \pmod{m}$, so that x_1 is also a solution. Hence, if one member of a congruence class modulo m is a solution, then all members of this class are solutions. Therefore, we may ask how many of the m congruence classes modulo m give solutions; this is exactly the same as asking how many incongruent solutions there are modulo m. The following theorem tells us when a linear congruence in one

variable has solutions, and if it does, tells exactly how many incongruent solutions there are modulo m.

Theorem 4.10. Let a, b, and m be integers such that $m > 0$ and $(a, m) = d$. If $d \nmid b$, then $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d incongruent solutions modulo m.

Proof. By Theorem 4.1, the linear congruence $ax \equiv b \pmod{m}$ is equivalent to the linear diophantine equation in two variables $ax - my = b$. The integer x is a solution of $ax \equiv b \pmod{m}$ if and only if there is an integer y such that $ax - my = b$. By Theorem 3.23, we know that if $d \nmid b$, there are no solutions, whereas if $d \mid b$, $ax - my = b$ has infinitely many solutions, given by

$$x = x_0 + (m/d)t, \quad y = y_0 + (a/d)t,$$

where $x = x_0$ and $y = y_0$ is a particular solution of the equation. The values of x given above,

$$x = x_0 + (m/d)t,$$

are the solutions of the linear congruence; there are infinitely many of these.

To determine how many incongruent solutions there are, we find the condition that describes when two of the solutions $x_1 = x_0 + (m/d)t_1$ and $x_2 = x_0 + (m/d)t_2$ are congruent modulo m. If these two solutions are congruent, then

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2 \pmod{m}.$$

Subtracting x_0 from both sides of this congruence, we find that

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}.$$

Now $(m, m/d) = m/d$ since $(m/d) \mid m$, so that by Theorem 4.4, we see that

$$t_1 \equiv t_2 \pmod{d}.$$

This shows that a complete set of incongruent solutions is obtained by taking $x = x_0 + (m/d)t$, where t ranges through a complete system of residues modulo d. One such set is given by $x = x_0 + (m/d)t$, where $t = 0, 1, 2, \ldots, d - 1$. ∎

A linear congruence where the multiplier a and the modulus m are relatively prime has a unique solution, as Corollary 4.10.1 shows.

Corollary 4.10.1. If a and m are relatively prime integers with $m > 0$ and b is an integer, then the linear congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m.

Proof. Because $(a, m) = 1$, we know that $(a, m) \mid b$. Consequently, by Theorem 4.10, it follows that the congruence $ax \equiv b \pmod{m}$ has exactly $(a, m) = 1$ incongruent solution modulo m. ∎

We now illustrate the use of Theorem 4.10.

Example 4.12. To find all solutions of $9x \equiv 12 \pmod{15}$, we first note that since $(9, 15) = 3$ and $3 \mid 12$, there are exactly three incongruent solutions. We can find these solutions by first finding a particular solution and then adding the appropriate multiples of $15/3 = 5$.

To find a particular solution, we consider the linear diophantine equation $9x - 15y = 12$. The Euclidean algorithm shows that

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2, \end{aligned}$$

so that $3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15$. Hence, $9 \cdot 8 - 15 \cdot 4 = 12$, and a particular solution of $9x - 15y = 12$ is given by $x_0 = 8$ and $y_0 = 4$.

From the proof of Theorem 4.10, we see that a complete set of three incongruent solutions is given by $x = x_0 \equiv 8 \pmod{15}$, $x = x_0 + 5 \equiv 13 \pmod{15}$, and $x = x_0 + 5 \cdot 2 \equiv 18 \equiv 3 \pmod{15}$. ◀

Modular Inverses We now consider congruences of the special form $ax \equiv 1 \pmod{m}$. By Theorem 4.10, there is a solution to this congruence if and only if $(a, m) = 1$, and then all solutions are congruent modulo m.

Definition. Given an integer a with $(a, m) = 1$, a solution of $ax \equiv 1 \pmod{m}$ is called an *inverse of* a modulo m.

Example 4.13. Because the solutions of $7x \equiv 1 \pmod{31}$ satisfy $x \equiv 9 \pmod{31}$, 9, and all integers congruent to 9 modulo 31, are inverses of 7 modulo 31. Analogously, since $9 \cdot 7 \equiv 1 \pmod{31}$, 7 is an inverse of 9 modulo 31. ◀

When we have an inverse of a modulo m, we can use it to solve any congruence of the form $ax \equiv b \pmod{m}$. To see this, let $\bar{a}$ be an inverse of a modulo m, so that $a\bar{a} \equiv 1 \pmod{m}$. Then, if $ax \equiv b \pmod{m}$, we can multiply both sides of this congruence by $\bar{a}$ to find that $\bar{a}(ax) \equiv \bar{a}b \pmod{m}$, so that $x \equiv \bar{a}b \pmod{m}$.

Example 4.14. To find the solutions of $7x \equiv 22 \pmod{31}$, we multiply both sides of this congruence by 9, an inverse of 7 modulo 31, to obtain $9 \cdot 7x \equiv 9 \cdot 22 \pmod{31}$. Hence, $x \equiv 198 \equiv 12 \pmod{31}$. ◀

Example 4.15. To find all solutions of $7x \equiv 4 \pmod{12}$, we note that since $(7, 12) = 1$, there is a unique solution modulo 12. To find this, we need only obtain a solution of the linear diophantine equation $7x - 12y = 4$. The Euclidean algorithm gives

$$\begin{aligned} 12 &= 7 \cdot 1 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2. \end{aligned}$$

Hence, $1 = 5 - 2 \cdot 2 = 5 - (7 - 5 \cdot 1) \cdot 2 = 5 \cdot 3 - 2 \cdot 7 = (12 - 7 \cdot 1) \cdot 3 - 2 \cdot 7 = 12 \cdot 3 - 5 \cdot 7$. Therefore, a particular solution to the linear diophantine equation is $x_0 = -20$ and $y_0 = 12$. Hence, all solutions of the linear congruences are given by $x \equiv -20 \equiv 4 \pmod{12}$. ◀

Later we will want to know which integers are their own inverses modulo p, where p is prime. The following theorem tells us which integers have this property.

Theorem 4.11. Let p be prime. The positive integer a is its own inverse modulo p if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof. If $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$, so that a is its own inverse modulo p.

Conversely, if a is its own inverse modulo p, then $a^2 = a \cdot a \equiv 1 \pmod{p}$. Hence, $p \mid (a^2 - 1)$. Since $a^2 - 1 = (a - 1)(a + 1)$, either $p \mid (a - 1)$ or $p \mid (a + 1)$. Therefore, either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ■

4.2 Exercises

1. Find all solutions of each of the following linear congruences.

   a) $2x \equiv 5 \pmod{7}$
   b) $3x \equiv 6 \pmod{9}$
   c) $19x \equiv 30 \pmod{40}$
   d) $9x \equiv 5 \pmod{25}$
   e) $103x \equiv 444 \pmod{999}$
   f) $980x \equiv 1500 \pmod{1600}$

2. Find all solutions of each of the following linear congruences.

   a) $3x \equiv 2 \pmod{7}$
   b) $6x \equiv 3 \pmod{9}$
   c) $17x \equiv 14 \pmod{21}$
   d) $15x \equiv 9 \pmod{25}$
   e) $128x \equiv 833 \pmod{1001}$
   f) $987x \equiv 610 \pmod{1597}$

3. Find all solutions to the congruence $6{,}789{,}783x \equiv 2{,}474{,}010 \pmod{28{,}927{,}591}$.

4. Suppose that p is prime and that a and b are positive integers with $(p, a) = 1$. The following method can be used to solve the linear congruence $ax \equiv b \pmod{p}$.

   a) Show that if the integer x is a solution of $ax \equiv b \pmod{p}$, then x is also a solution of the linear congruence

   $$a_1 x \equiv -b[m/a] \pmod{p},$$

   where a_1 is the least positive residue of p modulo a. Note that this congruence is of the same type as the original congruence, with a positive integer smaller than a as the coefficient of x.

   b) When the procedure of part (a) is iterated, one obtains a sequence of linear congruences with coefficients of x equal to $a_0 = a > a_1 > a_2 > \cdots$. Show that there is a positive integer n with $a_n = 1$, so that at the nth stage, one obtains a linear congruence $x \equiv B \pmod{p}$.

   c) Use the method described in part (b) to solve the linear congruence $6x \equiv 7 \pmod{23}$.

5. An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

6. For which integers c, $0 \leq c < 30$, does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

7. For which integers c, $0 \leq c < 1001$, does the congruence $154x \equiv c \pmod{1001}$ have solutions? When there are solutions, how many incongruent solutions are there?

8. Find an inverse modulo 13 of each of the following integers.

   a) 2 c) 5
   b) 3 d) 11

9. Find an inverse modulo 17 of each of the following integers.

   a) 4 c) 7
   b) 5 d) 16

10. a) Determine which integers a, where $1 \leq a \leq 14$, have an inverse modulo 14.
    b) Find the inverse of each of the integers from part (a) that have an inverse modulo 14.

11. a) Determine which integers a, where $1 \leq a \leq 30$, have an inverse modulo 30.
    b) Find the inverse of each of the integers from part (a) that have an inverse modulo 30.

12. Show that if $\bar{a}$ is an inverse of a modulo m and $\bar{b}$ is an inverse of b modulo m, then $\bar{a}\,\bar{b}$ is an inverse of ab modulo m.

13. Show that the linear congruence in two variables $ax + by \equiv c \pmod{m}$, where a, b, c, and m are integers, $m > 0$, with $d = (a, b, m)$, has exactly dm incongruent solutions if $d \mid c$, and no solutions otherwise.

14. Find all solutions of each of the following linear congruences in two variables.

    a) $2x + 3y \equiv 1 \pmod{7}$ c) $6x + 3y \equiv 0 \pmod{9}$
    b) $2x + 4y \equiv 6 \pmod{8}$ d) $10x + 5y \equiv 9 \pmod{15}$

15. Let p be an odd prime and k a positive integer. Show that the congruence $x^2 \equiv 1 \pmod{p^k}$ has exactly two incongruent solutions, namely $x \equiv \pm 1 \pmod{p^k}$.

16. Show that the congruence $x^2 \equiv 1 \pmod{2^k}$ has exactly four incongruent solutions, namely $x \equiv \pm 1$ or $\pm(1 + 2^{k-1}) \pmod{2^k}$, when $k > 2$. Show that when $k = 1$ there is one solution and that when $k = 2$ there are two incongruent solutions.

17. Show that if a and m are relatively prime positive integers such that $a < m$, then an inverse of a modulo m can be found using $O(\log^3 m)$ bit operations.

18. Show that if p is an odd prime and a is a positive integer not divisible by p, then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or exactly two incongruent solutions.

4.2 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 solutions of $123{,}456{,}789x \equiv 9{,}876{,}543{,}210 \pmod{10{,}000{,}000{,}001}$.
2. Find the solutions of $333{,}333{,}333x \equiv 87{,}543{,}211{,}376 \pmod{967{,}454{,}302{,}211}$.
3. Find the inverses of 734,342; 499,999; and 1,000,001 modulo 1,533,331.

Programming Projects

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

1. Solve linear congruences using the method given in the text.
2. Solve linear congruences using the method given in Exercise 4.
3. Find inverses modulo m of integers relatively prime to m, where m is a positive integer.
4. Solve linear congruences using inverses.
5. Solve linear congruences in two variables.

4.3 The Chinese Remainder Theorem

In this and in the following section, we discuss systems of simultaneous congruences. We will study two types of such systems: In the first type, there are two or more linear congruences in one variable, with different moduli. The second type consists of more than one simultaneous congruence in more than one variable, where all congruences have the same modulus.

First, we consider systems of congruences that involve only one unknown, but different moduli. Such systems arose in ancient Chinese puzzles such as the following problem, which appears in *Master Sun's Mathematical Manual*, written late in the third century C.E.. Find a number that leaves a remainder of 1 when divided by 3, a remainder of 2 when divided by 5, and a remainder of 3 when divided by 7. This puzzle leads to the following system of congruences:

$$x \equiv 1 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}.$$

Problems involving systems of congruences occur in the writings of the Greek mathematician Nicomachus in the first century. They also can be found in the works of Brahmagupta in India in the seventh century. However, it was not until the year 1247 that a general method for solving systems of linear congruences was published by *Ch'in Chiu-Shao* in his *Mathematical Treatise in Nine Sections*. We now present the main theorem concerning the solution of systems of linear congruences in one unknown. This theorem is called the Chinese remainder theorem, most likely because of the contributions of Chinese mathematicians such as Ch'in Chiu-Shao to its solution. (For more information

about the history of the Chinese remainder theorem, consult [Ne69], [LiDu87], [Li73], and [Ka98].)

Theorem 4.12. ***The Chinese Remainder Theorem.*** Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \ldots m_r$.

Proof. First, we construct a simultaneous solution to the system of congruences. To do this, let $M_k = M/m_k = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$. We know that $(M_k, m_k) = 1$ by Exercise 14 of Section 3.3, because $(m_j, m_k) = 1$ whenever $j \neq k$. Hence, by Theorem 4.10 we can find an inverse y_k of M_k modulo m_k, so that $M_k y_k \equiv 1 \pmod{m_k}$. We now form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r.$$

The integer x is a simultaneous solution of the r congruences. To demonstrate this, we must show that $x \equiv a_k \pmod{m_k}$ for $k = 1, 2, \ldots, r$. Since $m_k \mid M_j$ whenever $j \neq k$, we have $M_j \equiv 0 \pmod{m_k}$. Therefore, in the sum for x, all terms except the kth term are congruent to 0 (mod m_k). Hence, $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, since $M_k y_k \equiv 1 \pmod{m_k}$. We now show that any two solutions are congruent modulo M. Let x_0 and x_1 both be simultaneous solutions to the system of r congruences. Then, for each

CH'IN CHIU-SHAO (1202–1261) was born in the Chinese province of Sichuan. He studied astronomy at Hangzhou, the capital of the Song dynasty. He spent ten years in dangerous and difficult conditions at the frontier, where battles with the Mongols under Genghis Khan were under way. He wrote that he was instructed in mathematics by a "recluse scholar." During his time at the frontier, he investigated mathematical problems. He selected 81 of these, divided them into nine classes, and described them in his book *Mathematical Treatise in Nine Sections.* This book covers systems of linear congruences, the Chinese remainder theorem, algebraic equations, areas of geometrical figures, systems of linear equations, and other topics.

Ch'in Chiu-Shao was considered to be a mathematical genius and was talented in architecture, music, and poetry, as well as in many sports, including archery, fencing, and horsemanship. He held several different positions in government, but was relieved of his duties many times because of corruption. He was considered to be extravagant, boastful, and obsessed with his own advancement. He managed to amass great wealth and through deceit had an immense house constructed at a magnificent site. The back of this house contained a series of rooms for lodging female musicians and singers. Ch'in Chiu-Shao developed a notorious reputation in love affairs.

k, $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$, so that $m_k \mid (x_0 - x_1)$. Using Theorem 4.8, we see that $M \mid (x_0 - x_1)$. Therefore, $x_0 \equiv x_1 \pmod{M}$. This shows that the simultaneous solution of the system of r congruences is unique modulo M. ■

We illustrate the use of the Chinese remainder theorem by solving the system that arises from the ancient Chinese puzzle.

Example 4.16. To solve the system

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7,$$

we have $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, and $M_3 = 105/7 = 15$. To determine y_1, we solve $35y_1 \equiv 1 \pmod 3$, or equivalently, $2y_1 \equiv 1 \pmod 3$. This yields $y_1 \equiv 2 \pmod 3$. We find y_2 by solving $21y_2 \equiv 1 \pmod 5$; this immediately gives $y_2 \equiv 1 \pmod 5$. Finally, we find y_3 by solving $15y_3 \equiv 1 \pmod 7$. This gives $y_3 \equiv 1 \pmod 7$. Hence,

$$\begin{aligned} x &\equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \\ &\equiv 157 \equiv 52 \pmod{105}. \end{aligned}$$

We can check that x satisfies this system of congruences whenever $x \equiv 52 \pmod{105}$ by noting that $52 \equiv 1 \pmod 3$, $52 \equiv 2 \pmod 5$, and $52 \equiv 3 \pmod 7$. ◀

There is also an iterative method for solving simultaneous systems of congruences. We illustrate this method with an example.

Example 4.17. Suppose we wish to solve the system

$$x \equiv 1 \pmod 5$$
$$x \equiv 2 \pmod 6$$
$$x \equiv 3 \pmod 7.$$

We use Theorem 4.1 to rewrite the first congruence as an equality, namely $x = 5t + 1$, where t is an integer. Inserting this expression for x into the second congruence, we find that

$$5t + 1 \equiv 2 \pmod 6,$$

which can easily be solved to show that $t \equiv 5 \pmod 6$. Using Theorem 4.1 again, we write $t = 6u + 5$, where u is an integer. Hence, $x = 5(6u + 5) + 1 = 30u + 26$. When we insert this expression for x into the third congruence, we obtain

$$30u + 26 \equiv 3 \pmod 7.$$

When this congruence is solved, we find that $u \equiv 6 \pmod 7$. Consequently, Theorem 4.1 tells us that $u = 7v + 6$, where v is an integer. Hence,

$$x = 30(7v + 6) + 26 = 210v + 206.$$

Translating this equality into a congruence, we find that

$$x \equiv 206 \pmod{210},$$

and this is the simultaneous solution. ◀

Note that the method we have just illustrated shows that a system of simultaneous questions can be solved by successively solving linear congruences. This can be done even when the moduli of the congruences are not relatively prime as long as congruences are consistent (see Exercises 15–20 at the end of this section).

Computer Arithmetic Using the Chinese Remainder Theorem The Chinese remainder theorem provides a way to perform computer arithmetic with large integers. To store very large integers and do arithmetic with them requires special techniques. The Chinese remainder theorem tells us that given pairwise relatively prime moduli $m_1, m_2, \ldots, m_r$, a positive integer n such that $n < M = m_1 m_2 \cdots m_r$ is uniquely determined by its least positive residues modulo m_j for $j = 1, 2, \ldots, r$. Suppose that the word size of a computer is only 100, but that we wish to do arithmetic with integers as large as 10^6. First, we find pairwise relatively prime integers less than 100 with a product exceeding 10^6; for instance, we can take $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, and $m_4 = 95$. We convert integers less than 10^6 into 4-tuples consisting of their least positive residues modulo m_1, m_2, m_3, and m_4. (To convert integers as large as 10^6 into their list of least positive residues, we need to work with large integers using multiprecision techniques. However, this is done only once for each integer in the input and once for the output.) Then, for instance, to add integers, we simply add their respective least positive residues modulo m_1, m_2, m_3, and m_4, making use of the fact that if $x \equiv x_i \pmod{m_i}$ and $y \equiv y_i \pmod{m_i}$, then $x + y \equiv x_i + y_i \pmod{m_i}$. We then use the Chinese remainder theorem to convert the set of four least positive residues for the sum back to an integer.

The following example illustrates this technique.

Example 4.18. We wish to add $x = 123{,}684$ and $y = 413{,}456$ on a computer of word size 100. We have

$$\begin{aligned} x &\equiv 33 \pmod{99} \quad y \equiv 32 \pmod{99}, \\ x &\equiv 8 \pmod{98} \quad y \equiv 92 \pmod{98}, \\ x &\equiv 9 \pmod{97} \quad y \equiv 42 \pmod{97}, \\ x &\equiv 89 \pmod{95} \quad y \equiv 16 \pmod{95}, \end{aligned}$$

so that

$$\begin{aligned} x + y &\equiv 65 \pmod{99}, \\ x + y &\equiv 2 \pmod{98}, \\ x + y &\equiv 51 \pmod{97}, \\ x + y &\equiv 10 \pmod{95}. \end{aligned}$$

We now use the Chinese remainder theorem to find $x + y$ modulo $99 \cdot 98 \cdot 97 \cdot 95$. We have $M = 99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$, $M_1 = M/99 = 903{,}070$, $M_2 = M/98 = 912{,}285$, $M_3 = M/97 = 921{,}690$, and $M_4 = M/95 = 941{,}094$. We need to find the

inverse of $M_i \pmod{y_i}$ for $i = 1, 2, 3, 4$. To do this, we solve the following congruences (using the Euclidean algorithm):

$$903{,}070y_1 \equiv 91y_1 \equiv 1 \pmod{99},$$
$$912{,}285y_2 \equiv 3y_2 \equiv 1 \pmod{98},$$
$$921{,}690y_3 \equiv 93y_3 \equiv 1 \pmod{97},$$
$$941{,}094y_4 \equiv 24y_4 \equiv 1 \pmod{95}.$$

We find that $y_1 \equiv 37 \pmod{99}$, $y_2 \equiv 35 \pmod{98}$, $y_3 \equiv 24 \pmod{97}$, and $y_4 \equiv 4 \pmod{95}$. Hence,

$$\begin{aligned} x + y &\equiv 65 \cdot 903{,}070 \cdot 37 + 2 \cdot 912{,}285 \cdot 33 + 51 \cdot 921{,}690 \cdot 24 + 10 \cdot 941{,}094 \cdot 4 \\ &= 3{,}397{,}886{,}480 \\ &\equiv 537{,}140 \pmod{89{,}403{,}930}. \end{aligned}$$

Since $0 < x + y < 89{,}403{,}930$, we conclude that $x + y = 537{,}140$. ◀

On most computers, the word size is a large power of 2, with 2^{35} a common value. Hence, to use modular arithmetic and the Chinese remainder theorem to do computer arithmetic, we need integers less than 2^{35} that are pairwise relatively prime and that multiply together to give a large integer. To find such integers, we use numbers of the form $2^m - 1$, where m is a positive integer. Computer arithmetic with these numbers turns out to be relatively simple (see [Kn97]). To produce a set of pairwise relatively prime numbers of this form, we first prove two lemmas.

Lemma 4.2. If a and b are positive integers, then the least positive residue of $2^a - 1$ modulo $2^b - 1$ is $2^r - 1$, where r is the least positive residue of a modulo b.

Proof. From the division algorithm, $a = bq + r$, where r is the least positive residue of a modulo b. We have $2^a - 1 = 2^{bq+r} - 1 = (2^b - 1)(2^{b(q-1)+r} + \cdots + 2^{b+r} + 2^r) + (2^r - 1)$, which shows that the remainder when $2^a - 1$ is divided by $2^b - 1$ is $2^r - 1$; this is the least positive residue of $2^a - 1$ modulo $2^b - 1$. ■

We use Lemma 4.2 to prove the following result.

Lemma 4.3. If a and b are positive integers, then the greatest common divisor of $2^a - 1$ and $2^b - 1$ is $2^{(a,b)} - 1$.

Proof. When we perform the Euclidean algorithm with $a = r_0$ and $b = r_1$, we obtain

$$\begin{aligned} r_0 &= r_1q_1 + r_2 && 0 \le r_2 < r_1 \\ r_1 &= r_2q_2 + r_3 && 0 \le r_3 < r_2 \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-2} + r_{n-1} && 0 \le r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1}q_{n-1}, \end{aligned}$$

where the last remainder, r_{n-1}, is the greatest common divisor of a and b.

Using Lemma 4.2, and the steps of the Euclidean algorithm with $a = r_0$ and $b = r_1$, when we perform the Euclidean algorithm on the pair $2^a - 1 = R_0$ and $2^b - 1 = R_1$, we obtain

$$\begin{aligned} R_0 &= R_1Q_1 + R_2 & R_2 &= 2^{r_2} - 1 \\ R_1 &= R_2Q_2 + R_3 & R_3 &= 2^{r_3} - 1 \\ &\vdots \\ R_{n-3} &= R_{n-2}Q_{n-2} + R_{n-1} & R_{n-1} &= 2^{r_{n-1}} - 1 \\ R_{n-2} &= R_{n-1}Q_{n-1}. \end{aligned}$$

Here, the last nonzero remainder, $R_{n-1} = 2^{r_{n-1}} - 1 = 2^{(a,b)} - 1$, is the greatest common divisor of R_0 and R_1. ∎

Using Lemma 4.3, we have the following theorem.

Theorem 4.13. The positive integers $2^a - 1$ and $2^b - 1$ are relatively prime if and only if a and b are relatively prime.

We can now use Theorem 4.13 to produce a set of pairwise relatively prime integers, each of which is less than 2^{35}, with product greater than a specified integer. Suppose that we wish to do arithmetic with integers as large as 2^{184}. We pick $m_1 = 2^{35} - 1$, $m_2 = 2^{34} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{31} - 1$, $m_5 = 2^{29} - 1$, and $m_6 = 2^{23} - 1$. Since the exponents of 2 in the expressions for the m_j are pairwise relatively prime, by Theorem 4.13, the m_j are pairwise relatively prime. Also, we have $M = m_1m_2m_3m_4m_5m_6 > 2^{184}$. We can now use modular arithmetic and the Chinese remainder theorem to perform arithmetic with integers as large as 2^{184}.

Although it is somewhat awkward to do computer operations with large integers using modular arithmetic and the Chinese remainder theorem, there are some definite advantages to this approach. First, on many high-speed computers, operations can be performed simultaneously. So, reducing an operation involving two large integers to a set of operations involving smaller integers, namely the least positive residues of the large integers with respect to the various moduli, leads to simultaneous computations which may be performed more rapidly than one operation with large integers, especially when parallel processing is used. Second, even without taking into account the advantages of simultaneous computations, multiplication of large integers may be done faster using these ideas than with many other multiprecision methods. The interested reader should consult Knuth [Kn97].

4.3 Exercises

1. Which integers leave a remainder of 1 when divided by both 2 and 3?
2. Find an integer that leaves a remainder of 1 when divided by either 2 or 5, but that is divisible by 3.
3. Find an integer that leaves a remainder of 2 when divided by either 3 or 5, but that is divisible by 4.

4. Find all the solutions of each of the following systems of linear congruences.

a) $x \equiv 4 \pmod{11}$
$x \equiv 3 \pmod{17}$

b) $x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$

c) $x \equiv 0 \pmod{2}$
$x \equiv 0 \pmod{3}$
$x \equiv 1 \pmod{5}$
$x \equiv 6 \pmod{7}$

d) $x \equiv 2 \pmod{11}$
$x \equiv 3 \pmod{12}$
$x \equiv 4 \pmod{13}$
$x \equiv 5 \pmod{17}$
$x \equiv 6 \pmod{19}$

5. Find all the solutions to the system of linear congruences $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$, and $x \equiv 5 \pmod{11}$.

6. Find all the solutions to the system of linear congruences $x \equiv 1 \pmod{999}$, $x \equiv 2 \pmod{1001}$, $x \equiv 3 \pmod{1003}$, $x \equiv 4 \pmod{1004}$, and $x \equiv 5 \pmod{1007}$.

7. A troop of 17 monkeys store their bananas in 11 piles of equal size, each containing more than 1 banana, with a twelfth pile of 6 left over. When they divide the bananas into 17 equal groups, none remain. What is the smallest number of bananas they can have?

8. As an odometer check, a special counter measures the miles a car travels modulo 7. Explain how this counter can be used to determine whether the car has been driven 49,335; 149,335; or 249,335 miles when the odometer reads 49,335 and works modulo 100,000.

9. Chinese generals counted troops remaining after a battle by lining them up in rows of different lengths, counting the number left over each time, and calculating the total from these remainders. If a general had 1200 troops at the start of a battle and if there were 3 left over when they lined up 5 at a time, 3 left over when they lined up 6 at a time, 1 left over when they lined up 7 at a time, and none left over when they lined up 11 at a time, how many troops remained after the battle?

10. Find an integer that leaves a remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

11. Find a multiple of 11 that leaves a remainder of 1 when divided by each of the integers 2, 3, 5, and 7.

12. Solve the following ancient Indian problem: If eggs are removed from a basket 2, 3, 4, 5, and 6 at a time, there remain, respectively, 1, 2, 3, 4, and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?

13. Show that there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1. (*Hint:* Use the Chinese remainder theorem to show that there is a simultaneous solution to the system of congruences $x \equiv 0 \pmod{4}$, $x \equiv -1 \pmod{9}$, $x \equiv -2 \pmod{25}$, $\ldots$, $x \equiv -k + 1 \pmod{p_k^2}$, where p_k is the kth prime.)

* **14.** Show that if a, b, and c are integers such that $(a, b) = 1$, then there is an integer n such that $(an + b, c) = 1$.

In Exercises 15–18, we will consider systems of congruences where the moduli of the congruences are not necessarily relatively prime.

15. Show that the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

has a solution if and only if $(m_1, m_2) \mid (a_1 - a_2)$. Show that when there is a solution, it is unique modulo $[m_1, m_2]$. (*Hint:* Write the first congruence as $x = a_1 + km_1$, where k is an integer, and then insert this expression for x into the second congruence.)

16. Using Exercise 15, solve each of the following simultaneous systems of congruences.

a) $x \equiv 4 \pmod{6}$
$x \equiv 13 \pmod{15}$

b) $x \equiv 7 \pmod{10}$
$x \equiv 4 \pmod{15}$

17. Using Exercise 15, solve each of the following simultaneous systems of congruences.

a) $x \equiv 10 \pmod{60}$
$x \equiv 80 \pmod{350}$

b) $x \equiv 2 \pmod{910}$
$x \equiv 93 \pmod{1001}$

18. Does the system of congruences $x \equiv 1 \pmod{8}$, $x \equiv 3 \pmod{9}$, and $x \equiv 2 \pmod{12}$ have any simultaneous solutions?

What happens when the moduli in a simultaneous system of more than two congruences in one unknown are not pairwise relatively prime (such as in Exercise 18)? The following exercise provides compatability conditions for there to be a unique solution of such a system, modulo the least common multiple of the moduli.

19. Show that the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

has a solution if and only if $(m_i, m_j) \mid (a_i - a_j)$ for all pairs of integers (i, j), where $1 \leq i < j \leq r$. Show that if a solution exists, then it is unique modulo $[m_1, m_2, \ldots, m_r]$. (*Hint:* Use Exercise 15 and mathematical induction.)

20. Using Exercise 19, solve each of the following systems of congruences.

a) $x \equiv 5 \pmod{6}$
$x \equiv 3 \pmod{10}$
$x \equiv 8 \pmod{15}$

b) $x \equiv 2 \pmod{14}$
$x \equiv 16 \pmod{21}$
$x \equiv 10 \pmod{30}$

c) $x \equiv 2 \pmod{9}$
$x \equiv 8 \pmod{15}$
$x \equiv 10 \pmod{25}$

d) $x \equiv 2 \pmod{6}$
$x \equiv 4 \pmod{8}$
$x \equiv 2 \pmod{14}$
$x \equiv 14 \pmod{15}$

e) $x \equiv 7 \pmod{9}$
$x \equiv 2 \pmod{10}$
$x \equiv 3 \pmod{12}$
$x \equiv 6 \pmod{15}$

21. What is the smallest number of lobsters in a tank if 1 lobster is left over when they are removed 2, 3, 5, or 7 at a time, but no lobsters are left over when they are removed 11 at a time?

22. An ancient Chinese problem asks for the least number of gold coins a band of 17 pirates could have stolen. The problem states that when the pirates divided the coins into equal piles, 3 coins were left over. When they fought over who should get the extra coins, one of the pirates was slain. When the remaining pirates divided the coins into equal piles, 10 coins were left over. When the pirates fought again over who should get the extra coins, another pirate was slain. When they divided the coins in equal piles again, no coins were left over. What is the answer to this problem?

23. Solve the following problem originally posed by Ch'in Chiu-Shao (using different weight units). Three farmers equally divide a quantity of rice with a weight that is an integral number of pounds. The farmers each sell their rice, selling as much as possible, at three different markets where the markets use weights of 83 pounds, 110 pounds, and 135 pounds, and only buy rice in multiples of these weights. What is the least amount of rice the farmers could have divided if the farmers return home with 32 pounds, 70 pounds, and 30 pounds, respectively?

24. Using the Chinese remainder theorem, explain how to add and how to multiply 784 and 813 on a computer of word size 100.

A positive integer $x \neq 1$ with n base b digits is called an *automorph to the base b* if the last n base b digits of x^2 are the same as those of x.

* **25.** Find the base 10 automorphs with four digits (with initial zeros allowed).

* **26.** How many base b automorphs are there with n or fewer base b digits, if b has prime-power factorization $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$?

According to the theory of *biorhythms,* there are three cycles in your life that start the day you are born. These are the *physical, emotional,* and *intellectual cycles,* of lengths 23, 28, and 33 days, respectively. Each cycle follows a sine curve with period equal to the length of that cycle, starting with value 0, climbing to value 1 one-quarter of the way through the cycle, dropping back to value 0 one-half of the way through the cycle, dropping further to value -1 three-quarters of the way through the cycle, and climbing back to value 0 at the end of the cycle.

Answer the following questions about biorhythms, measuring time in quarter days (so that the units will be integers).

27. For which days of your life will you be at a triple peak, where all of your three cycles are at maximum values?

28. For which days of your life will you be at a triple nadir, where all three of your cycles have minimum values?

29. When in your life will all three cycles be at a neutral position (value 0)?

A set of congruences to distinct moduli greater than 1 that has the property that every integer satisfies at least one of the congruences is called a *covering set of congruences.*

30. Show that the set of congruences $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 1 \pmod 6$, and $x \equiv 11 \pmod{12}$ is a covering set of congruences.

31. Show that the set of congruences $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 0 \pmod 5$, $x \equiv 0 \pmod 7$, $x \equiv 1 \pmod 6$, $x \equiv 1 \pmod{10}$, $x \equiv 1 \pmod{14}$, $x \equiv 2 \pmod{15}$, $x \equiv 2 \pmod{21}$, $x \equiv 23 \pmod{30}$, $x \equiv 4 \pmod{35}$, $x \equiv 5 \pmod{42}$, $x \equiv 59 \pmod{70}$, and $x \equiv 104 \pmod{105}$ is a covering set of congruences.

* 32. Let m be a positive integer with prime-power factorization $m = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Show that the congruence $x^2 \equiv 1 \pmod m$ has exactly 2^{r+e} solutions, where $e = 0$ if $a_0 = 0$ or 1, $e = 1$ if $a_0 = 2$, and $e = 2$ if $a_0 > 2$. (*Hint:* Use Exercises 15 and 16 of Section 4.2.)

33. The three children in a family have feet that are 5 inches, 7 inches, and 9 inches long. When they measure the length of the dining room of their house using their feet, they each find that there are 3 inches left over. How long is the dining room?

34. Find all solutions of the congruence $x^2 + 6x - 31 \equiv 0 \pmod{72}$. (*Hint:* First note that $72 = 2^3 3^2$. Find, by trial and error, the solutions of this congruence modulo 8 and modulo 9. Then apply the Chinese remainder theorem.)

35. Find all solutions of the congruence $x^2 + 18x - 823 \equiv 0 \pmod{1800}$. (*Hint:* First note that $1800 = 2^3 3^2 5^2$. Find, by trial and error, the solutions of this congruence modulo 8, modulo 9, and modulo 25. Then apply the Chinese remainder theorem.)

* 36. Give a positive integer R, a prime p that is the only prime between $p - R$ and $p + R$, including the end points, is called *R-reclusive*. Show that for every positive integer R, there are infinitely many R-reclusive primes. (*Hint:* Use the Chinese remainder theorem to find an integer x such that $x - j$ is divisible by p_j and $x + j$ is divisible by p_{R+j}, where p_k is the kth prime. Then invoke Dirichlet's theorem on primes in arithmetic progressions.)

4.3 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. Solve the simultaneous system of congruences $x \equiv 1 \pmod{12{,}341{,}234{,}567}$, $x \equiv 2 \pmod{750{,}000{,}057}$, and $x \equiv 3 \pmod{1{,}099{,}511{,}627{,}776}$.
2. Solve the simultaneous system of congruences $x \equiv 5269 \pmod{40{,}320}$, $x \equiv 1248 \pmod{11{,}111}$, $x \equiv 16{,}645 \pmod{30{,}003}$, and $x \equiv 2911 \pmod{12{,}321}$.
3. Using Exercise 13 of this section, find a string of 100 consecutive positive integers each divisible by a perfect square. Can you find such a set of smaller integers?
4. Find a covering set of congruences (as described in the preamble to Exercise 30) where the smallest modulus of one of the congruences in the covering set is 3; where the smallest modulus of one of the congruences in the covering set is 6; and where the smallest modulus of one of the congruences in the covering set is 8.

Programming Projects

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

1. Solve systems of linear congruences of the type found in the Chinese remainder theorem.
2. Solve systems of linear congruences of the type given in Exercises 15–20.

3. Add large integers exceeding the word size of a computer using the Chinese remainder theorem.
4. Multiply large integers exceeding the word size of a computer using the Chinese remainder theorem.
5. Find automorphs to the base b, where b is a positive integer greater than 1 (see the preamble to Exercise 25).
6. Plot biorhythm charts and find triple peaks and triple nadirs (see the preamble to Exercise 27).

4.4 Solving Polynomial Congruences

This section provides a useful tool that can be used to help find solutions of congruences of the form $f(x) \equiv 0 \pmod{m}$, where $f(x)$ is a polynomial of degree greater than 1 with integer coefficients. An example of such a congruence is $2x^3 + 7x - 4 \equiv 0 \pmod{200}$.

We first note that if m has prime-power factorization $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, then solving the congruence $f(x) \equiv 0 \pmod{m}$ is equivalent to finding the simultaneous solutions to the system of congruences

$$f(x) \equiv 0 \pmod{p_i^{a_i}}, \quad i = 1, 2, \dots, k.$$

Once the solutions of each of the k congruences modulo $p_i^{a_i}$ are known, the solutions of the congruence modulo m can be found by the Chinese remainder theorem. This is illustrated in the following example.

Example 4.19. Solving the congruence

$$2x^3 + 7x - 4 \equiv 0 \pmod{200}$$

reduces to finding the solutions of

$$2x^3 + 7x - 4 \equiv 0 \pmod{8}$$

and

$$2x^3 + 7x - 4 \equiv 0 \pmod{25}$$

since $200 = 2^3 5^2$. The solutions of the congruence modulo 8 are all integers $x \equiv 4 \pmod{8}$ (for x to be a solution x must be even; the cases where x is odd can be quickly checked). In Example 4.20, we will see that the solutions modulo 25 are all integers $x \equiv 16 \pmod{25}$. When we use the Chinese remainder theorem to solve the simultaneous congruences $x \equiv 4 \pmod{8}$ and $x \equiv 16 \pmod{25}$, we find that the solutions are all $x \equiv 116 \pmod{200}$ (as the reader should verify). These are solutions of $2x^3 + 7x - 4 \equiv 0 \pmod{200}$. ◀

We will see that there is a relatively simple way to solve polynomial congruences modulo p^k, once all solutions modulo p are known. We will show that solutions modulo p can be used to find solutions modulo p^2, solutions modulo p^2 can be used to find solutions modulo p^3, and so on. Before introducing the general method, we present an

example illustrating the basic idea used to find solutions of a polynomial congruence modulo p^2 from those modulo p.

Example 4.20. The solutions of

$$2x^3 + 7x - 4 \equiv 0 \pmod 5$$

are the integers with $x \equiv 1 \pmod 5$, as can be seen by testing $x = 0, 1, 2, 3$, and 4. How can we find the solutions modulo 25? We could check all 25 different values $x = 0, 1, 2, \ldots, 24$. However, there is a more systematic method. Since any solution of

$$2x^3 + 7x - 4 \equiv 0 \pmod{25}$$

is also a solution modulo 5 and all solutions modulo 5 satisfy $x \equiv 1 \pmod 5$, it follows that $x = 1 + 5t$, where t is an integer. We can solve for t by substituting $1 + 5t$ for x. We obtain

$$2(1 + 5t)^3 + 7(1 + 5t) - 4 \equiv 0 \pmod{25}.$$

Simplifying, we obtain a linear congruence for t, namely

$$65t + 5 \equiv 15t + 5 \equiv 0 \pmod{25}.$$

By Theorem 4.4, we can eliminate a factor of 5, so that

$$3t + 1 \equiv 0 \pmod 5.$$

The solutions of this congruence are $t \equiv 3 \pmod 5$. This means that the solutions modulo 25 are those x for which $x \equiv 1 + 5t \equiv 1 + 5 \cdot 3 \equiv 16 \pmod{25}$. The reader should verify that these are indeed solutions. ◀

We will now introduce a general method that will help us find the solutions of congruences modulo prime powers. In particular, we will show how the solutions of the congruence $f(x) \equiv 0 \pmod{p^k}$, where p is prime and k is a positive integer with $k \geq 2$, can be found from those of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$. The solutions of the congruence modulo p^k are said to be *lifted* from those modulo p^{k-1}. The theorem uses $f'(x)$, the derivative of f. However, we will not need results from calculus. Instead, we can define the derivative of a polynomial directly and describe the properties that we will need.

Definition. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where a_i is a real number for $i = 0, 1, 2, \ldots, n$. The *derivative* of $f(x)$, denoted by $f'(x)$, equals $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$.

Starting with a polynomial, we can find its derivative and then find the derivative of its derivative, and so on. We can define the kth derivative of a polynomial $f(x)$, denoted by $f^{(k)}(x)$, as the derivative of the $(k-1)$st derivative, that is, $f^{(k)}(x) = (f^{(k-1)})'(x)$.

We will find the following two lemmas helpful. We leave their proofs to the reader.

Lemma 4.4. If $f(x)$ and $g(x)$ are polynomials, then $(f+g)'(x) = f'(x) + g'(x)$ and $(cf)'(x) = c(f'(x))$, where c is a constant. Furthermore, if k is a positive integer, then $(f+g)^{(k)}(x) = f^{(k)}(x) + g^{(k)}(x)$ and $(cf)^{(k)}(x) = c(f^{(k)}(x))$, where c is a constant.

Lemma 4.5. If m and k are positive integers and $f(x) = x^m$, then $f^{(k)}(x) = m(m-1)\cdots(m-k+1)x^{m-k}$.

We can now state the result that can be used to lift solutions of polynomial congruences. It is called *Hensel's lemma* after the German mathematician *Kurt Hensel*, who discovered it in work leading to the invention of the field of mathematics known as p-adic analysis.

Theorem 4.14. ***Hensel's Lemma.*** Suppose that $f(x)$ is a polynomial with integer coefficients and that k is an integer with $k \geq 2$. Suppose further that r is a solution of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$. Then,

(i) if $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique integer t, $0 \leq t < p$, such that $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$, given by

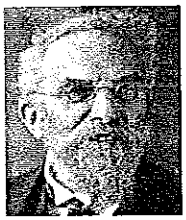
$$t \equiv -\overline{f'(r)}(f(r)/p^{k-1}) \pmod{p},$$

where $\overline{f'(r)}$ is an inverse of $f'(r)$ modulo p;

(ii) if $f'(r) \equiv 0 \pmod{p}$ and $f(r) \equiv 0 \pmod{p^k}$, then $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$ for all integers t;

(iii) if $f'(r) \equiv 0 \pmod{p}$ and $f(r) \not\equiv 0 \pmod{p^k}$, then $f(x) \equiv 0 \pmod{p^k}$ has no solutions with $x \equiv r \pmod{p^{k-1}}$.

In case (i), we see that a solution to $f(x) \equiv 0 \pmod{p^{k-1}}$ lifts to a unique solution of $f(x) \equiv 0 \pmod{p^k}$, and in case (ii), such a solution either lifts to p incongruent solutions modulo p^k or to none at all. ■



KURT HENSEL (1861–1941) was born in Königsberg, Prussia (now Kaliningrad, Russia). He studied mathematics in Berlin, and later in Bonn, under many leading mathematicians, including Kronecker and Weierstrass. Much of his work involved the development of arithmetic in algebraic number fields. Hensel is best known for inventing the p-adic numbers in 1902, in work on representations of algebraic numbers in terms of power series. The p-adic numbers can be thought of as a completion of the set of rational numbers that is different from the usual completion that produces the set of real numbers. Hensel was able to use the p-adic numbers to prove many results in number theory, and these numbers have had a major impact on the development of algebraic number theory. Hensel served as a professor at the University of Marburg until 1930. He was the editor for many years of the famous mathematical journal known as *Crelle's Journal*, whose official name is *Journal für die reine und angewandte Mathematik*.

We will need the following lemma about Taylor expansions for the proof of Hensel's lemma.

Lemma 4.6. If $f(x)$ is a polynomial of degree n with integer coefficients, then

$$f(a+b) = f(a) + f'(a)b + f''(a)b^2/2! + \cdots + f^{(n)}(a)b^n/n!,$$

where the coefficients (namely 1, $f'(a)$, $f''(a)/2! \ldots, f^{(n)}(a)/n!$) are polynomials in a with integer coefficients.

Proof. Every polynomial f of degree n is the sum of multiples of the functions x^m, where $m \leq n$. Furthermore, by Lemma 4.4, we need only establish Lemma 4.6 for the polynomials $f_m(x) = x^m$, where m is a positive integer.

By the binomial theorem, we have

$$(a+b)^m = \sum_{j=0}^{m} \binom{m}{j} a^{m-j} b^j.$$

By Lemma 4.5, we know that $f_m^{(j)}(a) = m(m-1)\cdots(m-j+1)a^{m-j}$. Hence,

$$f_m^{(j)}(a)/j! = \binom{m}{j} a^{m-j}.$$

Because $\binom{m}{j}$ is an integer for all integers m and j such that $0 \leq j \leq m$, the coefficients $f_m(j)/j!$ are integers. This completes the proof. ∎

We now have all the ingredients needed to prove Hensel's lemma.

Proof. If r is a solution of $f(r) \equiv 0 \pmod{p^k}$, then it is also a solution of $f(r) \equiv 0 \pmod{p^{k-1}}$. Hence, it equals $r + tp^{k-1}$ for some integer t. The proof follows once we have determined the conditions on t.

By Lemma 4.6, it follows that

$$f(r+tp^{k-1}) = f(r) + f'(r)tp^{k-1} + \frac{f''(r)}{2!}(tp^{k-1})^2 + \cdots + \frac{f^{(n)}(r)}{n!}(tp^{k-1})^n,$$

where $f^{(k)}(r)/k!$ is an integer for $k = 1, 2, \ldots, n$. Given that $k \geq 2$, it follows that $k \leq m(k-1)$ and $p^k \mid p^{m(k-1)}$ for $2 \leq m \leq n$. Hence,

$$f(r+tp^{k-1}) \equiv f(r) + f'(r)tp^{k-1} \pmod{p^k}.$$

Because $r + tp^{k-1}$ is a solution of $f(r+tp^{k-1}) \equiv 0 \pmod{p^k}$, it follows that $f'(r)tp^{k-1} \equiv -f(r) \pmod{p^k}$.

Furthermore, we can divide this congruence by p^{k-1}, because $f(r) \equiv 0 \pmod{p^{k-1}}$. When we do so and rearrange terms, we obtain a linear congruence in t, namely

$$f'(r)t \equiv -f(r)/p^{k-1} \pmod{p}.$$

By examining its solutions modulo p we can prove the three cases of the theorem.

Suppose that $f'(r) \not\equiv 0 \pmod{p}$. It follows that $(f'(r), p) = 1$. Applying Theorem 4.10, we see that the congruence for t has a unique solution,

$$t \equiv (-f(r)/p^{k-1})\overline{f'(r)} \pmod{p},$$

where $\overline{f'(r)}$ is an inverse of $f'(r)$ modulo p. This establishes case (i).

When $f'(r) \equiv 0 \pmod{p}$, we have $(f'(r), p) = p$. By Theorem 4.10, if $p \mid (f(r)/p^{k-1})$, which holds if and only if $f(r) \equiv 0 \pmod{p^k}$, then all values t are solutions. This means that $x = r + tp^{k-1}$ is a solution for $t = 0, 1, \ldots, p-1$. This establishes case (ii).

Finally, consider the case when $f'(r) \equiv 0 \pmod{p}$, but $p \nmid (f(r)/p^{k-1})$. We have $(f'(r), p) = p$ and $f(r) \not\equiv 0 \pmod{p^k}$; so, by Theorem 4.10, no values of t are solutions. This completes case (iii). ∎

The following corollary shows that we can repeatedly lift solutions, starting with a solution modulo p, when case (i) of Hensel's lemma applies.

Corollary 4.14.1. Suppose that r is a solution of the polynomial congruence $f(x) \equiv 0 \pmod{p}$, where p is a prime. If $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique solution r_k modulo p^k, $k = 2, 3, \ldots$, such that

$$r_k = r_{k-1} - f(r_{k-1})\overline{f'(r)},$$

where $\overline{f'(r)}$ is an inverse of $f'(r)$ modulo p.

Proof. Using the hypotheses, we see by Hensel's lemma that r lifts to a unique solution r_2 modulo p^2 with $r_2 = r + tp$, where $t = -\overline{f'(r)}(f(r)/p)$. Hence,

$$r_2 = r - f(r)\overline{f'(r)}.$$

Because $r_2 \equiv r \pmod{p}$, it follows that $f'(r_2) \equiv f'(r) \not\equiv 0 \pmod{p}$. Using Hensel's lemma again, we see that there is a unique solution r_3 modulo p^3, which can be shown to be $r_3 = r_2 - f(r_2)\overline{f'(r)}$. If we continue in this way, we find that the corollary follows for all integers $k \geq 2$. ∎

The following examples illustrate how Hensel's lemma is applied.

Example 4.21. Find the solutions of

$$x^3 + x^2 + 29 \equiv 0 \pmod{25}.$$

Let $f(x) = x^3 + x^2 + 29$. We see (by inspection) that solutions of $f(x) \equiv 0 \pmod{5}$ have $x \equiv 3 \pmod{5}$. Because $f'(x) = 3x^2 + 2x$ and $f'(3) = 33 \equiv 3 \not\equiv 0 \pmod{5}$, Hensel's lemma tells us that there is a unique solution modulo 25 of the form $3 + 5t$, where

$$t \equiv -\overline{f'(3)}(f(3)/5) \pmod{5}.$$

Note that $\overline{f'(3)} = \overline{3} = 2$, because 2 is inverse to 3 modulo 5. Also note that $f(3)/5 = 65/5 = 13$. It follows that $t \equiv -2 \cdot 13 = 4 \pmod{5}$. We conclude that $x \equiv 3 + 5 \cdot 4 = 23$ is the unique solution of $f(x) \equiv 0 \pmod{25}$. ◀

Example 4.22. Find the solutions of

$$x^2 + x + 7 \equiv 0 \pmod{27}.$$

Let $f(x) = x^2 + x + 7$. We find (by inspection) that the solutions of $f(x) \equiv 0 \pmod 3$ are the integers with $x \equiv 1 \pmod 3$. Because $f'(x) = 2x + 1$, we see that $f'(1) = 3 \equiv 0 \pmod 3$. Furthermore, because $f(1) = 9 \equiv 0 \pmod 9$, we can apply case (ii) of Hensel's lemma to conclude that $1 + 3t$ is a solution modulo 9 for all integers t. This means that the solutions modulo 9 are $x \equiv 1, 4$, or $7 \pmod 9$.

Now, by case (iii) of Hensel's lemma, because $f(1) = 9 \not\equiv 0 \pmod{27}$, there are no solutions of $f(x) \equiv 0 \pmod{27}$ with $x \equiv 1 \pmod 9$. Because $f(4) = 27 \equiv 0 \pmod{27}$, by case (ii), $4 + 9t$ is a solution modulo 27 for all integers t. This shows that all $x \equiv 4, 13$, or $22 \pmod{27}$ are solutions. Finally, by case (iii), because $f(7) = 63 \not\equiv 0 \pmod{27}$, there are no solutions of $f(x) \equiv 0 \pmod{27}$ with $x \equiv 7 \pmod 9$.

Putting everything together, we see that all solutions of $f(x) \equiv 0 \pmod{27}$ are those $x \equiv 4, 13$, or $22 \pmod{27}$. ◀

Example 4.23. What are the solutions of $f(x) = x^3 + x^2 + 2x + 26 \equiv 0 \pmod{343}$? By inspection, we see that the solutions of $x^3 + x^2 + 2x + 26 \equiv 0 \pmod 7$ are the integers $x \equiv 2 \pmod 7$. Because $f'(x) = 3x^2 + 2x + 2$, it follows that $f'(2) = 18 \not\equiv 0 \pmod 7$. We can use Corollary 4.14.1 to find solutions modulo 7^k for $k = 2, 3, \ldots$. Noting that $\overline{f'(2)} = \overline{4} = 2$, we find that $r_2 = 2 - f(2)\overline{f'(2)} = 2 - 42 \cdot 2 = -82 \equiv 16 \pmod{49}$, and $r_3 = 16 - f(16)\overline{f'(2)} = 16 - 4410 \cdot 2 = -8804 \equiv 114 \pmod{343}$. It follows that the solutions modulo 343 are the integers $x \equiv 114 \pmod{343}$. ◀

4.4 Exercises

1. Find all the solutions of each of the following congruences.
   a) $x^2 + 4x + 2 \equiv 0 \pmod 7$
   b) $x^2 + 4x + 2 \equiv 0 \pmod{49}$
   c) $x^2 + 4x + 2 \equiv 0 \pmod{343}$
2. Find all the solutions of each of the following congruences.
   a) $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{11}$
   b) $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{121}$
   c) $x^3 + 8x^2 - x - 1 \equiv 0 \pmod{1331}$
3. Find the solutions of the congruence $x^2 + x + 47 \equiv 0 \pmod{2401}$. (Note that $2401 = 7^4$.)
4. Find the solutions of $x^2 + x + 34 \equiv 0 \pmod{81}$.
5. Find all solutions of $13x^7 - 42x - 649 \equiv 0 \pmod{1323}$.
6. Find all solutions of $x^8 - x^4 + 1001 \equiv 0 \pmod{539}$.
7. Find all solutions of $x^4 + 2x + 36 \equiv 0 \pmod{4375}$.
8. Find all solutions of $x^6 - 2x^5 - 35 \equiv 0 \pmod{6125}$.

9. How many incongruent solutions are there to the congruence $5x^3 + x^2 + x + 1 \equiv 0 \pmod{64}$?

10. How many incongruent solutions are there to the congruence $x^5 + x - 6 \equiv 0 \pmod{144}$?

11. Let a be an integer and p a prime such that $(a, p) = 1$. Use Hensel's lemma to solve the congruence $ax \equiv 1 \pmod{p^k}$, for all positive integers k.

* 12. a) Let $f(x)$ be a polynomial with integer coefficients. Let p be a prime, k a positive integer, and j an integer such that $k \geq 2j + 1$. Let a be a solution of $f(a) \equiv 0 \pmod{p^k}$, with p^j exactly dividing $f'(a)$. Show that if $b \equiv a \pmod{p^{k-j}}$, then $f(b) \equiv f(a) \pmod{p^k}$, p^j exactly divides $f'(b)$, and there is a unique t modulo p such that $f(a + tp^{k-j}) \equiv 0 \pmod{p^{k+1}}$. (*Hint:* Using a Taylor expansion, first show that $f(a + tp^{k-j}) \equiv f(a) + tp^{k-j} f'(a) \pmod{p^{2k-2j}}$.)

b) Show that when the hypotheses of part (a) hold, the solutions of $f(x) \equiv 0 \pmod{p^k}$ may be lifted to solutions of arbitrarily high powers of p.

* 13. How many solutions are there to $x^2 + x + 223 \equiv 0 \pmod{3^j}$, where j is a positive integer? (*Hint:* First find the solutions modulo 3^5 and then apply Exercise 12.)

4.4 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 solutions of $x^4 - 13x^3 + 11x - 3 \equiv 0 \pmod{7^8}$.

2. Find all solutions of $x^9 + 13x^3 - x + 100{,}336 \equiv 0 \pmod{17^9}$.

Programming Projects

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

1. Use Hensel's lemma to solve congruences of the form $f(x) \equiv 0 \pmod{p^n}$, where $f(x)$ is a polynomial, p is prime, and n is a positive integer.

4.5 Systems of Linear Congruences

We will consider systems of more than one congruence that involve the same number of unknowns as congruences, where all congruences have the same modulus. We begin our study with an example.

Suppose that we wish to find all integers x and y such that both of the congruences

$$3x + 4y \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 7 \pmod{13}$$

are satisfied. To attempt to find the unknowns x and y, we multiply the first congruence

by 5 and the second by 4, to obtain

$$15x + 20y \equiv 25 \pmod{13}$$
$$8x + 20y \equiv 28 \pmod{13}.$$

We subtract the second congruence from the first, to find that

$$7x \equiv -3 \pmod{13}.$$

Since 2 is an inverse of 7 (mod 13), we multiply both sides of the above congruence by 2. This gives

$$2 \cdot 7x \equiv -2 \cdot 3 \pmod{13},$$

which tells us that

$$x \equiv 7 \pmod{13}.$$

Likewise, we can multiply the first congruence by 2 and the second by 3 (of the original system), to see that

$$6x + 8y \equiv 10 \pmod{13}$$
$$6x + 15y \equiv 21 \pmod{13}.$$

When we subtract the first congruence from the second, we obtain

$$7y \equiv 11 \pmod{13}.$$

To solve for y, we multiply both sides of this congruence by 2, an inverse of 7 modulo 13. We get

$$2 \cdot 7y \equiv 2 \cdot 11 \pmod{13},$$

so that

$$y \equiv 9 \pmod{13}.$$

What we have shown is that any solution (x, y) must satisfy

$$x \equiv 7 \pmod{13}, \quad y \equiv 9 \pmod{13}.$$

When we insert these congruences for x and y into the original system, we see that these pairs actually are solutions:

$$3x + 4y \equiv 3 \cdot 7 + 4 \cdot 9 = 57 \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 2 \cdot 7 + 5 \cdot 9 = 59 \equiv 7 \pmod{13}.$$

Hence, the solutions of this system of congruences are all pairs (x, y) such that $x \equiv 7 \pmod{13}$ and $y \equiv 9 \pmod{13}$.

We now give a general result concerning certain systems of two congruences in two unknowns. (This result resembles Cramer's rule for solving systems of linear equations.)

Theorem 4.15. Let a, b, c, d, e, f, and m be integers, $m > 0$, such that $(\Delta, m) = 1$, where $\Delta = ad - bc$. Then the system of congruences

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

has a unique solution modulo m, given by

$$x \equiv \bar{\Delta}(de - bf) (\text{mod } m)$$
$$y \equiv \bar{\Delta}(af - ce) \ (\text{mod } m),$$

where $\bar{\Delta}$ is an inverse of Δ modulo m.

Proof. We multiply the first congruence of the system by d and the second by b, to obtain

$$adx + bdy \equiv de (\text{mod } m)$$
$$bcx + bdy \equiv bf \ (\text{mod } m).$$

Then we subtract the second congruence from the first, to find that

$$(ad - bc)x \equiv de - bf \ (\text{mod } m),$$

or, since $\Delta = ad - bc$,

$$\Delta x \equiv de - bf \ (\text{mod } m).$$

Next, we multiply both sides of this congruence by $\bar{\Delta}$, an inverse of Δ modulo m, to conclude that

$$x \equiv \bar{\Delta}(de - bf) \ (\text{mod } m).$$

In a similar way, we multiply the first congruence by c and the second by a, to obtain

$$acx + bcy \equiv ce \ (\text{mod } m)$$
$$acx + ady \equiv af \ (\text{mod } m).$$

We subtract the first congruence from the second, to find that

$$(ad - bc)y \equiv af - ce \ (\text{mod } m)$$

or

$$\Delta y \equiv af - ce \ (\text{mod } m).$$

Finally, we multiply both sides of this congruence by $\bar{\Delta}$ to see that

$$y \equiv \bar{\Delta}(af - ce) \ (\text{mod } m).$$

We have shown that if (x, y) is a solution of the system of congruences, then

$$x \equiv \bar{\Delta}(de - bf) \ (\text{mod } m), \quad y \equiv \bar{\Delta}(af - ce) \ (\text{mod } m).$$

We can easily check that any such pair (x, y) is a solution. When $x \equiv \bar{\Delta}(de - bf) \ (\text{mod } m)$ and $y \equiv \bar{\Delta}(af - ce) \ (\text{mod } m)$, we have

$$\begin{aligned} ax + by &\equiv a\bar{\Delta}(de - bf) + b\bar{\Delta}(af - ce) \\ &\equiv \bar{\Delta}(ade - abf - abf - bce) \\ &\equiv \bar{\Delta}(ad - bc)e \\ &\equiv \bar{\Delta}\Delta e \\ &\equiv e \pmod{m}, \end{aligned}$$

and

$$\begin{aligned} cx + dy &\equiv c\bar{\Delta}(de - bf) + d\bar{\Delta}(af - ce) \\ &\equiv \bar{\Delta}(cde - bcf + adf - cde) \\ &\equiv \bar{\Delta}(ad - bc)f \\ &\equiv \bar{\Delta}\Delta f \\ &\equiv f \pmod{m}. \end{aligned}$$

This establishes the theorem. ∎

By similar methods, we may solve systems of n congruences involving n unknowns. However, we will develop the theory of solving such systems, as well as larger systems, by methods taken from linear algebra. Readers unfamiliar with linear algebra may wish to skip the remainder of this section.

Systems of n linear congruences involving n unknowns will arise in our subsequent cryptographic studies. To study such systems when n is large, it is helpful to use the language of matrices. We will use some of the basic notions of matrix arithmetic, which are discussed in most linear algebra texts.

Before we proceed, we need to define congruences of matrices.

Definition. Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times k$ matrices with integer entries, with (i, j)th entries a_{ij} and b_{ij}, respectively. We say that $\mathbf{A}$ is *congruent to* $\mathbf{B}$ *modulo* m if $a_{ij} \equiv b_{ij} \pmod{m}$ for all pairs (i, j) with $1 \leq i \leq n$ and $1 \leq j \leq k$. We write $\mathbf{A} \equiv \mathbf{B} \pmod{m}$ if $\mathbf{A}$ is congruent to $\mathbf{B}$ modulo m.

The matrix congruence $\mathbf{A} \equiv \mathbf{B} \pmod{m}$ provides a succinct way of expressing the nk congruences $a_{ij} \equiv b_{ij} \pmod{m}$ for $1 \leq i \leq n$ and $1 \leq j \leq k$.

Example 4.24. We easily see that

$$\begin{pmatrix} 15 & 3 \\ 8 & 12 \end{pmatrix} \equiv \begin{pmatrix} 4 & 3 \\ -3 & 1 \end{pmatrix} \pmod{11}.$$

◀

The following proposition will be needed.

Theorem 4.16. If $\mathbf{A}$ and $\mathbf{B}$ are $n \times k$ matrices with $\mathbf{A} \equiv \mathbf{B} \pmod{m}$, $\mathbf{C}$ is a $k \times p$ matrix, and $\mathbf{D}$ is a $p \times n$ matrix, all with integer entries, then $\mathbf{AC} \equiv \mathbf{BC} \pmod{m}$ and $\mathbf{DA} \equiv \mathbf{DB} \pmod{m}$.

Proof. Let the entries of $\mathbf{A}$ and $\mathbf{B}$ be a_{ij} and b_{ij}, respectively, for $1 \le i \le n$ and $1 \le j \le k$, and let the entries of $\mathbf{C}$ be c_{ij} for $1 \le i \le k$ and $1 \le j \le p$. The (i, j)th entries of $\mathbf{AC}$ and $\mathbf{BC}$ are $\sum_{t=1}^{k} a_{it}c_{tj}$ and $\sum_{t=1}^{k} b_{it}c_{tj}$, respectively, for $1 \le i \le n$ and $1 \le j \le p$. Because $\mathbf{A} \equiv \mathbf{B} \pmod{m}$, we know that $a_{it} \equiv b_{it} \pmod{m}$ for all i and k. Hence, by Theorem 4.3, we see that $\sum_{t=1}^{k} a_{it}c_{tj} \equiv \sum_{t=1}^{k} b_{it}c_{tj} \pmod{m}$. Consequently, $\mathbf{AC} \equiv \mathbf{BC} \pmod{m}$.

The proof that $\mathbf{DA} \equiv \mathbf{DB} \pmod{m}$ is similar and is omitted. ∎

Now let us consider the system of congruences

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \pmod{m} \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &\equiv b_n \pmod{m}. \end{aligned}$$

Using matrix notation, we see that this system of n congruences is equivalent to the matrix congruence $\mathbf{AX} \equiv \mathbf{B} \pmod{m}$, where

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & & \ddots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad \mathbf{X} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Example 4.25. The system

$$\begin{aligned} 3x + 4y &\equiv 5 \pmod{13} \\ 2x + 5y &\equiv 7 \pmod{13} \end{aligned}$$

can be written as

$$\begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 7 \end{pmatrix} \pmod{13}.$$ ◀

We now develop a method for solving congruences of the form $\mathbf{AX} \equiv \mathbf{B} \pmod{m}$. This method is based on finding a matrix $\bar{\mathbf{A}}$ such that $\bar{\mathbf{A}}\mathbf{A} \equiv \mathbf{I} \pmod{m}$, where $\mathbf{I}$ is the identity matrix.

Definition. If $\mathbf{A}$ and $\bar{\mathbf{A}}$ are $n \times n$ matrices of integers and $\bar{\mathbf{A}}\mathbf{A} \equiv \mathbf{A}\bar{\mathbf{A}} \equiv \mathbf{I} \pmod{m}$, where $\mathbf{I} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & 1 \end{pmatrix}$ is the identity matrix of order n, then $\bar{\mathbf{A}}$ is said to be an *inverse of* $\mathbf{A}$ *modulo* m.

If $\bar{\mathbf{A}}$ is an inverse of $\mathbf{A}$ and $\mathbf{B} \equiv \bar{\mathbf{A}} \pmod{m}$, then $\mathbf{B}$ is also an inverse of $\mathbf{A}$. This follows from Theorem 4.16, because $\mathbf{BA} \equiv \bar{\mathbf{A}}\mathbf{A} \equiv \mathbf{I} \pmod{m}$. Conversely, if $\mathbf{B}_1$ and $\mathbf{B}_2$ are both inverses of $\mathbf{A}$, then $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod{m}$. To see this, using Theorem 4.16 and the congruence $\mathbf{B}_1\mathbf{A} \equiv \mathbf{B}_2\mathbf{A} \equiv \mathbf{I} \pmod{m}$, we have $\mathbf{B}_1\mathbf{A}\mathbf{B}_1 \equiv \mathbf{B}_2\mathbf{A}\mathbf{B}_1 \pmod{m}$. Because $\mathbf{A}\mathbf{B}_1 \equiv \mathbf{I} \pmod{m}$, we conclude that $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod{m}$.

Example 4.26. Given that

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 10 & 16 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5$$

and

$$\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 11 & 25 \\ 5 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 5,$$

we see that the matrix $\begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix}$ is an inverse of $\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$ modulo 5. ◀

The following proposition gives an easy method for finding inverses for 2×2 matrices.

Theorem 4.17. Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix of integers, such that $\Delta = \det \mathbf{A} = ad - bc$ is relatively prime to the positive integer m. Then, the matrix

$$\bar{\mathbf{A}} = \bar{\Delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

where $\bar{\Delta}$ is the inverse of Δ modulo m, is an inverse of $\mathbf{A}$ modulo m.

Proof. To verify that the matrix $\bar{\mathbf{A}}$ is an inverse of $\mathbf{A}$ modulo m, we need only verify that $\mathbf{A}\bar{\mathbf{A}} \equiv \bar{\mathbf{A}}\mathbf{A} \equiv \mathbf{I} \pmod m$.

To see this, note that

$$\begin{aligned} \mathbf{A}\bar{\mathbf{A}} &\equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}\bar{\Delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \equiv \bar{\Delta}\begin{pmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{pmatrix} \\ &\equiv \bar{\Delta}\begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} \equiv \begin{pmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I} \pmod m \end{aligned}$$

and

$$\begin{aligned} \bar{\mathbf{A}}\mathbf{A} &\equiv \bar{\Delta}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \bar{\Delta}\begin{pmatrix} ad-bc & 0 \\ 0 & -bc+ad \end{pmatrix} \\ &\equiv \bar{\Delta}\begin{pmatrix} \Delta & 0 \\ 0 & \Delta \end{pmatrix} \equiv \begin{pmatrix} \bar{\Delta}\Delta & 0 \\ 0 & \bar{\Delta}\Delta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I} \pmod m, \end{aligned}$$

where $\bar{\Delta}$ is an inverse of $\Delta \pmod m$, which exists because $(\Delta, m) = 1$. ■

Example 4.27. Let $\mathbf{A} = \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}$. Because 2 is an inverse of $\det \mathbf{A} = 7$ modulo 13, we have

$$\bar{\mathbf{A}} \equiv 2\begin{pmatrix} 5 & -4 \\ -2 & 3 \end{pmatrix} \equiv \begin{pmatrix} 10 & -8 \\ -4 & 6 \end{pmatrix} \equiv \begin{pmatrix} 10 & 5 \\ 9 & 6 \end{pmatrix} \pmod{13}.$$

◀

To provide a formula for an inverse of an $n \times n$ matrix, where n is a positive integer greater than 2, we need a result from linear algebra. It involves the notion of the adjoint of a matrix, which is defined as follows.

Definition. The *adjoint* of an $n \times n$ matrix $\mathbf{A}$ is the $n \times n$ matrix with (i, j)th entry C_{ji}, where C_{ij} is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the ith row and jth column from $\mathbf{A}$. The adjoint of $\mathbf{A}$ is denoted by adj $(\mathbf{A})$, or simply adj $\mathbf{A}$.

Theorem 4.18. If $\mathbf{A}$ is an $n \times n$ matrix with $\det \mathbf{A} \neq 0$, then $\mathbf{A}\,(\text{adj}\,\mathbf{A}) = (\det \mathbf{A})\mathbf{I}$, where adj $\mathbf{A}$ is the adjoint of $\mathbf{A}$.

Using this theorem, the following theorem follows readily.

Theorem 4.19. If $\mathbf{A}$ is an $n \times n$ matrix with integer entries and m is a positive integer such that $(\det \mathbf{A}, m) = 1$, then the matrix $\bar{\mathbf{A}} = \bar{\Delta}\,(\text{adj}\,\mathbf{A})$ is an inverse of $\mathbf{A}$ modulo m, where $\bar{\Delta}$ is an inverse of $\Delta = \det \mathbf{A}$ modulo m.

Proof. If $(\det \mathbf{A}, m) = 1$, then we know that $\det \mathbf{A} \neq 0$. Hence, by Theorem 4.18, we have

$$\mathbf{A}\,(\text{adj}\,\mathbf{A}) = (\det \mathbf{A})\mathbf{I} = \Delta\mathbf{I}.$$

Since $(\det \mathbf{A}, m) = 1$, there is an inverse $\bar{\Delta}$ of $\Delta = \det \mathbf{A}$ modulo m. Hence,

$$\mathbf{A}(\bar{\Delta}\,\text{adj}\,\mathbf{A}) \equiv \mathbf{A} \cdot (\text{adj}\,\mathbf{A})\bar{\Delta} \equiv \Delta\bar{\Delta}\mathbf{I} \equiv \mathbf{I} \pmod{m},$$

and

$$\bar{\Delta}\,(\text{adj}\,\mathbf{A})\mathbf{A} \equiv \bar{\Delta}\,((\text{adj}\,\mathbf{A})\mathbf{A}) \equiv \bar{\Delta}\Delta\mathbf{I} \equiv \mathbf{I} \pmod{m}.$$

This shows that $\bar{\mathbf{A}} = \bar{\Delta}\,(\text{adj}\,\mathbf{A})$ is an inverse of $\mathbf{A}$ modulo m. ∎

Example 4.28. Let $\mathbf{A} = \begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$. Then $\det \mathbf{A} = -5$. Furthermore, we have $(\det \mathbf{A}, 7) = 1$, and we see that 4 is an inverse of $\det \mathbf{A} = -5 \pmod 7$. Consequently, we find that

$$\bar{\mathbf{A}} = 4(\text{adj}\,\mathbf{A}) = 4\begin{pmatrix} -2 & -3 & 5 \\ -5 & 0 & 10 \\ 4 & 1 & -10 \end{pmatrix} = \begin{pmatrix} -8 & -12 & 20 \\ -20 & 0 & 40 \\ 16 & 4 & -40 \end{pmatrix} \equiv \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} \pmod 7.$$

◀

We can use an inverse of $\mathbf{A}$ modulo m to solve the system

$$\mathbf{AX} \equiv \mathbf{B} \pmod{m},$$

where $(\det \mathbf{A}, m) = 1$. By Theorem 4.16, when we multiply both sides of this congruence by an inverse $\bar{\mathbf{A}}$ of $\mathbf{A}$, we obtain

$$\bar{\mathbf{A}}(\mathbf{AX}) \equiv \bar{\mathbf{A}}\mathbf{B} \pmod{m}$$
$$(\bar{\mathbf{A}}\mathbf{A})\mathbf{X} \equiv \bar{\mathbf{A}}\mathbf{B} \pmod{m}$$
$$\mathbf{X} \equiv \bar{\mathbf{A}}\mathbf{B} \pmod{m}.$$

Hence, we find the solution $\mathbf{X}$ by forming $\bar{\mathbf{A}}\mathbf{B} \pmod{m}$.

Note that this method provides another proof of Theorem 4.15. To see this, let $\mathbf{AX} = \mathbf{B}$, where $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\mathbf{X} = \begin{pmatrix} x \\ y \end{pmatrix}$, and $\mathbf{B} = \begin{pmatrix} e \\ f \end{pmatrix}$. If $\Delta = \det \mathbf{A} = ad - bc$ is relatively prime to m, then

$$\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{X} \equiv \bar{\mathbf{A}}\mathbf{B} \equiv \bar{\Delta} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} e \\ f \end{pmatrix} = \bar{\Delta} \begin{pmatrix} de & -bf \\ af & -ce \end{pmatrix} \pmod{m}.$$

This demonstrates that (x, y) is a solution if and only if

$$x \equiv \bar{\Delta}(de - bf) \pmod{m}, \quad y \equiv \bar{\Delta}(af - ce) \pmod{m}.$$

Next, we give an example of the solution of a system of three congruences in three unknowns using matrices.

Example 4.29. We consider the system of three congruences

$$2x_1 + 5x_2 + 6x_3 \equiv 3 \pmod{7}$$
$$2x_1 + x_3 \equiv 4 \pmod{7}$$
$$x_1 + 2x_2 + 3x_3 \equiv 1 \pmod{7}.$$

This is equivalent to the matrix congruence

$$\begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} \pmod{7}.$$

We have previously shown that the matrix $\begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix}$ is an inverse of $\begin{pmatrix} 2 & 5 & 6 \\ 2 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ (mod 7). Hence, we have

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 32 \\ 8 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \pmod{7}.$$

◀

Before leaving this subject, we should mention that many methods for solving systems of linear equations may be adapted to solve systems of congruences. For instance, Gaussian elimination may be adapted to solve systems of congruences, where division is always replaced by multiplication by inverses modulo m. Also, there is a method for solving systems of congruences analogous to Cramer's rule. We leave the development of these methods as exercises for those readers familiar with linear algebra.

4.5 Exercises

1. Find the solutions of each of the following systems of linear congruences.
   a) $x + 2y \equiv 1 \pmod 5$
      $2x + y \equiv 1 \pmod 5$
   b) $x + 3y \equiv 1 \pmod 5$
      $3x + 4y \equiv 2 \pmod 5$
   c) $4x + y \equiv 2 \pmod 5$
      $2x + 3y \equiv 1 \pmod 5$

2. Find the solutions of each of the following systems of linear congruences.
   a) $2x + 3y \equiv 5 \pmod 7$
      $x + 5y \equiv 6 \pmod 7$
   b) $4x + y \equiv 5 \pmod 7$
      $x + 2y \equiv 4 \pmod 7$

* 3. What are the possibilities for the number of incongruent solutions of the system of linear congruences

$$ax + by \equiv c \pmod p$$
$$dx + ey \equiv f \pmod p,$$

where p is a prime and a, b, c, d, e, and f are positive integers?

4. Find the matrix $\mathbf{C}$ such that

$$\mathbf{C} \equiv \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 2 & 1 \end{pmatrix} \pmod 5$$

and all entries of $\mathbf{C}$ are nonnegative integers less than 5.

5. Use mathematical induction to prove that if $\mathbf{A}$ and $\mathbf{B}$ are $n \times n$ matrices with integer entries such that $\mathbf{A} \equiv \mathbf{B} \pmod m$, then $\mathbf{A}^k \equiv \mathbf{B}^k \pmod m$ for all positive integers k.

A matrix $\mathbf{A} \neq \mathbf{I}$ is called *involutory modulo m* if $\mathbf{A}^2 \equiv \mathbf{I} \pmod m$.

6. Show that $\begin{pmatrix} 4 & 11 \\ 1 & 22 \end{pmatrix}$ is involutory modulo 26.

7. Prove or disprove that if $\mathbf{A}$ is a 2×2 involutory matrix modulo m, then $\det \mathbf{A} \equiv \pm 1 \pmod m$.

8. Find an inverse modulo 5 of each of the following matrices.
   a) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ c) $\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$

9. Find an inverse modulo 7 of each of the following matrices.
   a) $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ b) $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{pmatrix}$ c) $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$

10. Using Exercise 9, find all the solutions of each of the following systems.

a) $x + y \equiv 1 \pmod 7$
$x + z \equiv 2 \pmod 7$
$y + z \equiv 3 \pmod 7$

b) $x + 2y + 3z \equiv 1 \pmod 7$
$x + 2y + 5z \equiv 1 \pmod 7$
$x + 4y + 6z \equiv 1 \pmod 7$

c) $x + y + z \equiv 1 \pmod 7$
$x + y + w \equiv 1 \pmod 7$
$x + z + w \equiv 1 \pmod 7$
$y + z + w \equiv 1 \pmod 7$

11. How many incongruent solutions does each of the following systems of congruences have?

a) $x + y + z \equiv 1 \pmod 5$
$2x + 4y + 3z \equiv 1 \pmod 5$

b) $2x + 3y + z \equiv 3 \pmod 5$
$x + 2y + 3z \equiv 1 \pmod 5$
$2x + z \equiv 1 \pmod 5$

c) $3x + y + 3z \equiv 1 \pmod 5$
$x + 2y + 4z \equiv 2 \pmod 5$
$4x + 3y + 2z \equiv 3 \pmod 5$

d) $2x + y + z \equiv 1 \pmod 5$
$x + 2y + z \equiv 1 \pmod 5$
$x + y + 2z \equiv 1 \pmod 5$

* **12.** Develop an analogue of Cramer's rule for solving systems of n linear congruences in n unknowns.

* **13.** Develop an analogue of Gaussian elimination to solve systems of n linear congruences in m unknowns (where m and n may differ).

A *magic square* is a square array of integers with the property that the sum of the integers in a row or in a column is always the same. In this exercise, we present a method for producing magic squares.

* **14.** Show that the n^2 integers $0, 1, \ldots, n^2 - 1$ are put into the n^2 positions of an $n \times n$ square, without putting two integers in the same position, if the integer k is placed in the ith row and jth column, where

$$i \equiv a + ck + e[k/n] \pmod n,$$
$$j \equiv b + dk + f[k/n] \pmod n,$$

$1 \le i \le n$, $1 \le j \le n$, and a, b, c, d, e, and f are integers with $(cf - de, n) = 1$.

* **15.** Show that a magic square is produced in Exercise 14 if $(c, n) = (d, n) = (e, n) = (f, n) = 1$.

* **16.** The *positive* and *negative diagonals* of an $n \times n$ square consist of the integers in positions (i, j), where $i + j \equiv k \pmod n$ and $i - j \equiv k \pmod n$, respectively, where k is a given integer. A square is called *diabolic* if the sum of the integers in a positive or negative diagonal is always the same. Show that a diabolic square is produced using the procedure given in Exercise 14 if $(c + d, n) = (c - d, n) = (e + f, n) = (e - f, n) = 1$.

4.5 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. Produce 4×4, 5×5, and 6×6 magic squares.

Programming Projects

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

1. Find the solutions of a system of two linear congruences in two unknowns using Theorem 4.15.
2. Find inverses of 2×2 matrices using Theorem 4.17.
3. Find inverses of $n \times n$ matrices using Theorem 4.19.
4. Solve systems of n linear congruences in n unknowns using inverses of matrices.
5. Solve systems of n linear congruences in n unknowns using an analogue of Cramer's rule (see Exercise 12).
6. Solve systems of n linear congruences in m unknowns using an analogue of Gaussian elimination (see Exercise 13).
7. Given a positive integer, produce an $n \times n$ magic square by the method given in Exercise 14.

4.6 Factoring Using the Pollard Rho Method

In this section, we will describe a factorization method based on congruences that was developed in 1974 by J. M. Pollard. Pollard called this technique the *Monte Carlo method* because it relies on generating integers that behave as though they were randomly chosen; it is now commonly known as the *Pollard rho method,* for reasons which will be explained.

Suppose that n is a large composite integer and that p is its smallest prime divisor. Our goal is to choose integers $x_0, x_1, \ldots, x_s$ so that these integers have distinct least nonnegative residues modulo n, but where their least nonnegative residues modulo p are not all distinct. As can be seen using probabilistic arguments (see [Ri94]), this is likely to be the case when s is large compared to $\sqrt{p}$ but small when compared to $\sqrt{n}$, and the numbers are chosen randomly.

Once we have found integers x_i and x_j, $0 \leq i < j \leq s$, such that $x_i \equiv x_j \pmod{p}$ but $x_i \not\equiv x_j \pmod{n}$, it follows that $(x_i - x_j, n)$ is a nontrivial divisor of n, as p divides $x_i - x_j$, but n does not. The number $(x_i - x_j, n)$ can be found quickly using the Euclidean algorithm. However, to find $(x_i - x_j, n)$ for each pair (i, j) with $0 \leq i < j \leq s$ requires that we find $O(s^2)$ greatest common divisors. We will show how to reduce the number of times we must use the Euclidean algorithm.

To find such integers x_i and x_j, we use the following procedure: We start with a seed value x_0 that is chosen randomly and a polynomial function $f(x)$ with integer coefficients of degree greater than 1. We compute the terms x_k, $k = 1, 2, 3, \ldots$, using the recursive definition

$$x_{k+1} \equiv f(x_k) \pmod{n}, \quad 0 \leq x_{k+1} < n.$$

The polynomial $f(x)$ should be chosen so that the probability is high that a suitably large number of integers x_i are generated before they repeat. Empirical evidence indicates that the polynomial $f(x) = x^2 + 1$ performs well for this test. The following example illustrates how this sequence is generated.

Example 4.30. Let $n = 8051$, and suppose that $x_0 = 2$ and $f(x) = x^2 + 1$. We find that $x_1 = 5$, $x_2 = 26$, $x_3 = 677$, $x_4 = 7474$, $x_5 = 2839$, $x_6 = 871$, and so on. ◀

Now, note that by the recursive definition of x_k, it follows that if

$$x_i \equiv x_j \pmod{d},$$

where d is a positive integer, then

$$x_{i+1} \equiv f(x_i) \equiv f(x_j) \equiv x_{j+1} \pmod{d}.$$

It follows that if $x_i \equiv x_j \pmod{d}$, then the sequence x_k becomes periodic modulo d with a period dividing $j - i$. That is, $x_q \equiv x_r \pmod{d}$ whenever $q \equiv r \pmod{j - i}$, and $q \geq i$ and $r \geq i$. It follows that if s is the smallest multiple of $j - i$ that is at least as large as i, then $x_s \equiv x_{2s} \pmod{d}$.

It follows further that to look for a factor of n, we find the greatest common divisor of $x_{2k} - x_k$ and n for $k = 1, 2, 3, \ldots$. We have found a factor of n when we have found a value k for which $1 < (x_{2k} - x_k, n) < n$. From our observations, we see that it is likely that we will find such an integer k with k close to $\sqrt{p}$.

In practice, when the Pollard rho method is used, the polynomial $f(x) = x^2 + 1$ is often chosen to generate the sequence of integers $x_0, x_1, x_2, \ldots, x_k, \ldots$. Furthermore, the seed $x_0 = 2$ is often used. This choice of polynomial and seed produces a sequence that behaves much like a random sequence for the purposes of this factorization method.

Example 4.31. We use the Pollard rho method with seed $x_0 = 2$ and generator polynomial $f(x) = x^2 + 1$ to find a nontrivial factor of $n = 8051$. We find that $x_1 = 5$, $x_2 = 26$, $x_3 = 677$, $x_4 = 7474$, $x_5 = 2839$, $x_6 = 871$. Using the Euclidean algorithm, it follows that $(x_2 - x_1, 8051) = (26 - 5, 8051) = (21, 8051) = 1$ and $(x_4 - x_2, 8051) = (7474 - 26, 8051) = (7448, 8051) = 1$. However, we find a nontrivial factor of 8051 at the next step, as $(x_6 - x_3, 8051) = (871 - 677, 8051) = (194, 8051) = 97$. We see that 97 is a factor of 8051. ◀

To see why this method is called the Pollard rho method, look at Figure 4.1 on the next page. This figure shows the periodic behavior of the sequence x_i, where $x_0 = 2$

and $x_i + 1 = x_i^2 + 1 \pmod{97}$, $i \geq 1$. The part of this sequence that occurs before the periodicity is the tail of the rho, and the loop is the periodic part.

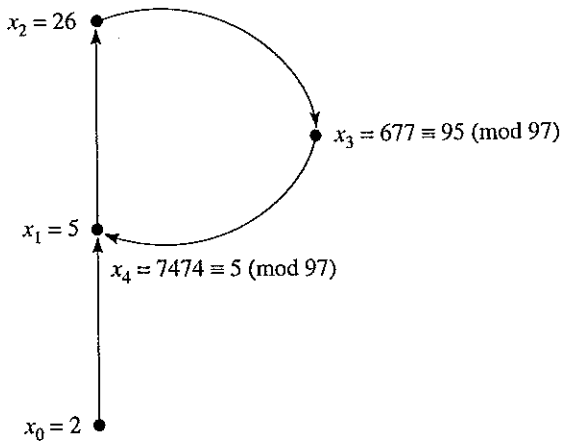


Figure 4.1 *The Pollard rho method.*

The Pollard rho method has proved to be practical for the factorization of integers with moderately large prime factors. In practice, the first attempt to factor a large integer is to do trial division by small primes, say by all primes less than 10,000. Next, the Pollard rho method is used to look for prime factors of intermediate size (up to 10^{15}, for instance). Only after trial division by small primes and the Pollard rho method have failed are the really big guns brought in, such as the quadratic sieve or the elliptic curve method.

4.6 Exercises

1. Use the Pollard rho method with $x_0 = 2$ and $f(x) = x^2 + 1$ to find the prime factorization of each of the following integers.

   a) 133 c) 1927 e) 36,287
   b) 1189 d) 8131 f) 48,227

2. Use the Pollard rho method to factor the integer 1387, with the following seeds and generating polynomials.
   a) $x_0 = 2$, $f(x) = x^2 + 1$
   b) $x_0 = 3$, $f(x) = x^2 + 1$
   c) $x_0 = 2$, $f(x) = x^2 - 1$
   d) $x_0 = 2$, $f(x) = x^3 + x + 1$

* 3. Explain why the choice of $f(x)$ as a linear polynomial, that is, a function of the form $f(x) = ax + b$, where a and b are integers, is a poor choice.

4.6 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. Use the Pollard rho method to factor ten different integers that have between 15 and 20 decimal digits.
2. Use the Pollard rho method to factor a large number of integers that are close to 100,000, keeping track of the number of steps required. Can you make any conjectures based on your data?
3. Factor $2^{58} + 1$ using the Pollard rho method.

Programming Projects

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

1. Given a positive integer n, find a prime factor of this integer using the Pollard rho method.

5 Applications of Congruences

Introduction

Congruences have diverse applications. We have already seen some examples of this, such as in Section 4.3, where we saw how large integers can be multiplied on a computer using congruences. This chapter covers a wide variety of interesting applications of congruences. First, we will show how congruences can be used to develop divisibility tests, such as the simple tests you may already know for checking whether an integer is divisible by 3 or by 9. Next, we will develop a congruence that determines the day of the week for any date in history. Then, we will show how congruences can be used to schedule round-robin tournaments. We will discuss some applications of congruences in computer science; for example, we will show how congruences are used in hashing functions, which themselves have many applications, such as determining computer memory locations where data is stored. Finally, we will show how congruences can be used to construct check digits, which are used to determine whether an identification number has been copied in error.

In subsequent chapters, we will discuss additional applications of congruences. For example, in Chapter 8, we will show how congruences can be used in different ways to make messages secret, and in Chapter 10, we will show how congruences can be used to generate pseudorandom numbers.

5.1 Divisibility Tests

You may have learned in primary school that to check whether an integer is divisible by 3, you need only check whether the sum of its digits is divisible by 3. This is an example of a divisibility test that uses the digits of an integer to check whether it is divisible by a particular divisor, without actually dividing the integer by that possible divisor. In this section, we will develop the theory behind such tests. In particular, we will use

congruences to develop divisibility tests for integers based on their base b expansions, where b is a positive integer. Taking $b = 10$ will give us the well-known tests for checking integers for divisibility by 2, 3, 4, 5, 7, 9, 11, and 13. Although you may have learned these divisibility tests a long time ago, you will learn why they work here.

Divisibility by Powers of 2 First, we develop tests for divisibility by powers of 2. Let $n = 32{,}688{,}048$. It is easy to see that n is divisible by 2 since its last digit is even. Consider the following questions. Does $2^2 = 4$ divide n? Does $2^3 = 8$ divide n? Does $2^4 = 16$ divide n? What is the highest power of 2 that divides n? We will develop a test that does not require that we actually divide n by 4, 8, and successive powers of 2, which answers these questions.

In the following discussion let $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$. Then $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$, with $0 \leq a_j \leq 9$ for $j = 0, 1, 2, \ldots, k$.

Because $10 \equiv 0 \pmod 2$, it follows that $10^j \equiv 0 \pmod{2^j}$ for all positive integers j. Hence,

$$\begin{aligned} n &\equiv (a_0)_{10} \pmod 2, \\ n &\equiv (a_1 a_0)_{10} \pmod{2^2}, \\ n &\equiv (a_2 a_1 a_0)_{10} \pmod{2^3}, \\ &\vdots \\ n &\equiv (a_{k-1} a_{k-2} \ldots a_2 a_1 a_0)_{10} \pmod{2^k}. \end{aligned}$$

These congruences tell us that to determine whether an integer n is divisible by 2, we only need to examine its last digit for divisibility by 2. Similarly, to determine whether n is divisible by 4, we only need to check the integer made up of the last two digits of n for divisibility by 4. In general, to test n for divisibility by 2^j, we only need to check the integer made up of the last j digits of n for divisibility by 2^j.

Example 5.1. Let $n = 32{,}688{,}048$. We see that $2 \mid n$ because $2 \mid 8$, $4 \mid n$ because $4 \mid 48$, $8 \mid n$ because $8 \mid 48$, $16 \mid n$ because $16 \mid 8048$, but $32 \nmid n$ since $32 \nmid 88{,}048$. ◀

Divisibility by Powers of 5 Next, we develop divisibility tests for powers of 5.

To develop tests for divisibility by powers of 5, first note that because $10 \equiv 0 \pmod 5$, we have $10^j \equiv 0 \pmod{5^j}$. Hence, divisibility tests for powers of 5 are analogous to those for powers of 2. We only need to check the integer made up of the last j digits of n to determine whether n is divisible by 5^j.

Example 5.2. Let $n = 15{,}535{,}375$. Because $5 \mid 5$, $5 \mid n$, because $25 \mid 75$, $25 \mid n$, because $125 \mid 375$, $125 \mid n$, but because $625 \nmid 5375$, $625 \nmid n$. ◀

Divisibility by 3 and 9 Next, we develop tests for divisibility by 3 and by 9.

Note that both the congruences $10 \equiv 1 \pmod 3$ and $10 \equiv 1 \pmod 9$ hold. Hence, $10^k \equiv 1 \pmod 3$ and $10^k \equiv 1 \pmod 9$. This gives us the useful congruences

$$\begin{aligned}(a_k a_{k-1} \cdots a_1 a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3 \text{ and } \pmod 9.\end{aligned}$$

Hence, we only need to check whether the sum of the digits of n is divisible by 3, or by 9, to see whether n is divisible by 3, or by 9, respectively.

Example 5.3. Let $n = 4{,}127{,}835$. Then, the sum of the digits of n is $4 + 1 + 2 + 7 + 8 + 3 + 5 = 30$. Because $3 \mid 30$ but $9 \nmid 30$, $3 \mid n$ but $9 \nmid n$. ◀

Divisibility by 11 A rather simple test can be found for divisibility by 11.

Because $10 \equiv -1 \pmod{11}$, we have

$$\begin{aligned}(a_k a_{k-1} \ldots a_1 a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + \cdots - a_1 + a_0 \pmod{11}.\end{aligned}$$

This shows that $(a_k a_{k-1} \ldots a_1 a_0)_{10}$ is divisible by 11 if and only if $a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$, the integer formed by alternately adding and subtracting the digits, is divisible by 11.

Example 5.4. We see that 723,160,823 is divisible by 11, because alternately adding and subtracting its digits yields $3 - 2 + 8 - 0 + 6 - 1 + 3 - 2 + 7 = 22$, which is divisible by 11. On the other hand, 33,678,924 is not divisible by 11, because $4 - 2 + 9 - 8 + 7 - 6 + 3 - 3 = 4$ is not divisible by 11. ◀

Divisibility by 7, 11, and 13 Next, we develop a test to simultaneously check for divisibility by the primes 7, 11, and 13.

Note that $7 \cdot 11 \cdot 13 = 1001$ and $10^3 = 1000 \equiv -1 \pmod{1001}$. Hence,

$$\begin{aligned}(a_k a_{k-1} \ldots a_0)_{10} &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv (a_0 + 10a_1 + 100a_2) + 1000(a_3 + 10a_4 + 100a_5) \\ &\quad + (1000)^2 (a_6 + 10a_7 + 100a_8) + \cdots \\ &\equiv (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) \\ &\quad + (100a_8 + 10a_7 + a_6) - \cdots \\ &= (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} - \cdots \pmod{1001}.\end{aligned}$$

This congruence tells us that an integer is congruent modulo 1001 to the integer formed by successively adding and subtracting the three-digit integers with decimal expansions formed from successive blocks of three decimal digits of the original number, where digits are grouped starting with the rightmost digit. As a consequence, because 7, 11, and 13 are divisors of 1001, to determine whether an integer is divisible by 7, 11, or 13, we only need to check whether this alternating sum and difference of blocks of three digits is divisible by 7, 11, or 13.

Example 5.5. Let $n = 59{,}358{,}208$. Because the alternating sum and difference of the integers formed from blocks of three digits, $208 - 358 + 59 = -91$, is divisible by 7 and 13, but not by 11, we see that n is divisible by 7 and 13, but not by 11. ◀

Divisibility Tests Using Base b Representations All of the divisibility tests we have developed thus far are based on decimal representations. We now develop divisibility tests using base b representations, where b is a positive integer.

Theorem 5.1. If $d \mid b$ and j and k are positive integers with $j < k$, then $(a_k \cdots a_1 a_0)_b$ is divisible by d^j if and only if $(a_{j-1} \cdots a_1 a_0)_b$ is divisible by d^j.

Proof. Because $b \equiv 0 \pmod{d}$, it follows that $b^j \equiv 0 \pmod{d^j}$. Hence,

$$\begin{aligned}(a_k a_{k-1} \cdots a_1 a_0)_b &= a_k b^k + \cdots + a_j b^j + a_{j-1} b^{j-1} + \cdots + a_1 b + a_0 \\ &\equiv a_{j-1} b^{j-1} + \cdots + a_1 b + a_0 \\ &= (a_{j-1} \cdots a_1 a_0)_b \pmod{d^j}.\end{aligned}$$

Consequently, $d^j \mid (a_k a_{k-1} \cdots a_1 a_0)_b$ if and only if $d^j \mid (a_{j-1} \cdots a_1 a_0)_b$. ■

Theorem 5.1 extends to other bases the divisibility tests of integers expressed in decimal notation by powers of 2 and by powers of 5.

Theorem 5.2. If $d \mid (b-1)$, then $n = (a_k \ldots a_1 a_0)_b$ is divisible by d if and only if the sum of digits $a_k + \cdots + a_1 + a_0$ is divisible by d.

Proof. Because $d \mid (b-1)$, we have $b \equiv 1 \pmod{d}$, so that by Theorem 4.7 we have $b^j \equiv 1 \pmod{d}$ for all positive integers j. Hence, $n = (a_k \ldots a_1 a_0)_b = a_k b^k + \cdots + a_1 b + a_0 \equiv a_k + \cdots + a_1 + a_0 \pmod{d}$. This shows that $d \mid n$ if and only if $d \mid (a_k + \cdots + a_1 + a_0)$. ■

Theorem 5.2 extends to other bases the tests for divisibility of integers expressed in decimal notation by 3 and by 9.

Theorem 5.3. If $d \mid (b+1)$, then $n = (a_k \ldots a_1 a_0)_b$ is divisible by d if and only if the alternating sum of digits $(-1)^k a_k + \cdots - a_1 + a_0$ is divisible by d.

Proof. Because $d \mid (b+1)$, we have $b \equiv -1 \pmod{d}$. Hence, $b^j \equiv (-1)^j \pmod{d}$, and consequently, $n = (a_k \ldots a_1 a_0)_b \equiv (-1)^k a_k + \cdots - a_1 + a_0 \pmod{d}$. Hence, $d \mid n$ if and only if $d \mid ((-1)^k a_k + \cdots - a_1 + a_0)$. ■

Theorem 5.3 extends to other bases the test for divisibility by 11 of integers expressed in decimal notation.

Example 5.6. Let $n = (7F28A6)_{16}$ (in hex notation). Then, because $2 \mid 16$, from Theorem 5.1 we know that $2 \mid n$, because $2 \mid 6$. Likewise, because $4 \mid 16$, we see that $4 \nmid n$, because $4 \nmid 6$. By Theorem 5.2, because $3 \mid (16 - 1)$, $5 \mid (16 - 1)$, and $15 \mid (16 - 1)$, and $7 + F + 2 + 8 + A + 6 = (30)_{16}$, we know that $3 \mid n$, since $3 \mid (30)_{16}$, whereas $5 \nmid n$ and $15 \nmid n$, because $5 \nmid (30)_{16}$ and $15 \nmid (30)_{16}$. Furthermore, by Theorem 5.3, because $17 \mid (16 + 1)$ and $n \equiv 6 - A + 8 - 2 + F - 7 = (A)_{16} \pmod{17}$, we conclude that $17 \nmid n$, because $17 \nmid (A)_{16}$. ◀

Example 5.7. Let $n = (1001001111)_2$. Then, using Theorem 5.3 we see that $3 \mid n$, because $n \equiv 1 - 1 + 1 - 1 + 0 - 0 + 1 - 0 + 0 - 1 \equiv 0 \pmod{3}$ and $3 \mid (2 + 1)$. ◀

5.1 Exercises

1. Determine the highest power of 2 that divides each of the following positive integers.

   a) 201,984 c) 89,375,744
   b) 1,423,408 d) 41,578,912,246

2. Determine the highest power of 5 that divides each of the following positive integers.

   a) 112,250 c) 235,555,790
   b) 4,860,625 d) 48,126,953,125

3. Which of the following integers are divisible by 3? Of those that are, which are divisible by 9?

   a) 18,381 c) 987,654,321
   b) 65,412,351 d) 78,918,239,735

4. Which of the following integers are divisible by 11?

   a) 10,763,732 c) 674,310,976,375
   b) 1,086,320,015 d) 8,924,310,064,537

5. Find the highest power of 2 that divides each of the following integers.

   a) $(101111110)_2$ c) $(111000000)_2$
   b) $(1010000011)_2$ d) $(1011011101)_2$

6. Determine which of the integers in Exercise 5 are divisible by 3.

7. Which of the following integers are divisible by 2?

   a) $(1210122)_3$ c) $(1112201112)_3$
   b) $(211102101)_3$ d) $(10122222011101)_3$

8. Which of the integers in Exercise 7 are divisible by 4?

9. Which of the following integers are divisible by 3, and which are divisible by 5?

a) $(3EA235)_{16}$ c) $(F117921173)_{16}$
b) $(ABCDEF)_{16}$ d) $(10AB987301F)_{16}$

10. Which of the integers in Exercise 9 are divisible by 17?

A *repunit* is an integer with decimal expansion containing all 1s.

11. Determine which repunits are divisible by 3, and which are divisible by 9.

12. Determine which repunits are divisible by 11.

13. Determine which repunits are divisible by 1001. Which are divisible by 7? by 13?

14. Determine which repunits with fewer than 10 digits are prime.

A *base b repunit* is an integer with base b expansion containing all 1s.

15. Determine which base b repunits are divisible by factors of $b - 1$.

16. Determine which base b repunits are divisible by factors of $b + 1$.

A *base b palindromic integer* is an integer whose base b representation reads the same forward and backward.

17. Show that every decimal palindromic integer with an even number of digits is divisible by 11.

18. Show that every base 7 palindromic integer with an even number of digits is divisible by 8.

19. Develop a test for divisibility by 37, based on the fact that $10^3 \equiv 1 \pmod{37}$. Use this to check 443,692 and 11,092,785 for divisibility by 37.

20. Devise a test for integers represented in base b notation to check for divisibility by n, where n is a divisor of $b^2 + 1$. (*Hint:* Split the digits of the base b representation of the integer into blocks of two, starting on the right.)

21. Use the test that you developed in Exercise 20 to decide whether

a) $(101110110)_2$ is divisible by 5.
b) $(12100122)_3$ is divisible by 2, and whether it is divisible by 5.
c) $(364701244)_8$ is divisible by 5, and whether it is divisible by 13.
d) $(5837041320219)_{10}$ is divisible by 101.

22. An old receipt has faded. It reads 88 chickens at a total of $\$x4.2y$, where x and y are unreadable digits. How much did each chicken cost?

23. Use a congruence modulo 9 to find the missing digit, indicated by a question mark: $89{,}878 \cdot 58{,}965 = 5299\,?\,56270$.

We can check a multiplication $c = ab$ by determining whether the congruence $c \equiv ab \pmod{m}$ is valid, where m is any modulus. If we find that c is not congruent to ab modulo m, then we know that an error has been made. When we take $m = 9$ and use the fact that an integer in decimal notation is congruent modulo 9 to the sum of its digits, this check is called *casting out nines.*

24. Check each of the following multiplications by casting out nines.

a) $875{,}961 \cdot 2753 = 2{,}410{,}520{,}633$
b) $14{,}789 \cdot 23{,}567 = 348{,}532{,}367$
c) $24{,}789 \cdot 43{,}717 = 1{,}092{,}700{,}713$

25. Is a check of a multiplication by casting out nines foolproof?

26. What combinations of digits of a decimal expansion of an integer are congruent to this integer modulo 99? Use your answer to devise a check for multiplication based on *casting out ninety-nines*. Then use the test to check the multiplications in Exercise 24.

5.1 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. Determine whether the repunit with n digits is prime, where n is a positive integer not exceeding 30. Can you go further?

Programming Projects

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

1. Given a positive integer n, determine the highest powers of 2 and of 5 that divide n.
2. Given a positive integer n, test n for divisibility by 3, 7, 9, 11, and 13. (Use congruences modulo 1001 for divisibility by 7 and 13.)
3. Given a positive integer n, determine the highest power of each factor of b that divides an integer from the base b expansion of n.
4. Test a positive integer n, from its base b expansion, for divisibility by factors of $b - 1$ and of $b + 1$.

5.2 The Perpetual Calendar

In this section, we derive a formula that gives us the day of the week of any day of any year. Because the days of the week form a cycle of length seven, we use a congruence modulo 7. We denote each day of the week by a number in the set 0, 1, 2, 3, 4, 5, 6, setting

- *Sunday* $= 0$,
- *Monday* $= 1$,
- *Tuesday* $= 2$,
- *Wednesday* $= 3$,
- *Thursday* $= 4$,
- *Friday* $= 5$,
- *Saturday* $= 6$.

Julius Caesar changed the Egyptian calendar, which was based on a year of exactly 365 days, to a new calendar, called the *Julian calendar,* with a year of average length 365 1/4 days, with leap years every fourth year, to better reflect the true length of the year. However, more recent calculations have shown that the true length of the year is approximately 365.2422 days. As the centuries passed, the discrepancies of 0.0078 days per year added up, so that by the year 1582 approximately 10 extra days had been added unnecessarily in leap years. To remedy this, in 1582 Pope Gregory set up a new calendar. First, 10 days were added to the date, so that October 5, 1582, became October 15, 1582 (and the 6th through the 14th of October were skipped). It was decided that leap years would be precisely the years divisible by 4, except that those exactly divisible by 100, the years that mark centuries, would be leap years only when divisible by 400. As an example, the years 1700, 1800, 1900, and 2100 are not leap years but 1600 and 2000 are. With this arrangement, the average length of a calendar year became 365.2425 days, rather close to the true year of 365.2422 days. An error of 0.0003 days per year remains, which is 3 days per 10,000 years. In the future, this discrepancy will have to be accounted for, and various possibilities have been suggested to correct for this error.

In dealing with calendar dates for various parts of the world, we must also take into account the fact that the Gregorian calendar was not adopted everywhere in 1582. In Britain and what is now the United States, the Gregorian calendar was adopted only in 1752, and by then it was necessary to add 11 days. In these places September 3, 1752, in the Julian calendar became September 14, 1752, in the Gregorian calendar. Japan changed over in 1873, Russia and nearby countries in 1917, while Greece held out until 1923.

We now set up our procedure for finding the day of the week for a given date in the Gregorian calendar. We first must make some adjustments, because the extra day in a leap year comes at the end of February. We take care of this by renumbering the months, starting each year in March, and considering the months of January and February part of the preceding year. For instance, February 2000 is considered the twelfth month of 1999, and May 2000 is considered the third month of 2000. With this convention, for the day of interest, let

- k = day of the month,
- m = month,
  with

January = 11	*July* = 5
February = 12	*August* = 6
March = 1	*September* = 7
April = 2	*October* = 8
May = 3	*November* = 9
June = 4	*December* = 10

- N =year,
  where N is the current year unless the month is January or February in which case N is the previous year, and where $N = 100C + Y$, where

- C =century,
- Y =particular year of the century.

Example 5.8. For the date April 3, 1951, we have $k = 3$, $m = 2$, $N = 1951$, $C = 19$, and $Y = 51$. But note that for February 28, 1951, we have $k = 28$, $m = 12$, $N = 1950$, $C = 19$, and $Y = 50$, because, for our calculations, we consider February to be the twelfth month of the previous year. ◀

We use March 1 of each year as our basis. Let d_N represent the day of the week of March 1 in year N. We start with the year 1600, and compute the day of the week March 1 falls on in any given year. Note that between March 1 of year $N-1$ and March 1 of year N, if year N is not a leap year, 365 days have passed; and because $365 \equiv 1 \pmod 7$, we see that $d_N \equiv d_{N-1} + 1 \pmod 7$, whereas if year N is a leap year, because there is an extra day between the consecutive firsts of March, we see that

$$d_N \equiv d_{N-1} + 2 \pmod 7.$$

Hence, to find d_N from d_{1600}, we must first find out how many leap years have occurred between the year 1600 and the year N (not including 1600, but including N); let us call this number x. To compute x, first note that by the division algorithm there are $[(N-1600)/4]$ years divisible by 4 between 1600 and N, there are $[(N-1600)/100]$ years divisible by 100 between 1600 and N, and there are $[(N-1600)/400]$ years divisible by 400 between 1600 and N. Hence,

$$\begin{aligned} x &= [(N-1600)/4] - [(N-1600)/100] + [(N-1600)/400] \\ &= [N/4] - 400 - [N/100] + 16 + [N/400] - 4 \\ &= [N/4] - [N/100] + [N/400] - 388. \end{aligned}$$

(We have used the identity from Example 1.34 to simplify this expression.) Putting this in terms of C and Y, we see that

$$\begin{aligned} x &= [25C + (Y/4)] - [C + (Y/100)] + [(C/4) + (Y/400)] - 388 \\ &= 25C + [Y/4] - C + [C/4] - 388 \\ &\equiv 3C + [C/4] + [Y/4] - 3 \pmod 7. \end{aligned}$$

Here we have again used the identity from Example 1.4, the inequality $Y/100 < 1$, and the equation $[(C/4) + (Y/400)] = [C/4]$ (which follows from Exercise 19 of Section 1.5, because $Y/400 < 1/4$).

We can now compute d_N from d_{1600} by shifting d_{1600} by one day for every year that has passed, plus an extra day for each leap year between 1600 and N. This gives the following formula:

$$\begin{aligned} d_N &\equiv d_{1600} + N - 1600 + x \\ &= d_{1600} + 100C + Y - 1600 + 3C + [C/4] + [Y/4] - 3 \pmod 7. \end{aligned}$$

Simplifying, we have

$$d_N \equiv d_{1600} - 2C + Y + [C/4] + [Y/4] \pmod 7.$$

Now that we have a formula relating the day of the week for March 1 of any year to the day of the week of March 1, 1600, we can use the fact that March 1, 1982, is a Monday to find the day of the week of March 1, 1600. For 1982, because $N = 1982$, we have $C = 19$, and $Y = 82$, and since $d_{1982} = 1$, it follows that

$$1 \equiv d_{1600} - 38 + 82 + [19/4] + [82/4] \equiv d_{1600} - 2 \pmod 7.$$

Hence, $d_{1600} = 3$, so that March 1, 1600, was a Wednesday. When we insert the value of d_{1600}, the formula for d_N becomes

$$d_N \equiv 3 - 2C + Y + [C/4] + [Y/4] \pmod 7.$$

We now use this formula to compute the day of the week of the first day of each month of year N. To do this, we have to use the number of days of the week that the first of the month of a particular month is shifted from the first of the month of the preceding month. The months with 30 days shift the first of the following month up 2 days, because $30 \equiv 2 \pmod 7$, and those with 31 days shift the first of the following month up 3 days, because $31 \equiv 3 \pmod 7$. Therefore, we must add the following amounts:

from March 1 to April 1:	3 days
from April 1 to May 1:	2 days
from May 1 to June 1:	3 days
from June 1 to July 1:	2 days
from July 1 to August 1:	3 days
from August 1 to September 1:	3 days
from September 1 to October 1:	2 days
from October 1 to November 1:	3 days
from November 1 to December 1:	2 days
from December 1 to January 1:	3 days
from January 1 to February 1:	3 days.

We need a formula that gives us the same increments. Notice that we have 11 increments totaling 29 days, so that each increment averages 2.6 days. By inspection, we find that the function $[2.6m - 0.2] - 2$ has exactly the same increments as m goes from 2 to 12, and is zero when $m = 1$. (This formula was originally found by Christian Zeller;[1] he apparently found it by trial and error.) Hence, the day of the week of the first day of month m of year N is given by the least nonnegative residue of $d_N + [2.6m - 0.2] - 2$ modulo 7.

To find W, the day of the week of day k of month m of year N, we simply add $k - 1$ to the formula we have devised for the day of the week of the first day of the same month.

[1] Christian Julius Johannes Zeller (1849–1899) was born in Muhlhausen on the Neckar in Germany. He became a priest at Schokingen after completing his theological studies. He served as the principal of a women's college at Markgroningen from 1847 until 1898. He published his formula for the day of the week of a date in 1882.

We obtain the formula:

$$W \equiv k + [2.6m - 0.2] - 2C + Y + [Y/4] + [C/4] \pmod 7.$$

We can use this formula to find the day of the week of any date of any year in the Gregorian calendar.

Example 5.9. To find the day of the week of January 1, 1900, we have $C = 18$, $Y = 99$, $m = 11$, and $k = 1$ (because we consider January as the eleventh month of the preceding year). Hence, we have $W \equiv 1 + 28 - 36 + 99 + 24 + 4 \equiv 1 \pmod 7$, so that January 1, 1900, was a Monday. ◀

5.2 Exercises

1. Find the day of the week of the day you were born, and of your birthday this year.
2. Find the day of the week of the following important dates in U. S. history (use the Julian calendar before September 3, 1752, and the Gregorian calendar from September 14, 1752, to the present)

* a)	October 12, 1492	(Columbus sights land in the Caribbean)
* b)	May 6, 1692	(Peter Minuit buys Manhattan from the natives)
* c)	June 15, 1752	(Benjamin Franklin invents the lightning rod)
d)	July 4, 1776	(U. S. Declaration of Independence)
e)	March 30, 1867	(U. S. buys Alaska from Russia)
f)	March 17, 1888	(Great blizzard in the Eastern U. S.)
g)	February 15, 1898	(U. S. Battleship *Maine* blown up in Havana Harbor)
h)	July 2, 1925	(Scopes convicted of teaching evolution)
i)	July 16, 1945	(First atomic bomb exploded)
j)	July 20, 1969	(First man on the moon)
k)	August 9, 1974	(President Nixon resigns)
l)	March 28, 1979	(Three Mile Island nuclear accident)
m)	January 1, 1984	("Ma Bell" breakup)
n)	December 25, 1991	(Demise of the U.S.S.R.)
o)	June 5, 2027	(First man on Mars)

3. How many times will the 13th of the month fall on a Friday in the year 2020?
4. How many leap years will there be from the year 1 until the year 10,000, inclusive?
5. To correct the small discrepancy between the number of days in a year of the Gregorian calendar and an actual year, it has been suggested that the years exactly divisible by 4000 should not be leap years. Adjust the formula for the day of the week of a given date to take this correction into account.
6. Show that days with the same calendar date in two different years of the same century, 28, 56, or 84 years apart, fall on the identical day of the week.
7. Which of your birthdays, until your one hundredth, fall on the same day of the week as the day you were born?

8. What is the next term in the sequence 1995, 1997, 1998, 1999, 2001, 2002, 2003?
9. What is the next term in the sequence 1700, 1800, 1900, 2100, 2200, 2300?
10. Show that the number of leap years that occur in any 400 consecutive years is always the same and find this number of years.
11. Show the 13th day of each of two consecutive months is a Friday if and only if these months are the February and March of a year for which January 1 falls on a Thursday.
* 12. A new calendar called the *International Fixed Calendar* has been proposed. In this calendar, there are 13 months, including all of our present months, plus a new month, called *Sol,* which is placed between June and July. Each month has 28 days, except for the June of leap years, which has an extra day (leap years are determined the same way as in the Gregorian calendar). There is an extra day, *Year End Day,* which is not in any month, which we may consider as December 29. Devise a perpetual calendar for the International Fixed Calendar to give the day of the week for any calendar date.
13. Show that every year in the Gregorian calendar includes at least one Friday the 13th.
14. Show that for every year of the Gregorian calendar and for every integer k with $1 \leq k \leq 30$, as the 12 months of the year pass, the kth day of the month falls on all seven days of the week.
15. Given a year in the Gregorian calendar, determine on how many different days of the week the 31st of a month falls.
16. Determine the largest possible number of years in a century during which the month of February has 5 Sundays.

5.2 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 number of times that the thirteenth of a month falls on a Friday for all years between 1800 and 2300. Can you make and prove a conjecture based on your evidence?

Programming Projects

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

1. Give the day of the week of any date.
2. Print out a calendar of any year.
3. Print out a calendar for the International Fixed Calendar (see Exercise 12).

5.3 Round-Robin Tournaments

Congruences can be used to schedule round-robin tournaments. In this section, we show how to schedule a tournament for N different teams, so that each team plays every other team exactly once. The method we describe was developed by Freund [Fr56].

First, note that if N is odd, not all teams can be scheduled in each round, because when teams are paired, the total number of teams playing is even. So, if N is odd, we add a dummy team, and if a team is paired with the dummy team during a particular round, it draws a bye in that round and does not play. Hence, we can assume that we always have an even number of teams, with the addition of a dummy team if necessary.

We label the N teams with the integers $1, 2, 3, \ldots, N-1, N$. We construct a schedule, pairing teams in the following way. We have team i, with $i \neq N$, play team j, with $j \neq N$ and $j \neq i$, in the kth round if $i + j \equiv k \pmod{N-1}$. This schedules games for all teams in round k, except for team N and the one team i for which $2i \equiv k \pmod{N-1}$. There is one such team because Theorem 4.10 tells us that the congruence $2x \equiv k \pmod{N-1}$ has exactly one solution with $1 \leq x \leq N-1$, because $(2, N-1) = 1$. We match this team i with team N in the kth round.

We must now show that each team plays every other team exactly once. We consider the first $N-1$ teams. Note that team i, where $1 \leq i \leq N-1$, plays team N in round k, where $2i \equiv k \pmod{N-1}$, and this happens exactly once. In the other rounds, team i does not play the same team twice, for if team i played team j in both rounds k and k', then $i + j \equiv k \pmod{N-1}$, and $i + j \equiv k' \pmod{N-1}$, which is an obvious contradiction because $k \not\equiv k' \pmod{N-1}$. Hence, because each of the first $N-1$ teams plays $N-1$ games, and does not play any team more than once, it plays every team exactly once. Also, team N plays $N-1$ games, and since every other team plays team N exactly once, team N plays every other team exactly once.

Example 5.10. To schedule a round-robin tournament with five teams, labeled 1, 2, 3, 4, and 5, we include a dummy team labeled 6. In round one, team 1 plays team j, where $1 + j \equiv 1 \pmod{5}$. This is the team $j = 5$ so that team 1 plays team 5. Team 2 is scheduled in round one with team 4, since the solution of $2 + j \equiv 1 \pmod{5}$ is $j = 4$. Because $i = 3$ is the solution of the congruence $2i \equiv 1 \pmod{5}$, team 3 is paired with the dummy team 6, and hence, draws a bye in the first round. If we continue this procedure and finish scheduling the other rounds, we end up with the pairings shown in Table 5.1, where the opponent of team i in round k is given in the kth row and ith column. ◀

	Team				
Round	**1**	**2**	**3**	**4**	**5**
1	5	4	bye	2	1
2	bye	5	4	3	2
3	2	1	5	bye	3
4	3	bye	1	5	4
5	4	3	2	1	bye

Table 5.1 *Round-robin schedule for five teams.*

5.3 Exercises

1. Set up a round-robin tournament schedule for the following.

   a) 7 teams b) 8 teams c) 9 teams d) 10 teams

2. In round-robin tournament scheduling, we wish to assign a *home team* and an *away team* for each game so that each of n teams, where n is odd, plays an equal number of home games and away games. Show that if, when $i + j$ is odd, we assign the smaller of i and j as the home team, whereas if $i + j$ is even, we assign the larger of i and j as the home team, then each team plays an equal number of home and away games.

3. In a round-robin tournament scheduling, use Exercise 2 to determine the home team for each game for the following numbers of teams.

   a) 5 teams b) 7 teams c) 9 teams

5.3 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. Construct a round-robin schedule for a tournament with 13 teams, specifying a home team for each game.

Programming Projects

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

1. Schedule round-robin tournaments for n teams, where n is a positive integer.
2. Using Exercise 2, schedule round-robin tournaments for n teams, where n is an odd positive integer, specifying the home team for each game.

5.4 Hashing Functions

A university wishes to store a file in its computer for each of its students. The identifying number or *key* for each file is the social security number of the student. The social security number is a nine-digit integer, so it is extremely infeasible to reserve a memory location for each possible social security number. Instead, a systematic way to arrange the files in memory, using a reasonable number of memory locations, should be used so that each file can be easily accessed. Systematic methods of arranging files have been developed based on *hashing functions.* A hashing function assigns to the key of each file a particular memory location. Various types of hashing functions have been suggested, but the type most commonly used involves modular arithmetic. We discuss this type of hashing function here; for a general discussion of hashing functions, see Knuth [Kn97] or [CoLeRi01].

Let k be the key of the file to be stored; in our example, k is the social security number of a student. Let m be a positive integer. We define the hashing function $h(k)$ by

$$h(k) \equiv k \pmod{m},$$

where $0 \leq h(k) < m$, so that $h(k)$ is the least positive residue of k modulo m. We wish to pick m intelligently, so that the files are distributed in a reasonable way throughout the m different memory locations $0, 1, 2, \ldots, m-1$.

The first thing to keep in mind is that m should not be a power of the base b that is used to represent the keys. For instance, when using social security numbers as keys, m should not be a power of 10, such as 10^3, because the value of the hashing function would simply be the last several digits of the key; this may not distribute the keys uniformly throughout the memory locations. For instance, the last three digits of early issued social security numbers may often be between 000 and 099, but seldom between 900 and 999. Likewise, it is unwise to use a number dividing $b^k \pm a$, where k and a are small integers for the modulus m. In such a case, $h(k)$ would depend too strongly on the particular digits of the key, and different keys with similar, but rearranged, digits may be sent to the same memory location. For instance, if $m = 111$, then, since $111 \mid (10^3 - 1) = 999$, we have $10^3 \equiv 1 \pmod{111}$, so that the social security numbers 064 212 848 and 064 848 212 are sent to the same memory location, because

$$h(064\ 212\ 848) \equiv 064\ 212\ 848 \equiv 064 + 212 + 848 \equiv 1124 \equiv 14 \pmod{111}$$

and

$$h(064\ 848\ 212) \equiv 064\ 848\ 212 \equiv 064 + 848 + 212 \equiv 1124 \equiv 14 \pmod{111}.$$

To avoid such difficulties, m should be a prime that approximates the number of available memory locations devoted to file storage. For instance, if there are 5000 memory locations available for storage of 2000 student files, we could pick m to be equal to the prime 4969.

If the hashing function assigns the same memory location to two different files, we say that there is a *collision*. We need a method to resolve collisions, so that files are assigned to unique memory locations. There are two kinds of collision resolution policies. In the first kind, when a collision occurs, extra memory locations are linked together to the first memory location. When one wishes to access a file where this collision resolution policy has been used, it is necessary to first evaluate the hashing function for the particular key involved. Then the list linked to this memory location is searched.

The second kind of collision resolution policy is to look for an open memory location when an occupied location is assigned to a file. Various suggestions have been made for accomplishing this, such as the following techniques.

Starting with our original hashing function $h_0(k) = h(k)$, we define a sequence of memory locations $h_1(k), h_2(k), \ldots$. We first attempt to place the file with key k at location $h_0(k)$. If this location is occupied, we move to location $h_1(k)$. If this is occupied, we move to location $h_2(k)$, and so on.

We can choose the sequence of functions $h_j(k)$ in various ways. The simplest way is to let

$$h_j(k) \equiv h(k) + j \pmod{m}, \quad 0 \leq h_j(k) < m.$$

This places the file with key k as near as possible past location $h(k)$. Note that with this choice of $h_j(k)$, all memory locations are checked, so if there is an open location, it will be found. Unfortunately, this simple choice of $h_j(k)$ leads to difficulties; files tend to *cluster*. We see that if $k_1 \neq k_2$ and $h_i(k_1) = h_j(k_2)$ for nonnegative integers i and j, then $h_{i+k}(k_1) = h_{j+k}(k_2)$ for $k = 1, 2, 3, \ldots$, so that exactly the same sequence of locations is traced out once there is a collision. This lowers the efficiency of the search for files in the table. We would like to avoid this problem of clustering, so we choose the function $h_j(k)$ in a different way.

To avoid clustering, we use a technique called *double hashing*. We choose, as before,

$$h(k) \equiv k \pmod{m},$$

with $0 \leq h(k) < m$, where m is prime, as the hashing function. We take a second hashing function

$$g(k) \equiv k + 1 \pmod{m - 2},$$

where $0 < g(k) \leq m - 1$, so that $(g(k), m) = 1$. We take as a *probing sequence*

$$h_j(k) \equiv h(k) + j \cdot g(k) \pmod{m},$$

where $0 \leq h_j(k) < m$. Because $(g(k), m) = 1$, as j runs through the integers $0, 1, 2, \ldots, m - 1$, all memory locations are traced out. The ideal situation would be for $m - 2$ also to be prime, so that the values $g(k)$ are distributed in a reasonable way. Hence, we would like $m - 2$ and m to be twin primes.

Example 5.11. In our example using social security numbers, both $m = 4969$ and $m - 2 = 4967$ are prime. Our probing sequence is

$$h_j(k) \equiv h(k) + j \cdot g(k) \pmod{4969},$$

where $0 \leq h_j(k) < 4969$, $h(k) \equiv k \pmod{4969}$, and $g(k) \equiv k + 1 \pmod{4967}$.

Suppose that we wish to assign memory locations to files for students with the following social security numbers:

$k_1 = 344\,401\,659$	$k_6 = 372\,500\,191$
$k_2 = 325\,510\,778$	$k_7 = 034\,367\,980$
$k_3 = 212\,228\,844$	$k_8 = 546\,332\,190$
$k_4 = 329\,938\,157$	$k_9 = 509\,496\,993$
$k_5 = 047\,900\,151$	$k_{10} = 132\,489\,973.$

Because $k_1 \equiv 269$, $k_2 \equiv 1526$, and $k_3 \equiv 2854 \pmod{4969}$, we assign the first three files to locations 269, 1526, and 2854, respectively.

Because $k_4 \equiv 1526 \pmod{4969}$, but memory location 1526 is taken, we compute $h_1(k_4) \equiv h(k_4) + g(k_4) = 1526 + 216 = 1742 \pmod{4969}$; this follows because $g(k_4) \equiv 1 + k_4 \equiv 216 \pmod{4967}$.

Because location 1742 is free, we assign the fourth file to this location. The fifth, six, seventh, and eighth files go into the available locations 3960, 4075, 2376, and 578, respectively, because $k_5 \equiv 3960$, $k_6 \equiv 4075$, $k_7 \equiv 2376$, and $k_8 \equiv 578 \pmod{4969}$.

We find that $k_9 \equiv 578 \pmod{4969}$; because location 578 is occupied, we compute $h_1(k_9) \equiv h(k_9) + g(k_9) = 578 + 2002 = 2580 \pmod{4969}$, where $g(k_9) \equiv 1 + k_9 \equiv 2002 \pmod{4967}$. Hence, we assign the ninth file to the free location 2580.

Finally, we find that $k_{10} \equiv 1526 \pmod{4969}$, but location 1526 is taken. We compute $h_1(k_{10}) \equiv h(k_{10}) + g(k_{10}) = 1526 + 216 = 1742 \pmod{4969}$, because $g(k_{10}) \equiv 1 + k_{10} \equiv 216 \pmod{4967}$, but location 1742 is taken. Hence, we continue by finding $h_2(k_{10}) \equiv h(k_{10}) + 2g(k_{10}) \equiv 1958 \pmod{4969}$ and in this available location we place the tenth file.

Table 5.2 lists the assignments for the files of students by their social security numbers. In the table, the file locations are shown in boldface. ◀

We wish to find conditions in which double hashing leads to clustering. Hence, we find conditions when

$$h_i(k_1) = h_j(k_2) \tag{5.1}$$

and

$$h_{i+1}(k_1) = h_{j+1}(k_2), \tag{5.2}$$

Social Security Number	$h(k)$	$h_1(k)$	$h_2(k)$
344 401 659	**269**		
325 510 778	**1526**		
212 228 844	**2854**		
329 938 157	1526	**1742**	
047 900 151	**3960**		
372 500 191	**4075**		
034 367 980	**2376**		
546 332 190	**578**		
509 496 993	578	**2580**	
132 489 973	1526	1742	**1958**

Table 5.2 *Hashing function for student files.*

so that the two consecutive terms of two probe sequences agree. If both (5.1) and (5.2) occur, then

$$h(k_1) + ig(k_1) \equiv h(k_2) + jg(k_2) \pmod{m} \tag{5.3}$$

and

$$h(k_1) + (i+1)g(k_1) \equiv h(k_2) + (j+1)g(k_2) \pmod{m}. \tag{5.4}$$

Subtracting congruence (5.3) from (5.4), we obtain

$$g(k_1) \equiv g(k_2) \pmod{m}.$$

Because $0 < g(k) \leq m-1$, the congruence $g(k_1) \equiv g(k_2) \pmod{m}$ implies that $g(k_1) = g(k_2)$. Consequently,

$$k_1 + 1 \equiv k_2 + 1 \pmod{m-2},$$

which tells us that

$$k_1 \equiv k_2 \pmod{m-2}.$$

Because $g(k_1) = g(k_2)$, we can simplify congruence (5.3) to obtain

$$h(k_1) \equiv h(k_2) \pmod{m},$$

which shows that

$$k_1 \equiv k_2 \pmod{m}.$$

Consequently, because $(m-2, m) = 1$, Theorem 4.8 tells us that

$$k_1 \equiv k_2 \pmod{m(m-2)}.$$

Therefore, the only way that two probing sequences can agree for two consecutive terms is if the two keys involved, k_1 and k_2, are congruent modulo $m(m-2)$. Hence, clustering is extremely rare. Indeed, if $m(m-2) > k$ for all keys k, clustering will never occur.

5.4 Exercises

1. A parking lot has 101 parking places. A total of 500 parking stickers are sold and only 50–75 vehicles are expected to be parked at any time. Set up a hashing function and collision resolution policy for assigning parking places based on license plates displaying six-digit numbers.
2. Assign memory locations for students in your class, using as keys the day of the month of birthdays of students, with hashing function $h(K) \equiv K \pmod{19}$, and
   a) with probing sequence $h_j(K) \equiv h(K) + j \pmod{19}$.
   b) with probing sequence $h_j(K) \equiv h(K) + j \cdot g(K), 0 \leq j \leq 16$, where $g(K) \equiv 1 + K \pmod{17}$.

* 3. Let a hashing function be $h(K) \equiv K \pmod{m}$, with $0 \leq h(K) < m$, and let the probing sequence for collision resolution be $h_j(K) \equiv h(K) + jq \pmod{m}$, $0 \leq h_j(K) < m$, for $j = 1, 2, \ldots, m-1$. Show that all memory locations are probed

a) if m is prime and $1 \leq q \leq m-1$.
b) if $m = 2^r$ and q is odd.

* 4. A probing sequence for resolving collisions where the hashing function is $h(K) \equiv K \pmod{m}$, $0 \leq h(K) < m$, is given by $h_j(K) \equiv h(K) + j(2h(K)+1) \pmod{m}$, $0 \leq h_j(K) < m$.
   a) Show that if m is prime, then all memory sequences are probed.
   b) Determine conditions for clustering to occur; that is, when $h_j(K_1) = h_j(K_2)$ and $h_{j+r}(K_1) = h_{j+r}(K_2)$ for $r = 1, 2, \ldots$.

5. Using the hashing function and probing sequence of the example in the text, find open memory locations for the files of additional students with social security numbers $k_{11} = 137\ 612\ 044$, $k_{12} = 505\ 576\ 452$, $k_{13} = 157\ 170\ 996$, $k_{14} = 131\ 220\ 418$. (Add these to the ten files already stored.)

5.4 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. Assign memory locations to the files of all the students in your class, using the hashing function and probing function from Example 5.11. After doing so, assign memory locations to other files with social security numbers that you make up.

Programming Projects

Write programs using Maple, *Mathematica,* or a language of your choice to assign memory locations to student files, using the hashing function $h(k) \equiv k \pmod{1021}$, $0 \leq h(k) < 1021$, where the keys are the social security numbers of students,

1. linking files together when collisions occur.
2. using $h_j(k) \equiv h(k) + j \pmod{1021}$, $j = 0, 1, 2, \ldots$ as the probing sequence.
3. using $h_j(k) \equiv h(k) + j \cdot g(k)$, $j = 0, 1, 2, \ldots$, where $g(k) \equiv 1 + k \pmod{1019}$, as the probing sequence.

5.5 Check Digits

Congruences can be used to check for errors in strings of digits. In this section, we will discuss error detection for bit strings, which are used to represent computer data. Then we will describe how congruences are used to detect errors in strings of decimal digits, which are used to identify passports, checks, books, and other types of objects.

Manipulating or transmitting bit strings can introduce errors. A simple error detection method is to append the bit string $x_1x_2 \ldots x_n$ with a *parity check bit* x_{n+1} defined by

$$x_{n+1} \equiv x_1 + x_2 + \cdots + x_n \pmod{2},$$

so that $x_{n+1} = 0$ if an even number of the first n bits in the string are 1, whereas $x_{n+1} = 1$ if an odd number of these bits are 1. The appended string $x_1x_2 \ldots x_nx_{n+1}$ satisfies the congruence

$$x_1 + x_2 + \cdots + x_n + x_{n+1} \equiv 0 \pmod 2. \tag{5.5}$$

We use this congruence to look for errors.

Suppose that we send $x_1x_2 \ldots x_nx_{n+1}$, and the string $y_1y_2 \ldots y_ny_{n+1}$ is received. These two strings are equal, that is, $y_i = x_i$ for $i = 1, 2, \ldots, n+1$, when there are no errors. But if an error was made, they differ in one or more positions. We check whether

$$y_1 + y_2 + \cdots + y_n + y_{n+1} \equiv 0 \pmod 2 \tag{5.6}$$

holds. If this congruence fails, at least one error is present, but if it holds, errors may still be present. However, when errors are rare and random, the most common type of error is a single error, which is always detected. In general, we can detect an odd number of errors, but not an even number of errors (see Exercise 4).

Example 5.12. Suppose that we receive 1101111 and 11001000, where the last bit in each string is a parity check bit. For the first string, note that $1+1+0+1+1+1+1 \equiv 0 \pmod 2$, so that either the received string is what was transmitted or it contains an even number of errors. For the second string, note that $1+1+0+0+1+0+0+0 \equiv 1 \pmod 2$, so that the received string was not the string sent; we ask for retransmission. ◀

Strings of decimal digits are used for identification numbers in many different contexts. Check digits, computed using a variety of schemes, are used to find errors in these strings. For instance, check digits are used to detect errors in passport numbers. In a scheme used by several European countries, if $x_1x_2x_3x_4x_5x_6$ is the identification number of a passport, the check digit x_7 is chosen so that

$$x_7 \equiv 7x_1 + 3x_2 + x_3 + 7x_4 + 3x_5 + x_6 \pmod{10}.$$

Example 5.13. Suppose that the identification number of a passport is 211894. To find the check digit x_7, we compute

$$x_7 \equiv 7 \cdot 2 + 3 \cdot 1 + 1 \cdot 1 + 7 \cdot 8 + 3 \cdot 9 + 1 \cdot 4 \equiv 5 \pmod{10},$$

so that the check digit is 5, and the seven-digit number 2118945 is printed on the passport. ◀

We can always detect a single error in a passport identification number appended with a check digit computed in this way. To see this, suppose that we make an error of a in a digit; that is, $y_j = x_j + a \pmod{10}$, where x_j is the correct jth digit and y_j is the incorrect digit that replaces it. From the definition of the check digit, it follows that we change x_7 by either $7a$, $3a$, or $a \pmod{10}$, each of which changes x_7. However, errors caused by transposing two digits will be detected if and only if the difference between these two digits is not 5 or -5, that is, if they are not digits x_i and x_j with $|x_i - x_j| = 5$

(see Exercise 7). This scheme also detects a large number of possible errors involving the scrambling of three digits.

ISBNs

We now turn our attention to the use of check digits in publishing. Almost all recent books are identified by their *International Standard Book Number (ISBN)*, which is a ten-digit code assigned by the publisher. For instance, the ISBN for the first edition of this text is 0-201-06561-4. Here the first block of digits, 0, represents the language of the book (English), the second block of digits, 201, represents the publishing company (Addison-Wesley), the third block of digits, 06561, is the number assigned by the publishing company to this book, and the final digit, in this case 4, is the check digit. (The sizes of the blocks differ for different languages and publishers). The check digit in an ISBN can be used to detect the errors most commonly made when ISBNs are copied, namely single errors and errors made when two digits are transposed.

We will describe how this check digit is determined and then show that it can be used to detect the commonly occurring types of errors. Suppose that the ISBN of a book is $x_1x_2 \ldots x_{10}$, where x_{10} is the check digit. (We ignore the hyphens in the ISBN, because the grouping of digits does not affect how the check digit is computed.) The first nine digits are decimal digits, that is, belong to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, whereas the check digit x_{10} is a base 11 digit, belonging to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \text{X}\}$, where X is the base 11 digit representing the integer 10 (in decimal notation). The check digit is selected so that the congruence

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$$

holds. As is easily seen (see Exercise 10), the check digit x_{10} can be computed from the congruence $x_{10} \equiv \sum_{i=1}^{9} ix_i \pmod{11}$; that is, the check digit is the remainder upon division by 11 of a weighted sum of the first nine digits.

Example 5.14. We find the check digit for the ISBN of the first edition of this text, which begins with 0-201-06561, by computing

$$x_{10} \equiv 1 \cdot 0 + 2 \cdot 2 + 3 \cdot 0 + 4 \cdot 1 + 5 \cdot 0 + 6 \cdot 6 + 7 \cdot 5 + 8 \cdot 6 + 9 \cdot 1 \equiv 4 \pmod{11}.$$

Hence, the ISBN is 0-201-06561-4, as previously stated. Similarly, if the ISBN number of a book begins with 3-540-19102, we find the check digit using the congruence

$$x_{10} \equiv 1 \cdot 3 + 2 \cdot 5 + 3 \cdot 4 + 4 \cdot 0 + 5 \cdot 1 + 6 \cdot 9 + 7 \cdot 1 + 8 \cdot 0 + 9 \cdot 2 \equiv 10 \pmod{11}.$$

This means that the check digit is X, the base 11 digit for the decimal number 10. Hence, the ISBN number is 3-540-19102-X. ◀

We will show that a single error, or a transposition of two digits, can be detected using the check digit of an ISBN. First, suppose that $x_1x_2 \ldots x_{10}$ is a valid ISBN, but that this number has been printed as $y_1y_2 \ldots y_{10}$. We know that $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$, because $x_1x_2 \ldots x_{10}$ is a valid ISBN.

Suppose that exactly one error has been made in printing the ISBN. Then, for some integer j, we have $y_i = x_i$ for $i \neq j$ and $y_j = x_j + a$, where $-10 \leq a \leq 10$ and $a \neq 0$. Here $a = y_j - x_j$ is the error in the jth place. Note that

$$\sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + ja \equiv ja \not\equiv 0 \pmod{11}$$

because $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$ and, by Lemma 3.5, it follows that $11 \nmid ja$ because $11 \nmid j$ and $11 \nmid a$. We conclude that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN so that we can investigate the error.

Now suppose that two unequal digits have been transposed; then there are distinct integers j and k such that $y_j = x_k$ and $y_k = x_j$, and $y_i = x_i$ if $i \neq j$ and $i \neq k$. It follows that

$$\sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + (jx_k - jx_j) + (kx_j - kx_k) \equiv (j-k)(x_k - x_j) \not\equiv 0 \pmod{11}$$

because $\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$, and $11 \nmid (j-k)$ and $11 \nmid (x_k - x_j)$. We see that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN, so that we can detect the interchange of two unequal digits.

We have discussed how a single check digit can be used to detect errors in strings of digits. However, using a single check digit, we cannot detect an error and then correct it, that is, replace the digit in error with the valid one. It is possible to detect and correct an error using additional digits satisfying certain congruences (see Exercises 20 and 22, for example). The reader is referred to any text on coding theory for more information on error detection and correction. Coding theory uses many results from different parts of mathematics, including number theory, abstract algebra, combinatorics, and even geometry. To find good sources of information, consult Chapter 14 of [Ro99a]. We also refer the reader to the excellent articles by J. Gallian on check digits, [Ga92], [Ga91], and [Ga96], [GaWi88], for related information, including how check digits for drivers license numbers are found, and the book [Ki01] entirely devoted to check digits and identification numbers.

5.5 Exercises

1. What is the parity check bit that should be added to each of the following bit strings?

a) 111111 c) 101010 e) 11111111
b) 000000 d) 100000 f) 11001011

2. Suppose that you receive the following bit strings, where the last bit is a parity check bit. Which strings do you know are incorrect?

a) 111111111 b) 0101010101010 c) 1111010101010101

3. Assume that each of the following strings, ending with a parity check bit, was received correctly except for a missing bit indicated with a question mark. What is the missing bit?

   a) 1?11111 b) 000?10101 c) ?0101010100

4. Show that a parity check bit can detect an odd number of errors, but not an even number of errors.

5. Using the check digit scheme described in the text, find the check digit that should be added to the following passport identification numbers.

   a) 132999 b) 805237 c) 645153

6. Are the following passport identification numbers valid, where the seventh digit is the check digit computed as described in the text?

   a) 3300118 b) 4501824 c) 1873336

7. Show that the passport check digit scheme described in the text detects transposition of the digits x_i and x_j if and only if $|x_i - x_j| \neq 5$.

8. The bank identification number printed on a check consists of eight digits, $x_1x_2 \ldots x_8$, followed by a ninth check digit x_9, where $x_9 \equiv 7x_1 + 3x_2 + 9x_3 + 7x_4 + 3x_5 + 9x_6 + 7x_7 + 3x_8 \pmod{10}$.
   a) What is the check digit following the eight-digit identification number 00185403?
   b) Which single errors in bank identification numbers does a check digit computed in this way detect?
   c) Which transpositions of two digits does this scheme detect?

9. What should the check digit be to complete each of the following ISBNs?

   a) 2-113-54001 c) 1-2123-9940
   b) 0-19-081082 d) 0-07-038133

10. Show that the check digit x_{10} in an ISBN $x_1x_2 \ldots x_{10}$ can be computed from the congruence $x_{10} \equiv \sum_{i=1}^{9} ix_i \pmod{11}$.

11. Determine whether each of the following ISBNs is valid.

    a) 0-394-38049-5 c) 0-8218-0123-6 e) 90-6191-705-2
    b) 1-09-231221-3 d) 0-404-50874-X

12. Suppose that one digit, indicated with a question mark, in each of the following ISBNs has been smudged and cannot be read. What should this missing digit be?

    a) 0-19-8?3804-9 b) 91-554-212?-6 c) ?-261-05073-X

13. While copying the ISBN for a book, a clerk accidentally transposed two digits. If the clerk copied the ISBN as 0-07-289095-0 and did not make any other mistakes, what is the correct ISBN for this book?

Retail products are often identified by *Universal Product Codes (UPCs)*, the most common of which consists of 12 decimal digits. The first digit identifies a product category, the next five the manufacturer, the following five the particular product, and the last digit is a check digit. The check digit is determined by the following three steps that use the first 11 digits of

the UPC. First, digits in odd-numbered positions, starting from the left, are added, and the resulting sum is tripled. Second, the sum of digits in even-numbered positions is added to the result of the first step. Third, the check is found by determining which decimal digit, when added to the overall result of the second step, produces an integer divisible by 10.

14. Give a formula using a congruence that produces the check digit for a UPC from the 11 digits representing the product category, manufacturer, and particular product.

15. Determine whether each of the following 12-digit strings can be the UPC of a product.

a) 0 47000 00183 6 c) 0 58000 00127 5
b) 3 11000 01038 9 d) 2 26500 01179 4

16. What is the check digit for the 12-digit UPC code that begins with each of the following 11-digit strings?

a) 3 81370 02918 c) 0 33003 31439
b) 5 01175 00557 d) 4 11000 01028

17. Determine whether the 12-digit UPC code can always detect an error in exactly one digit.

18. Determine whether the 12-digit UPC code can always detect the transposition of two digits.

19. Suppose we specify that the valid 10-digit decimal code words $x_1x_2 \ldots x_{10}$ are those satisfying the congruence $\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}$.
a) Can we detect all single errors in a code word?
b) Can we detect transposition of two digits in a code word?

*** 20.** Suppose that the only valid 10-digit code words $x_1x_2 \ldots x_{10}$ are those satisfying the congruences $\sum_{i=1}^{10} x_i \equiv \sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}$.
a) Show that the valid code words, where the first digits are decimal digits, that is, in the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, are those where the last two digits satisfy the congruences $x_9 \equiv \sum_{j=1}^{8}(i+1)x_i \pmod{11}$ and $x_{10} \equiv \sum_{j=1}^{8}(9-i)x_i \pmod{11}$.
b) Find the number of valid decimal code words.
c) Show that any single error in a code word can be detected and corrected, because the location and value of the error can be determined.
d) Show that we can detect any error caused by transposing two digits in a code word.

21. The government of Norway assigns an 11-digit decimal registration number $x_1x_2 \ldots x_{11}$ to each of its citizens using a scheme designed by Norwegian number theorist E. Selmer. The digits $x_1x_2 \ldots x_6$ represent the date of birth, the digits $x_7x_8x_9$ identify the particular person born that day, and x_{10} and x_{11} are check digits that are computed using the congruences $x_{10} \equiv 8x_1 + 4x_2 + 5x_3 + 10x_4 + 3x_5 + 2x_6 + 7x_7 + 6x_8 + 9x_9 \pmod{11}$, and $x_{11} \equiv 6x_1 + 7x_2 + 8x_3 + 9x_4 + 4x_5 + 5x_6 + 6x_7 + 7x_8 + 8x_9 + 9x_{10} \pmod{11}$.
a) Determine the check digits that follow the first nine digits 110491238.
b) Show that this scheme detects all single errors in a registration number.
* c) Which double errors are detected?

* **22.** Suppose that we specify that the valid 10-digit code words $x_1x_2 \ldots x_{10}$, where each digit is a decimal digit, are those satisfying the congruences $\sum_{i=1}^{10} x_i \equiv \sum_{i=1}^{10} ix_i \equiv \sum_{i=1}^{10} i^2x_i \equiv \sum_{i=1}^{10} i^3x_i \equiv 0 \pmod{11}$.
  a) How many valid 10-digit code words are there?
  b) Show how any two errors in a code word can be corrected.
  c) Suppose a code word has been received as 0204906710. If two errors have been made, what is the correct code word?

Airline tickets carry 15-digit identification numbers $a_1a_2 \ldots a_{14}a_{15}$, where a_{15} is a check digit which equals the least nonnegative residue of the integer $a_1a_2 \ldots a_{14}$ modulo 7.

23. Find the check digit a_{15} when the first 14 digits of the identification of an airplane ticket are

a) 00032781811224 b) 10238544122339 c) 00611133123278

24. Determine whether these are valid airline ticket identification numbers.

a) 102284711033122 b) 004113711331240 c) 100261413001533

25. Determine which errors in a single digit can be detected and which cannot be detected using the check digit for airline tickets.

26. Determine which errors involving the transposition of two adjacent digits in the identification number of an airline ticket can be detected and which cannot be detected using the check digit for airline tickets.

The *International Standard Serial Number (ISSN)* used to identify a periodical consists of two blocks of four digits, where the last digit in the second block is a base 11 check digit. As in an ISBN, the character X represents 10 (in decimal notation). The check digit d_8 is determined by the congruence $d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$.

27. For each of the following initial seven digits of an ISSN, determine the correct check digit.

a) 0317-847 c) 1063-669
b) 0423-555 d) 1363-837

28. Is it always possible to detect a single error in an ISSN? That is, is it always possible to detect that an error was made when one digit of an ISSN has been copied incorrectly? Justify your answer.

29. Is it always possible to detect when two consecutive digits in an ISSN have been accidentally transposed? Justify your answer.

5.5 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. Check the ISBN numbers of a selection of books to see whether the check digit was computed correctly.

Programming Projects

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

1. Determine whether a bit string, ending with a parity check bit, has either an odd or an even number of errors.
2. Determine the check digit for an ISBN, given the first nine digits.
3. Determine whether a 10-digit string, where the first nine digits are decimal digits and the last is a decimal digit or an X, is a valid ISBN.
4. Determine whether a 12-digit decimal string is a valid UPC.

6 Some Special Congruences

Introduction

In this chapter, we discuss three congruences that have both theoretical and practical significance: Wilson's theorem shows that when p is prime, the remainder when $(p-1)!$ is divided by p is -1. Fermat's little theorem provides a congruence for the pth powers of integers modulo p. In particular, it shows that if p is prime, then a^p and a have the same remainder when divided by p whenever a is an integer. Euler's theorem provides a generalization of Fermat's little theorem for moduli that are not prime.

These three congruences have many applications. For example, we will explain how Fermat's little theorem can be used as the basis for primality tests and factoring algorithms. We will also discuss composite integers, called pseudoprimes, that masquerade as primes by satisfying the same congruence that primes do in Fermat's little theorem. We will use the fact that pseudoprimes are relatively rare to develop some tests that can provide overwhelming evidence that an integer is prime.

6.1 Wilson's Theorem and Fermat's Little Theorem

In a book published in 1770, English mathematician Edward Waring stated that one of his students, John Wilson, had discovered that $(p-1)!+1$ is divisible by p whenever p is prime. Furthermore, he stated that neither he nor Wilson knew how to prove it. Most likely, Wilson made this conjecture based on numerical evidence. For example, we can easily see that 2 divides $1!+1=2$, 3 divides $2!+1=3$, 5 divides $4!+1=25$, 7 divides $6!+1=721$, and so on. Although Waring thought it would be difficult to find a proof, *Joseph Lagrange* proved this result in 1771. Nevertheless, the fact that p divides $(p-1)!+1$ is known as *Wilson's theorem*. We now state this theorem in the form of a congruence.

Theorem 6.1. ***Wilson's Theorem.*** If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Before proving Wilson's theorem, we use an example to illustrate the idea behind the proof.

Example 6.1. Let $p = 7$. We have $(7-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. We will rearrange the factors in the product, grouping together pairs of inverses modulo 7. We note that $2 \cdot 4 \equiv 1 \pmod{7}$ and $3 \cdot 5 \equiv 1 \pmod{7}$. Hence, $6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod{7}$. Thus, we have verified a special case of Wilson's theorem. ◀

We now use the technique illustrated in the example to prove Wilson's theorem.

Proof. When $p = 2$, we have $(p-1)! \equiv 1 \equiv -1 \pmod{2}$. Hence, the theorem is true for $p = 2$. Now let p be a prime greater than 2. Using Theorem 4.10, for each integer a with $1 \leq a \leq p-1$, there is an inverse $\bar{a}$, $1 \leq \bar{a} \leq p-1$, with $a\bar{a} \equiv 1 \pmod{p}$. By Theorem 4.11 the only positive integers less than p that are their own inverses are 1 and $p-1$. Therefore, we can group the integers from 2 to $p-2$ into $(p-3)/2$ pairs of integers, with the product of each pair congruent to 1 modulo p. Hence, we have

$$2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod{p}.$$

We multiply both sides of the this congruence by 1 and $p-1$ to obtain

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

This completes the proof. ■

An interesting observation is that the converse of Wilson's theorem is also true, as the following theorem shows.

Theorem 6.2. If n is a positive integer with $n \geq 2$ such that $(n-1)! \equiv -1 \pmod{n}$, then n is prime.

JOSEPH LOUIS LAGRANGE (1736–1813) was born in Italy and studied physics and mathematics at the University of Turin. Although he originally planned to pursue a career in physics, Lagrange's growing interest in mathematics led him to change course. At the age of 19, he was appointed as a mathematics professor at the Royal Artillery School in Turin. In 1766, he filled the post Euler vacated at the Royal Academy of Berlin when Frederick the Great sought him out. Lagrange directed the mathematics section of the Royal Academy for 20 years. In 1787, when his patron Frederick the Great died, Lagrange moved to France at the invitation of Louis XVI, to join the French Academy. In France he had a distinguished career in teaching and writing. He was a favorite of Marie Antoinette, but managed to win the favor of the new regime that came into power after the French Revolution. Lagrange's contributions to mathematics include unifying the mathematical theory of mechanics. He made fundamental discoveries in group theory and helped put calculus on a rigorous foundation. His contributions to number theory include the first proof of Wilson's theorem, and the result that every positive integer can be written as the sum of four squares.

Proof. Assume that n is a composite integer and that $(n-1)! \equiv -1 \pmod{n}$. Because n is composite, we have $n = ab$, where $1 < a < n$ and $1 < b < n$. Because $a < n$, we know that $a \mid (n-1)!$, because a is one of the $n-1$ numbers multiplied together to form $(n-1)!$. Because $(n-1)! \equiv -1 \pmod{n}$ it follows that $n \mid ((n-1)!+1)$. This means, by Theorem 1.8, that a also divides $(n-1)!+1$. By Theorem 1.9, because $a \mid (n-1)!$ and $a \mid ((n-1)!+1)$, we conclude that $a \mid ((n-1)!+1) - (n-1)! = 1$. This is a contradiction, because $a > 1$. ∎

Wilson's theorem can be used to demonstrate that a composite integer is not prime, as Example 6.2 shows.

Example 6.2. Because $(6-1)! = 5! = 120 \equiv 0 \pmod{6}$, Theorem 6.1 verifies the obvious fact that 6 is not prime. ◀

As we can see, Wilson's theorem and its converse give us a primality test. To decide whether an integer n is prime, we determine whether $(n-1)! \equiv -1 \pmod{n}$. Unfortunately, this is an impractical test because $n-2$ multiplications modulo n are needed to find $(n-1)!$, requiring $O(n(\log_2 n)^2)$ bit operations.

Fermat made many important discoveries in number theory, including the fact that p divides $a^{p-1} - 1$ whenever p is prime and a is an integer not divisible by p. He stated this result in a letter to one of his mathematical correspondents, Frènicle de Bessy, in 1640. Fermat did not bother to enclose a proof with his letter, stating that he feared that a proof would be too long. Unlike Fermat's notorious last theorem, discussed in Chapter 13, there is little doubt that Fermat really knew how to prove this theorem (which is called "Fermat's little theorem" to distinguish it from his "last theorem"). Leonhard Euler is responsible for the first published proof, in 1736. Euler also generalized Fermat's little theorem; we will explain how in Section 6.3.

Theorem 6.3. ***Fermat's Little Theorem.*** If p is prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Consider the $p-1$ integers $a, 2a, \ldots, (p-1)a$. None of these integers are divisible by p, for if $p \mid ja$, then by Lemma 3.4, $p \mid j$, because $p \nmid a$. This is impossible, because $1 \leq j \leq p-1$. Furthermore, no two of the integers $a, 2a, \ldots, (p-1)a$ are congruent modulo p. To see this, assume that $ja \equiv ka \pmod{p}$, where $1 \leq j < k \leq p-1$. Then, by Corollary 4.4.1, because $(a, p) = 1$, we have $j \equiv k \pmod{p}$. This is impossible, because j and k are positive integers less than $p-1$.

Because the integers $a, 2a, \ldots, (p-1)a$ are a set of $p-1$ integers all incongruent to 0, and no two are congruent modulo p, we know that the least positive residues of $a, 2a, \ldots, (p-1)a$, taken in some order, must be the integers $1, 2, \ldots, p-1$. As a consequence, the product of the integers $a, 2a, \ldots, (p-1)a$ is congruent modulo p to the product of the first $p-1$ positive integers. Hence,

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

Therefore,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Because $((p-1)!, p) = 1$, using Corollary 4.4.1, we cancel $(p-1)!$ to obtain

$$a^{p-1} \equiv 1 \pmod{p}.$$ ■

We illustrate the ideas of the proof with an example.

Example 6.3. Let $p = 7$ and $a = 3$. Then, $1 \cdot 3 \equiv 3 \pmod 7$, $2 \cdot 3 \equiv 6 \pmod 7$, $3 \cdot 3 \equiv 2 \pmod 7$, $4 \cdot 3 \equiv 5 \pmod 7$, $5 \cdot 3 \equiv 1 \pmod 7$, and $6 \cdot 3 \equiv 4 \pmod 7$. Consequently,

$$(1 \cdot 3) \cdot (2 \cdot 3) \cdot (3 \cdot 3) \cdot (4 \cdot 3) \cdot (5 \cdot 3) \cdot (6 \cdot 3) \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod 7,$$

so that $3^6 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \pmod 7$. Hence, $3^6 \cdot 6! \equiv 6! \pmod 7$, and therefore $3^6 \equiv 1 \pmod 7$. ◀

Theorem 6.4. If p is prime and a is a positive integer, then $a^p \equiv a \pmod p$.

Proof. If $p \nmid a$, by Fermat's little theorem we know that $a^{p-1} \equiv 1 \pmod p$. Multiplying both sides of this congruence by a, we find that $a^p \equiv a \pmod p$. If $p \mid a$, then $p \mid a^p$ as well, so that $a^p \equiv a \equiv 0 \pmod p$. This finishes the proof, because $a^p \equiv a \pmod p$ if $p \nmid a$ and if $p \mid a$. ■

Finding the least positive residue of powers of integers is often required in number theory and its applications—especially cryptography, as we will see in Chapter 8. Fermat's little theorem is a useful tool in such computations, as the following example shows.

Example 6.4. We can find the least positive residue of 3^{201} modulo 11 with the help of Fermat's little theorem. We know that $3^{10} \equiv 1 \pmod{11}$. Hence, $3^{201} = (3^{10})^{20} \cdot 3 \equiv 3 \pmod{11}$. ◀

A useful application of Fermat's little theorem is provided by the following result.

Theorem 6.5. If p is prime and a is an integer such that $p \nmid a$, then a^{p-2} is an inverse of a modulo p.

Proof. If $p \nmid a$, by Fermat's little theorem we have $a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod p$. Hence, a^{p-2} is an inverse of a modulo p. ■

Example 6.5. By Theorem 6.5, we know that $2^9 = 512 \equiv 6 \pmod{11}$ is an inverse of 2 modulo 11. ◀

Theorem 6.5 gives us another way to solve linear congruences with respect to prime moduli.

Corollary 6.5.1. If a and b are positive integers and p is prime with $p \nmid a$, then the solutions of the linear congruence $ax \equiv b \pmod{p}$ are the integers x such that $x \equiv a^{p-2}b \pmod{p}$.

Proof. Suppose that $ax \equiv b \pmod{p}$. Because $p \nmid a$, we know from Theorem 6.5 that a^{p-2} is an inverse of $a \pmod{p}$. Multiplying both sides of the original congruence by a^{p-2}, we have

$$a^{p-2}ax \equiv a^{p-2}b \pmod{p}.$$

Hence,

$$x \equiv a^{p-2}b \pmod{p}.$$

■

The Pollard $p-1$ Factorization Method

Fermat's little theorem is the basis of a factorization method invented by J. M. Pollard in 1974. This method, known as the *Pollard $p-1$ method,* can find a nontrivial factor of an integer n when n has a prime factor p such that the primes dividing $p-1$ are relatively small.

To see how this method works, suppose that we want to find a factor of the positive integer n. Furthermore, suppose that n has a prime factor p such that $p-1$ divides $k!$, where k is a positive integer. We want $p-1$ to have only small prime factors, so that there is such an integer k that is not too large. For example, if $p = 2269$, then $p - 1 = 2268 = 2^2 3^4 7$, so that $p-1$ divides $9!$, but no smaller value of the factorial function.

The reason we want $p-1$ to divide $k!$ is so that we can apply Fermat's little theorem. By Fermat's little theorem we know that $2^{p-1} \equiv 1 \pmod{p}$. Now, since $p-1$ divides $k!$, $k! = (p-1)q$ for some integer q. Hence

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

which implies that p divides $2^{k!} - 1$. Now, let M be the least positive residue of $2^{k!} - 1$ modulo n, so that $M = (2^{k!} - 1) - nt$ for some integer t. We see that p divides M because it divides both $2^{k!} - 1$ and n.

Now, to find a divisor of n, we need only compute the greatest common divisor of M and n, $d = (M, n)$. This can be done rapidly using the Euclidean algorithm. For this divisor d to be a nontrivial divisor, it is necessary that M not be 0. This is the case when n does not itself divide $2^{k!} - 1$, which is likely when n has large prime divisors.

To use this method, we must compute $2^{k!}$, where k is a positive integer. This can be done efficiently because modular exponentiation can be done efficiently. To find the least positive remainder of $2^{k!}$ modulo n, we set $r_1 = 2$ and use the following sequence of computations: $r_2 \equiv r_1^2 \pmod{n}$, $r_3 \equiv r_2^3 \pmod{n}$, $\ldots$, $r_k \equiv r_{k-1}^k \pmod{n}$. We illustrate this procedure in the following example.

Example 6.6. To find $2^{9!} \pmod{5,157,437}$, we perform the following sequence of computations:

$$r_2 \equiv r_1^2 = 2^2 \equiv 4 \pmod{5,157,437}$$
$$r_3 \equiv r_2^3 = 4^3 \equiv 64 \pmod{5,157,437}$$
$$r_4 \equiv r_3^4 = 64^4 \equiv 1,304,905 \pmod{5,157,437}$$
$$r_5 \equiv r_4^5 = 1,304,905^5 \equiv 404,913 \pmod{5,157,437}$$
$$r_6 \equiv r_5^6 = 404,913^6 \equiv 2,157,880 \pmod{5,157,437}$$
$$r_7 \equiv r_6^7 = 2,157,880^7 \equiv 4,879,227 \pmod{5,157,437}$$
$$r_8 \equiv r_7^8 = 4,879,227^8 \equiv 4,379,778 \pmod{5,157,437}$$
$$r_9 \equiv r_8^9 = 4,379,778^9 \equiv 4,381,440 \pmod{5,157,437}.$$

It follows that $2^{9!} \equiv 4,381,440 \pmod{5,157,437}$. ◀

The following example illustrates the use of the Pollard $p-1$ method to find a factor of the integer 5,157,437.

Example 6.7. To factor 5,157,437 using the Pollard $p-1$ method, we successively find r_k, the least positive residue of $2^{k!}$ modulo 5,157,437, for $k = 1, 2, 3, \ldots$, as was done in Example 6.6. We compute $(r_k - 1, 5,157,437)$ at each step. To find a factor of 5,157,437 requires nine steps, because $(r_k - 1, 5,157,437) = 1$ for $k = 1, 2, 3, 4, 5, 6, 7, 8$ (as the reader can verify), but $(r_9 - 1, 5,157,437) = (4,381,439, 5,157,437) = 2269$. It follows that 2269 is a divisor of 5,157,437. ◀

The Pollard $p-1$ method does not always work. However, because nothing in the method depends on the choice of 2 as the base, we can extend the method and find a factor for more integers by using integers other than 2 as the base. In practice, the Pollard $p-1$ method is used after trial divisions by small primes, but before the heavy artillery of such methods as the quadratic sieve and the elliptic curve method.

6.1 Exercises

1. Show that $10! + 1$ is divisible by 11, by grouping together pairs of inverses modulo 11 that occur in 10!.
2. Show that $12! + 1$ is divisible by 13, by grouping together pairs of inverses modulo 13 that occur in 12!.
3. What is the remainder when 16! is divided by 19?
4. What is the remainder when 5!25! is divided by 31?
5. Using Wilson's theorem, find the least positive residue of $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13$ modulo 7.
6. What is the remainder when $7 \cdot 8 \cdot 9 \cdot 15 \cdot 16 \cdot 17 \cdot 23 \cdot 24 \cdot 25 \cdot 43$ is divided by 11?

7. What is the remainder when 18! is divided by 437?
8. What is the remainder when 40! is divided by 1763?
9. What is the remainder when 5^{100} is divided by 7?
10. What is the remainder when 6^{2000} is divided by 11?
11. Using Fermat's little theorem, find the least positive residue of $3^{999,999,999}$ modulo 7.
12. Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.
13. Show that $3^{10} \equiv 1 \pmod{11^2}$.
14. Using Fermat's little theorem, find the last digit of the base 7 expansion of 3^{100}.
15. Using Fermat's little theorem, find the solutions of the following linear congruences.
    a) $7x \equiv 12 \pmod{17}$ b) $4x \equiv 11 \pmod{19}$
16. Show that if n is a composite integer with $n \neq 4$, then $(n-1)! \equiv 0 \pmod{n}$.
17. Show that if p is an odd prime, then $2(p-3)! \equiv -1 \pmod{p}$.
18. Show that if n is odd and $3 \nmid n$, then $n^2 \equiv 1 \pmod{24}$.
19. Show that $a^{12} - 1$ is divisible by 35 whenever $(a, 35) = 1$.
20. Show that $a^6 - 1$ is divisible by 168 whenever $(a, 42) = 1$.
21. Show that $42 \mid (n^7 - n)$ for all positive integers n.
22. Show that $30 \mid (n^9 - n)$ for all positive integers n.
23. Show that $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{(p-1)} \equiv -1 \pmod{p}$ whenever p is prime. (It has been conjectured that the converse of this is also true.)
24. Show that $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$ when p is an odd prime.
25. Show that if p is prime and a and b are integers not divisible by p, with $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.
26. Use the Pollard $p-1$ method to find a divisor of 689.
27. Use the Pollard $p-1$ method to find a divisor of 7,331,117. (For this exercise, you will need to use either a calculator or computational software.)
28. Show that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
29. Show that if p is prime and a is an integer, then $p \mid (a^p + (p-1)!\,a)$.
30. Show that if p is an odd prime, then $1^2 3^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.
31. Show that if p is prime and $p \equiv 3 \pmod 4$, then $((p-1)/2)! \equiv \pm 1 \pmod{p}$.
32. a) Let p be prime, and suppose that r is a positive integer less than p such that $(-1)^r r! \equiv -1 \pmod{p}$. Show that $(p-r+1)! \equiv -1 \pmod{p}$.
    b) Using part (a), show that $61! \equiv 63! \equiv -1 \pmod{71}$.
33. Using Wilson's theorem, show that if p is a prime and $p \equiv 1 \pmod 4$, then the congruence $x^2 \equiv -1 \pmod{p}$ has two incongruent solutions given by $x \equiv \pm((p-1)/2)! \pmod{p}$.

34. Show that if p is a prime and $0 < k < p$, then $(p-k)!(k-1)! \equiv (-1)^k \pmod{p}$.

35. Show that if n is an integer, then

$$\pi(n) = \sum_{j=2}^{n} \left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j} \right] \right].$$

* **36.** For which positive integers n is $n^4 + 4^n$ prime?

37. Show that the pair of positive integers n and $n+2$ are twin primes if and only if $4((n-1)!+1)+n \equiv 0 \pmod{n(n+2)}$, where $n \neq 1$.

38. Show that if the positive integers n and $n+k$, where $n > k$ and k is an even positive integer, are both prime, then $(k!)^2((n-1)!+1)+n(k!-1)(k-1)! \equiv 0 \pmod{n(n+k)}$.

39. Show that if p is prime, then $\binom{2p}{p} \equiv 2 \pmod{p}$.

40. Exercise 74 of Section 3.5 shows that if p is prime and k is a positive integer less than p, then the binomial coefficient $\binom{p}{k}$ is divisible by p. Use this fact and the binomial theorem to show that if a and b are integers, then $(a+b)^p \equiv a^p + b^p \pmod{p}$.

41. Prove Fermat's little theorem by mathematical induction. (*Hint:* In the induction step, use Exercise 40 to obtain a congruence for $(a+1)^p$.)

* **42.** Using Exercise 30 of Section 4.3, prove *Gauss's generalization of Wilson's theorem,* namely that the product of all the positive integers less than m that are relatively prime to m is congruent to 1 (mod m), unless $m = 4$, p^t, or $2p^t$, where p is an odd prime and t is a positive integer, in which case it is congruent to -1 (mod m).

43. A deck of cards is shuffled by cutting the deck into two piles of 26 cards. Then, the new deck is formed by alternating cards from the two piles, starting with the bottom pile.

a) Show that if a card begins in the cth position in the deck, it will be in the bth position in the new deck, where $b \equiv 2c \pmod{53}$ and $1 \leq b \leq 52$.

b) Determine the number of shuffles of the type described above that are needed to return the deck of cards to its original order.

44. Let p be prime and let a be a positive integer not divisible by p. We define the *Fermat quotient* $q_p(a)$ by $q_p(a) = (a^{p-1} - 1)/p$. Show that if a and b are positive integers not divisible by the prime p, then $q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$.

45. Let p be prime and let $a_1, a_2, \ldots, a_p$ and $b_1, b_2, \ldots, b_p$ be complete systems of residues modulo p. Show that $a_1b_1, a_2b_2, \ldots, a_pb_p$ is not a complete system of residues modulo p.

* **46.** Show that if n is a positive integer with $n \geq 2$, then n does not divide $2^n - 1$.

* **47.** Let p be an odd prime. Show that $(p-1)!^{p^{n-1}} \equiv -1 \pmod{p^n}$.

48. Show that if p is a prime with $p > 5$, then $(p-1)!+1$ has at least two different prime divisors.

49. Show that if a and n are relatively prime integers with $n > 1$, then n is prime if and only if $(x-a)^n$ and $x^n - a$ are congruent modulo n as polynomials. (Recall from the preamble to Exercise 40 in Section 4.1 that two polynomials are congruent modulo n as

polynomials if for each power of x the coefficients of that power in the polynomials are congruent modulo n.) (The proof of Agrawal, Kayal, and Saxena [AgKaSa02] that there is a polynomial-time algorithm for determining whether an integer is prime begins with this result.)

6.1 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. A *Wilson prime* is a prime p for which $(p-1) \equiv -1 \pmod{p^2}$. Find all Wilson primes less than 10,000.
2. Find all primes p less than 10,000 for which $2^{p-1} \equiv 1 \pmod{p^2}$.
3. Find a factor of each of several different odd integers of your choice using the Pollard $p-1$ method.
4. Verify the conjecture that $1^{n-1} + 2^{n-1} + 3^{n-1} + \cdots + (n-1)^{(n-1)} \not\equiv -1 \pmod{n}$ if n is composite, for as many integers n as you can.

Programming Projects

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

1. Find all Wilson primes less than a given positive integer n.
2. Find the primes p less than a given positive integer n for which $2^{p-1} \equiv 1 \pmod{p^2}$.
3. Solve linear congruences with prime moduli via Fermat's little theorem.
4. Factor a given positive integer n using the Pollard $p-1$ method.

6.2 Pseudoprimes

Fermat's little theorem tells us that if n is prime and b is any integer, then $b^n \equiv b \pmod{n}$. Consequently, if we can find an integer b such that $b^n \not\equiv b \pmod{n}$, then we know that n is composite.

Example 6.8. We can show that 63 is not prime by observing that

$$2^{63} = 2^{60} \cdot 2^3 = (2^6)^{10} \cdot 2^3 = 64^{10}2^3 \equiv 2^3 \equiv 8 \not\equiv 2 \pmod{63}. \quad \blacktriangleleft$$

Using Fermat's little theorem, we can show that an integer is composite. It would be even more useful if it also provided a way to show that an integer is prime. It is commonly reported that the ancient Chinese believed that if $2^n \equiv 2 \pmod{n}$, then n must be prime. This statement is true for $1 \leq n \leq 340$. Unfortunately, the converse of Fermat's little theorem is not true, as the following example, which was discovered by Sarrus in 1919, shows.

Example 6.9. Let $n = 341 = 11 \cdot 31$. By Fermat's little theorem, we see that $2^{10} \equiv 1 \pmod{11}$, so that $2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$. Also, $2^{340} = (2^5)^{68} \equiv (32)^{68} \equiv 1 \pmod{31}$. Hence, by Corollary 4.8.1, we have $2^{340} \equiv 1 \pmod{341}$. By multiplying both sides of this congruence by 2, we have $2^{341} \equiv 2 \pmod{341}$, even though 341 is not prime. ◀

Examples such as this lead to the following definition.

Definition. Let b be a positive integer. If n is a composite positive integer and $b^n \equiv b \pmod{n}$, then n is called a *pseudoprime to the base b.*

Note that if $(b, n) = 1$, then the congruence $b^n \equiv b \pmod{n}$ is equivalent to the congruence $b^{n-1} \equiv 1 \pmod{n}$. To see this, note that by Corollary 4.4.1 we can divide both sides of the first congruence by b, because $(b, n) = 1$, to obtain the second congruence. By part (iii) of Theorem 4.3, we can multiply both sides of the second congruence by b to obtain the first. We will often use this equivalent condition.

Example 6.10. The integers $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, and $645 = 3 \cdot 5 \cdot 43$ are pseudoprimes to the base 2, since it is easily verified that $2^{340} \equiv 1 \pmod{341}$, $2^{560} \equiv 1 \pmod{561}$, and $2^{644} \equiv 1 \pmod{645}$. ◀

If there are relatively few pseudoprimes to the base b, then checking to see whether the congruence $b^n \equiv b \pmod{n}$ holds is a useful test; only a small fraction of composite numbers pass this test. In fact, there are far fewer pseudoprimes to the base b not exceeding a specified bound than prime numbers not exceeding that bound. In particular, there are 455,052,511 primes, but only 14,884 pseudoprimes to the base 2, less than 10^{10}. Although pseudoprimes to any given base are rare, there are, nevertheless, infinitely many pseudoprimes to any given base. We will prove this for the base 2. The following lemma is useful in the proof.

Lemma 6.1. If d and n are positive integers such that d divides n, then $2^d - 1$ divides $2^n - 1$.

An Historical Inaccuracy

Apparently, the story that the ancient Chinese believed that n is prime if $2^n \equiv 2 \pmod{n}$ is due to a mistaken translation and an error by a nineteenth-century Chinese mathematician. In 1897, J. H. Jeans reported that this statement dates "from the time of Confucius," which seems to be the result of an erroneous translation from the book *The Nine Chapters of Mathematical Art.* In 1869, Alexander Wade published an article, "A Chinese theorem," in the journal *Notes and Queries on China,* crediting the mathematician Li Shan-Lan (1811–1882) for this "theorem." Li learned that this result was false, but the error was perpetuated by later authors. These historical details come from a letter from Chinese mathematician Man-Keung Siu to Paulo Ribenboim (see [Ri96] for more information).

Proof. Given that $d \mid n$, there is a positive integer t with $dt = n$. By setting $x = 2^d$ in the identity $x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \cdots + 1)$, we find that $2^n - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 2^d + 1)$. Consequently, we have $(2^d - 1) \mid (2^n - 1)$. ∎

We can now prove that there are infinitely many pseudoprimes to the base 2.

Theorem 6.6. There are infinitely many pseudoprimes to the base 2.

Proof. We will show that if n is an odd pseudoprime to the base 2, then $m = 2^n - 1$ is also an odd pseudoprime to the base 2. Because we have at least one odd pseudoprime to the base 2, namely $n_0 = 341$, we will be able to construct infinitely many odd pseudoprimes to the base 2 by taking $n_0 = 341$ and $n_{k+1} = 2^{n_k} - 1$ for $k = 0, 1, 2, 3, \ldots$. These integers are all different, because $n_0 < n_1 < n_2 < \cdots < n_k < n_{k+1} < \cdots$.

To continue the proof, let n be an odd pseudoprime to the base 2, so that n is composite and $2^{n-1} \equiv 1 \pmod{n}$. Because n is composite, we have $n = dt$, with $1 < d < n$ and $1 < t < n$. We will show that $m = 2^n - 1$ is also pseudoprime, by first showing that it is composite, and then by showing that $2^{m-1} \equiv 1 \pmod{m}$.

To see that m is composite, we use Lemma 6.1 to note that $(2^d - 1) \mid (2^n - 1) = m$. To show that $2^{m-1} \equiv 1 \pmod{m}$, note that because $2^n \equiv 2 \pmod{n}$, there is an integer k with $2^n - 2 = kn$. Hence, $2^{m-1} = 2^{2^n - 2} = 2^{kn}$. By Lemma 6.1, it follows that $m = (2^n - 1) \mid (2^{kn} - 1) = 2^{m-1} - 1$. Hence, $2^{m-1} - 1 \equiv 0 \pmod{m}$, so that $2^{m-1} \equiv 1 \pmod{m}$. We conclude that m is also a pseudoprime to the base 2. ∎

If we want to know whether an integer n is prime, and we find that $2^{n-1} \equiv 1 \pmod{n}$, we know that n is either prime or a pseudoprime to the base 2. One follow-up approach is to test n with other bases. That is, we check to see whether $b^{n-1} \equiv 1 \pmod{n}$ for various positive integers b. If we find any values of b with $(b, n) = 1$ and $b^{n-1} \not\equiv 1 \pmod{n}$, then we know that n is composite.

Example 6.11. We have seen that 341 is a pseudoprime to the base 2. Because

$$7^3 = 343 \equiv 2 \pmod{341}$$

and

$$2^{10} = 1024 \equiv 1 \pmod{341},$$

we have

$$\begin{aligned} 7^{340} = (7^3)^{113}7 &\equiv 2^{113}7 = (2^{10})^{11} \cdot 2^3 \cdot 7 \\ &\equiv 8 \cdot 7 \equiv 56 \not\equiv 1 \pmod{341}. \end{aligned}$$

Hence, by the contrapositive of Fermat's little theorem, we see that 341 is composite, because $7^{340} \not\equiv 1 \pmod{341}$. ◀

Carmichael Numbers

Unfortunately, there are composite integers n that cannot be shown to be composite using the above approach, because there are integers that are pseudoprimes to every base, that is, there are composite integers n such that $b^{n-1} \equiv 1 \pmod{n}$, for all b with $(b, n) = 1$. This leads to the following definition.

Definition. A composite integer n that satisfies $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $(b, n) = 1$ is called a *Carmichael number* (after *Robert Carmichael*, who studied them in the early part of the twentieth century) or an *absolute pseudoprime.*

Example 6.12. The integer $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. To see this, note that if $(b, 561) = 1$, then $(b, 3) = (b, 11) = (b, 17) = 1$. Hence, from Fermat's little theorem, we have $b^2 \equiv 1 \pmod{3}$,$b^{10} \equiv 1 \pmod{11}$, and $b^{16} \equiv 1 \pmod{17}$. Consequently, $b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$, $b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$, and $b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$. Therefore, by Corollary 4.8.1, $b^{560} \equiv 1 \pmod{561}$ for all b with $(b, n) = 1$. ◀

In 1912, Carmichael conjectured that there are infinitely many Carmichael numbers. It took 80 years to resolve this conjecture. In 1992, Alford, Granville, and Pomerance showed that Carmichael was correct.[1] Because of the complicated, nonelementary nature of their proof, we will not describe it here. However, we will prove one of the key ingredients, a theorem that can be used to find Carmichael numbers.

Theorem 6.7. If $n = q_1 q_2 \ldots q_k$, where the q_j are distinct primes that satisfy $(q_j - 1) \mid (n - 1)$ for all j and $k > 2$, then n is a Carmichael number.

Proof. Let b be a positive integer with $(b, n) = 1$. Then $(b, q_j) = 1$ for $j = 1, 2, \ldots, k$, and hence, by Fermat's little theorem, $b^{q_j - 1} \equiv 1 \pmod{q_j}$ for $j = 1, 2, \ldots, k$. Because $(q_j - 1) \mid (n - 1)$ for each integer $j = 1, 2, \ldots, k$, there are integers t_j with $t_j(q_j - 1) = n - 1$. Hence, for each j, we know that $b^{n-1} = b^{(q_j-1)t_j} \equiv 1 \pmod{q_j}$. Therefore, by Corollary 4.8.1, we see that $b^{n-1} \equiv 1 \pmod{n}$, and we conclude that n is a Carmichael number. ■

[1] In particular, they showed that $C(x)$, the number of Carmichael numbers not exceeding x, satisfies the inequality $C(x) > x^{2/7}$ for sufficiently large numbers x.

ROBERT DANIEL CARMICHAEL (1879–1967) was born in Goodwater, Alabama. He received his B.A. from Lineville College in 1898 and his Ph.D. in 1911 from Princeton University. Carmichael taught at Indiana University from 1911 to 1915, and at the University of Illinois from 1915 until 1947. His thesis, written under the direction of G. D. Birkhoff, was considered the first significant American contribution to differential equations. Carmichael worked in a wide range of areas, including real analysis, differential equations, mathematical physics, group theory, and number theory.

Example 6.13. Theorem 6.7 shows that $6601 = 7 \cdot 23 \cdot 41$ is a Carmichael number, because 7, 23, and 41 are all prime, $6 = (7-1) \mid 6600$, $22 = (23-1) \mid 6600$, and $40 = (41-1) \mid 6600$. ◀

The converse of Theorem 6.7 is also true, that is, all Carmichael numbers are of the form $q_1 q_2 \cdots q_k$, where the q_j are distinct primes and $(q_j - 1) \mid (n-1)$ for all j. We will prove this fact in Chapter 9.

By the way, we can show that although there are only 43 Carmichael numbers not exceeding 10^6, there are 105,212 of them not exceeding 10^{15}.

Miller's Test

Once the congruence $b^{n-1} \equiv 1 \pmod{n}$, where n is an odd integer, has been verified, another possible approach is to consider the least positive residue of $b^{(n-1)/2}$ modulo n. We note that if $x = b^{(n-1)/2}$, then $x^2 = b^{n-1} \equiv 1 \pmod{n}$. If n is prime, by Theorem 4.11 we know that either $x \equiv 1$ or $x \equiv -1 \pmod{n}$. Consequently, once we have found that $b^{n-1} \equiv 1 \pmod{n}$, we can check to see whether $b^{(n-1)/2} \equiv \pm 1 \pmod{n}$. If this congruence does not hold, then we know that n is composite.

Example 6.14. Let $b = 5$ and let $n = 561$, the smallest Carmichael number. We find that $5^{(561-1)/2} = 5^{280} \equiv 67 \pmod{561}$. Hence, 561 is composite. ◀

To continue developing primality tests, we need the following definitions.

Definition. Let n be a positive integer with $n > 2$ and $n - 1 = 2^s t$, where s is a nonnegative integer and t is an odd positive integer. We say that n passes *Miller's test for the base* b if either $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j with $0 \leq j \leq s-1$.

The following example shows that 2047 passes Miller's test for the base 2.

Example 6.15. Let $n = 2047 = 23 \cdot 89$. Then $2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1 \pmod{2047}$, so that 2047 is a pseudoprime to the base 2. Because $2^{2046/2} = 2^{1023} = (2^{11})^{93} = (2048)^{93} \equiv 1 \pmod{2047}$, 2047 passes Miller's test for the base 2. ◀

We now show that if n is prime, then n passes Miller's test for all bases b with $n \nmid b$.

Theorem 6.8. If n is prime and b is a positive integer with $n \nmid b$, then n passes Miller's test for the base b.

Proof. Let $n - 1 = 2^s t$, where s is a nonnegative integer and t is an odd positive integer. Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$, for $k = 0, 1, 2, \ldots, s$. Because n is prime, Fermat's little theorem tells us that $x_0 = b^{n-1} \equiv 1 \pmod{n}$. By Theorem 4.11, because $x_1^2 = (b^{(n-1)/2})^2 = x_0 \equiv 1 \pmod{n}$, either $x_1 \equiv -1 \pmod{n}$ or $x_1 \equiv 1 \pmod{n}$. If $x_1 \equiv 1 \pmod{n}$, because $x_2^2 = x_1 \equiv 1 \pmod{n}$, either $x_2 \equiv -1 \pmod{n}$ or $x_2 \equiv 1 \pmod{n}$. In general, if we have found that $x_0 \equiv x_1 \equiv x_2 \equiv \cdots \equiv x_k \equiv 1 \pmod{n}$, with $k < s$, then, because $x_{k+1}^2 = x_k \equiv 1 \pmod{n}$, we know that either $x_{k+1} \equiv -1 \pmod{n}$ or $x_{k+1} \equiv 1 \pmod{n}$.

Continuing this procedure for $k = 1, 2, \ldots, s$, we find that either $x_s \equiv 1 \pmod{n}$, or $x_k \equiv -1 \pmod{n}$ for some integer k, with $0 \leq k \leq s$. Hence, n passes Miller's test for the base b. ∎

If the positive integer n passes Miller's test for the base b, then either $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j with $0 \leq j \leq s-1$, where $n - 1 = 2^s t$ and t is odd.

In either case, we have $b^{n-1} \equiv 1 \pmod{n}$, because $b^{n-1} = (b^{2^j t})^{2^{s-j}}$ for $j = 0, 1, 2, \ldots, s$, so that a composite integer n that passes Miller's test for the base b is automatically a pseudoprime to the base b. With this observation, we are led to the following definition.

Definition. If n is composite and passes Miller's test for the base b, then we say n is a *strong pseudoprime to the base b.*

Example 6.16. By Example 6.15, we see that 2047 is a strong pseudoprime to the base 2. ◀

Although strong pseudoprimes are exceedingly rare, there are still infinitely many of them. We demonstrate this for the base 2 with the following theorem.

Theorem 6.9. There are infinitely many strong pseudoprimes to the base 2.

Proof. We shall show that if n is a pseudoprime to the base 2, then $N = 2^n - 1$ is a *strong* pseudoprime to the base 2.

Let n be an odd integer that is a pseudoprime to the base 2. Hence, n is composite, and $2^{n-1} \equiv 1 \pmod{n}$. From this congruence, we see that $2^{n-1} - 1 = nk$ for some integer k; furthermore, k must be odd. We have

$$N - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk;$$

this is the factorization of $N - 1$ into an odd integer and a power of 2.

We now note that

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1 \pmod{N},$$

because $2^n = (2^n - 1) + 1 = N + 1 \equiv 1 \pmod{N}$. This demonstrates that N passes Miller's test.

In the proof of Lemma 6.1, we showed that if n is composite, then $N = 2^n - 1$ also is composite. Hence, N passes Miller's test and is composite, so that N is a strong pseudoprime to the base 2. Because every pseudoprime n to the base 2 yields a strong pseudoprime $2^n - 1$ to the base 2, and because there are infinitely many pseudoprimes to the base 2, we conclude that there are infinitely many strong pseudoprimes to the base 2. ∎

The following observations are useful in combination with Miller's test for checking the primality of relatively small integers. The smallest odd strong pseudoprime to the base 2 is 2047, so that if $n < 2047$, n is odd, and n passes Miller's test to the base 2, then n

is prime. Likewise, 1,373,653 is the smallest odd strong pseudoprime to both the bases 2 and 3, giving us a primality test for integers less than 1,373,653. The smallest odd strong pseudoprime to the bases 2, 3, and 5 is 25,326,001, and the smallest odd strong pseudoprime to all the bases 2, 3, 5, and 7 is 3,215,031,751. Furthermore, there are no other strong pseudoprimes to all these bases that are less than $25 \cdot 10^9$. (The reader should verify these statements.) This leads us to a primality test for integers less than $25 \cdot 10^9$. An odd integer n is prime if $n < 25 \cdot 10^9$, n passes Miller's test for the bases 2, 3, 5, and 7, and $n \neq 3{,}215{,}031{,}751$.

Computations show that there are only 101 integers less than 10^{12} that are strong pseudoprimes to the bases 2, 3, and 5 simultaneously. Only 9 of these are also strong pseudoprimes to the base 7, and none of these is a strong pseudoprime to the base 11. The smallest strong pseudoprime to the bases 2, 3, 5, 7, and 11 simultaneously is 2,152,302,898,747. Therefore, if an odd integer n is prime and $n < 2{,}152{,}302{,}898{,}747$, then n is prime if it passes Miller's test for the bases 2, 3, 5, 7, and 11. If we want to test even bigger integers for primality in this way, we can use the observation that no positive integer less than 341,550,071,728,321 is a strong pseudoprime to the bases 2, 3, 5, 7, 11, 13, and 17. A positive odd integer not exceeding this number is prime if it passes Miller's test for the seven primes, 2, 3, 5, 7, 11, 13, and 17.

There is no analogue to a Carmichael number for strong pseudoprimes. This is a consequence of the following theorem.

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 $1 \leq b \leq n-1$.

We prove Theorem 6.10 in Chapter 9. Note that Theorem 6.10 tells us that if n passes Miller's tests for more than $(n-1)/4$ bases less than n, then n must be prime. However, this is a rather lengthy way to show that a positive integer n is prime, worse than performing trial divisions. Miller's test does give an interesting and quick way of showing that an integer n is "probably prime." To see this, take at random an integer b with $1 \leq b \leq n-1$ (we will see how to make this "random" choice in Chapter 10). From Theorem 6.10, we see that if n is composite, the probability that n passes Miller's test for the base b is less than $1/4$. If we pick k different bases less than n and perform Miller's tests for each of these bases, we are led to the following result.

Theorem 6.11. ***Rabin's Probabilistic Primality Test.*** Let n be a positive integer. Pick k different positive integers less than n and perform Miller's test on n for each of these bases. If n is composite, the probability that n passes all k tests is less than $(1/4)^k$.

Let n be a composite positive integer. Using Rabin's probabilistic primality test, if we pick 100 different integers at random between 1 and n and perform Miller's test for each of these 100 bases, then the probability that n passes all the tests is less than 10^{-60}, an extremely small number. In fact, it may be more likely that a computer error was made than that a composite integer passes all 100 tests. Using Rabin's primality test does not definitely prove that an integer n that passes some large number of tests is prime, but

does give extremely strong, indeed almost overwhelming, evidence that the integer is prime.

There is a famous conjecture in analytic number theory called the *generalized Riemann hypothesis,* which is a statement about the famous Riemann zeta function, named after the German mathematician *Georg Friedrich Bernhard Riemann*, which is discussed in Section 3.2. The following conjecture is a consequence of this hypothesis.

Conjecture 6.1. For every composite positive integer n, there is a base b, with $b < 2(\log_2 n)^2$, such that n fails Miller's test for the base b. ■

If this conjecture is true, as many number theorists believe, the following result provides a rapid primality test.

Theorem 6.12. If the generalized Riemann hypothesis is valid, then there is an algorithm to determine whether a positive integer n is prime using $O((\log_2 n)^5)$ bit operations.

Proof. Let b be a positive integer less than n. To perform Miller's test for the base b on n takes $O((\log_2 n)^3)$ bit operations, because this test requires that we perform no more than $\log_2 n$ modular exponentiations, each using $O((\log_2 b)^2)$ bit operations. Assume that the generalized Riemann hypothesis is true. If n is composite, then by Conjecture 6.1, there is a base b with $1 < b < 2(\log_2 n)^2$ such that n fails Miller's test for b. To discover this b requires less than $O((\log_2 n)^3) \cdot O((\log_2 n)^2) = O((\log_2 n)^5)$ bit operations. Hence, using $O((\log_2 n)^5)$ bit operations, we can determine whether n is composite or prime. ■

The important point about Rabin's probabilistic primality test and Theorem 6.12 is that both results indicate that it is possible to check an integer n for primality using only $O((\log_2 n)^k)$ bit operations, where k is a positive integer. (Also, the recent result of Agrawal, Kayal, and Saxena [AgKaSa02] shows that there is a deterministic test using $O\left((\log_2 n)^k\right)$ bit operations.) This contrasts strongly with the problem of factoring. The best algorithm known for factoring an integer requires a number of bit operations

GEORG FRIEDRICH BERNHARD RIEMANN (1826–1866), the son of a minister, was born in Breselenz, Germany. His elementary education came from his father. After completing his secondary education, he entered Göttingen University to study theology. However, he also attended lectures on mathematics. After receiving the approval of his father to concentrate on mathematics, Riemann transfered to Berlin University where he studied under several prominent mathematicians, including Dirichlet and Jacobi. He subsequently returned to Göttingen where he obtained his Ph.D.

Riemann was one of the most imaginative and creative mathematicians of all time. He made fundamental contributions to geometry, mathematical physics, and analysis. He wrote only one paper on number theory, which was eight pages long, but this paper has had tremendous impact. Riemann died of tuberculosis at the early age of 39.

exponential in the square root of the logarithm of the number of bits in the integer being factored, whereas primality testing seems to require only a number of bit operations less than a polynomial in the number of bits of the integer tested. We capitalize on this difference by presenting a recently invented cipher system in Chapter 8.

6.2 Exercises

1. Show that 91 is a pseudoprime to the base 3.
2. Show that 45 is a pseudoprime to the bases 17 and 19.
3. Show that the even integer $n = 161{,}038 = 2 \cdot 73 \cdot 1103$ satisfies the congruence $2^n \equiv 2 \pmod{n}$. The integer 161,038 is the smallest even pseudoprime to the base 2.
4. Show that every odd composite integer is a pseudoprime to both the base 1 and the base -1.
5. Show that if n is an odd composite integer and n is a pseudoprime to the base a, then n is a pseudoprime to the base $n - a$.

* 6. Show that if $n = (a^{2p} - 1)/(a^2 - 1)$, where a is an integer, $a > 1$, and p is an odd prime not dividing $a(a^2 - 1)$, then n is a pseudoprime to the base a. Conclude that there are infinitely many pseudoprimes to any base a. (*Hint*: To establish that $a^{n-1} \equiv 1 \pmod{n}$, show that $2p \mid (n - 1)$, and demonstrate that $a^{2p} \equiv 1 \pmod{n}$.)

7. Show that every composite Fermat number $F_m = 2^{2^m} + 1$ is a pseudoprime to the base 2.
8. Show that if p is prime and $2^p - 1$ is composite, then $2^p - 1$ is a pseudoprime to the base 2.
9. Show that if n is a pseudoprime to the bases a and b, then n is also a pseudoprime to the base ab.
10. Suppose that a and n are relatively prime positive integers. Show that if n is a pseudoprime to the base a, then n is a pseudoprime to the base $\overline{a}$, where $\overline{a}$ is an inverse of a modulo n.
11. a) Show that if n is a pseudoprime to the base a, but not a pseudoprime to the base b, where $(a, n) = (b, n) = 1$, then n is not a pseudoprime to the base ab.
    b) Show that if there is an integer b with $(b, n) = 1$ such that n is not a pseudoprime to the base b, then n is a pseudoprime to less than or equal to $\phi(n)$ different bases a with $1 \leq a < n$, where $\phi(n)$ is the number of positive integers not exceeding n that are relatively prime to n. (*Hint*: Show that the sets $a_1, a_2, \ldots, a_r$ and $ba_1, ba_2, \ldots, ba_r$ have no common elements, where $a_1, a_2, \ldots, a_r$ are the bases less than n to which n is a pseudoprime.)
12. Show that 25 is a strong pseudoprime to the base 7.
13. Show that 1387 is a pseudoprime, but not a strong pseudoprime, to the base 2.
14. Show that 1,373,653 is a strong pseudoprime to both bases 2 and 3.
15. Show that 25,326,001 is a strong pseudoprime to bases 2, 3, and 5.

16. Show that the following integers are Carmichael numbers.
    a) $2821 = 7 \cdot 13 \cdot 31$
    b) $10{,}585 = 5 \cdot 29 \cdot 73$
    c) $29{,}341 = 13 \cdot 37 \cdot 61$
    d) $314{,}821 = 13 \cdot 61 \cdot 397$
    e) $278{,}545 = 5 \cdot 17 \cdot 29 \cdot 113$
    f) $172{,}081 = 7 \cdot 13 \cdot 31 \cdot 61$
    g) $564{,}651{,}361 = 43 \cdot 3361 \cdot 3907$

17. Find a Carmichael number of the form $7 \cdot 23 \cdot q$, where q is an odd prime other than $q = 41$, or show that there are no others.

18. a) Show that every integer of the form $(6m + 1)(12m + 1)(18m + 1)$, where m is a positive integer such that $6m + 1$, $12m + 1$, and $18m + 1$ are all primes, is a Carmichael number.
    b) Conclude from part (a) that $1729 = 7 \cdot 13 \cdot 19$; $294{,}409 = 37 \cdot 73 \cdot 109$; $56{,}052{,}361 = 211 \cdot 421 \cdot 631$; $118{,}901{,}521 = 271 \cdot 541 \cdot 811$; and $172{,}947{,}529 = 307 \cdot 613 \cdot 919$ are Carmichael numbers.

19. The smallest Carmichael number with six prime factors is $5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137 = 321{,}197{,}185$. Verify that this number is a Carmichael number.

* 20. Show that if n is a Carmichael number, then n is square-free.

21. Show that if n is a positive integer with $n \equiv 3 \pmod 4$, then Miller's test takes $O((\log_2 n)^3)$ bit operations.

6.2 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. Determine for which positive integers n, $n \leq 100$, the integer $n \cdot 2^n - 1$ is prime.
2. Find as many Carmichael numbers of the form $(6m + 1)(12m + 1)(18m + 1)$, where $6m + 1$, $12m + 1$, and $18m + 1$ are all prime, as you can.
3. Find as many even pseudoprimes to the base 2 that are the product of three primes as you can. Do you think that there are infinitely many?
4. The integers of the form $n \cdot 2^n + 1$, where n is a positive integer greater than 1, are called *Cullen numbers.* Can you find a prime Cullen number?

Programming Projects

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

1. Given a positive integer n, determine whether n satisfies the congruence $b^{n-1} \equiv 1 \pmod n$, where b is a positive integer less than n; if it does, then n is either a prime or a pseudoprime to the base b.

2. Given a positive integer n, determine whether n passes Miller's test to the base b; if it does, then n is either prime or a strong pseudoprime to the base b.
3. Perform a primality test for integers less than $25 \cdot 10^9$ based on Miller's test for the bases 2, 3, 5, and 7. (Use the remarks that follow Theorem 6.9.)
4. Perform a primality test for integers less than 2,152,302,898,747 based on Miller's test for the bases 2, 3, 5, 7, and 11. (Use the remarks that follow Theorem 6.9.)
5. Perform a primality test for integers less than 341,550,071,728,321 based on Miller's test for the bases 2, 3, 5, 7, 11, 13, and 17. (Use the remarks that follow Theorem 6.9.)
6. Given an odd positive integer n, determine whether n passes Rabin's probabilistic primality test.
7. Given a positive integer n, find all Carmichael numbers less than a given integer n.

6.3 Euler's Theorem

Fermat's little theorem tells us how to work with certain congruences involving exponents when the modulus is a prime. How do we work with the corresponding congruences modulo a composite integer?

For this purpose, we would like to establish a congruence analogous to that provided by Fermat's little theorem for composite integers. As mentioned in Section 6.1, the great Swiss mathematician *Leonhard Euler* published a proof of Fermat's little theorem in 1736. In 1760, Euler managed to find a natural generalization of the congruence in Fermat's little theorem that holds for composite integers. Before introducing this result, we need to define a special counting function (introduced by Euler) used in the theorem.

Definition. Let n be a positive integer. The *Euler phi-function* $\phi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.

In Table 6.1, we display the values of $\phi(n)$ for $1 \leq n \leq 12$. The values of $\phi(n)$ for $1 \leq n \leq 100$ are given in Table 2 of Appendix E.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Table 6.1 *The values of Euler's phi-function for* $1 \leq n \leq 12$.

In Chapter 7, we study the Euler phi-function further. In this section, we use the phi-function to give an analogue of Fermat's little theorem for composite moduli. To do this, we need to lay some groundwork.

Definition. A *reduced residue system modulo n* is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.

Example 6.17. The set $1, 3, 5, 7$ is a reduced residue system modulo 8. The set $-3, -1, 1, 3$ is also such a set. ◀

We will need the following theorem about reduced residue systems.

Theorem 6.13. If $r_1, r_2, \ldots, r_{\phi(n)}$ is a reduced residue system modulo n, and if a is a positive integer with $(a, n) = 1$, then the set $ar_1, ar_2, \ldots, ar_{\phi(n)}$ is also a reduced residue system modulo n.

Proof. To show that each integer ar_j is relatively prime to n, we assume that $(ar_j, n) > 1$. Then, there is a prime divisor p of (ar_j, n). Hence, either $p \mid a$ or $p \mid r_j$. Thus, we have either $p \mid a$ and $p \mid n$, or $p \mid r_j$ and $p \mid n$. However, we cannot have both $p \mid r_j$ and $p \mid n$, because r_j is a member of a reduced residue system modulo n, and both $p \mid a$ and $p \mid n$ cannot hold because $(a, n) = 1$. Hence, we can conclude that ar_j and n are relatively prime for $j = 1, 2, \ldots, \phi(n)$.

To demonstrate that no two ar_j are congruent modulo n, we assume that $ar_j \equiv ar_k \pmod{n}$, where j and k are distinct positive integers with $1 \leq j \leq \phi(n)$ and $1 \leq k \leq \phi(n)$. Because $(a, n) = 1$, by Corollary 4.4.1 we see that $r_j \equiv r_k \pmod{n}$. This is a contradiction, because r_j and r_k come from the original set of reduced residues modulo n, so that $r_j \not\equiv r_k \pmod{n}$. ■

We illustrate the use of Theorem 6.13 by the following example.

LEONHARD EULER (1707–1783) was the son of a minister from the vicinity of Basel, Switzerland, who, besides theology, had also studied mathematics. At 13, Euler entered the University of Basel with the aim of pursuing a career in theology, as his father wished. At the university, Euler was tutored in mathematics by Johann Bernoulli, of the famous Bernoulli family of mathematicians, and became friends with Johann's sons Nicklaus and Daniel. His interest in mathematics led him to abandon his plans to follow in his father's footsteps. Euler obtained his master's degree in philosophy at the age of 16. In 1727, Peter the Great invited Euler to join the Imperial Academy in St. Petersburg, at the insistence of Nicklaus and Daniel Bernoulli, who had entered the academy in 1725 when it was founded. Euler spent the years 1727–1741 and 1766–1783 at the Imperial Academy. He spent the interval 1741–1766 at the Royal Academy of Berlin. Euler was incredibly prolific; he wrote more than 700 books and papers, and he left so much unpublished work that the Imperial Academy did not finish publication of Euler's work for 47 years after his death. During his life, his papers accumulated so rapidly that he kept a pile of papers to be published for the academy. They published the top papers in the pile first, so that later results were published before results they superseded or depended on. Euler was blind for the last 17 years of his life, but had a fantastic memory, so that his blindness did not deter his mathematical output. He also had 13 children, and was able to continue his research while a child or two bounced on his knees. The publication of the collected works and letters of Euler, the *Opera Omnia*, by the Swiss Academy of Science will require more than 85 large volumes, of which 76 have aleady been published (as of late 1999).

Example 6.18. The set $1, 3, 5, 7$ is a reduced residue system modulo 8. Because $(3, 8) = 1$, from Theorem 6.13, the set $3 \cdot 1 = 3, 3 \cdot 3 = 9, 3 \cdot 5 = 15, 3 \cdot 7 = 21$ is also a reduced residue system modulo 8. ◀

We now state Euler's theorem.

Theorem 6.14. ***Euler's Theorem.*** If m is a positive integer and a is an integer with $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Before we prove Euler's theorem, we illustrate the idea behind the proof with an example.

Example 6.19. We know that both the sets $1, 3, 5, 7$ and $3 \cdot 1, 3 \cdot 3, 3 \cdot 5, 3 \cdot 7$ are reduced residue systems modulo 8. Hence, they have the same least positive residues modulo 8. Therefore,

$$(3 \cdot 1) \cdot (3 \cdot 3) \cdot (3 \cdot 5) \cdot (3 \cdot 7) \equiv 1 \cdot 3 \cdot 5 \cdot 7 \pmod{8},$$

and

$$3^4 \cdot 1 \cdot 3 \cdot 5 \cdot 7 \equiv 1 \cdot 3 \cdot 5 \cdot 7 \pmod{8}.$$

Because $(1 \cdot 3 \cdot 5 \cdot 7, 8) = 1$, we conclude that

$$3^4 = 3^{\phi(8)} \equiv 1 \pmod{8}.$$ ◀

We now use the ideas illustrated by this example to prove Euler's theorem.

Proof. Let $r_1, r_2, \ldots, r_{\phi(m)}$ denote the reduced residue system made up of the positive integers not exceeding m that are relatively prime to m. By Theorem 6.13, because $(a, m) = 1$, the set $ar_1, ar_2, \ldots, ar_{\phi(m)}$ is also a reduced residue system modulo m. Hence, the least positive residues of $ar_1, ar_2, \ldots, ar_{\phi(m)}$ must be the integers $r_1, r_2, \ldots, r_{\phi(m)}$, in some order. Consequently, if we multiply together all terms in each of these reduced residue systems, we obtain

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Thus,

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Because $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, from Corollary 4.4.1, we can conclude that $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

We can use Euler's theorem to find inverses modulo m. If a and m are relatively prime, we know that

$$a \cdot a^{\phi(m)-1} = a^{\phi(m)} \equiv 1 \pmod{m}.$$

Hence, $a^{\phi(m)-1}$ is an inverse of a modulo m.

Example 6.20. We know that $2^{\phi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod 9$ is an inverse of 2 modulo 9. ◀

We can solve linear congruences using this observation. To solve $ax \equiv b \pmod m$, where $(a, m) = 1$, we multiply both sides of this congruence by $a^{\phi(m)-1}$ to obtain

$$a^{\phi(m)-1}ax \equiv a^{\phi(m)-1}b \pmod m.$$

Therefore, the solutions are those integers x such that $x \equiv a^{\phi(m)-1}b \pmod m$.

Example 6.21. The solutions of $3x \equiv 7 \pmod{10}$ are given by $x \equiv 3^{\phi(10)-1} \cdot 7 \equiv 3^3 \cdot 7 \equiv 9 \pmod{10}$, because $\phi(10) = 4$. ◀

6.3 Exercises

1. Find a reduced residue system modulo each of the following integers.

   a) 6 b) 9 c) 10 d) 14 e) 16 f) 17

2. Find a reduced residue system modulo 2^m, where m is a positive integer.

3. Show that if $c_1, c_2, \ldots, c_{\phi(m)}$ is a reduced residue system modulo m, where m is a positive integer with $m \neq 2$, then $c_1 + c_2 + \cdots + c_{\phi(m)} \equiv 0 \pmod m$.

4. Show that if a and m are positive integers with $(a, m) = (a - 1, m) = 1$, then $1 + a + a^2 + \ldots + a^{\phi(m)-1} \equiv 0 \pmod m$.

5. Find the last digit of the decimal expansion of 3^{1000}.

6. Find the last digit of the decimal expansion of $7^{999,999}$.

7. Use Euler's theorem to find the least positive residue of $3^{100,000}$ modulo 35.

8. Show that if a is an integer such that a is not divisible by 3 or such that a is divisible by 9, then $a^7 \equiv a \pmod{63}$.

9. Show that if a is an integer relatively prime to 32,760, then $a^{12} \equiv 1 \pmod{32{,}760}$.

10. Show that $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$, if a and b are relatively prime positive integers.

11. Solve each of the following linear congruences using Euler's theorem.

    a) $5x \equiv 3 \pmod{14}$ b) $4x \equiv 7 \pmod{15}$ c) $3x \equiv 5 \pmod{16}$

12. Show that the solutions to the simultaneous system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

    where the m_j are pairwise relatively prime, are given by

$$x \equiv a_1 M_1^{\phi(m_1)} + a_2 M_2^{\phi(m_2)} + \cdots + a_r M_r^{\phi(m_r)} \pmod M,$$

    where $M = m_1 m_2 \cdots m_r$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, r$.

13. Use Exercise 12 to solve each of the systems of congruences in Exercise 4 of Section 4.3.
14. Use Exercise 12 to solve the system of congruences in Exercise 5 of Section 4.3.
15. Use Euler's theorem to find the last digit in the decimal expansion of 7^{1000}.
16. Use Euler's theorem to find the last digit in the hexadecimal expansion of $5^{1,000,000}$.
17. Find $\phi(n)$ for the integers n with $13 \leq n \leq 20$.
18. Show that every positive integer relatively prime to 10 divides infinitely many repunits (see the preamble to Exercise 11 of Section 5.1). (*Hint:* Note that the n-digit repunit $111\ldots11 = (10^n - 1)/9$.)
19. Show that every positive integer relatively prime to b divides infinitely many base b repunits (see the preamble to Exercise 15 of Section 5.1).

* 20. Show that if m is a positive integer, $m > 1$, then $a^m \equiv a^{m-\phi(m)} \pmod{m}$ for all positive integers a.

6.3 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 $\phi(n)$ for all integers n less than 1000. What conjectures can you make about the values of $\phi(n)$?
2. Let $\Phi(n) = \sum_{i=1}^{n} \phi(n)$. Investigate the value of $\Phi(n)/n^2$ for increasingly large values of n, such as $n = 100$, $n = 1000$, and $n = 10{,}000$. Can you make a conjecture about the limit of this ratio as n grows large without bound?

Programming Projects

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

1. Construct a reduced residue system modulo n for a given positive integer n.
2. Solve linear congruences using Euler's theorem.
3. Find the solutions of a simultaneous system of linear congruences using Euler's theorem and the Chinese remainder theorem (see Exercise 12).

7 Multiplicative Functions

Introduction

In this chapter, we will study a special class of functions on the set of integers called *multiplicative functions*. A multiplicative function has the property that its value at an integer is the product of its values at each of the prime powers in its prime-power factorization. We will show that some important functions are multiplicative, including the number of divisors function, the sum of divisors function, and the Euler phi-function. We will use the fact that each of these functions is multiplicative to obtain a closed formula for the value of these functions at a positive integer n based on the prime-power factorization of n.

Furthermore, we will study a special type of positive integer, called a *perfect number*, which is equal to the sum of its proper divisors. We will show that all even perfect numbers are generated by a special kind of prime, called a Mersenne prime, which is a prime that is 1 less than a power of 2. The quest for new Mersenne primes has been under way since ancient times, accelerated by the invention of powerful computers, and accelerated even more with the advent of the Internet.

We will also show how the summatory function of an arithmetic function can be used to obtain information about the function itself. The summatory function of a function f takes a value at n equal to the sum of the values of f at each of the positive divisors of n. The famous Möbius inversion formula shows how to obtain the values of f from the values of its summatory function.

7.1 The Euler Phi-Function

The Euler phi-function has the property that its value at an integer n is the product of the values of the Euler phi-function at the prime powers that occur in the factorization of n. Functions with this property are called multiplicative; such functions arise throughout

number theory. In this section, we will show that the Euler phi-function is multiplicative. From this fact, we will derive a formula for its values based on prime factorizations. Later in this chapter we will study other multiplicative functions, including the number of divisors function and the sum of divisors function.

We first present some definitions.

Definition. An *arithmetic function* is a function that is defined for all positive integers.

Throughout this chapter, we are interested in arithmetic functions that have a special property.

Definition. An arithmetic function f is called *multiplicative* if $f(mn) = f(m)f(n)$ whenever m and n are relatively prime positive integers. It is called *completely multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m and n.

Example 7.1. The function $f(n) = 1$ for all n is completely multiplicative, and hence also multiplicative, because $f(mn) = 1$, $f(m) = 1$, and $f(n) = 1$, so that $f(mn) = f(m)f(n)$. Similarly, the function $g(n) = n$ is completely multiplicative, and hence multiplicative, since $g(mn) = mn = g(m)g(n)$. ◀

If f is a multiplicative function, then we can find a simple formula for $f(n)$ given the prime-power factorization of n. This result is particularly useful, because it shows us how to find $f(n)$ from the values of $f(p_i^{a_i})$ for $i = 1, 2, \ldots, s$, where $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ is the prime-power factorization of n.

Theorem 7.1. If f is a multiplicative function and if $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ is the prime-power factorization of the positive integer n, then $f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_s^{a_s})$.

Proof. We will prove this theorem using mathematical induction on the number of different primes in the prime factorization of the integer n. If n has one prime in its prime-power factorization, then $n = p_1^{a_1}$ for some prime p_1, and it follows that the result is trivially true.

Suppose that the theorem is true for all integers with k different primes in their prime-power factorization. Now suppose that n has $k + 1$ different primes in its prime-power factorization, say $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}p_{k+1}^{a_{k+1}}$. Because f is multiplicative and $(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}, p_{k+1}^{a_{k+1}}) = 1$, we see that $f(n) = f(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k})f(p_{k+1}^{a_{k+1}})$. By the inductive hypothesis, we know that $f(p_1^{a_1}p_2^{a_2}p_3^{a_3}\cdots p_k^{a_k}) = f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3})\cdots f(p_k^{a_k})$. It follows that $f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_k^{a_k})f(p_{k+1}^{a_{k+1}})$. This completes the inductive proof. ■

We now return to the Euler phi-function. We first consider its values at primes and then at prime powers.

Theorem 7.2. If p is prime, then $\phi(p) = p - 1$. Conversely, if p is a positive integer with $\phi(p) = p - 1$, then p is prime.

Proof. If p is prime, then every positive integer less than p is relatively prime to p. Because there are $p-1$ such integers, we have $\phi(p) = p-1$. Conversely, if p is not prime, then $p = 1$ or p is composite. If $p = 1$, then $\phi(p) \neq p-1$ because $\phi(1) = 1$. If p is composite, then p has a divisor d with $1 < d < p$, and, of course, p and d are not relatively prime. Because we know that at least one of the $p-1$ integers $1, 2, \ldots, p-1$, namely d, is not relatively prime to p, $\phi(p) \leq p-2$. Hence, if $\phi(p) = p-1$, then p must be prime. ∎

We now find the values of the phi-function at prime powers.

Theorem 7.3. Let p be a prime and a a positive integer. Then $\phi(p^a) = p^a - p^{a-1}$.

Proof. The positive integers less than p^a that are not relatively prime to p are those integers not exceeding p^a that are divisible by p. These are the integers kp, where $1 \leq k \leq p^{a-1}$. Since there are exactly p^{a-1} such integers, there are $p^a - p^{a-1}$ integers less than p^a that are relatively prime to p^a. Hence, $\phi(p^a) = p^a - p^{a-1}$. ∎

Example 7.2. Using Theorem 7.3, we find that $\phi(5^3) = 5^3 - 5^2 = 100$, $\phi(2^{10}) = 2^{10} - 2^9 = 512$, and $\phi(11^2) = 11^2 - 11 = 110$. ◀

To find a formula for $\phi(n)$, given the prime factorization of n, it suffices to show that ϕ is multiplicative. We illustrate the idea behind the proof with the following example.

Example 7.3. Let $m = 4$ and $n = 9$, so that $mn = 36$. We list the integers from 1 to 36 in a rectangular chart, as shown in Figure 7.1.

(1)	(5)	9	(13)	(17)	21	(25)	(29)	33
2	6	10	14	18	22	26	30	34
3	(7)	(11)	15	(19)	(23)	27	(31)	(35)
4	8	12	16	20	24	28	32	36

Figure 7.1 *Demonstrating that* $\phi(36) = \phi(4)\phi(9)$.

Neither the second nor the fourth row contains integers relatively prime to 36, since each element in these rows is not relatively prime to 4, and hence not relatively prime to 36. We enclose the other two rows; each element of these rows is relatively prime to 4. Within each of these rows, there are 6 integers relatively prime to 9. We circle these; they are the 12 integers in the list relatively prime to 36. Hence, $\phi(36) = 2 \cdot 6 = \phi(4)\phi(9)$. ◀

We now state and prove the theorem that shows that ϕ is multiplicative.

Theorem 7.4. Let m and n be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

Proof. We display the positive integers not exceeding mn in the following way.

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\ \vdots & \vdots & \vdots & & \vdots \\ r & m+r & 2m+r & \dots & (n-1)m+r \\ \vdots & \vdots & \vdots & & \vdots \\ m & 2m & 3m & \dots & mn \end{array}$$

Now, suppose that r is a positive integer not exceeding m, and suppose that $(m, r) = d > 1$. Then no number in the rth row is relatively prime to mn, because any element of this row is of the form $km + r$, where k is an integer with $1 \leq k \leq n - 1$, and $d \mid (km + r)$, because $d \mid m$ and $d \mid r$.

Consequently, to find those integers in the display that are relatively prime to mn, we need to look at the rth row only if $(m, r) = 1$. If $(m, r) = 1$ and $1 \leq r \leq m$, we must determine how many integers in this row are relatively prime to mn. The elements in this row are $r, m + r, 2m + r, \dots, (n - 1)m + r$. Because $(r, m) = 1$, each of these integers is relatively prime to m. By Theorem 4.6 the n integers in the rth row form a complete system of residues modulo n. Hence, exactly $\phi(n)$ of these integers are relatively prime to n. Because these $\phi(n)$ integers are also relatively prime to m, they are relatively prime to mn.

Because there are $\phi(m)$ rows, each containing $\phi(n)$ integers relatively prime to mn, we can conclude that $\phi(mn) = \phi(m)\phi(n)$. ∎

Combining Theorems 7.3 and 7.4, we derive the following formula for $\phi(n)$.

Theorem 7.5. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime-power factorization of the positive integer n. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Proof. Because ϕ is multiplicative, Theorem 7.1 tells us that

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k}).$$

In addition, by Theorem 7.3, we know that

$$\phi(p_j^{a_j}) = p_j^{a_j} - p_j^{a_j - 1} = p_j^{a_j}\left(1 - \frac{1}{p_j}\right)$$

for $j = 1, 2, \dots, k$. Hence,

$$\begin{aligned}\phi(n) &= p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{a_k}\left(1-\frac{1}{p_k}\right)\\ &= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

This is the desired formula for $\phi(n)$. ■

We illustrate the use of Theorem 7.5 by the following example.

Example 7.4. Using Theorem 7.5, we note that

$$\phi(100) = \phi(2^2 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$$

and

$$\phi(720) = \phi(2^4 3^2 5) = 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 192.$$ ◀

Note that $\phi(n)$ is even except when $n = 2$, as the following theorem shows.

Theorem 7.6. Let n be a positive integer greater than 2. Then $\phi(n)$ is even.

Proof. Suppose that $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ is the prime-power factorization of n. Because ϕ is multiplicative, it follows that $\phi(n) = \prod_{j=1}^{s}\phi(p_j^{a_j})$. By Theorem 7.3, we know that $\phi(p_j^{a_j}) = p_j^{a_j-1}(p_j - 1)$. We can see that $\phi(p_j^{a_j})$ is even if p_j is an odd prime, because then $p_j - 1$ is even; or if $p_j = 2$ and $a_j > 1$, because then $p_j^{a_j-1}$ is even. Given that $n > 2$, at least one of these two conditions holds, so that $\phi(p_j^{a_j})$ is even for at least one integer j, $1 \le j \le s$. We conclude that $\phi(n)$ is even. ■

Let f be an arithmetic function. Then

$$F(n) = \sum_{d|n} f(d)$$

represents the sum of the values of f at all the positive divisors of n. The function F is called the *summatory function* of f.

Example 7.5. If f is an arithmetic function with summatory function F, then

$$F(12) = \sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12).$$

For instance, if $f(d) = d^2$ and F is the summatory function of f, then $F(12) = 210$, because

$$\begin{aligned}\sum_{d|12} d^2 &= 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2\\ &= 1 + 4 + 9 + 16 + 36 + 144 = 210.\end{aligned}$$ ◀

The following result, which states that n is the sum of the values of the phi-function at all the positive divisors of n, will also be useful in the sequel. It says that the summatory function of $\phi(n)$ is the identity function, that is, the function whose value at n is just n.

Theorem 7.7. Let n be a positive integer. Then

$$\sum_{d|n} \phi(d) = n.$$

Proof. We split the set of integers from 1 to n into classes. Put the integer m into the class C_d if the greatest common divisor of m and n is d. We see that m is in C_d, that is, $(m, n) = d$, if and only if $(m/d, n/d) = 1$. Hence, the number of integers in C_d is the number of positive integers not exceeding n/d that are relatively prime to the integer n/d. From this observation, we see that there are $\phi(n/d)$ integers in C_d. Because we divided the integers 1 to n into disjoint classes and each integer is in exactly one class, n is the sum of the numbers of elements in the different classes. Consequently, we see that

$$n = \sum_{d|n} \phi(n/d).$$

As d runs through the positive integers that divide n, n/d also runs through these divisors, so that

$$n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

This proves the theorem. ∎

Example 7.6. We illustrate the proof of Theorem 7.7 when $n = 18$. The integers from 1 to 18 can be split into classes C_d, where $d \mid 18$ such that the class C_d contains those integers m with $(m, 18) = d$. We have

$$\begin{aligned} C_1 &= \{1, 5, 7, 11, 13, 17\} & C_6 &= \{6, 12\} \\ C_2 &= \{2, 4, 8, 10, 14, 16\} & C_9 &= \{9\} \\ C_3 &= \{3, 15\} & C_{18} &= \{18\}. \end{aligned}$$

We see that the class C_d contains $\phi(18/d)$ integers, as the six classes contain $\phi(18) = 6$, $\phi(9) = 6$, $\phi(6) = 2$, $\phi(3) = 2$, $\phi(2) = 1$, and $\phi(1) = 1$ integers, respectively. We note that $18 = \phi(18) + \phi(9) + \phi(6) + \phi(3) + \phi(2) + \phi(1) = \sum_{d|18} \phi(d)$. ◀

A useful tool for finding all positive integers n with $\phi(n) = k$, where k is a positive integer, is the equation $\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$, where the prime-power factorization of n is $n = \prod_{i=1}^{k} p_i^{a_i}$. This is illustrated in the following example.

Example 7.7. What are the solutions to the equation $\phi(n) = 8$, where n is a positive integer? Suppose that the prime-power factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Because

$$\phi(n) = \prod_{j=1}^{k} p_j^{a_j - 1}(p_j - 1),$$

the equation $\phi(n) = 8$ implies that no prime exceeding 9 divides n (otherwise $\phi(n) > p_j - 1 > 8$). Furthermore, 7 cannot divide n because if it did, $7 - 1 = 6$ would be a factor of $\phi(n)$. It follows that $n = 2^a 3^b 5^c$, where a, b, and c are nonnegative integers. We can also conclude that $b = 0$ or $b = 1$ and that $c = 0$ or $c = 1$; otherwise, 3 or 5 would divide $\phi(n) = 8$.

To find all solutions we need only consider four cases. When $b = c = 0$, we have $n = 2^a$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1}$, which means that $a = 4$ and $n = 16$. When $b = 0$ and $c = 1$, we have $n = 2^a \cdot 5$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1} \cdot 4$, so $a = 2$ and $n = 20$. When $b = 1$ and $c = 0$, we have $n = 2^a \cdot 3$, where $a \geq 1$. This implies that $\phi(n) = 2^{a-1} \cdot 2 = 2^a$, so $a = 3$ and $n = 24$. Finally, when $b = 1$ and $c = 1$, we have $n = 2^a \cdot 3 \cdot 5$. We need to consider the case where $a = 0$, as well as the case where $a \geq 1$. When $a = 0$, we have $n = 15$, which is a solution because $\phi(15) = 8$. When $a \geq 1$, we have $\phi(n) = 2^{a-1} \cdot 2 \cdot 4 = 2^{a+2}$. This means that $a = 1$ and $n = 30$. Putting everything together, we see that all the solutions to $\phi(n) = 8$ are $n = 15, 16, 20, 24$ and 30. ◀

7.1 Exercises

1. Determine whether each of the following arithmetic functions is completely multiplicative. Prove your answers.

   a) $f(n) = 0$ d) $f(n) = \log n$ g) $f(n) = n + 1$
   b) $f(n) = 2$ e) $f(n) = n^2$ h) $f(n) = n^n$
   c) $f(n) = n/2$ f) $f(n) = n!$ i) $f(n) = \sqrt{n}$

2. Find the value of the Euler phi-function at each of the following integers.

   a) 100 d) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
   b) 256 e) 10!
   c) 1001 f) 20!

3. Show that $\phi(5186) = \phi(5187) = \phi(5188)$.

4. Find all positive integers n such that $\phi(n)$ has each of the following values. Be sure to prove that you have found all solutions.

   a) 1 b) 2 c) 3 d) 4

5. Find all positive integers n such that $\phi(n) = 6$. Be sure to prove that you have found all solutions.

6. Find all positive integers n such that $\phi(n) = 12$. Be sure to prove that you have found all solutions.

7. Find all positive integers n such that $\phi(n) = 24$. Be sure to prove that you have found all solutions.

8. Show that there is no positive integer n such that $\phi(n) = 14$.

9. Can you find a rule involving the Euler phi-function for producing the terms of the sequence 1, 2, 2, 4, 4, 4, 6, 8, 6, . . .?

10. Can you find a rule involving the Euler phi-function for producing the terms of the sequence 2, 3, 0, 4, 0, 4, 0, 5, 0, . . .?

11. For which positive integers n does $\phi(3n) = 3\phi(n)$?

12. For which positive integers n is $\phi(n)$ divisible by 4?

13. For which positive integers n is $\phi(n)$ equal to $n/2$?

14. For which positive integers n does $\phi(n) \mid n$?

15. Show that if n is a positive integer, then

$$\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd;} \\ 2\phi(n) & \text{if } n \text{ is even.} \end{cases}$$

16. Show that if n is a positive integer having k distinct odd prime divisors, then $\phi(n)$ is divisible by 2^k.

17. For which positive integers n is $\phi(n)$ a power of 2?

18. Show that if n is an odd integer, then $\phi(4n) = 2\phi(n)$.

19. Show that if $n = 2\phi(n)$, where n is a positive integer, then $n = 2^j$ for some positive integer j.

20. Let p be prime. Show that $p \nmid n$, where n is a positive integer, if and only if $\phi(np) = (p-1)\phi(n)$.

21. Show that if m and n are positive integers and $(m, n) = p$, where p is prime, then $\phi(mn) = p\phi(m)\phi(n)/(p-1)$.

22. Show that if m and k are positive integers, then $\phi(m^k) = m^{k-1}\phi(m)$.

23. Show that if a and b are positive integers, then

$$\phi(ab) = (a, b)\phi(a)\phi(b)/\phi((a, b)).$$

Conclude that $\phi(ab) > \phi(a)\phi(b)$ when $(a, b) > 1$.

24. Find the least positive integer n such that the following hold.

a) $\phi(n) \geq 100$ c) $\phi(n) \geq 10{,}000$
b) $\phi(n) \geq 1000$ d) $\phi(n) \geq 100{,}000$

25. Use the Euler phi-function to show that there are infinitely many primes. (*Hint:* Assume there are only a finite number of primes $p_1, \ldots, p_k$. Consider the value of the Euler phi-function at the product of these primes.)

26. Show that if the equation $\phi(n) = k$, where k is a positive integer, has exactly one solution n, then $36 \mid n$.

27. Show that the equation $\phi(n) = k$, where k is a positive integer, has finitely many solutions in integers n whenever k is a positive integer.

28. Show that if p is prime, $2^a p + 1$ is composite for $a = 1, 2, \ldots, r$ and p is not a Fermat prime, where r is a positive integer, then $\phi(n) = 2^r p$ has no solution.

* 29. Show that there are infinitely many positive integers k such that the equation $\phi(n) = k$ has exactly two solutions, where n is a positive integer. (*Hint:* Take $k = 2 \cdot 3^{6j+1}$, where $j = 1, 2, \ldots$.)

30. Show that if n is a positive integer with $n \neq 2$ and $n \neq 6$, then $\phi(n) \geq \sqrt{n}$.

*** 31.** Show that if n is a composite positive integer and $\phi(n) \mid n - 1$, then n is square-free and is the product of at least three distinct primes.

32. Show that if m and n are positive integers with $m \mid n$, then $\phi(m) \mid \phi(n)$.

*** 33.** Prove Theorem 7.5, using the principle of inclusion-exclusion (see Exercise 16 of Appendix B).

34. Show that a positive integer n is composite if and only if $\phi(n) \leq n - \sqrt{n}$.

35. Let n be a positive integer. Define the sequence of positive integers $n_1, n_2, n_3, \ldots$ recursively by $n_1 = \phi(n)$ and $n_{k+1} = \phi(n_k)$ for $k = 1, 2, 3, \ldots$. Show that there is a positive integer r such that $n_r = 1$.

A multiplicative function is called *strongly multiplicative* if and only if $f(p^k) = f(p)$ for every prime p and every positive integer k.

36. Show that $f(n) = \phi(n)/n$ is a strongly multiplicative function.

Two arithmetic functions f and g may be multiplied using the *Dirichlet product,* which is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

37. Show that $f * g = g * f$.

38. Show that $(f * g) * h = f * (g * h)$.

We define the *ι function* by

$$\iota(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

39. a) Show that ι is a multiplicative function.

b) Show that $\iota * f = f * \iota = f$ for all arithmetic functions f.

40. The arithmetic function g is said to be the *inverse* of the arithmetic function f if $f * g = g * f = \iota$. Show that the arithmetic function f has an *inverse* if and only if $f(1) \neq 0$. Show that if f has an inverse it is unique. (*Hint:* When $f(1) \neq 0$, find the inverse f^{-1} of f by calculating $f^{-1}(n)$ recursively, using the fact that $\iota(n) = \sum_{d|n} f(d)f^{-1}(n/d)$.)

41. Show that if f and g are multiplicative functions, then the Dirichlet product $f * g$ is also multiplicative.

42. Show that if f and g are arithmetic functions, $F = f * g$, and h is the Dirichlet inverse of g, then $f = F * h$.

We define *Liouville's function* $\lambda(n)$, named after French mathematician *Joseph Liouville*, by $\lambda(1) = 1$, and for $n > 1$, $\lambda(n) = (-1)^{a_1+a_2+\cdots+a_m}$, where the prime-power factorization of n is $n = p_1^{a_1}p_2^{a_2} \cdots p_m^{a_m}$.

43. Find $\lambda(n)$ for each of the following values of n.

a) 12 c) 210 e) 1001 g) 20!
b) 20 d) 1000 f) 10!

44. Show that $\lambda(n)$ is completely multiplicative.

45. Show that if n is a positive integer, then $\sum_{d|n} \lambda(d)$ equals 0 if n is not a perfect square, and equals 1 if n is a perfect square.

46. Show that if f and g are multiplicative functions, then fg is also multiplicative, where $(fg)(n) = f(n)g(n)$ for every positive integer n.

47. Show that if f and g are completely multiplicative functions, then fg is also completely multiplicative.

48. Show that if f is completely multiplicative, then $f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_m)^{a_m}$, where the prime-power factorization of n is $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$.

A function f that satisfies the equation $f(mn) = f(m) + f(n)$ for all relatively prime positive integers m and n is called *additive*, and if the above equation holds for all positive integers m and n, f is called *completely additive*.

49. Show that the function $f(n) = \log n$ is completely additive.

The function $\omega(n)$ is the function that denotes the number of distinct prime factors of the positive integer n.

50. Find $\omega(n)$ for each of the following integers.

a) 1 b) 2 c) 20 d) 84 e) 128

JOSEPH LIOUVILLE (1809–1882), born in Saint-Omer, France, was the son of a captain in Napoleon's army. He studied mathematics at the Collège St. Louis in Paris, and in 1825 he enrolled in the École Polytechnique; after graduating, he entered the École des Ponts et Chaussées (School of Bridges and Roads). Health problems while working on engineering projects and his interest in theoretical topics convinced him to pursue an academic career. He left the École des Ponts et Chaussées in 1830, but during his time there he wrote papers on electrodynamics, the theory of heat, and partial differential equations.

Liouville's first academic appointment was as an assistant at the École Polytechnique in 1831. He had a teaching load of around 40 hours a week at several different institutions. Some of his less able students complained that he lectured at too high a level. In 1836, Liouville founded the *Journal de Mathématiques Pures et Appliquées*, which played an important role in French mathematics in the nineteenth century. In 1837, he was appointed to lecture at the Collège de France and the following year he was appointed Professor at the École Polytechnique. Besides his academic interests, Liouville was also involved in politics. He was elected to Constituting Assembly in 1848 as a moderate republican, but lost in the election of 1849, embittering him. Liouville was appointed to a chair at the Collège de France in 1851, and the chair of mechanics at the Faculté des Sciences in 1857. Around this time, his heavy teaching load began to take its toll. Liouville was a perfectionist and was unhappy when he could not devote sufficient time to his lectures.

Liouville's work covered many diverse areas of mathematics, including mathematical physics, astronomy, and many areas of pure mathematics. He was the first person to provide an explicit example of a transcendental number. He is also known today for what is now called Sturm-Liouville theory, used in the solution of integral equations, and he made important contributions to differential geometry. His total output exceeds 400 papers in the mathematical sciences, with nearly half of those in number theory alone.

51. Find $\omega(n)$ for each of the following integers.

    a) 12 b) 30 c) 32 d) 10! e) 20! f) 50!

52. Show that $\omega(n)$ is additive, but not completely additive.

53. Show that if f is an additive function and $g(n) = 2^{f(n)}$, then g is multiplicative.

54. Show that the function n^k is completely multiplicative for every real number k.

7.1 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 $\phi(n)$ when n takes each of the following values.

   a) 185,888,434,028 b) 1,111,111,111,111

2. Find the number of iterations of the Euler phi-function required to reach 1, starting with each of the integers in Computation 1.

3. Find the largest integer n such that $\phi(n) \leq k$ for each of the following values of k.

   a) 1,000,000 b) 10,000,000

4. Find as many positive integers n as you can, such that $\phi(n) = \phi(n+1)$. Can you formulate any conjectures based on the evidence that you have found?

5. Can you find a positive integer n other than 5186 such that $\phi(n) = \phi(n+1) = \phi(n+2)$? Can you find four consecutive positive integers $n, n+1, n+2, n+3$, such that $\phi(n) = \phi(n+1) = \phi(n+2) = \phi(n+3)$?

6. An open conjecture of D. H. Lehmer asserts that n is prime if $\phi(n)$ divides $n-1$. Explore the truth of this conjecture.

7. An open conjecture of Carmichael asserts that for every positive integer n there is a positive integer m such that $\phi(m) = \phi(n)$. Gather as much evidence as possible for this conjecture.

Programming Projects

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

1. Given a positive integer n, find the value of $\phi(n)$.

2. Given a positive integer n, find the number of iterations of the phi-function, starting with n, required to reach 1. (This is the the integer r in Exercise 35.)

3. Given a positive integer k, find the number of solutions of $\phi(n) = k$.

7.2 The Sum and Number of Divisors

As we mentioned in Section 7.1, the number of divisors and the sum of divisors are both multiplicative functions. We will show that these functions are multiplicative, and derive formulas for their values at a positive integer n from the prime factorization of n.

Definition. The *sum of divisors function*, denoted by σ, is defined by setting $\sigma(n)$ equal to the sum of all the positive divisors of n.

In Table 7.1, we give $\sigma(n)$ for $1 \leq n \leq 12$. The values of $\sigma(n)$ for $1 \leq n \leq 100$ are given in Table 2 of Appendix E. (These values can also be computed using Maple or *Mathematica*.)

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

Table 7.1 *The sum of the divisors for* $1 \leq n \leq 12$.

Definition. The *number of divisors function*, denoted by τ, is defined by setting $\tau(n)$ equal to the number of positive divisors of n.

In Table 7.2, we give $\tau(n)$ for $1 \leq n \leq 12$. The values of $\tau(n)$ for $1 \leq n \leq 100$ are given in Table 2 of Appendix E. (These values can also be computed using Maple or *Mathematica*.)

n	1	2	3	4	5	6	7	8	9	10	11	12
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6

Table 7.2 *The number of divisors for* $1 \leq n \leq 12$.

Note that we can express $\sigma(n)$ and $\tau(n)$ in summation notation. It is simple to see that

$$\sigma(n) = \sum_{d|n} d$$

and

$$\tau(n) = \sum_{d|n} 1.$$

To prove that σ and τ are multiplicative, we use the following theorem.

Theorem 7.8. If f is a multiplicative function, then the summatory function of f, namely $F(n) = \sum_{d|n} f(d)$, is also multiplicative.

Before we prove the theorem, we illustrate the idea behind its proof with the following example. Let f be a multiplicative function, and let $F(n) = \sum_{d|n} f(d)$. We will show that $F(60) = F(4)F(15)$. Each of the divisors of 60 may be written as the product of a divisor of 4 and a divisor of 15 in the following way: $1 = 1 \cdot 1$, $2 = 2 \cdot 1$, $3 = 1 \cdot 3$, $4 = 4 \cdot 1$, $5 = 1 \cdot 5$, $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $12 = 4 \cdot 3$, $15 = 1 \cdot 15$, $20 = 4 \cdot 5$, $30 = 2 \cdot 15$, $60 = 4 \cdot 15$ (in each product, the first factor is the divisor of 4, and the second is the divisor of 15). Hence,

$$\begin{aligned}
F(60) &= f(1) + f(2) + f(3) + f(4) + f(5) + f(6) + f(10) + f(12) \\
&\quad + f(15) + f(20) + f(30) + f(60) \\
&= f(1 \cdot 1) + f(2 \cdot 1) + f(1 \cdot 3) + f(4 \cdot 1) + f(1 \cdot 5) + f(2 \cdot 3) \\
&\quad + f(2 \cdot 5) + f(4 \cdot 3) + f(1 \cdot 15) + f(4 \cdot 5) + f(2 \cdot 15) + f(4 \cdot 15) \\
&= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(4)f(1) + f(1)f(5) \\
&\quad + f(2)f(3) + f(2)f(5) + f(4)f(3) + f(1)f(15) + f(4)f(5) \\
&\quad + f(2)f(15) + f(4)f(15) \\
&= (f(1) + f(2) + f(4))(f(1) + f(3) + f(5) + f(15)) \\
&= F(4)F(15).
\end{aligned}$$

We now prove Theorem 7.8 using the idea illustrated by the example.

Proof. To show that F is a multiplicative function, we must show that if m and n are relatively prime positive integers, then $F(mn) = F(m)F(n)$. So let us assume that $(m, n) = 1$. We have

$$F(mn) = \sum_{d|mn} f(d).$$

By Lemma 3.6, because $(m, n) = 1$, each divisor of mn can be written uniquely as the product of relatively prime divisors d_1 of m and d_2 of n, and each pair of divisors d_1 of m and d_2 of n corresponds to a divisor $d = d_1d_2$ of mn. Hence, we can write

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2).$$

Because f is multiplicative, and $(d_1, d_2) = 1$, we see that

$$\begin{aligned}
F(mn) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2) \\
&= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\
&= F(m)F(n).
\end{aligned}$$

■

We can now use Theorem 7.8 to show that σ and τ are multiplicative.

Corollary 7.8.1. The sum of divisors function σ and the number of divisors function τ are multiplicative functions.

Proof. Let $f(n) = n$ and $g(n) = 1$. Both f and g are multiplicative. By Theorem 7.8, we see that $\sigma(n) = \sum_{d|n} f(d)$ and $\tau(n) = \sum_{d|n} g(d)$ are multiplicative. ∎

Now that we know that σ and τ are multiplicative, we can derive formulas for their values based on prime factorizations. First, we find formulas for $\sigma(n)$ and $\tau(n)$ when n is the power of a prime.

Lemma 7.1. Let p be prime and a a positive integer. Then

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

and

$$\tau(p^a) = a + 1.$$

Proof. The divisors of p^a are $1, p, p^2, \ldots, p^{a-1}, p^a$. Consequently, p^a has exactly $a + 1$ divisors, so that $\tau(p^a) = a + 1$. Also, we note that $\sigma(p^a) = 1 + p + p^2 + \cdots + p^{a-1} + p^a = \frac{p^{a+1}-1}{p-1}$, using the formula in Example 1.15 for the sum of terms of a geometric progression. ∎

Example 7.8. When we apply Lemma 7.1 with $p = 5$ and $a = 3$, we find that $\sigma(5^3) = 1 + 5 + 5^2 + 5^3 = \frac{5^4-1}{5-1} = 156$ and $\tau(5^3) = 1 + 3 = 4$. ◀

Lemma 7.1 and Corollary 7.8.1 lead to the following formulas.

Theorem 7.9. Let the positive integer n have prime factorization $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$. Then

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \cdots \cdot \frac{p_s^{a_s+1} - 1}{p_s - 1} = \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

and

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_s + 1) = \prod_{j=1}^{s} (a_j + 1).$$

Proof. Because both σ and τ are multiplicative, we see that $\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \cdots \sigma(p_s^{a_s})$ and $\tau(n) = \tau(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) = \tau(p_1^{a_1})\tau(p_2^{a_2}) \cdots \tau(p_s^{a_s})$. Inserting the values for $\sigma(p_i^{a_i})$ and $\tau(p_i^{a_i})$ found in Lemma 7.1, we obtain the desired formulas. ∎

We illustrate how to use Theorem 7.9 with the following example.

Example 7.9. Using Theorem 7.9 we find

$$\sigma(200) = \sigma(2^3 5^2) = \frac{2^4 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15 \cdot 31 = 465,$$

$$\tau(200) = \tau(2^3 5^2) = (3 + 1)(2 + 1) = 12.$$

Similarly, we have

$$\sigma(720) = \sigma(2^4 \cdot 3^2 \cdot 5) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 31 \cdot 13 \cdot 6 = 2418,$$

$$\tau(2^4 \cdot 3^2 \cdot 5) = (4 + 1)(2 + 1)(1 + 1) = 30.$$

◀

7.2 Exercises

1. Find the sum of the positive integer divisors of each of the following integers.
   a) 35
   b) 196
   c) 1000
   d) 2^{100}
   e) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$
   f) $2^5 3^4 5^3 7^2 11$
   g) 10!
   h) 20!

2. Find the number of positive integer divisors of each of the following integers.
   a) 36
   b) 99
   c) 144
   d) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$
   e) $2 \cdot 3^2 \cdot 5^3 \cdot 7^4 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5$
   f) 20!

3. Which positive integers have an odd number of positive divisors?

4. For which positive integers n is the sum of divisors of n odd?

* 5. Find all positive integers n with $\sigma(n)$ equal to each of the following integers.
   a) 12
   b) 18
   c) 24
   d) 48
   e) 52
   f) 84

* 6. Find the smallest positive integer n with $\tau(n)$ equal to each of the following integers.
   a) 1
   b) 2
   c) 3
   d) 6
   e) 14
   f) 100

7. Show that if $k > 1$ is an integer, then the equation $\tau(n) = k$ has infinitely many solutions.

8. Which positive integers have exactly two positive divisors?

9. Which positive integers have exactly three positive divisors?

10. Which positive integers have exactly four positive divisors?

11. What is the product of the positive divisors of a positive integer n?

12. Show that the equation $\sigma(n) = k$ has at most a finite number of solutions when k is a positive integer.

13. For each of the following sequences, can you find a rule for producing the terms of the sequence that involves the τ and/or the σ function?
   a) 3, 7, 12, 15, 18, 28, 24, 31, . . .
   b) 0, 1, 2, 4, 4, 8, 6, 11, . . .

c) 1, 2, 4, 6, 16, 12, 64, 24, 36, 48, ...
d) 1, 0, 1, 1, 0, 1, 1, 1, 0, 0, 0, 2, 1, ...

14. For each of the following sequences, can you find a rule for producing the terms of the sequence that involves the τ and/or the σ function?
a) 2, 5, 6, 10, 8, 16, 10, 19, 16, 22, ...
b) 1, 4, 6, 8, 13, 12, 14, 24, 18, ...
c) 6, 8, 10, 14, 15, 21, 22, 26, 27, 33, 34, 35, ...
d) 1, 2, 2, 2, 3, 2, 2, 4, 2, 2, 4, 2, 3, ...

A positive integer n, $n > 1$, is *highly composite*, a concept introduced by the famous Indian mathematician *Srinivasa Ramanujan*, if $\tau(m) < \tau(n)$ for all integers m with $1 \leq m < n$.

15. Find the first six highly composite positive integers.

16. Show that if n is a highly composite positive integer and m is a positive integer with $\tau(m) > \tau(n)$, then there exists a highly composite integer k such that $n < k \leq m$. Conclude that there are infinitely many highly composite integers.

17. Show that if $n \geq 1$, there exists a highly composite number k such that $n < k \leq 2n$. Use this to provide an upper bound on the mth highly composite number, where m is a positive integer.

18. Show that if n is a highly composite positive integer, there exists a positive integer k such that $n = 2^{a_1}3^{a_2}5^{a_3} \cdots p_k^{a_k}$, where p_k is the kth prime and $a_1 \geq a_2 \geq \cdots \geq a_k \geq 1$.

* **19.** Find all highly composite numbers of the form 2^a3^b, where a and b are nonnegative integers.

Let $\sigma_k(n)$ denote the sum of the kth powers of the divisors of n, so that $\sigma_k(n) = \sum_{d|n} d^k$. Note that $\sigma_1(n) = \sigma(n)$.

20. Find $\sigma_3(4)$, $\sigma_3(6)$, and $\sigma_3(12)$.

21. Give a formula for $\sigma_k(p)$, where p is prime.

22. Give a formula for $\sigma_k(p^a)$, where p is prime and a is a positive integer.

23. Show that the function σ_k is multiplicative.

24. Using Exercises 22 and 23, find a formula for $\sigma_k(n)$, where n has prime-power factorization $n = p_1^{a_1}p_2^{a_2} \cdots p_m^{a_m}$.

* **25.** Find all positive integers n such that $\phi(n) + \sigma(n) = 2n$.

* **26.** Show that no two positive integers have the same product of divisors.

27. Show that the number of ordered pairs of positive integers with least common multiple equal to the positive integer n is $\tau(n^2)$.

28. Let n be a positive integer, $n \geq 2$. Define the sequence of integers $n_1, n_2, n_3, \ldots$ by $n_1 = \tau(n)$ and $n_{k+1} = \tau(n_k)$ for $k = 1, 2, 3, \ldots$. Show that there is a positive integer r such that $2 = n_r = n_{r+1} = n_{r+2} = \ldots$.

29. Show that a positive integer n is composite if and only if $\sigma(n) > n + \sqrt{n}$.

30. Let n be a positive integer. Show that $\tau(2^n - 1) \geq \tau(n)$.

* **31.** Show that $\sum_{j=1}^{n} \tau(j) = 2\sum_{j=1}^{[\sqrt{n}]}[n/j] - [\sqrt{n}]^2$ whenever n is a positive integer. Then use this formula to find $\sum_{j=1}^{100} \tau(j)$.

* **32.** Let a and b be positive integers. Show that $\sigma(a)/a \leq \sigma(ab)/(ab) \leq \sigma(a)\sigma(b)/(ab)$.

* **33.** Show that if a and b are positive integers, then $\sigma(a)\sigma(b) = \sum_{d|(a,b)} d\sigma(ab/d^2)$.

SRINIVASA RAMANUJAN (1887–1920) was born and raised in southern India, near Madras. His father was a clerk in a cloth shop and his mother contributed to the family income by singing at a local temple. Ramanujan studied at a local English language school, displaying a talent in mathematics. At 13 he mastered a textbook used by college students; when he was 15, a university student lent him a copy of *Synopsis of Pure Mathematics,* and Ramanujan decided to work out the more than 6000 results in this book. He graduated from high school in 1904, winning a scholarship to the University of Madras. Enrolling in a fine arts curriculum, he neglected subjects other than mathematics and lost his scholarship. During this time he filled his notebooks with original writings, sometimes rediscovering already published work and at other times making new discoveries.

Lacking a university degree, Ramanujan found it difficult to land a decent job. To survive, he depended on the good will of friends. He tutored students, but his uncoventional ways of thinking and failure to stick to the syllabus caused problems. He was married in 1909 in an arranged marriage to a woman who was 13 years old. Needing to support himself and his wife, he moved to Madras looking for a job. He showed his notebooks to potential employers, but his writings bewildered them. However, a professor at the Presidency College recognized his genius and supported him, and in 1912 he found work as an accounts clerk, which earned him a small salary.

Ramanujan continued his mathematical investigations, publishing his first paper in 1910 in an Indian journal. Realizing that his work was beyond that of Indian mathematicians, he decided to write to leading English mathematicians. Although the first mathematicians turned down his request for help, G. H. Hardy arranged a scholarship for Ramanujan, bringing him to England in 1914. Hardy initially was inclined to turn Ramanujan down, but the mathematical results Ramanujan stated without proof in his letter puzzled Hardy. He examined Ramanujan's writings with the aid of his collaborator, J. E. Littlewood. They decided that Ramanujan was probably a genius, as his statements "could only be written down by a mathematician of the highest class; they must be true, because if they were not true, no one would have the imagination to invent them." Hardy personally tutored Ramanujan and they collaborated for five years, proving significant theorems about the partitions of integers. During this time, Ramanujan made important contributions to number theory, and worked on elliptic functions, infinite series, and continued fractions. Ramanujan had amazing insight involving certain types of functions and series, but his purported theorems on prime numbers were often wrong, illustrating his vague idea of what makes up a correct proof.

Ramanujan was one of the youngest members ever appointed a Fellow of the Royal Society. Unfortunately, in 1917, he became extremely ill. Although it was once thought he contracted turberculosis, it is now thought that he suffered from a vitamin deficiency brought on by his strict vegetarianism and shortages in wartime England. He returned to India in 1919 and continued his mathematical work even while confined to bed. He was highly religious and thought that his mathematical talent came from his family deity, Namaigiri. He said that "an equation for me has no meaning unless it expresses a thought of God." He died in April 1920, leaving several notebooks of unpublished results. Mathematicians have devoted many years of study to the explanation and justification of the results jotted down in Ramanujan's notebooks.

* **34.** Show that if n is a positive integer, then $\left(\sum_{d|n} \tau(d)\right)^2 = \sum_{d|n} \tau(d)^3$.

35. Show that if n is a positive integer, then $\tau(n^2) = \sum_{d|n} 2^{\omega(n)}$, where $\omega(n)$ equals the number of prime divisors of n.

36. Show that $\sum_{d|n} n\sigma(d)/d = \sum_{d|n} d\tau(d)$ whenever n is a positive integer.

* **37.** Find the determinant of the $n \times n$ matrix with (i, j)th entry equal to (i, j).

* **38.** Let n be a positive integer such that $24 \mid (n + 1)$. Show that $\sigma(n)$ is divisible by 24.

39. Show that there are infinitely many pairs of positive integers m, n such that $\phi(m) = \sigma(n)$, if there are infinitely many pairs of twin primes or infinitely many Mersenne primes (that is, primes of the form $2^p - 1$, where p is prime).

40. Prove that $\sum_{d|n} \phi(d) = n$ (Theorem 7.7) as a consequence of Theorem 7.8.

7.2 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 $\tau(n)$, $\sigma(n)$, and $\sigma_2(n)$ (as defined in the preamble to Exercise 20) for each of the following values of n.

a) 121,110,987,654 b) 11,111,111,111 c) 98,989,898,989

2. Find as many pairs, triples, and quadruples as you can of consecutive integers, each with the same number of positive divisors.

3. Determine the number of iterations required for the sequence $n_1 = \tau(n)$, $n_2 = \tau(n_1), \ldots, n_{k+1} = \tau(n_k), \ldots$ to reach the integer 2, for all positive integers n not exceeding 1000. Formulate some conjectures based on your evidence.

4. Find all the highly composite integers (as defined in the preamble to Exercise 15) not exceeding 10,000.

* **5.** Show that 29,331,862,500 is a highly composite integer.

Programming Projects

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

1. Given a positive integer n, find $\tau(n)$, the number of positive divisors of n.

2. Given a positive integer n, find $\sigma(n)$, the sum of the positive divisors of n.

3. Given a positive integer n and a positive integer k, find $\sigma_k(n)$, the sum of the kth powers of the positive divisors of n.

4. Given a positive integer n, find the integer r defined in Exercise 28.

5. Given a positive integer n, determine whether n is highly composite.

7.3 Perfect Numbers and Mersenne Primes

Because of certain mystical beliefs, the ancient Greeks were interested in those integers that are equal to the sum of all their proper positive divisors. Such integers are called *perfect numbers.*

Definition. If n is a positive integer and $\sigma(n) = 2n$, then n is called a *perfect number.*

Example 7.10. Because $\sigma(6) = 1 + 2 + 3 + 6 = 12$, we see that 6 is perfect. We also note that $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$, so that 28 is another perfect number. ◀

The ancient Greeks knew how to find all even perfect numbers. The following theorem tells us which even positive integers are perfect.

Theorem 7.10. The positive integer n is an even perfect number if and only if

$$n = 2^{m-1}(2^m - 1),$$

where m is an integer such that $m \geq 2$ and $2^m - 1$ is prime.

Proof. First, we show that if $n = 2^{m-1}(2^m - 1)$, where $2^m - 1$ is prime, then n is perfect. We note that because $2^m - 1$ is odd, we have $(2^{m-1}, 2^m - 1) = 1$. Because σ is a multiplicative function, we see that

$$\sigma(n) = \sigma(2^{m-1})\sigma(2^m - 1).$$

Lemma 7.1 tells us that $\sigma(2^{m-1}) = 2^m - 1$ and $\sigma(2^m - 1) = 2^m$, because we are assuming that $2^m - 1$ is prime. Consequently,

$$\sigma(n) = (2^m - 1)2^m = 2n,$$

demonstrating that n is a perfect number.

To show that the converse is true, let n be an even perfect number. Write $n = 2^s t$, where s and t are positive integers and t is odd. Because $(2^s, t) = 1$, we see from Lemma 7.1 that

$$\sigma(n) = \sigma(2^s t) = \sigma(2^s)\sigma(t) = (2^{s+1} - 1)\sigma(t). \tag{7.1}$$

Because n is perfect, we have

$$\sigma(n) = 2n = 2^{s+1}t. \tag{7.2}$$

Combining (7.1) and (7.2) shows that

$$(2^{s+1} - 1)\sigma(t) = 2^{s+1}t. \tag{7.3}$$

Because $(2^{s+1}, 2^{s+1} - 1) = 1$, from Lemma 3.4 we see that $2^{s+1} \mid \sigma(t)$. Therefore, there is an integer q such that $\sigma(t) = 2^{s+1}q$. Inserting this expression for $\sigma(t)$ into (7.3) tells us that

$$(2^{s+1} - 1)2^{s+1}q = 2^{s+1}t,$$

and, therefore,

$$(2^{s+1} - 1)q = t. \tag{7.4}$$

Hence, $q \mid t$ and $q \neq t$.

When we add q to both sides of (7.4), we find that

$$t + q = (2^{s+1} - 1)q + q = 2^{s+1}q = \sigma(t). \tag{7.5}$$

We will show that $q = 1$. Note that if $q \neq 1$, then there are at least three distinct positive divisors of t, namely 1, q, and t. This implies that $\sigma(t) \geq t + q + 1$, which contradicts (7.5). Hence, $q = 1$ and, from (7.4), we conclude that $t = 2^{s+1} - 1$. Also, from (7.5), we see that $\sigma(t) = t + 1$, so that t must be prime, because its only positive divisors are 1 and t. Therefore, $n = 2^s(2^{s+1} - 1)$, where $2^{s+1} - 1$ is prime. ∎

By Theorem 7.10, we see that to find even perfect numbers, we must find primes of the form $2^m - 1$. In our search for primes of this form, we first show that the exponent m must be prime.

Theorem 7.11. If m is a positive integer and $2^m - 1$ is prime, then m must be prime.

Proof. Assume that m is not prime, so that $m = ab$, where $1 < a < m$ and $1 < b < m$. (Note that $m > 1$, since $2^m - 1$ is prime.) Then

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Because both factors on the right side of the equation are greater than 1, we see that $2^m - 1$ is composite if m is not prime. Therefore, if $2^m - 1$ is prime, then m must also be prime. ∎

By Theorem 7.11, we see that to search for primes of the form $2^m - 1$, we need to consider only integers m that are prime. Integers of the form $2^m - 1$ have been studied in great depth; these integers are named after a French monk of the seventeenth century, *Marin Mersenne*, who studied them.

Definition. If m is a positive integer, then $M_m = 2^m - 1$ is called the mth *Mersenne number;* if p is prime and $M_p = 2^p - 1$ is also prime, then M_p is called a *Mersenne prime.*

Example 7.11. The Mersenne number $M_7 = 2^7 - 1$ is prime, whereas the Mersenne number $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ is composite. ◀

It is possible to prove various theorems that help decide whether Mersenne numbers are prime. One such theorem will now be given. Related results are found in Exercises 37–39 in Section 11.1.

Theorem 7.12. If p is an odd prime, then any divisor of the Mersenne number $M_p = 2^p - 1$ is of the form $2kp + 1$, where k is a positive integer.

Proof. Let q be a prime dividing $M_p = 2^p - 1$. By Fermat's little theorem, we know that $q \mid (2^{q-1} - 1)$. Also, from Lemma 3.2, we know that

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1. \tag{7.6}$$

Because q is a common divisor of $2^p - 1$ and $2^{q-1} - 1$, we know that $(2^p - 1, 2^{q-1} - 1) > 1$. Hence, $(p, q - 1) = p$, because the only other possibility, namely $(p, q - 1) = 1$, would imply from (7.6) that $(2^p - 1, 2^{q-1} - 1) = 1$. Hence $p \mid (q - 1)$ and, therefore, there is a positive integer m such that $q - 1 = mp$. Because q is odd, we see that m must be even, so that $m = 2k$, where k is a positive integer. Hence, $q = mp + 1 = 2kp + 1$. Because any divisor of M_p is a product of prime divisors of M_p, each prime divisor of M_p is of the form $2kp + 1$, and the product of numbers of this form is also of this form, the result follows. ∎

We can use Theorem 7.12 to help decide whether Mersenne numbers are prime. We illustrate this by the following examples.

Example 7.12. To decide whether $M_{13} = 2^{13} - 1 = 8191$ is prime, we need only look for a prime factor not exceeding $\sqrt{8191} = 90.504\ldots$. Furthermore, by Theorem 7.12, any such prime divisor must be of the form $26k + 1$. The only candidates for primes dividing M_{13} less than or equal to $\sqrt{M_{13}}$ are 53 and 79. Trial division easily rules out these cases, so that M_{13} is prime. ◀

Example 7.13. To decide whether $M_{23} = 2^{23} - 1 = 8{,}388{,}607$ is prime, we only need to determine whether M_{23} is divisible by a prime less than or equal to $\sqrt{M_{23}} = 2896.309\ldots$ of the form $46k + 1$. The first prime of this form is 47. A trial division shows that $8{,}388{,}607 = 47 \cdot 178{,}481$, so that M_{23} is composite. ◀

MARIN MERSENNE (1588–1648) was born in Maine, France, into a family of workers. He attended the College of Mans and the Jesuit College at La Flèche. He continued his education at the Sorbonne, studying theology. He joined the order of the Minims in 1611, a group whose name comes from the word *minimi* indicating that the members considered themselves the least religious order. Besides prayer, members pursued scholarship and study. In 1612, Mersenne became a priest at the Palace Royale in Paris; between 1614 and 1618, he taught philosophy at the Minim Convent in Nevers. He returned to Paris in 1619, where his cell in the Minims de l'Annociade was a meeting place for scientists, philosophers, and mathematicians, including Fermat and Pascal. Mersenne corresponded extensively with scholars throughout Europe, serving as a clearinghouse for new ideas. Mersenne wrote books on mechanics, mathematical physics, mathematics, music, and acoustics. He studied prime numbers and tried unsuccessfully to develop a formula representing all primes. In 1644, he claimed to have the complete list of primes p with $p \leq 257$ for which $2^p - 1$ is prime; this claim was far from accurate. Mersenne is also noted for his defense of two of the most famous men of his time, Descartes and Galileo, from religious critics. He also helped expose alchemists and astrologers as frauds.

Because there are special primality tests for Mersenne numbers, it has been possible to determine whether extremely large Mersenne numbers are prime.

A particularly useful primality test follows, known as the Lucas-Lehmer test after *Edouard Lucas*, who developed the theory the test is based on in the 1870s, and *Derrick H. Lehmer*, who developed a simplified version of the test in 1930. This test has been used to find the largest known Mersenne primes and is being used today in the ongoing search for new Mersenne primes, described later in this section. For most of recent history, the largest known Mersenne prime was the largest known prime as is currently the case. However, from late 1990 until early 1992, the largest known prime was $391{,}581 \cdot 2^{216{,}193} - 1$. Because this number is of the form $k \cdot 2^n - 1$, it was possible to use special tests to show that it is prime.

Theorem 7.13. ***The Lucas-Lehmer Test.*** Let p be a prime and let $M_p = 2^p - 1$ denote the pth Mersenne number. Define a sequence of integers recursively by setting $r_1 = 4$ and, for $k \geq 2$,

$$r_k \equiv r_{k-1}^2 - 2 \pmod{M_p}, 0 \leq r_k < M_p.$$

Then M_p is prime if and only if $r_{p-1} \equiv 0 \pmod{M_p}$.

FRANÇOIS-EDOUARD-ANATOLE LUCAS (1842–1891) was born in Amiens, France, and was educated at the École Normale. After finishing his studies, he worked as an assistant at the Paris Observatory, and during the Franco-Prussian war he served as an artillery officer. After the war he became a teacher at a secondary school. He was considered to be an excellent and entertaining teacher. Lucas was extremely fond of calculating and devised plans for a computer, which unfortunately were never realized. Besides his contributions to number theory, Lucas is also remembered for his work in recreational mathematics. The most famous of his contributions in this area is the well-known tower of Hanoi problem. A freak accident led to Lucas's death. He was gashed in the cheek by a piece of a plate which was accidentally dropped at a banquet. An infection in the resulting wound killed him several days later.

DERRICK H. LEHMER (1905–1991) was born in Berkeley, California. He received his undergraduate degree in 1927 from the University of California and his master's and doctorate degrees from Brown University in 1929 and 1930, respectively. He served on the staffs of the California Institute of Technology, the Institute for Advanced Study, Lehigh University, and Cambridge University before joining the mathematics department at the University of California, Berkeley, in 1940. Lehmer made many contributions to number theory. He invented many special purpose devices for number theoretic computations, some with his father, who was also a mathematician. Lehmer was the thesis advisor of Harold Stark, who in turn was the thesis advisor of the author of this book.

The proof of the Lucas-Lehmer test may be found in [Le80] and [Si64]. We give an example to illustrate how the Lucas-Lehmer test is used.

Example 7.14. Consider the Mersenne number $M_5 = 2^5 - 1 = 31$. Then $r_1 = 4$, $r_2 \equiv 4^2 - 2 = 14 \pmod{31}$, $r_3 \equiv 14^2 - 2 \equiv 8 \pmod{31}$, and $r_4 \equiv 8^2 - 2 \equiv 0 \pmod{31}$. Because $r_4 \equiv 0 \pmod{31}$, we conclude that $M_5 = 31$ is prime. ◀

The Lucas-Lehmer test can be performed quite rapidly, as the following corollary states. It lets us test whether Mersenne numbers are prime without factoring them and makes it possible to determine whether extremely large Mersenne numbers are prime, whereas other numbers of similar size that are not of special form are beyond testing.

Corollary 7.13.2. Let p be prime and let $M_p = 2^p - 1$ denote the pth Mersenne number. It is possible to determine whether M_p is prime using $O(p^3)$ bit operations.

Proof. To determine whether M_p is prime using the Lucas-Lehmer test requires $p - 1$ squarings modulo M_p, each requiring $O((\log M_p)^2) = O(p^2)$ bit operations. Hence, the Lucas-Lehmer test requires $O(p^3)$ bit operations. ■

It has been conjectured but not proved that there are infinitely many Mersenne primes. However, the search for larger and larger Mersenne primes has been quite successful.

The Search for Mersenne Primes

The history of the search for Mersenne primes can be divided into the eras before and after the advent of computers. In precomputer days, the search was littered with errors and unsubstantiated claims, many turning out to be false. By 1588, Pietro Cataldi had verified that M_{17} and M_{19} were primes, but he also stated, without any justification, that M_p was prime for $p = 23, 29, 31$, and 37 (of these, only M_{31} is prime). In his *Cogitata Physica-Mathematica,* published in 1644, Mersenne claimed (without providing a justification) that M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257, and for no other prime p with $p < 257$. In 1772, Euler showed that M_{31} was prime, using trial division by all primes up to 46,337, which is the largest prime not exceeding the square root of M_{31}. In 1811, the English mathematician Peter Barlow wrote in his *Theory of Numbers* that M_{31} would be the greatest Mersenne prime ever found—he thought that no one would ever attempt to find a larger Mersenne prime because they are "merely curious, without being useful." This turned out to be a terrible prediction; not only was Barlow wrong about people finding new Mersenne primes, but he was wrong about their utility, as our subsequent comments will show.

In 1876, Lucas used the test that he had developed to show that M_{67} was composite without finding a factorization; it took an additional 27 years for M_{67} to be factored. The American mathematician Frank Cole devoted 20 years of Sunday-afternoon computations to discover that $M_{67} = 193{,}707{,}721 \cdot 761{,}838{,}257{,}287$. When he presented this result at a meeting of the American Mathematical Society in 1903, writing the factorization on a blackboard and not saying a word, the audience gave him a standing ovation, as

they understood how much work had been required to find this factorization. The numbers M_{61}, M_{89}, M_{107}, and M_{127} were shown to be prime between 1876 and 1914. But it was not until 1947 that the primality of M_p for all primes p not exceeding 257 was tested, with the help of mechanical calculating machines. When this work was done, it was seen that Mersenne had made exactly five mistakes. He was wrong when he stated that M_{67} and M_{257} are primes, and he failed to include the Mersenne primes M_{61}, M_{89}, and M_{107} in his list.

As we have seen, only 12 Mersenne primes were known before the advent of modern computers, the last of which was discovered in 1914. But since the invention of computers, new Mersenne primes have been found at a fairly steady rate, averaging about one new Mersenne prime every two years since 1950. The first five Mersenne primes found with the help of a computer were the 13th through the 17th Mersenne primes. All five were found in 1952 by Raphael Robinson, using SWAC (the National Bureau of Standards Western Automatic Computer) with the help of D. H. and Emma Lehmer. The 13th and 14th Mersenne primes were found the first day SWAC was used to run the Lucas-Lehmer test, and the other three were found in the following nine months. Compared to computers today, SWAC was primitive. Its total memory was 1152 bytes, and half of this was used for the commands that ran the program. It is interesting to note that Robinson's program to implement the Lucas-Lehmer test was the first program he ever wrote.

Riesel found the 18th Mersenne prime using the Swedish BESK computer, Hurwitz found the 19th and 20th Mersenne primes using the IBM 7090, and Gillies found the 21st, 22nd, and 23rd Mersenne primes using the ILLIAC 2. Tuckerman found the 24th Mersenne prime using the IBM 360.

The 25th and 26th Mersenne primes were found by high school students Laura Nickel and Landon Noll using idle time on the Cyber 174 computer at California State University, Hayward. Nickel and Noll, who were 18 years old at the time, were also studying number theory with D. H. Lehmer and CSU professor Dan Jurca. Their discoveries were announced on the nightly news shows of major networks around the world. Nickel and Noll discovered the 25th Mersenne prime together, while only Noll went on to discover the 26th Mersenne prime by himself.

David Slowinski, working with several different collaborators, discovered the nth Mersenne prime for $n = 27$, 28, 30, 31, 32, 33, and 34 between 1979 and 1996. For example, Slowinski and Gage found the Mersenne prime $M_{1,257,787}$, a number with 378,632 digits, in 1996. The proof that this number is prime took approximately six hours on a Cray supercomputer. The Mersenne prime that Slowinski missed, the 29th, was found by Colquitt and Welsh in 1988 using a NEC SX-2 computer. You may wonder how Slowinski overlooked this prime. The reason is that he did not check whether M_p is prime for consecutive primes, but instead jumped around following hunches about the distribution of Mersenne primes, just as many researchers have done.

The Internet is another factor accelerating the discovery of Mersenne primes. Many people are cooperating to find new Mersenne primes as part of the Great Internet Mersenne Prime Search (GIMPS), founded by George Woltman in 1996. Approximately

15 trillion (10^{12}) floating point operations per second (15 Teraflops) are devoted to GIMPS on PrimeNet, the network linking the distributed computers in GIMPS into one virtual supercomputer. This virtual supercomputer is now the equivalent of more than a dozen of the largest supercomputers in the world, even though most of the individual computers used are Pentium PCs.

The six largest Mersenne primes known, the 35th through the 41st, were all found as part of the GIMPS project, with $M_{1,398,269}$ and $M_{2,976,221}$ discovered to be prime in 1996 and 1997, respectively. The Mersenne prime $M_{2,976,221}$ was shown to be prime using a 100 MHz Pentium computer using about 15 days of CPU time. In January 1998, $M_{3,021,377}$, a number with 909,526 decimal digits, was found to be prime by GIMPS. The lucky person who made this discovery, Roland Clarkson, was a 19-year-old student at California State University, Dominguez Hills, at the time. He used a 200 MHz Pentium computer, taking the equivalent of about a week of full-time CPU processing, to find this prime. The Mersenne $M_{6,972,593}$, a number with 2,098,960 decimal digits, was found in June 1999 by Nayan Hajratwala, a GIMPS participant, using a 350 MHz Pentium computer, using the equivalent of about three weeks of uninterrupted processing.

The 39th Mersenne prime, $M_{13,466,917}$, an integer with 4,053,946 decimal digits, was found in November 2001 by a 20-year-old Canadian university student, Michael Cameron. It took 42 days on an 800 MHz AMD personal computer to show that this number is prime. The 40th Mersenne prime is $M_{20,996,011}$, an integer with 6,320,430 decimal digits, which was shown to be prime in November 2003 by Michael Shafer, a 26-year-old chemical engineering graduate student at Michigan State University. He used a 2.4 GHz Pentium 4 personal computer running for 19 days to make this discovery. The 41st Mersenne prime, and the largest known prime as of June 2004, is $M_{24,036,583}$, an integer with 7,253,733 decimal digits which was shown to be prime in May 2004 by Josh Findley. He used a 2.4 GHz Pentium 4 PC running for 14 days to show this number is prime. The search for new Mersenne primes continues full blast, with more than 60,000 people looking for new ones by running GIMPS software on more than 200,000 personal computers. The next few years will show whether GIMPS can keep up their pace of finding a new Mersenne prime every year or two. (See Table 7.3 for a list of all the currently known Mersenne primes, along with information about their discovery.)

Why do people look for Mersenne primes? Many people are devoted to the quest for new Mersenne primes. Why do they spend so much time and energy on this task? There are many reasons. The discovery of a new Mersenne prime brings fame and notoriety. Some people may be motivated by the recent cash prizes being offered for finding new Mersenne primes; other people like to contribute to team efforts. By joining GIMPS and PrimeNet, anyone can begin making useful contributions to the search for new Mersenne primes. The quest for new Mersenne primes has sparked the development of new theoretical results, and this has motivated many people; others are interested in the distribution of primes and want evidence to use as the basis for conjectures. Many people have used software for the Lucas-Lehmer test to check out new hardware platforms, as these programs are CPU and computer bus intensive. For example, the Intel Pentium II chip was tested using GIMPS software. Some people would rather have their computer

No.	p	Decimal Digits in M_p	Date of Discovery	Discoverer(s)	Computer Used
1	2	1	ancient times		
2	3	1	ancient times		
3	5	2	ancient times		
4	7	3	ancient times		
5	13	4	1456	anonymous	
6	17	6	1588	Cataldi	
7	19	6	1588	Cataldi	
8	31	10	1772	Euler	
9	61	19	1883	Pervushin	
10	89	27	1911	Powers	
11	107	33	1914	Powers	
12	127	39	1876	Lucas	
13	521	157	1952	Robinson	SWAC
14	607	183	1952	Robinson	SWAC
15	1279	386	1952	Robinson	SWAC
16	2203	664	1952	Robinson	SWAC
17	2281	687	1952	Robinson	SWAC
18	3217	969	1957	Riesel	BESK
19	4253	1281	1961	Hurwitz	IBM 7090
20	4423	1332	1961	Hurwitz	IBM 7090
21	9689	2917	1963	Gillies	ILLIAC 2
22	9941	2993	1963	Gillies	ILLIAC 2
23	11,213	3376	1963	Gillies	ILLIAC 2
24	19,937	6002	1971	Tuckerman	IBM 360/91
25	21,701	6533	1978	Noll, Nickel	Cyber 174
26	23,209	6987	1979	Noll	Cyber 174
27	44,497	13,395	1979	Nelson, Slowinski	Cray 1
28	86,243	25,962	1983	Slowinski	Cray 1
29	110,503	33,265	1988	Colquitt, Welsh	NEC SX-2
30	132,049	39,751	1983	Slowinski	Cray X-MP
31	216,091	65,050	1985	Slowinski	Cray X-MP
32	756,839	227,832	1992	Slowinski, Gage	Cray 2
33	859,433	258,716	1994	Slowinski, Gage	Cray 2
34	1,257,787	378,632	1996	Slowinski, Gage	Cray T94
35	1,398,269	420,921	1996	Armendgaud, Woltman (GIMPS)	90 MHz Pentium
36	2,976,221	895,952	1997	Spence, Woltman (GIMPS)	100 MHz Pentium
37	3,021,377	909,526	1998	Clarkson, Woltman, Kurowski (GIMPS, PrimeNet)	200 MHz Pentium
38	6,972,593	2,098,960	1999	Hajratwala, Woltman, Kurowski (GIMPS, PrimeNet)	350 MHz Pentium
39	13,466,917	4,053,946	2001	Cameron (GIMPS, PrimeNet)	800 MHz AMD
40	20,996,011	6,320,430	2003	Shafer (GIMPS, PrimeNet)	2 GHz Pentium 4
41	24,036,583	7,253,733	2004	Findley (GIMPS, PrimeNet)	2.4 GHz Pentium 4

Table 7.3 *The known Mersenne primes.*

look for Mersenne primes during idle time than run a screen-saver. For these and other reasons, many people look for Mersenne primes.

If you catch the bug and become interested in the search for Mersenne primes, you should investigate the GIMPS Web site, as well as several other relevant Web sites (links for these can be found in Appendix D and on the Web site for this book). At the GIMPS site, you can obtain a program for running the Lucas-Lehmer test, and learn how to join PrimeNet. The GIMPS program for running the Lucas-Lehmer test has been optimized in many ways, so that it runs much more efficiently than a naive implementation of the test. You can reserve a particular range of exponents to check. If history is a guide, it should not be too much longer before the world's record for Mersenne (and all) primes is smashed. If you join GIMPS, you may be the lucky one to break this record!

Odd Perfect Numbers

We have reduced the study of even perfect numbers to the study of Mersenne primes. But are there odd perfect numbers? The answer is still unknown. It is possible to demonstrate that if they exist, odd perfect numbers must have certain properties (see Exercises 32–36, for example). Furthermore, it is known that there are no odd perfect numbers less than 10^{300}; an odd perfect number must have at least eight different prime divisors and at least 37 prime divisors counting multiplicities; and the largest prime factor of the number must be at least 10^{20}. A discussion of odd perfect numbers may be found in [Gu94] or [Ri96], and information about recent results may be found in [BrCote93], [Co87], and [Ha83].

7.3 Exercises

1. Find the six smallest even perfect numbers.
2. Find the seventh and eighth even perfect numbers.
3. Find a factor of each of the following integers.
   a) $2^{15} - 1$
   b) $2^{91} - 1$
   c) $2^{1001} - 1$

A Prime Jackpot

When Nayan Hajratwala found the Mersenne prime $2^{6,972,593} - 1$, he was the first person to find a prime with more than 1 million decimal digits. This made him eligible for a prize of $50,000 from the Electronic Frontier Foundation (EFF), an organization devoted to protecting the health and growth of the Internet. You still have a chance to collect a prize from the EFF by finding large primes. They offer $100,000 for the first person who finds a prime with 10 million digits, a prize that most likely will be claimed within the next few years. Prizes of $150,000 and $250,000 are offered for the first person to find a prime with 100 million and 1 billion decimal digits, respectively. An anonymous donor has funded these prizes to spur cooperative work on scientific problems that involve massive computation.

4. Find a factor of each of the following integers.
   a) $2^{111} - 1$
   b) $2^{289} - 1$
   c) $2^{46,189} - 1$

If n is a positive integer, we say that n is *deficient* if $\sigma(n) < 2n$, and we say that n is *abundant* if $\sigma(n) > 2n$. Every integer is either deficient, perfect, or abundant.

5. Find the six smallest abundant positive integers.

* 6. Find the smallest odd abundant positive integer.

7. Show that every prime power is deficient.

8. Show that any proper divisor of a deficient or perfect number is deficient.

9. Show that any multiple of an abundant or perfect number, other than the perfect number itself, is abundant.

10. Show that if $n = 2^{m-1}(2^m - 1)$, where m is a positive integer such that $2^m - 1$ is composite, then n is abundant.

11. Show that there are infinitely many deficient numbers.

12. Show that there are infinitely many even abundant numbers.

13. Show that there are infinitely many odd abundant numbers.

14. Show that if $n = p^a q^b$, where p and q are distinct odd primes and a and b are positive integers, then n is deficient.

Two positive integers m and n are called an *amicable pair* if $\sigma(m) = \sigma(n) = m + n$.

15. Show that each of the following pairs of integers are amicable pairs.
   a) 220, 284
   b) 1184, 1210
   c) 79750, 88730

16. a) Show that if n is a positive integer with $n \geq 2$, such that $3 \cdot 2^{n-1} - 1$, $3 \cdot 2^n - 1$, and $3^2 \cdot 2^{2n-1} - 1$ are all prime, then $2^n(3 \cdot 2^{n-1} - 1)(3 \cdot 2^n - 1)$ and $2^n(3^2 \cdot 2^{2n-1} - 1)$ form an amicable pair.
   b) Find three amicable pairs using part (a).

An integer n is called *k-perfect* if $\sigma(n) = kn$. Note that a perfect number is 2-perfect.

17. Show that $120 = 2^3 \cdot 3 \cdot 5$ is 3-perfect.

18. Show that $30{,}240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$ is 4-perfect.

19. Show that $14{,}182{,}439{,}040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ is 5-perfect.

20. Find all 3-perfect numbers of the form $n = 2^k \cdot 3 \cdot p$, where p is an odd prime.

21. Show that if n is 3-perfect and $3 \nmid n$, then $3n$ is 4-perfect.

An integer n is *k-abundant* if $\sigma(n) > (k + 1)n$.

22. Find a 3-abundant integer.

23. Find a 4-abundant integer.

** 24. Show that for each positive integer k there are an infinite number of k-abundant integers.

A positive integer n is called *superperfect* if $\sigma(\sigma(n)) = 2n$.

25. Show that 16 is superperfect.

26. Show that if $n = 2^q$, where $2^{q+1} - 1$ is prime, then n is superperfect.

27. Show that every even superperfect number is of the form $n = 2^q$, where $2^{q+1} - 1$ is prime.

* **28.** Show that if $n = p^2$, where p is an odd prime, then n is not superperfect.

29. Use Theorem 7.12 to determine whether each of the following Mersenne numbers is prime.

a) M_7 c) M_{17}
b) M_{11} d) M_{29}

30. Use the Lucas-Lehmer test, Theorem 7.13, to determine whether each of the following Mersenne numbers is prime.

a) M_3 c) M_{11}
b) M_7 d) M_{13}

* **31.** Show that if n is a positive integer and $2n + 1$ is prime, then either $(2n + 1) \mid M_n$ or $(2n + 1) \mid (M_n + 2)$. (*Hint:* Use Fermat's little theorem to show that $M_n(M_n + 2) \equiv 0 \pmod{2n + 1}$.)

* **32.** a) Show that if n is an odd perfect number, then $n = p^a m^2$, where p is an odd prime, $p \equiv a \equiv 1 \pmod 4$, and m is an integer.

b) Use part (a) to show that if n is an odd perfect number, then $n \equiv 1 \pmod 4$.

* **33.** Show that if $n = p^a m^2$ is an odd perfect number, where p is prime, then $n \equiv p \pmod 8$.

* **34.** Show that if n is an odd perfect number, then 3, 5, and 7 are not all divisors of n.

* **35.** Show that if n is an odd perfect number, then n has at least three different prime divisors.

** **36.** Show that if n is an odd perfect number, then n has at least four different prime divisors.

37. Find all positive integers n such that the product of all divisors of n other than n is exactly n^2. (These integers are multiplicative analogues of perfect numbers.)

38. Let n be a positive integer. Define the *aliquot sequence* $n_1, n_2, n_3, \ldots$, recursively by $n_1 = \sigma(n) - n$ and $n_{k+1} = \sigma(n_k) - n_k$ for $k = 1, 2, 3, \ldots$. (The word *aliquot* is an adjective that means "contained an exact number of times in something else." Archaically, the *aliquot parts* of an integer were the divisors of this integer.)

a) Show that if n is perfect, then $n = n_1 = n_2 = n_3 = \cdots$.

b) Show that if n and m are an amicable pair, then $n_1 = m, n_2 = n, n_3 = m, n_4 = n, \ldots$ and so on; that is, the sequence $n_1, n_2, n_3, \ldots$ is periodic with period 2.

c) Find the aliquot sequence of integers generated if $n = 12{,}496 = 2^4 \cdot 11 \cdot 71$.

Before computers were used to examine the behavior of aliquot sequences, it was conjectured that for all integers n the aliquot sequence of integers $n_1, n_2, n_3, \ldots$ is bounded. However, evidence obtained from calculations with large integers suggests that some of these sequences are unbounded.

* **39.** Show that if n is a positive integer greater than 1, then the Mersenne number M_n cannot be the power of a positive integer.

7.3 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. Verify by direct computation that $2^{30}(2^{31} - 1)$ is perfect.
2. Show that the number 154,345,556,085,770,649,600 is a 6-perfect number (as defined in the preamble to Exercise 17).
3. Show that each of the following pairs of integers is an amicable pair (as defined in the preamble to Exercise 15).
   a) 609928, 686072
   b) 643336, 652664
   c) 938304290, 1344480478
   d) 4000783984, 4001351168
4. Find factors of as many Mersenne numbers of the form M_p, where p is prime, as you can, using Theorem 7.12.
5. Verify the primality of as many Mersenne primes as you can, using the Lucas-Lehmer test. (You may want to use GIMPS software to do this.)
6. Join the GIMPS and search for Mersenne primes.
7. Find all amicable pairs, where both integers in the pair are less than 10,000.
8. Show that the aliquot sequence (as defined in Exercise 38) obtained by taking $n = 14{,}316$ is periodic with period 28.
9. Find as many aliquot sequences as you can that are periodic with period 4.
10. Find the number of terms in the aliquot sequence obtained by taking $n = 138$ before this sequence reaches the integer 1. What is the largest term of the sequence? Can you answer the same question for $n = 276$?

Programming Projects

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

1. Classify positive integers according to whether they are deficient, perfect, or abundant (see the preamble to Exercise 5).
2. Use Theorem 7.12 to look for factors of Mersenne numbers.
3. Determine whether the Mersenne number $2^p - 1$ is prime, where p is a prime, using the Lucas-Lehmer test.
4. Given a positive integer n, determine if the aliquot sequence defined in Exercise 32 is periodic.
5. Given a positive integer n, find all amicable pairs of integers a, b, where $a \leq n$ and $b \leq n$ (see the preamble to Exercise 15).

7.4 Möbius Inversion

Let f be an arithmetic function. The formula $F(n) = \sum_{d|n} f(d)$ expresses the values of F, the summatory function of f, in terms of the values of f. Can this relationship be inverted? That is, is there a convenient way to express the values of f in terms of those of F? In this section, we will provide a useful formula that does this. We will start with some exploration, to help us see what kind of formula might exist.

Suppose that f is an arithmetic function and F is its summatory function $F(n) = \sum_{d|n} f(d)$. Expanding the definition of $F(n)$ for $n = 1, 2, \ldots, 8$, we see that

$$\begin{aligned}
F(1) &= f(1) \\
F(2) &= f(1) + f(2) \\
F(3) &= f(1) + f(3) \\
F(4) &= f(1) + f(2) + f(4) \\
F(5) &= f(1) + f(5) \\
F(6) &= f(1) + f(2) + f(3) + f(6) \\
F(7) &= f(1) + f(7) \\
F(8) &= f(1) + f(2) + f(4) + f(8),
\end{aligned}$$

and so on. When we solve these equations successively for $f(n)$, for $n = 1, 2, \ldots, 8$, we find that

$$\begin{aligned}
f(1) &= F(1) \\
f(2) &= F(2) - F(1) \\
f(3) &= F(3) - F(1) \\
f(4) &= F(4) - F(2) \\
f(5) &= F(5) - F(1) \\
f(6) &= F(6) - F(3) - F(2) + F(1) \\
f(7) &= F(7) - F(1) \\
f(8) &= F(8) - F(4).
\end{aligned}$$

Note that $f(n)$ equals a sum of terms of the form $\pm F(n/d)$, where $d \mid n$. From this evidence, it might be fruitful to look for an identity of the form

$$f(n) = \sum_{d|n} \mu(d) F(n/d),$$

where μ is an arithmetic function. If this identity holds, our computations imply that $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = 1$, $\mu(7) = -1$, and $\mu(8) = 0$. Furthermore, $F(p) = f(1) + f(p)$, which implies that $f(p) = F(p) - F(1)$, whenever p is prime. This requires that $\mu(p) = -1$. Moreover, because

$$F(p^2) = f(1) + f(p) + f(p^2),$$

we have

$$f(p^2) = F(p^2) - (F(p) - F(1)) - F(1) = F(p^2) - F(p).$$

This implies that $\mu(p^2) = 0$ for every prime p. Similar reasoning can be used to show that $\mu(p^k) = 0$ for every prime p and integer $k > 1$. If we conjecture that μ is a multiplicative function, the values of μ are determined by those at prime powers. This leads to the following definition.

Definition. The *Möbius function*, $\mu(n)$, is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where the } p_i \text{ are distinct primes;} \\ 0 & \text{otherwise.} \end{cases}$$

The Möbius function is named after *August Ferdinand Möbius*.

From the definition, we see that $\mu(n) = 0$ whenever n is divisible by the square of a prime. The only values of n for which $\mu(n) \neq 0$ are those n that are square-free.

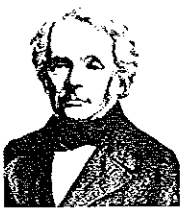
Example 7.15. From the definition of $\mu(n)$, we see that $\mu(1) = 1$, $\mu(2) = -1$, $\mu(3) = -1$, $\mu(4) = \mu(2^2) = 0$, $\mu(5) = -1$, $\mu(6) = \mu(2 \cdot 3) = 1$, $\mu(7) = -1$, $\mu(8) = \mu(2^3) = 0$, $\mu(9) = \mu(3^2) = 0$, and $\mu(10) = \mu(2 \cdot 5) = 1$. ◀

Example 7.16. We have $\mu(330) = \mu(2 \cdot 3 \cdot 5 \cdot 11) = (-1)^4 = 1$, $\mu(660) = \mu(2^2 \cdot 3 \cdot 5 \cdot 11) = 0$, and $\mu(4290) = \mu(2 \cdot 3 \cdot 5 \cdot 11 \cdot 13) = (-1)^5 = -1$. ◀

We now verify that the Möbius function is multiplicative, proceeding directly from its definition.

Theorem 7.14. The Möbius function $\mu(n)$ is a multiplicative function.

Proof. Suppose that m and n are relatively prime positive integers. To show that $\mu(n)$ is multiplicative requires that we show that $\mu(mn) = \mu(m)\mu(n)$. To establish this equality, we first consider the case when $m = 1$ or $n = 1$. When $m = 1$, we see that both $\mu(mn)$ and $\mu(m)\mu(n)$ equal $\mu(n)$. The case for $n = 1$ is similar.



AUGUST FERDINAND MÖBIUS (1790–1868) was born in the town of Schulpforta, near Naumburg, Germany. His father was a dancing teacher and his mother was a descendant of Martin Luther. Möbius was taught at home until he was 13, displaying an interest and talent in mathematics at a young age. He received formal training in mathematics from 1803 until 1809, when he entered Leipzig University. He intended to study law, but instead decided to concentrate on subjects more to his interest—mathematics, physics, and astronomy. After pursuing further studies at Göttingen, where he studied astronomy with Gauss, and at Halle, where he studied mathematics with Pfaff, he became professor of astronomy at Leipzig, remaining there until his death. Möbius made contributions to a wide range of subjects, including astronomy, mechanics, projective geometry, optics, statics, and number theory. Today, he is best known for his discovery of a surface with one side, called the *Möbius strip*, which can be formed by taking a strip of paper and connecting two opposite ends after twisting it.

Now suppose that at least one of m and n is divisible by a square of a prime. Then mn is also divisible by the square of a prime. Consequently, $\mu(mn)$ and $\mu(m)\mu(n)$ are both equal to 0. Finally, consider the remaining case when both m and n are square-free integers greater than 1. Suppose that $m = p_1 p_2 \cdots p_s$, where $p_1, p_2, \ldots, p_s$ are distinct primes, and $n = q_1 q_2 \cdots q_t$, where $q_1, q_2, \ldots, q_t$ are distinct primes. Because m and n are relatively prime, no prime occurs in both of the prime factorizations of m and n. Consequently, mn is the product of $s + t$ distinct primes. It follows that $\mu(mn) = (-1)^{s+t} = (-1)^s(-1)^t = \mu(m)\mu(n)$. ∎

We will now show that the summatory function of the Möbius function is a particularly simple function.

Theorem 7.15. The summatory function of the Möbius function at the integer n, $F(n) = \sum_{d|n} \mu(d)$, satisfies

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. First consider the case when $n = 1$. We have

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

Next, let $n > 1$. By Theorem 7.8, because μ is a multiplicative function, its summatory function $F(n) = \sum_{d|n} \mu(d)$ is also multiplicative. Now, suppose that p is prime and k is a positive integer. We see that

$$\begin{aligned} F(p^k) = \sum_{d|p^k} \mu(d) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= 1 + (-1) + 0 + \cdots + 0 = 0 \end{aligned}$$

because $\mu(p^i) = 0$ whenever $i \geq 2$. Finally, suppose that n is a positive integer, $n > 1$, with prime-power factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$. Because F is multiplicative, it follows that $F(n) = F(p_1^{a_1})F(p_2^{a_2}) \cdots F(p_t^{a_t})$. Because each of the factors on the right-hand side of this equation is 0, it follows that $F(n) = 0$. ∎

The Möbius inversion formula provides an answer to the question posed at the beginning of this section. It provides a way to express the values of f in terms of values of its summatory function F. This formula is used extensively in the study of multiplicative functions and can be used to establish new identities involving these functions.

Theorem 7.16. ***The Möbius Inversion Formula.*** Suppose that f is an arithmetic function and that F is the summatory function of f, so that

$$F(n) = \sum_{d|n} f(d).$$

Then, for all positive integers n,

$$f(n) = \sum_{d|n} \mu(d) F(n/d).$$

Proof. The proof of this formula involves some manipulations of double sums. We proceed as follows, starting with the sum on the right-hand side of the formula, substituting for $F(n/d)$ the expression $\sum_{e|(n/d)} f(e)$, which comes from the definition of the function F as the summatory function of f. We have

$$\begin{aligned}\sum_{d|n} \mu(d)F(n/d) &= \sum_{d|n}\left(\mu(d)\sum_{e|(n/d)} f(e)\right)\\ &= \sum_{d|n}\left(\sum_{e|(n/d)} \mu(d)f(e)\right).\end{aligned}$$

Note that the pairs of integers (d, e) with $d \mid n$ and $e \mid (n/d)$ are the same as those with $e \mid n$ and $d \mid (n/e)$. It follows that

$$\begin{aligned}\sum_{d|n}\left(\sum_{e|(n/d)} \mu(d)f(e)\right) &= \sum_{e|n}\left(\sum_{d|(n/e)} f(e)\mu(d)\right)\\ &= \sum_{e|n}\left(f(e)\sum_{d|(n/e)} \mu(d)\right).\end{aligned}$$

Now we see by Theorem 7.15 that $\sum_{d|(n/e)} \mu(d) = 0$ unless $n/e = 1$. When $n/e = 1$, that is, when $n = e$, this sum equals 1. Consequently,

$$\sum_{e|n}\left(f(e)\sum_{d|(n/e)} \mu(d)\right) = f(n)\cdot 1 = f(n).$$

This completes the proof. ∎

The Möbius inversion formula can be used to construct many new identities that would be difficult to prove in another manner, as the following example shows.

Example 7.17. The functions $\sigma(n)$ and $\tau(n)$ are the summatory functions of the functions $f(n) = n$ and $f(n) = 1$, respectively, as noted in Section 7.2. That is, $\sigma(n) = \sum_{d|n} d$ and $\tau(n) = \sum_{d|n} 1$. By the Möbius inversion formula, we can conclude that for all integers n,

$$n = \sum_{d|n} \mu(n/d)\sigma(d)$$

and

$$1 = \sum_{d|n} \mu(n/d)\tau(d).$$

Proving these two identities directly would be difficult. ◀

By Theorem 7.8, we know that if f is a multiplicative function, then so is its summary function, $F(n) = \sum_{d|n} f(d)$. Another useful consequence of the Möbius

inversion formula is that we can turn this statement around. That is, if the summatory function F of an arithmetic function f is multiplicative, then so is f.

Theorem 7.17. Let f be an arithmetic function with summatory $F = \sum_{d|n} f(d)$. Then, if F is multiplicative, f is also multiplicative.

Proof. Suppose that m and n are relatively prime positive integers. We want to show that $f(mn) = f(m)f(n)$. To show this, first note that by Lemma 3.7, if d is a divisor of mn, then $d = d_1d_2$ where $d_1 \mid m$, $d_2 \mid n$, and $(d_1, d_2) = 1$. Using the Möbius inversion formula and the fact that μ and F are multiplicative, we see that

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m,\, d_2|n} \mu(d_1d_2) F\left(\frac{mn}{d_1d_2}\right) \\ &= \sum_{d_1|m,\, d_2|n} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \cdot \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m)f(n). \end{aligned}$$

■

7.4 Exercises

1. Find the following values of the Möbius function.

   a) $\mu(12)$ d) $\mu(50)$ g) $\mu(10!)$
   b) $\mu(15)$ e) $\mu(1001)$
   c) $\mu(30)$ f) $\mu(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13)$

2. Find the following values of the Möbius function.

   a) $\mu(33)$ d) $\mu(740)$ g) $\mu(10!/(5!)^2)$
   b) $\mu(105)$ e) $\mu(999)$
   c) $\mu(110)$ f) $\mu(3 \cdot 7 \cdot 13 \cdot 19 \cdot 23)$

3. Find the value of $\mu(n)$ for each integer n with $100 \le n \le 110$.
4. Find the value of $\mu(n)$ for each integer n with $1000 \le n \le 1010$.
5. Find all integers n, $1 \le n \le 100$ with $\mu(n) = 1$.
6. Find all composite integers n, $100 \le n \le 200$ with $\mu(n) = -1$.

The *Mertens function* $M(n)$ is defined by $M(n) = \sum_{i=1}^{n} \mu(i)$.

7. Find $M(n)$ for all positive integers not exceeding 10.
8. Find $M(n)$ for $n = 100$.

9. Show that $M(n)$ is the difference between the number of square-free positive integers not exceeding n with an even number of prime divisors and those with an odd number of prime divisors.

10. Show that if n is a positive integer, then $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

11. Prove or disprove that there are infinitely many positive integers n such that $\mu(n) + \mu(n+1) = 0$.

12. Prove or disprove that there are infinitely many positive integers n such that $\mu(n-1) + \mu(n) + \mu(n+1) = 0$.

13. For how many consecutive integers can the Möbius function $\mu(n)$ take a nonzero value?

14. For how many consecutive integers can the Möbius function $\mu(n)$ take the value 0?

15. Show that if n is a positive integer, then $\phi(n) = n \sum_{d|n} \mu(d)/d$. (*Hint:* Use the Möbius inversion formula.)

16. Use the Möbius inversion formula and the identity $n = \sum_{d|n} \phi(n/d)$, demonstrated in Section 7.1, to show the following.
    a) $\phi(p^t) = p^t - p^{t-1}$, whenever p is prime and t is a positive integer.
    b) $\phi(n)$ is multiplicative.

17. Suppose that f is a multiplicative function with $f(1) = 1$. Show that

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_k)),$$

    where $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime-power factorization of n.

18. Use Exercise 17 to find a simple formula for $\sum_{d|n} d\mu(d)$ for all positive integers n.

19. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)/d$ for all positive integers n.

20. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)\tau(d)$ for all positive integers n.

21. Use Exercise 17 to find a simple formula for $\sum_{d|n} \mu(d)\sigma(d)$ for all positive integers n.

22. Let n be a positive integer. Show that

$$\prod_{d|n} \mu(d) = \begin{cases} -1 & \text{if } n \text{ is a prime;} \\ 0 & \text{if } n \text{ has a square factor;} \\ 1 & \text{if } n \text{ is square-free and composite.} \end{cases}$$

23. Show that

$$\sum_{d|n} \mu^2(d) = 2^{\omega(n)},$$

    where $\omega(n)$ denotes the number of distinct prime factors of n.

24. Use Exercise 23 and the Möbius inversion formula to show that

$$\mu^2(n) = \sum_{d|n} \mu(d) 2^{\omega(n/d)}.$$

25. Show that $\sum_{d|n} \mu(d)\lambda(d) = 2^{\omega(n)}$ for all positive integers n, where $\omega(n)$ is the number of distinct prime factors of n. (See the preamble to Exercise 43 in Section 7.1 for a definition of $\lambda(n)$.)

26. Show that $\sum_{d|n} \lambda(n/d)2^{\omega(d)} = 1$ for all positive integers n.

Exercises 27–29 provide a proof of the Möbius inversion formula and Theorem 7.17 using the concepts of the Dirichlet product and the Dirichlet inverse, defined in the exercise set of Section 7.1.

27. Show that the Möbius function $\mu(n)$ is the Dirichlet inverse of the function $\nu(n) = 1$.

28. Use Exercise 38 in Section 7.1 and Exercise 27 to prove the Möbius inversion formula.

29. Prove Theorem 7.17 by noting that if $F = f \star \nu$, where $\nu = 1$ for all positive integers n, then $f = F \star \mu$.

The *Mangoldt function* Λ is defined for all positive integers n by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ where } p \text{ is prime and } k \text{ is a positive integer;} \\ 0 & \text{otherwise.} \end{cases}$$

30. Show that $\sum_{d|n} \Lambda(d) = \log n$ whenever n is a positive integer.

31. Use the Möbius inversion formula and Exercise 30 to show that

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d.$$

7.4 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 $\mu(n)$ for each of the following values of n.

a) 421,602,180,943 b) 186,728,732,190 c) 737,842,183,177

2. Find $M(n)$, the value of the Mertens function at n, for each of the following integers. (See the preamble to Exercise 7 for the definition of $M(n)$.)

a) 1000 b) 10,000 c) 100,000

3. A famous conjecture made in 1897 by F. Mertens, and disproved in 1985 by A. Odlyzko and H. te Riele (in [Odte85]), was that $|M(n)| < \sqrt{n}$ for all positive integers n, where $M(n)$ is the Mertens function. Show that this conjecture, called Mertens' conjecture, is true for all integers n for as large a range as you can. Do not expect to find a counterexample, because the smallest n for which the conjecture is false is fantastically large. What is known is that there is a counterexample less than $3.21 \cdot 10^{64}$. Before the conjecture was shown to be false, it had been checked by computer for all integers n up to 10^{10}. This shows that even a tremendous amount of evidence can be misleading, because the smallest counterexample to a conjecture can nevertheless be titanically large.

Programming Projects

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

1. Given a positive integer n, find the value of $\mu(n)$.
2. Given a positive integer n, find the value of $M(n)$.
3. Given a positive integer n, check whether Mertens' conjecture holds for n, that is, whether $|M(n)| = |\sum_{i=1}^{n} \mu(i)| \leq \sqrt{n}$.

8 Cryptology

Introduction

How can you make a message secret, so that only the intended recipient of the message can recover it? This problem has interested people since ancient times, especially in diplomacy, military affairs, and commerce. In the modern world, making messages secret has become even more important, especially with the advent of electronic messaging and the Internet. This chapter is devoted to cryptology, the discipline devoted to secrecy systems. We will introduce some of the classical methods for making messages secret, starting with methods used in the Roman Empire, 2000 years ago. We will describe variations and modifications of these classical methods developed in the past two centuries, all based on modular arithmetic, and introduce the basic terminology and concepts of cryptology through our study of these methods. In all these classical systems, two people who wish to communicate privately must share a common secret key.

Since the 1970s, the notion of public key cryptography has been introduced and developed. In public key cryptography, two people who wish to communicate need not share a common key; instead, each person has both a private key that only this person knows and a public key that everyone knows. Using a public key system, you can send someone a message using their public key so that only that person can recover the message, using the corresponding private key. We will introduce the RSA cryptosystem, the most commonly used public key cryptosystem, whose security is based on the difficulty of factoring integers. We will also study a proposed public key cryptosystem, based on the knapsack problem, which (although promising) turned out not to be suitable.

Finally, we will discuss some cryptographic protocols. These are algorithms used to create agreements among two or more parties to achieve some common goal. We will show how cryptographic techniques that we have developed can be used to allow people to share common encryption keys, to sign electronic messages, to play poker electronically, and to share a secret.

8.1 Character Ciphers

Some Terminology

Before discussing specific secrecy systems, we present the basic terminology of secrecy systems. The discipline devoted to secrecy systems is called *cryptology*. *Cryptography* is the part of cryptology that deals with the design and implementation of secrecy systems, while *cryptanalysis* is aimed at "breaking" (defeating) these systems. A message that is to be altered into a secret form is called *plaintext*. A *cipher*, or *encryption, method* is a procedure method for altering a plaintext message into *ciphertext* by changing the letters of the plaintext using a transformation. The *key* determines a particular transformation from a set of possible transformations. The process of changing plaintext into ciphertext is called *encryption*, or *enciphering*, while the reverse process of changing the ciphertext back to the plaintext by the intended receiver, who possesses knowledge of the method for doing so, is called *decryption*, or *deciphering*. This, of course, is different from the process that someone other than the intended receiver uses to make the message intelligible, through cryptanalysis.

By a *cryptosystem* we mean the collection made up of a set of allowable plaintext messages, a set of possible ciphertext messages, a set of keys where each key specifies a particular encryption function, and the corresponding encryption functions and decryption functions. Formally, a cryptosystem is a system that consists of a finite set $\mathcal{P}$ of possible plaintext messages, a finite set $\mathcal{C}$ of possible ciphertext messages, a *keyspace* $\mathcal{K}$ of possible keys, and for each key k in the keyspace $\mathcal{K}$, an encryption function E_k and a corresponding decryption function D_k, such that $D_k(E_k(x)) = x$ for every plaintext message x.

The Caesar Cipher

In this chapter, we present secrecy systems based on modular arithmetic. The first of these had its origin with Julius Caesar; the newest systems that we will discuss were invented in the late 1970s. In all these systems, we start by translating letters into numbers. We take as our standard alphabet the letters of English and translate them into the integers from 0 to 25, as shown in Table 8.1.

Of course, if we were sending messages in Russian, Greek, Hebrew, or any other language, we would use the appropriate alphabet and range of integers. Also, we may want to include all ASCII characters, including punctuation marks, a symbol to indicate blanks, and the digits for representing numbers as part of the message. However, for

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical Equivalent	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 8.1 *The numerical equivalents of letters.*

the sake of simplicity, we restrict ourselves to the letters of the English alphabet. The transformation of letters to numbered equivalents can be done in many other ways (including translation to bit strings). Here we have chosen a simple and easily understood transformation for simplicity.

First, we discuss secrecy systems based on transforming each letter of the plaintext message into a different letter (or possibly the same) to produce the ciphertext. The encryption methods in these cryptosystems are called *character,* or *monographic, ciphers,* because each character is changed individually to another letter by a *substitution.* Altogether, there are 26! possible ways to produce a monographic transformation. We will discuss some particular monographic transformations based on modular arithmetic.

Julius Caesar used a cipher based on the substitution in which each letter is replaced by the letter three further down the alphabet, with the last three letters shifted to the first three letters of the alphabet. To describe this cipher using modular arithmetic, let P be the numerical equivalent of a letter in the plaintext and C be the numerical equivalent of the corresponding ciphertext letter. Then

$$C \equiv P + 3 \pmod{26}, \quad 0 \leq C \leq 25.$$

The correspondence between plaintext and ciphertext is given in Table 8.2.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table 8.2 *The correspondence of letters for the Caesar cipher.*

To encrypt a message using this transformation, we first change it to its numerical equivalent, grouping letters in blocks of five. Then we transform each number. The grouping of letters into blocks helps to prevent successful cryptanalysis based on recognizing particular words. We illustrate this procedure in Example 8.1

Example 8.1. To encrypt the message

THIS MESSAGE IS TOP SECRET,

we break it into groups of five letters. The message becomes

THISM ESSAG EISTO PSECR ET.

Converting the letters into their numerical equivalents, we obtain

19 7 8 18 12 4 18 18 0 6 4 8 18 19 14
15 18 4 2 17 4 19.

Using the Caesar transformation $C \equiv P + 3 \pmod{26}$, this becomes

22 10 11 21 15 7 21 21 3 9 7 11 21 22 17
18 21 7 5 20 7 22.

Translating back to letters, we have

WKLVP HVVDJ HLVWR SVHFU HW.

This is the encrypted message. ◀

The receiver decrypts a message in the following manner. First, the letters are converted to numbers. Then, the relationship $P \equiv C - 3 \pmod{26}$, $0 \leq P \leq 25$, is used to change the ciphertext back to the numerical version of the plaintext, and finally the message is converted to letters.

We illustrate the deciphering procedure in the following example.

Example 8.2. To decrypt the message

WKLVL VKRZZ HGHFL SKHU

encrypted by the Caesar cipher, we first change these letters into their numerical equivalents, to obtain

22 10 11 21 11 21 10 17 25 25 7 6 7 5 11 18 10 7 20.

Next, we perform the transformation $P \equiv C - 3 \pmod{26}$ to change this to plaintext, and we obtain

19 7 8 18 8 18 7 14 22 22 4 3 4 2 8 15 7 4 17.

We translate this back to letters and recover the plaintext message.

THISI SHOWW EDECI PHER

By combining the appropriate letters into words, we find that the message reads

THIS IS HOW WE DECIPHER ◀

Affine Transformation

The Caesar cipher is one of a family of similar ciphers described by a *shift transformation.*

$$C \equiv P + k \pmod{26}, \quad 0 \leq C \leq 25,$$

where k is the key representing the size of the shift of letters in the alphabet. There are 26 different transformations of this type, including the case of $k \equiv 0 \pmod{26}$, where letters are not altered, because in this case $C \equiv P \pmod{26}$.

More generally, we will consider transformations of the type

$$C \equiv aP + b \pmod{26}, \quad 0 \leq C \leq 25, \tag{8.1}$$

where a and b are integers with $(a, 26) = 1$. These are called *affine transformations*. Shift transformations are affine transformations with $a = 1$. We require that $(a, 26) = 1$, so that as P runs through a complete system of residues modulo 26, C also does. There are $\phi(26) = 12$ choices for a, and 26 choices for b, giving a total of $12 \cdot 26 = 312$ transformations of this type (one of these is $C \equiv P \pmod{26}$ obtained when $a = 1$ and $b = 0$). If the relationship between plaintext and ciphertext is described by (8.1), then the inverse relationship is given by

$$P \equiv \overline{a}(C - b) \pmod{26}, \quad 0 \leq P \leq 25,$$

where $\overline{a}$ is an inverse of $a \pmod{26}$, which can be found using the congruence $\overline{a} \equiv a^{\phi(26)-1} = a^{11} \pmod{26}$.

We illustrate how affine transformations work in Example 8.3.

Example 8.3. Let $a = 7$ and $b = 10$ in an affine cipher with $C \equiv aP + b \pmod{26}$, so that $C \equiv 7P + 10 \pmod{26}$. Note that $P \equiv 15(C - 10) \equiv 15C + 6 \pmod{26}$, because 15 is an inverse of 7 modulo 26. The correspondence between letters is given in Table 8.3.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	10	17	24	5	12	19	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3
Ciphertext	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D

Table 8.3 *The correspondence of letters for the cipher with* $C \equiv 7P + 10$ *(mod* 26*).*

To illustrate how we obtained this correspondence, note that the plaintext letter L with numerical equivalent 11 corresponds to the ciphertext letter J, because $7 \cdot 11 + 10 = 87 \equiv 9 \pmod{26}$ and 9 is the numerical equivalent of J.

To illustrate how to encrypt, note that

PLEASE SEND MONEY

is transformed to

LJMKG MGMXF QEXMW.

Also note that the ciphertext

FEXEN ZMBMK JNHMG MYZMN

corresponds to the plaintext

DONOT REVEA LTHES ECRET,

or, combining the appropriate letters,

DO NOT REVEAL THE SECRET. ◀

We now discuss some of the techniques directed at the cryptanalysis of ciphers based on affine transformations. In attempting to break a monographic cipher, the frequency of letters in the ciphertext is compared with the frequency of letters in ordinary text. This gives information concerning the correspondence between letters. In various frequency counts of English text, one finds the percentages listed in Table 8.4 for the occurrence of the 26 letters of the alphabet. Counts of letter frequencies in other languages may be found in [Fr78] and [Ku76].

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency (in %)	7	1	3	4	13	3	2	3	8	<1	<1	4	3	8	7	3	<1	8	6	9	3	1	1	<1	2	<1

Table 8.4 *The frequencies of occurrence of the letters of the alphabet.*

From this information, we see that the most frequently occurring letters in typical English text are E, T, N, R, I, O, and A, with E occurring substantially more than the other letters, 13% of the time, and T, N, R, I, O, and A each occurring between 7% and 9% of the time. We can use this information to determine which cipher based on an affine transformation has been used to encrypt a message. We illustrate how this cryptanalysis is done in the following example.

Example 8.4. Suppose that we know in advance that a shift cipher has been employed to encrypt a message; each letter of the message has been transformed by a correspondence $C \equiv P + k \pmod{26}$, $0 \leq C \leq 25$. To cryptanalyze the ciphertext

```
YFXMP  CESPZ  CJTDF  DPQFW  QZCPY
NTASP  CTYRX  PDDLR  PD,
```

we first count the number of occurrences of each letter in the ciphertext. This is displayed in Table 8.5.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number of Occurrences	1	0	4	5	1	3	0	0	0	1	0	1	1	1	0	7	2	2	2	3	0	0	1	2	3	2

Table 8.5 *The number of occurrences of letters in a ciphertext.*

We notice that the most frequently occurring letter in the ciphertext is P, with the letters C, D, F, T, and Y occurring with relatively high frequency. Our initial guess would be that P represents E, since E is the most frequently occurring letter in English text. If this is so, then $15 \equiv 4 + k \pmod{26}$, so that $k \equiv 11 \pmod{26}$. Consequently, we would have $C \equiv P + 11 \pmod{26}$ and $P \equiv C - 11 \pmod{26}$. This correspondence is given in Table 8.6.

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O

Table 8.6 *Correspondence of letters for the sample ciphertext.*

Using this correspondence, we attempt to decrypt the message. We obtain

NUMBE RTHEO RYISU SEFUL FOREN
CIPHE RINGM ESSAG ES.

This can easily be read as

NUMBER THEORY IS USEFUL FOR
ENCIPHERING MESSAGES.

Consequently, we made the correct guess. If we had tried this transformation, and instead of plaintext, it produced garbled text, we would have tried another likely transformation based on the frequency count of letters in the ciphertext. ◀

Example 8.5. Suppose we know that an affine transformation of the form $C \equiv aP + b \pmod{26}$, $0 \leq C \leq 25$, has been used for encryption. For instance, suppose that we wish to cryptanalyze the encrypted message

USLEL JUTCC YRTPS URKLT YGGFV
ELYUS LRYXD JURTU ULVCU URJRK
QLLQL YXSRV LBRYZ CYREK LVEXB
RYZDG HRGUS LJLLM LYPDJ LJTJU
FALGU PTGVT JULYU SLDAL TJRWU
SLJFE OLPU.

The first thing to do is to count the occurrences of each letter; this count is displayed in Table 8.7.

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number of Occurrences	2	2	4	4	5	3	6	1	0	10	3	22	1	0	1	4	2	12	7	8	16	5	1	3	10	2

Table 8.7 *The number of occurrences of letters in a ciphertext.*

With this information, we guess that the letter L, which is the most frequently occurring letter in the ciphertext, corresponds to E, while the letter U, which occurs with the second-highest frequency, corresponds to T. This implies, if the transformation is of the form $C \equiv aP + b \pmod{26}$, the pair of congruences

$$4a + b \equiv 11 \pmod{26}$$
$$19a + b \equiv 20 \pmod{26}.$$

By Theorem 4.15 we see that the solution of this system is $a \equiv 11 \pmod{26}$ and $b \equiv 19 \pmod{26}$.

If this is the correct enciphering transformation, then using the fact that 19 is an inverse of 11 modulo 26, the deciphering transformation is

$$P \equiv 19(C - 19) \equiv 19C - 361 \equiv 19C + 3 \pmod{26}, \ 0 \leq P \leq 25$$

This gives the correspondence found in Table 8.8.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ciphertext	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	0	19	12	5	24	17	10
Plaintext	D	W	P	I	B	U	N	G	Z	S	L	E	X	Q	J	C	V	O	H	A	T	M	F	Y	R	K

Table 8.8 *The correspondence of letters for the sample ciphertext.*

With this correspondence, we try to read the ciphertext, which becomes

THEBE	STAPP	ROACH	TOLEA	RNNUM
BERTH	EORYI	STOAT	TEMPT	TOSOL
VEEVE	RYHOM	EWORK	PROBL	EMBYW
ORKIN	GONTH	ESEEX	ERCIS	ESAST
UDENT	CANMA	STERT	HEIDE	ASOFT
HESUB	JECT			

We leave it to the reader to combine the appropriate letters into words to see that the message is intelligible. ◀

The methods described in this section can be extended to construct cryptosystems more difficult to break than character ciphers. For example, plaintext letters can be shifted by different amounts, as is done in Vigenère ciphers, described in Section 8.2. Additional methods based on enciphering blocks of letters, rather than individual characters will also be described in Section 8.2 and in subsequent sections of this chapter, as will ciphers where the key used to encrypt characters changes from character to character.

8.1 Exercises

1. Using the Caesar cipher, encrypt the message ATTACK AT DAWN.
2. Decrypt the ciphertext message LFDPH LVDZL FRQTX HUHG, which has been encrypted using the Caesar cipher.
3. Encrypt the message SURRENDER IMMEDIATELY using the affine transformation $C \equiv 11P + 18 \pmod{26}$.

4. Encrypt the message THE RIGHT CHOICE using the affine transformation $C \equiv 15P + 14 \pmod{26}$.

5. Decrypt the message YLFQX PCRIT, which was encrypted using the affine transformation $C \equiv 21P + 5 \pmod{26}$.

6. Decrypt the message RTOLK TOIK, which was encrypted using the affine transformation $C \equiv 3P + 24 \pmod{26}$.

7. If the most common letter in a long ciphertext, encrypted by a shift transformation $C \equiv P + k \pmod{26}$ is Q, then what is the most likely value of k?

8. The message KYVMR CLVFW KYVBV PZJJV MVEKV VE was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use frequencies of letters to determine the value of k. What is the plaintext message?

9. The message IVQLM IQATQ SMIKP QTLVW VMQAJ MBBMZ BPIVG WCZWE VNZWU KPQVM AMNWZ BCVMK WWSQM was encrypted using a shift transformation $C \equiv P + k \pmod{26}$. Use frequencies of letters to determine the value of k. What is the plaintext message?

10. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \pmod{26}$, are X and Q, respectively, then what are the most likely values for a and b?

11. If the two most common letters in a long ciphertext, encrypted by an affine transformation $C \equiv aP + b \pmod{26}$, are W and B, respectively, then what are the most likely values for a and b?

12. The message MJMZK CXUNM GWIRY VCPUW MPRRW GMIOP MSNYS RYRAZ PXMCD WPRYE YXD was encrypted using an affine transformation $C \equiv aP + b \pmod{26}$. Use frequencies of letters to determine the values of a and b. What is the plaintext message?

13. The message WEZBF TBBNJ THNBT ADZOE TGTYR BZAJN ANOOZ ATWGN ABOVG FNWZV A was encrypted using an affine transformation $C \equiv aP + b \pmod{26}$. the most common letters in the plaintext are A, E, N, and S. What is the plaintext message?

14. The message PJXFJ SWJNX JMRTJ FVSUJ OOJWF OVAJR WHEOF JRWJO DJFFZ BJF was encrypted using an affine transformation $C \equiv aP + b \pmod{26}$. Use frequencies of letters to determine the values of a and b. What is the plaintext message?

Given two ciphers, plaintext may be encrypted by first using one of the ciphers, and then using the other cipher on this result. This procedure produces a *product cipher.*

15. Find the product cipher obtained by using the transformation $C \equiv 5P + 13 \pmod{26}$ followed by the transformation $C \equiv 17P + 3 \pmod{26}$.

16. Find the product cipher obtained by using the transformation $C \equiv aP + b \pmod{26}$ followed by the transformation $C \equiv cP + d \pmod{26}$, where $(a, 26) = (c, 26) = 1$.

8.1 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 frequency of the letters of the English alphabet in different types of English text, such as in this book, in computer programs, and in a novel.
2. Encrypt some messages using affine transformations, as ciphertexts for your classmates to decipher.
3. Decrypt messages that were enciphered by your classmates using affine transformations, using letter-frequency analysis.

Programming Projects

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

1. Encrypt messages using the Caesar cipher.
2. Encrypt messages using the transformation $C \equiv P + k \pmod{26}$, where k is a given integer.
3. Encrypt messages using the transformation $C \equiv aP + b \pmod{26}$, where a and b are integers with $(a, 26) = 1$.
4. Decrypt messages that have been encrypted using the Caesar cipher.
5. Decrypt messages that have been encrypted using the transformation $C \equiv P + k \pmod{26}$, where k is a given integer.
6. Decrypt messages that have been encrypted using the transformation $C \equiv aP + b \pmod{26}$, where a and b are integers with $(a, 26) = 1$.

* 7. Cryptanalyze, using frequency counts, ciphertext that was encrypted using a transformation of the form $C \equiv P + k \pmod{26}$, where k is an unknown integer.

* 8. Cryptanalyze, using frequency counts, ciphertext that was encrypted using a transformation of the form $C \equiv aP + b \pmod{26}$, where a and b are unknown integers with $(a, 26) = 1$.

8.2 Block and Stream Ciphers

In Section 8.1, we studied character (or monographic) ciphers based on the substitution of characters. These ciphers are vulnerable to cryptanalysis based on the frequency of letters in the ciphertext. To avoid this weakness, we can use ciphers that substitute for each block of plaintext letters of a specified length a block of ciphertext letters of the same length. Ciphers of this sort are called *block,* or *polygraphic,* ciphers. In this section, we will discuss several varieties of block ciphers, including polygraphic ciphers based on modular arithmetic. We will describe a cipher known since the sixteenth century that employs several different character ciphers determined by a keyword, and a cipher

invented by Hill around 1930 (see [Hi31]) that encrypts blocks using modular matrix multiplication. We will also discuss (but not describe in full detail) a more complicated block cipher important in commercial use, the Data Encryption Algorithm. At the end of this section, we will describe another type of cipher, a stream cipher, where the key can change as successive characters (or bits) are encrypted.

Vigenère Ciphers

We begin by describing the *Vigenère cipher,* named for French diplomat and cryptographer *Blaise de Vigenère.* Instead of encrypting each letter of a plaintext message in the same way, we will vary how we encrypt letters. The key of a Vigenère cipher consists of a keyword $\ell_1\ell_2 \ldots \ell_n$. Suppose that the numerical equivalents of the letters $\ell_1, \ell_2, \ldots, \ell_n$ are $k_1, k_2, \ldots, k_n$, respectively. To encrypt a plaintext message, we first split it into blocks of length n. A block consisting of letters with numerical equivalents $p_1, p_2, \ldots, p_n$ is transformed into a ciphertext block of letters with numerical equivalents $c_1, c_2, \ldots, c_n$ using a sequence of shift ciphers with

$$c_i \equiv p_i + k_i \pmod{26}, \quad 0 \leq c_i \leq 25,$$

for $i = 1, 2, \ldots, n$. The *Vigenère ciphers* are the encryption algorithms for the cryptosystem where blocks of plaintext letters of length n are encrypted to blocks of ciphertext letters of the same length. The keys are n-tuples $(k_1, k_2, \ldots, k_n)$ of letters. (A terminal group of fewer than n dummy letters can be used to fill out a final block.) That is, Vigenère ciphers can be thought of as block ciphers operating on blocks of length n using keys of length n.

Example 8.6. To encrypt the plaintext message MILLENNIUM using the key YTWOK for a Vigenère cipher, we first translate the message and the key into their numerical

BLAISE DE VIGENÈRE (1523–1596), born in the village of Saint-Pourçain, France, received an excellent education. At 17 he was sent to court, and at 22 to the Diet of Worms as a secretary. He became a secretary for the Duke of Nevers in 1547, and in 1549 he was sent to Rome as a diplomat. While there he read numerous books on cryptography, a subject that he discussed with experts of the papal curia. In 1570, after a long career in diplomacy, interrupted by a period of study, Vigenère retired from court. He married a young wife, turned his annuity over to the poor of Paris, and dedicated himself to writing. He was the author of more than 20 books, the best known being his *Traicté des Chiffres,* written in 1585. In this book, Vigenère provides a comprehensive overview of cryptography. He discusses polyalphabetic ciphers at length and introduces several variations of known polyalphabetic ciphers, including the autokey cipher. Many historians believe that this cipher should have been called the "Vigenère" rather than the simpler one that now bears his name.

Vigenère did not write only about cryptography. His *Traicté des Chiffres* also contains discussions of magic, alchemy, and the mysteries of the universe. His *Traicté des Comètes* helped destroy the myth that God flings comets at Earth to warn people to stop sinning.

equivalents. The letters of the message and the letters of the key translate to

$$p_1p_2p_3p_4p_5p_6p_7p_8p_9p_{10} = 12\ 8\ 11\ 11\ 4\ 13\ 13\ 8\ 20\ 12$$

and

$$k_1k_2k_3k_4k_5 = 24\ 19\ 22\ 14\ 10,$$

respectively. Applying the Vigenère cipher with the specified key, we find that the characters in the encrypted message are:

$$\begin{aligned}
c_1 &= p_1 + k_1 = 12 + 24 \equiv 10 \pmod{26}\\
c_2 &= p_2 + k_2 = 8 + 19 \equiv 1 \pmod{26}\\
c_3 &= p_3 + k_3 = 11 + 22 \equiv 7 \pmod{26}\\
c_4 &= p_4 + k_4 = 11 + 14 \equiv 25 \pmod{26}\\
c_5 &= p_5 + k_5 = 4 + 10 \equiv 14 \pmod{26}\\
c_6 &= p_6 + k_1 = 13 + 24 \equiv 11 \pmod{26}\\
c_7 &= p_7 + k_2 = 13 + 19 \equiv 6 \pmod{26}\\
c_8 &= p_8 + k_3 = 8 + 22 \equiv 4 \pmod{26}\\
c_9 &= p_9 + k_4 = 20 + 14 \equiv 8 \pmod{26}\\
c_{10} &= p_{10} + k_5 = 12 + 10 \equiv 22 \pmod{26}.
\end{aligned}$$

Translating the numerical equivalents of numbers back to letters we see that the encrypted message is KBHZO LGEIW. ◀

Example 8.7. To decrypt the ciphertext message FFFLB CVFX encrypted using a Vigenère cipher with key ZORRO, we first translate the letters of the ciphertext message into their numerical equivalents to obtain $c_1c_2c_3c_4c_5c_6c_7c_8c_9 = 5\ 5\ 5\ 11\ 1\ 2\ 21\ 5\ 23$. The numerical equivalents of the letters in the key are $k_1k_2k_3k_4k_5 = 25\ 14\ 17\ 17\ 14$. To obtain the numerical equivalents of the plaintext letters, we proceed as follows:

$$\begin{aligned}
p_1 &\equiv c_1 - k_1 = 5 - 25 \equiv 6 \pmod{26}\\
p_2 &\equiv c_2 - k_2 = 5 - 14 \equiv 17 \pmod{26}\\
p_3 &\equiv c_3 - k_3 = 5 - 17 \equiv 14 \pmod{26}\\
p_4 &\equiv c_4 - k_4 = 11 - 17 \equiv 20 \pmod{26}\\
p_5 &\equiv c_5 - k_5 = 1 - 14 \equiv 13 \pmod{26}\\
p_6 &\equiv c_6 - k_1 = 2 - 25 \equiv 3 \pmod{26}\\
p_7 &\equiv c_7 - k_2 = 21 - 14 \equiv 7 \pmod{26}\\
p_8 &\equiv c_8 - k_3 = 5 - 17 \equiv 14 \pmod{26}\\
p_9 &\equiv c_9 - k_4 = 23 - 17 \equiv 6 \pmod{26}.
\end{aligned}$$

Translating the numerical equivalents back to letters, we see that the plaintext message was GROUNDHOG. ◀

Cryptanalysis of Vigenère Ciphers

The Vigenère cipher was considered unbreakable for many years. It was used extensively to encrypt sensitive information transmitted by telegraphy. However, by the mid-nineteenth century, techniques were developed that could successfully break Vigenère ciphers. In 1863, Friedrich Kasiski, a Prussian military officer, described a method, now known as *Kasiski's test,* for determining the key length of a Vigenère cipher. Once the key length is known, frequency analysis of letters in the ciphertext can be used to determine the characters of the key. As with many discoveries named after their presumed first inventor, Kasiski was not the first person to discover this method. We now know that Charles Babbage discovered the same test in 1854. However, the publication of Babbage's discovery was delayed for many years. The reason for this delay was British national security. The British military used Babbage's test to break secret messages sent by their adversaries and did not want this to become known.

Kasiski's method is based on finding identical strings in ciphertext. When a message is encrypted using a Vigenère cipher with key length n, identical strings of plaintext separated by a multiple of n are encrypted to the same string (see Exercise 5). Kasiski's test is based on locating identical strings in the ciphertext, generally of length three or more, which likely correspond to identical strings in the plaintext. For each pair of identical ciphertext strings, we determine the difference between the positions of their initial characters. Suppose ther are k such pairs of identical strings in the ciphertext and $d_1, d_2, d_3, \ldots, d_k$ are the differences in the positions of their initial characters. If these pairs of identical ciphertext strings really do correspond to identical plaintext strings, the key length n must divide each of the integers $d_i, i = 1, 2, \ldots, k$. It would then follow that n divides the greatest common divisor of these integers, $(d_1, d_2, \ldots, d_k)$.

Because different strings of plaintext may be encrypted to the same ciphertext by different parts of the encyption key, some differences in starting positions of identical strings of ciphertext are extraneous and should be discarded. To overcome this problem, we can compute the greatest common divisor of some, but not all, these differences.

We can run a second test to help us assess whether we have found the correct key length. This test, developed by the famous American cryptographer William Friedman in 1920, estimates the key length of a Vigenère cipher by studying the variation in frequencies of ciphertext letters. Friedman observed that there is considerable variation in the frequencies of the letters in English text, but as the length of the key used in a Vigenère cipher increases, this variation becomes smaller and smaller.

Friedman introduced a measure called the *index of coincidence.* Given a string of n characters $x_1, x_2, \ldots, x_n$, its index of coincidence, denoted by IC, is the probability that two randomly chosen elements of this string are the same. We now assume that we are working with strings of English letters and that the letters $A, B, \ldots, Y$, and Z occur $f_0, f_1, \ldots, f_{24}$, and f_{25} times, respectively, in a string.

Because the ith letter occurs f_i times, there are

$$\binom{f_i}{2} = \frac{f_i(f_i - 1)}{2}$$

ways to choose two of its elements so that both are the ith character. Because there are $\binom{n}{2} = n(n-1)/2$ ways to choose two characters in the string, we can conclude that the index of coincidence for this string is

$$IC = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}.$$

Now consider a string of English plaintext. If the plaintext is sufficiently long, we expect the frequencies of letters to approximate their frequencies in typical English (shown in Table 8.4). Suppose that $p_0, p_1, \ldots, p_{25}$ are the expected probabilities of $A, B, \ldots, Y$, and Z, respectively. It follows that the probability two randomly chosen letters are both A is p_0^2, the probability both are B is p_1^2, and so on. Consequently, we would expect the index of coincidence of this plaintext to be approximately

$$\sum_{i=0}^{25} p_i^2 \approx 0.065.$$

(The values $p_i, i = 0, 1, \ldots, 25$ used in this computation can be found in [St02].) Moreover, this reasoning applies for ciphertext produced by character ciphers. For a character cipher the probability of occurrence of a character in ciphertext equals the probability of occurrence of the corresponding plaintext character. Consequently, for ciphertext encrypted with a character cipher, the terms of the sum $\sum_{i=0}^{25} p_i^2$ are permuted, but the sum is not changed.

To use indices of coincidence to determine whether we have guessed correctly that the key has length k, we break the ciphertext message into k different parts. The first part contains characters in positions $1, k+1, 2k+1, \ldots$; the second part contains the characters in positions $2, k+2, 2k+2, \ldots$; and so on. We compute the index of coincidence for each of these different parts separately. If our guess was correct, each of these indices of coincidence should be approximately 0.065. However, if we guessed wrong, these values will most likely be less than 0.065. They probably will be considerably closer to the index of coincidence of a random string of English characters, namely $1/26 \approx 0.038$. (This index of coincidence can be computed using the probabilities of occurrence of letters in typical English text.)

For each part of the ciphertext, we attempt to find the letter of the key that was used to encrypt letters in this part by examining letter frequencies. We determine the most likely possibilities for the letters of the key by determining the letters that are most frequent in the ciphertext and presuming they correspond with the most common letters of English. To determine whether we have guessed correctly, we can compare the frequencies we expect when letters are encrypted by shifting them using this letter of the key with the observed frequencies for this part of the ciphertext.

Once we have made our best guess for each letter of the key, we attempt to decrypt the message using the key we have computed. If we recover a meaningful plaintext message we presume we have recovered the correct plaintext. On the other hand, if we end up with nonsense, we go back to the drawing board and check out other possibilities.

We illustrate the cryptanalysis of ciphertext encrypted using a Vigenère cipher in the following example.

Example 8.8. Suppose that the ciphertext produced by encrypting plaintext using a Vigenère cipher is

QWH I D	DNZEM	WTLMT	BKTIT	EMWLZ
WVCVE	HLTBS	TUDLG	WNUJE	WJEUL
EXWQO	SLNZA	NLHYQ	ALWEH	VOQWD
VQTBW	ILURY	STIJW	CLHWW	RNSIH
MNUDI	YFAVD	ELAGB	LSNZA	NSMIF
GNZEM	WALWL	CXEFA	BYJTS	SNXLH
YHULK	UCLOZ	ZAJHI	HWSM	

We describe the steps we use to break this message. We first use the Kasiski test, looking for repeated triples of letters in the ciphertext. We list our finding in a table.

Triple	Starting positions	Differences in starting positions
EMW	9, 21, 129	12, 108, 120
ZEM	8, 128	120
ZAN	59, 119	60
NZE	7, 127	120
NZA	58, 118	60
LHY	62, 149	87
ALW	66, 132	66

The differences between identical ciphertext blocks of length three are 12, 60, 66, 87, 108, and 120. Because $(12, 60, 66, 87, 108, 120) = 3$, we guess that the key length equals 3.

Assuming that this guess is correct, we split the ciphertext into three separate parts. The first contains the letters in positions $1, 4, 7, \ldots, 169$; the second contains the letters in positions $2, 5, 8, \ldots, 167$; and the third contains the letters in positions, $3, 6, 9, \ldots, 168$. To confirm that our guess is correct, we compute the indices of coincidence for each of these three parts of the ciphertext, obtaining 0.071, 0.109, and 0.091, respectively. (We leave the details of these computations to the reader. See Exercise 12.) One of these numbers is relatively close to the index of coincidence for English text, 0.065, and the other two are even larger. This indicates that 3 might be the correct key length. Because our ciphertext is rather short, we are not too worried that these indices of coincidence are not as close to 0.065 as we might like. Note that if our guess was wrong, we would expect some of these indices of coincidence to be smaller than 0.065, perhaps even near 0.038.

After some work, which we leave to the reader, we find the key used to encrypt the message is USA and the corresponding plaintext is

WEHOL	DTHES	ETRUT	HSTOB	ESELF
EVIDE	NTTHA	TALLM	ENARE	CREAT
EDEQU	ALTHA	TTHEY	AREEN	DOWED
BYTHE	IRCRE	ATORW	ITHCE	RTAIN
UNALI	ENABL	ERIGH	TSTHA	TAMON
GTHES	EAREL	IFELI	BERTY	ANDTH
EPURS	UITOF	HAPPI	NESS	

This plaintext comes from the Declaration of Independence of the United States. It reads: "We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness." For more information on cryptanalysis of Vigenère ciphers, see [St02] and [TrWa02]. ◀

Hill Ciphers

Hill ciphers are block ciphers invented by *Lester Hill* in 1929. To introduce Hill ciphers, we first consider *diagraphic ciphers*; in these ciphers, each block of two letters of plaintext is replaced by a block of two letters of ciphertext. We illustrate this process with an example.

Example 8.9. To encrypt a message using digraphic Hill ciphers, we first split a message into blocks of two letters (adding a dummy letter, say X, at the end of the message, if necessary, so that the final block has two letters). For instance, the message

THE GOLD IS BURIED IN ORONO

is split up as

TH EG OL DI SB UR IE DI NO RO NO.

Next, these letters are translated into their numerical equivalents (as in previous examples) to obtain

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8
13 14 17 14 13 14.

LESTER S. HILL (1891–1961) was born in New York City. He graduated from Columbia College and received his Ph.D. in mathematics from Yale University in 1926. He held positions at the University of Montana, Princeton University, the University of Maine, Yale University, and Hunter College. Hill was interested in applications of mathematics to communications. He developed methods for checking the accuracy of telegraphed code numbers and the encryption method known as the Hill cipher. Hill continued to submit cryptographic papers to the United States Navy mostly dealing with polygraphic ciphers for more than 30 years.

Each block of two plaintext numbers P_1P_2 is converted into a block of two ciphertext numbers C_1C_2 by defining C_1 to be the least nonnegative residue modulo 26 of a linear combination of P_1 and P_2, and defining C_2 to be the least nonnegative residue modulo 26 of a different linear combination of P_1 and P_2. For example, we can let

$$C_1 \equiv 5P_1 + 17P_2 \pmod{26}, \quad 0 \le C_1 < 26$$
$$C_2 \equiv 4P_1 + 15P_2 \pmod{26}, \quad 0 \le C_2 < 26,$$

in which case the first block 19 7 is converted to 6 25, because

$$C_1 \equiv 5 \cdot 19 + 17 \cdot 7 \equiv 6 \pmod{26}$$
$$C_2 \equiv 4 \cdot 19 + 15 \cdot 7 \equiv 25 \pmod{26}.$$

After performing this operation on the entire message, the following ciphertext is obtained:

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2 17 2 11 18 17 2.

When these blocks are translated into letters, we have the ciphertext message

GZ SC XN VC DJ ZX EO VC RC LS RC.

The decryption procedure for this cryptosystem is obtained by using Theorem 4.15. To find the plaintext block P_1P_2 corresponding to the ciphertext block C_1C_2, we use the relationship

$$P_1 \equiv 17C_1 + 5C_2 \pmod{26}$$
$$P_2 \equiv 18C_1 + 23C_2 \pmod{26}.$$

(The reader should verify that this relationship is implied by Theorem 4.15.) ◀

The digraphic cipher system in Example 8.9 is conveniently described using matrices. For this cryptosystem, we have

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \equiv \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \pmod{26}.$$

By Theorem 4.17, we see that the matrix $\begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix}$ is an inverse of $\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$ modulo 26. Hence, Theorem 4.16 tells us that decryption can be done using the relationship

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \pmod{26}.$$

In general, a Hill cryptosystem may be obtained by splitting plaintext into blocks of n letters, translating the letters into their numerical equivalents, and forming ciphertext using the relationship

$$\mathbf{C} \equiv \mathbf{AP} \pmod{26},$$

where $\mathbf{A}$ is an $n \times n$ matrix, $(\det \mathbf{A}, 26) = 1$, $\mathbf{C} = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix}$ and $\mathbf{P} = \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{pmatrix}$, and $C_1C_2 \ldots C_n$ is the ciphertext block that corresponds to the plaintext block $P_1P_2 \ldots P_n$. Finally, the ciphertext numbers are translated back to letters. For decryption, we use the matrix $\overline{\mathbf{A}}$, an inverse of $\mathbf{A}$ modulo 26, which may be obtained using Theorem 4.19. Because $\overline{\mathbf{A}}\mathbf{A} \equiv \mathbf{I} \pmod{26}$, we have

$$\overline{\mathbf{A}}\mathbf{C} \equiv \overline{\mathbf{A}}(\mathbf{AP}) \equiv (\overline{\mathbf{A}}\mathbf{A})\mathbf{P} \equiv \mathbf{P} \pmod{26}.$$

Hence, to obtain plaintext from ciphertext, we use the relationship

$$\mathbf{P} \equiv \overline{\mathbf{A}}\mathbf{C} \pmod{26}.$$

Example 8.10. We illustrate this procedure using $n = 3$ and the encrypting matrix

$$\mathbf{A} = \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}.$$

Because $\det \mathbf{A} \equiv 5 \pmod{26}$, we have $(\det \mathbf{A}, 26) = 1$. To encrypt a plaintext block of length three, we use the relationship

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \mathbf{A} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \pmod{26}.$$

To encrypt the message STOP PAYMENT, we first split the message into blocks of three letters, adding a final dummy letter X to fill out the last block. We have plaintext blocks.

STO PPA YME NTX.

We translate these letters into their numerical equivalents:

18 19 14 15 15 0 24 12 4 13 19 23.

We obtain the first block of ciphertext in the following way:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \equiv \begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix} \begin{pmatrix} 18 \\ 19 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 19 \\ 13 \end{pmatrix} \pmod{26}.$$

Encrypting the entire plaintext message in the same manner, we obtain the ciphertext message

8 19 13 13 4 15 0 2 22 20 11 0.

Translating this message into letters, we have our ciphertext message

ITN NEP ACW ULA.

The decrypting process for this polygraphic cipher system takes a ciphertext block and obtains a plaintext block using the transformation

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \equiv \overline{\mathbf{A}} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \pmod{26},$$

where

$$\overline{\mathbf{A}} = \begin{pmatrix} 6 & -5 & 11 \\ -5 & -1 & -10 \\ -7 & 3 & 7 \end{pmatrix}$$

is an inverse of $\mathbf{A}$ modulo 26, which may be obtained using Theorem 4.19.

Because polygraphic ciphers operate with blocks, rather than with individual letters, they are not vulnerable to cryptanalysis based on letter frequency. However, polygraphic ciphers operating with blocks of size n are vulnerable to cryptanalysis based on frequencies of blocks of size n. For instance, with a digraphic cryptosystem, there are $26^2 = 676$ digraphs, blocks of length two. Studies have been done to compile the relative frequencies of digraphs in typical English text. By comparing the frequencies of digraphs in the ciphertext with the average frequencies of digraphs, it is often possible to successfully attack digraphic ciphers. For example, according to some counts, the most common digraph in English is TH, followed closely by HE. If a Hill digraphic cryptosystem has been employed and the most common digraph is KX, followed by VZ, we may guess that the ciphertext digraphs KX and VZ correspond to TH and HE, respectively. This would mean that the blocks 19 7 and 7 4 are sent to 10 23 and 21 25, respectively. If $\mathbf{A}$ is the encrypting matrix, this implies that

$$\mathbf{A} \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} \equiv \begin{pmatrix} 10 & 21 \\ 23 & 25 \end{pmatrix} \pmod{26}.$$

Because $\begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$ is an inverse of $\begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}$ (mod 26), we find that

$$\mathbf{A} \equiv \begin{pmatrix} 10 & 21 \\ 23 & 25 \end{pmatrix} \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \equiv \begin{pmatrix} 23 & 17 \\ 21 & 2 \end{pmatrix} \pmod{26},$$

which gives a possible key. After attempting to decrypt the ciphertext using $\overline{\mathbf{A}} = \begin{pmatrix} 2 & 9 \\ 5 & 23 \end{pmatrix}$ to transform it, we would know whether our guess was correct. ◀

In general, if we know n correspondences between plaintext blocks of size n and ciphertext blocks of size n—for instance, if we know that the ciphertext blocks $C_{1j}C_{2j}\ldots C_{nj}$, $j = 1, 2, \ldots, n$, correspond to the plaintext blocks $P_{1j}P_{2j}\ldots P_{nj}$, $j = 1, 2, \ldots, n$, respectively—then we have

$$\mathbf{A}\begin{pmatrix} P_{1j} \\ \vdots \\ P_{nj} \end{pmatrix} \equiv \begin{pmatrix} C_{1j} \\ \vdots \\ C_{nj} \end{pmatrix} \pmod{26},$$

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

These n congruences can be succinctly expressed using the matrix congruence

$$\mathbf{AP} \equiv \mathbf{C} \pmod{26},$$

where $\mathbf{P}$ and $\mathbf{C}$ are $n \times n$ matrices with ijth entries P_{ij} and C_{ij}, respectively. If $(\det \mathbf{P}, 26) = 1$, then we can find the encrypting matrix $\mathbf{A}$ via

$$\mathbf{A} \equiv \mathbf{C}\overline{\mathbf{P}} \pmod{26},$$

where $\overline{\mathbf{P}}$ is an inverse of $\mathbf{P}$ modulo 26.

Cryptanalysis using frequencies of polygraphs is only worthwhile for small values of n, where n is the size of the polygraphs. When $n = 10$, for example, there are 26^{10}, which is approximately 1.4×10^{14}, polygraphs of this length. Any analysis of the relative frequencies of these polygraphs is extremely infeasible.

The Data Encryption Standard and Related Ciphers

The most important cipher that has been used for commercial and government applications during the past 20 years is the Data Encryption Algorithm (DEA), which was standardized in 1977 by the federal government as part of the Data Encryption Standard (DES) (Federal Information Processing Standard 46-1). It was developed by IBM and was known as Lucifer before it became a standard. The DEA is a block cipher that encrypts 64-bit blocks using a 64-bit key (where the last 8 bits of the key are parity check bits stripped off before use) transforming them into 64-bit ciphertext blocks.

The encryption procedure used by the DEA is extremely complicated and will not be described in detail here. Basically, a plaintext block of 64 bits is encrypted by first permuting the 64 bits, iterating a function that operates on the left and right halves of a string of 64 bits in a particular way 16 times, and then applying the inverse of the initial permutation. Details of this cipher can be found in [St02] and [MevaVa97]. These details are easily understandable by anyone of the mathematical maturity of students using this text; they are quite lengthy, however.

The DEA is a *symmetric cipher*. Both the sender and the receiver of a message must know the same secret key, which is used for both encryption and decryption. Distributing secure keys for use by the DEA is a difficult problem, which can be addressed using public key cryptography (discussed in Section 8.4).

Although the DEA has not been broken, in the sense that no easy attack on it has been found, it is vulnerable to brute-force analysis. An exhaustive search can now check all 2^{56} possible keys in less than a day. Because of the vulnerability of this algorithm to such attacks, the National Institute of Standards and Technology (NIST) decided not to certify DES for use after 1998.

In November 2000, NIST selected a new algorithm called the *Advanced Encryption Standard (AES)* as the official encryption standard for the U.S. government. This encryption algorithm was developed by two Belgian scientists, Joan Daemen and Vincent Rijmen, and is called *Rijndael* after its creators. The adoption of Rijndael as the Advanced Encryption Standard followed three years of competition among many encryption algorithms submitted as candidates for the standard. The AES algorithm is capable of using 128-, 192-, and 256-bit symmetric keys to encrypt and decrypt 128-bit blocks. The complexity of the AES and the size of the keys that it supports should make it resistant to brute-force attacks for many years. The U.S. government hopes that AES will remain secure for at least 20 years.

Stream Ciphers

The methods discussed so far have the property that the same key is used to determine the particular encryption transformation that is applied to each character (or block). Once a plaintext–ciphertext pair is known, the key can be found. To add additional security, we can change the key used to encrypt successive characters. To discuss this type of encryption, we must first define some terms.

A sequence $k_1, k_2, k_3, \ldots$ of elements from a keyspace $\mathcal{K}$ is called a *keystream*. The encryption function corresponding to the key k_i is denoted by E_{k_i}. A *stream cipher* is a cipher that sends a plaintext string $p_1p_2p_3\ldots$, using a keystream $k_1, k_2, k_3, \ldots$, to a ciphertext string $c_1c_2c_3\ldots$, where $c_i = E_{k_i}(p_i)$. The corresponding decryption function is $D_{d_i}(c_i) = p_i$, where d_i is a decryption key corresponding to the encryption key k_i.

We can generate the keystream for a stream cipher in different ways. For example, we can select the keys at random to construct a keystream, or we can use a *keystream generator*, a function that generates successive keys using an initial sequence of keys (the *seed*), perhaps also using previous plaintext symbols.

The simplest (nontrivial) stream cipher is the *Vernam Cipher*, proposed by *Gilbert Vernam* in 1917 for the automatic encryption and decryption of telegraph messages. In this stream cipher, the keystream is a bit string $k_1k_2\ldots k_m$ of the same length as the plaintext message, which is a bit string $p_1p_2\ldots p_m$. Plaintext bits are encrypted using the map

$$E_{k_i}(p_i) \equiv k_i + p_i \pmod 2.$$

Exactly two different encryption maps are used in a Vernam cipher. When $k_i = 0$, E_{k_i} is the identity map that sends 0 to 0 and 1 to 1. When $k_i = 1$, E_{k_i} is the map that sends 0 to 1 and 1 to 0. The corresponding decryption transformation D_{d_i} is identical to E_{k_i}.

Example 8.11. When we encrypt the plaintext bit string 0 1111 0111 using a Vernam cipher with keystream 1 1000 1111, we obtain the bit string 1 0111 1000, where each bit is obtained by adding corresponding bits of the plaintext and the keystream. Decrypting this just requires that we repeat the operation. ◀

Keystreams in the Vernam cipher should be used only once (see Exercise 38). When the keystream of a Vernam cipher is chosen at random and is used to encrypt exactly one plaintext message, it is called a *one-time pad.* It can be shown that a one-time pad is unbreakable, in the sense that someone with a ciphertext string encrypted using a random keystream used only once can do no better than to simply guess at the plaintext string. The problem with the Vernam cipher is that the keystream must be at least as long as the plaintext message, and must be transmitted securely between two parties who want to use a one-time pad. Consequently, the one-time pad is not used except for extremely sensitive communications, mostly of a diplomatic or military nature.

We will describe another stream cipher, the *autokey cipher* invented by Vigenère in the sixteenth century. The autokey cipher uses an initial seed key, which is a single character; subsequent keys are plaintext characters. In particular, the autokey cipher shifts each plaintext character, other than the first character, the numerical equivalent of the previous character modulo 26; it shifts the first character the numerical equivalent of the seed character modulo 26. That is, the autokey cipher encrypts a character p_i according to the transformation

$$c_i \equiv p_i + k_i \pmod{26},$$

where p_i is the numerical equivalent of the ith plaintext character, c_i is the numerical equivalent of the ith ciphertext character, and k_i the numerical equivalent of the ith character of the keystream, is given by $k_1 = s$, where s is the numerical equivalent of the seed character and $k_i = p_{i-1}$ for $i \geq 2$.

To decrypt a message encrypted with the autokey cipher we need to know the seed. We subtract the seed from the first ciphertext character modulo 26 to determine the first plaintext character, and then we subtract the numerical equivalent of each plaintext character modulo 26 from the next ciphertext character to obtain the next plaintext character.

We illustrate how to encrypt and decrypt using the autokey cipher in the following examples.

GILBERT S. VERNAM (1890–1960) was born in Brooklyn, New York. After graduating from Worcester Polytechnic Institute, he took a job at AT&T. He was able to visualize electrical circuits without actually implementing them. He was noted for his cleverness; one story quotes him as asking "What can I invent now?" each evening while stretched out on his couch. At AT&T he developed a method to make transmission via the teletypewriter, the first system that automated cryptology, secure. At AT&T he also developed a technique for encrypted digital images. Vernam also held positions with the International Communications Laboratories and the Postal Telegraph Cable Company. He was granted 65 patents for his inventions in cryptography and in telegraph switching systems.

Example 8.12. To encrypt the plaintext message HERMIT using the autokey cipher with seed X (with numerical equivalent 23), we first translate the letters of HERMIT into their numerical equivalents to obtain 7 4 17 12 8 19. The keystream consists of the numbers 23 7 4 17 12 8. The numerical equivalents of the characters in the ciphertext message are

$$\begin{aligned} p_1 + k_1 &= 7 + 23 \equiv 4 \pmod{26} \\ p_2 + k_2 &= 4 + 7 \equiv 11 \pmod{26} \\ p_3 + k_3 &= 17 + 4 \equiv 21 \pmod{26} \\ p_4 + k_4 &= 12 + 17 \equiv 3 \pmod{26} \\ p_5 + k_5 &= 8 + 12 \equiv 20 \pmod{26} \\ p_6 + k_6 &= 19 + 8 \equiv 1 \pmod{26}. \end{aligned}$$

Translating back to letters, we see that the ciphertext is ELVDUB. ◀

Example 8.13. To decrypt the ciphertext message RMNTU encrypted using the autokey cipher with seed F, we first translate the characters of the ciphertext into their numerical equivalents to obtain 17 12 13 19 20. We obtain the numerical equivalent of the first plaintext character by computing

$$p_1 = c_1 - s \equiv 17 - 5 = 12 \pmod{26}.$$

We obtain the numerical equivalent of successive plaintext characters as follows:

$$\begin{aligned} p_2 &= c_2 - p_1 = 12 - 12 = 0 \pmod{26} \\ p_3 &= c_3 - p_2 = 13 - 0 = 13 \pmod{26} \\ p_4 &= c_4 - p_3 = 19 - 13 = 6 \pmod{26} \\ p_5 &= c_5 - p_4 = 20 - 6 = 14 \pmod{26}. \end{aligned}$$

Translating these numerical equivalents back to letters, we find that the plaintext message was MANGO. ◀

We have only briefly touched the surface of the deep subject of stream ciphers. For more information about them, including descriptions of stream ciphers used in practice, consult [MevaVa97].

8.2 Exercises

1. Use the Vigenère cipher with encrypting key SECRET to encrypt the message

   DO NOT OPEN THIS ENVELOPE.

2. Decrypt the following message, which was enciphered using the Vigenère cipher with encrypting key SECRET:

   WBRCS LAZGJ MGKMF V.

3. Use the Vigenère cipher with encrypting key TWAIN to encrypt the message

   AN ENGLISHMAN IS A PERSON WHO DOES THINGS BECAUSE THEY HAVE BEEN DONE BEFORE. AN AMERICAN IS A PERSON WHO DOES THINGS BECAUSE THEY HAVE NOT BEEN DONE BEFORE.

4. Decrypt the following message, which was enciphered using the Vigenère cipher with encrypting key TWAIN.

PACWH	EZUAR	NLTEB	XPEZA	BPIMF
BJLMN	KJIVT	THLBU	TPIAG	HXETR
TNNMQ	TXOCG	HQRWJ	GSOZY	WWNLG
AATPB	NOAVQ	LKFVN	MEOVF	MDAB.U
TREIE	BOEVN	GZFTB	NNIAU	XZAVQ
OWNQF	AADNE	HIIBZ	TPHMZ	TPIKF
THOVR	PKUTQ	HYCCC	RIEMV	ZDTUV
EHIWA	RAAZF			

5. Suppose a plaintext message is encrypted using a Vigenère cipher. Show that identical strings of characters separated by a multiple of the key length are encrypted to the same string of ciphertext characters.

In Exercises 6–11, use the procedure described in the text to cryptanalyze the given ciphertext, which was encrypted using a Vigenère cipher.

6.

UCYFC	OOCQU	CYFHE	BHFTH	EFERF
GQJCK	XVBUV	BSHFT	BLCZB	SWKUV
BNKWE	HLTIC	GSOUV	BTZFO	UPBBA
BFOPK	PPTLV	HOBUB	PIPGC	OUIKF

7.

KMKRE	CCWSP	ISNEJ	RSXZI	ALKZS
QSLEH	NVWAM	SRIQM	YJKMK	RECCW
XMVOF	ELRLW	WEJCT	JCGAM	YKJMX
CPWQW	GLWLF	ELAEF	MRDWF	WJISP
RWBXZ	CLSPH	OYCML	PWQWA	RMKYJ
SREDK	MKREC	CAZGG	ZYXDC	EKRSL
FIJQG	SLPWY	VFDVG	K	

8.

SIIWZ	FDIBN	HUDEU	WQJHP	JKRNK
RLACT	WXBIM	MHMPJ	OFUFP	WVEOG
PQPEL	VPZYD	AXIAG	PITMA	XFSSS
GWPBW	IWOFO	TFWVF	JSXPL	BJOTP
SUDIJ	JXFNR	FPAFG	RPSXI	WXJOR
PPXSQ	I			

9.

JWEFF	PRGBA	GDSZF	ZBTZJ	IBLSP
VDBTP	FXMLV	UGWID	NWDHO	BNKJT
VLXIJ	KPMZQ	HQEDW	QCOBO	VJBZU
HOIEG	JNVOU	BYDUQ	NDTUF	UFLZV
UQEJV	QJKFL	SBUPR	WDQIF	VUJWB
VTHUP	RWJAY	RVTUK	BDVEF	MEEZI
EBFXR	XMMKL	DWLOE	PRYFE	FUO

10.

P D J V J	L F C J W	Z Q L G R	E V M U V	Z O W I D
A J Z P Z	D W E M U	Q L G G I	Q Z Z M E	N Z P J M
Y X S M W	I H Q Q P	D B W I E	K M S F B	G I Q W W
I J W Z E	Y M A I C	T J R R B	M I Y Q S	K P D J V
L A H I Y	L N R R M	A I C Q R	T C W A M	Y O U E E
P D S F S	S S H G T	Y H Q Q P	Y M A I C	O J X E W
Y L P M S	H Z N Y L	P R T Y C	V J C M C	Y X S Q X
W Z N F V	Q Z T Q O	Q X G Z C	W E R Q S	K Z V Q C
L L I W E	W Y L P R	T C L V I	K W W W C	Z N Y L P
K Q M X J				

11.

T U Z T U	W F G C G	L H G T F	G M K G R	F I A S R
K W K R R	D A A G U	W D G T Q	G E Y N B	L I S P Y
Q T N A G	S L R W U	G A X E Y	S U M H R	V A Z A E
W G K N V	M S K S G	Z E E L N	M G N E Q	S T I O Y
M M H U F	L H K Y Y	S U M H R	V A Z F H	D T U N G
Z E E L N	M G N E Q	S T Z H R	O R O G U	L B X O G
Z E X S O	M T Z H R	Q A R S B	D A A G U	W D G T O
G Z U T U	W C R O J	F		

12. Show how we find that the correct key in Example 8.8 is USA once we know the key has length three.

13. Using the digraphic cipher that sends the plaintext block P_1P_2 to the ciphertext block C_1C_2, with

$$C_1 \equiv 3P_1 + 10P_2 \pmod{26}$$
$$C_2 \equiv 9P_1 + 7P_2 \pmod{26}$$

encrypt the message BEWARE OF THE MESSENGER.

14. Using the digraphic cipher that sends the plaintext block P_1P_2 to the ciphertext block C_1C_2, with

$$C_1 \equiv 8P_1 + 9P_2 \pmod{26}$$
$$C_2 \equiv 3P_1 + 11P_2 \pmod{26}$$

encrypt the message DO NOT SHOOT THE MESSENGER.

15. Decrypt the ciphertext message RD SR QO VU QB CZ AN QW RD DS AK OB, which was encrypted using the digraphic cipher that sends the plaintext block P_1P_2 into the ciphertext block C_1C_2, with

$$C_1 \equiv 13P_1 + 4P_2 \pmod{26}$$
$$C_2 \equiv 9P_1 + P_2 \pmod{26}.$$

16. Decrypt the ciphertext message UW DM NK QB EK, which was encrypted using the digraphic cipher that sends the plaintext block P_1P_2 into the ciphertext block C_1C_2, with

$$C_1 \equiv 23P_1 + 3P_2 \pmod{26}$$
$$C_2 \equiv 10P_1 + 25P_2 \pmod{26}.$$

17. A cryptanalyst has determined that the two most common digraphs in a ciphertext message are RH and NI, and guesses that these ciphertext digraphs correspond to the two most common diagraphs in English text, TH and HE. If the plaintext was encrypted using a Hill digraphic cipher described by

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$
$$C_2 \equiv cP_1 + dP_2 \pmod{26},$$

what are a, b, c, and d?

18. How many pairs of letters remain unchanged when encryption is performed using each of the following digraphic ciphers?

a) $C_1 \equiv 4P_1 + 5P_2 \pmod{26}$
$C_2 \equiv 3P_1 + P_2 \pmod{26}$

b) $C_1 \equiv 7P_1 + 17P_2 \pmod{26}$
$C_2 \equiv P_1 + 6P_2 \pmod{26}$

c) $C_1 \equiv 3P_1 + 5P_2 \pmod{26}$
$C_2 \equiv 6P_1 + 3P_2 \pmod{26}$

19. Show that if the encrypting matrix $\mathbf{A}$ in the Hill cipher system is involutory modulo 26, that is, $\mathbf{A}^2 \equiv \mathbf{I} \pmod{26}$, then $\mathbf{A}$ also serves as a decrypting matrix for this cipher system.

20. A cryptanalyst has determined that the three most common trigraphs (blocks of length three) in a ciphertext are LME, WRI, and ZYC, and guesses that these ciphertext trigraphs correspond to the three most common trigraphs in English text, THE, AND, and THA. If the plaintext was encrypted using a Hill trigraphic cipher described by $\mathbf{C} \equiv \mathbf{AP} \pmod{26}$, what are the entries of the 3×3 encrypting matrix $\mathbf{A}$?

21. Find the product cipher obtained by using the digraphic Hill cipher with encrypting matrix $\begin{pmatrix} 2 & 3 \\ 1 & 17 \end{pmatrix}$ followed by using on the result the digraphic Hill cipher with encrypting matrix $\begin{pmatrix} 5 & 1 \\ 25 & 4 \end{pmatrix}$.

22. Show that the product cipher obtained from two digraphic Hill ciphers is again a digraphic Hill cipher.

23. Show that the product cipher obtained by encrypting first using a Hill cipher with blocks of size m and then using a Hill cipher with blocks of size n is again a Hill cipher that uses blocks of size $[m, n]$.

24. Find the 6×6 encrypting matrix corresponding to the product cipher obtained by first using the Hill cipher with encrypting matrix $\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$, followed by using the Hill cipher with encrypting matrix $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

* **25.** In *transposition cipher,* blocks of a specified size are encrypted by permuting their characters in a specified manner. For instance, plaintext blocks of length five, $P_1P_2P_3P_4P_5$, may be sent to ciphertext blocks $C_1C_2C_3C_4C_5 = P_4P_5P_2P_1P_3$. Show that every such transposition cipher is a Hill cipher with an encrypting matrix that contains only 0s and 1s as entries, with the property that each row and each column contains exactly one 1.

Hill ciphers are special cases of block ciphers based on *affine transformations*. To form such a transformation, let $\mathbf{A}$ be an $n \times n$ matrix with integer entries and $(\det \mathbf{A}, 26) = 1$, and let $\mathbf{B}$ be an $n \times 1$ matrix with integer entries. To encrypt a message, we split it into blocks of length n and put the numerical equivalents of the letters in each block into an $n \times 1$ matrix $\mathbf{P}$ (padding the last block with dummy letters, if necessary). We find the corresponding ciphertext block by computing $\mathbf{C} \equiv (\mathbf{AP} + \mathbf{B}) \pmod{26}$ and translating the entries in $\mathbf{C}$ back into letters.

26. Using the affine transformation $\mathbf{C} \equiv \begin{pmatrix} 3 & 2 \\ 7 & 11 \end{pmatrix} \mathbf{P} + \begin{pmatrix} 8 \\ 19 \end{pmatrix} \pmod{26}$ on blocks of two successive letters, encrypt the message HAVE A NICE DAY.

27. What is the decrypting transformation associated with the affine transformation in Exercise 26?

28. What is the decrypting transformation associated with the encrypting transformation $\mathbf{C} \equiv (\mathbf{AP} + \mathbf{B}) \pmod{26}$, where $\mathbf{A}$ is an $n \times n$ matrix with integer entries and $(\det \mathbf{A}, 26) = 1$, and $\mathbf{B}$ is an $n \times 1$ matrix with integer entries?

29. Decipher the message HG PM QR YN NM that was encrypted using the affine transformation $\mathbf{C} \equiv \begin{pmatrix} 5 & 2 \\ 11 & 15 \end{pmatrix} \mathbf{P} + \begin{pmatrix} 14 \\ 3 \end{pmatrix} \pmod{26}$.

30. Explain how you would go about decrypting a message that was encrypted in blocks of length two using an affine transformation $\mathbf{C} \equiv \mathbf{AP} + \mathbf{B} \pmod{26}$, where $\mathbf{A}$ is a 2×2 matrix with integer entries and $(\det \mathbf{A}, 26) = 1$, and $\mathbf{B}$ is a 2×1 matrix with integer entries.

31. Explain how you would go about decrypting a message that was encrypted in blocks of length three using an affine transformation $\mathbf{C} \equiv \mathbf{AP} + \mathbf{B} \pmod{26}$, where $\mathbf{A}$ is a 3×3 matrix with integer entries and $(\det \mathbf{A}, 26) = 1$, and $\mathbf{B}$ is a 3×1 matrix, with integer entries.

32. Is the product cipher composed of two digraphic block ciphers based on affine transformations also a digraphic block cipher based on an affine transformation?

* **33.** Is the product cipher composed of two block ciphers based on affine transformations, encrypting blocks of length m and blocks of length n, respectively, also a block cipher based on an affine transformation?

34. Encrypt the bit string 11 1010 0011 using the Vernam cipher with keystream 10 0111 1001.

35. Decrypt the bit string 11 1010 0011, assuming that it was encrypted using the Vernam cipher with keystream 10 0111 1001.

36. Encrypt the plaintext message MIDDLETOWN using the autokey cipher with seed Z.

37. Decrypt the ciphertext message ZVRQH DUJIM, assuming that it was encrypted using the autokey cipher with seed I.

38. Show that the Vernam cipher is vulnerable to a known-plaintext attack if a keystream is used repeatedly. In particular, show that if someone can encrypt a bit string and have access to the resulting ciphertext string, the keystring can be found.

39. Show that if a keystream is used to encrypt two different messages using a Vernam cipher, then the bit string obtained by adding corresponding bits of the two messages modulo 2 could be found by someone with the corresponding ciphertext messages. Why might this permit cryptanalysis?

8.2 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. Encrypt some messages using Vigenère ciphers for your classmates to decrypt.
* 2. Decrypt messages encrypted by your classmates using Vigenère ciphers.
3. Run the Kasiski test on some ciphertexts encrypted using Vigenère ciphers.
4. Find the index of coincidence for some character strings
5. Cryptanalyze some ciphertexts encrypted using Vigenère ciphers.
6. Find the frequencies of digraphs in various types of English texts, such as this text, computer programs, and a novel.
7. Find the frequencies of trigraphs in various types of English texts, such as this text, computer programs, and a novel.
8. Encrypt some messages using Hill ciphers for your classmates to decrypt.
9. Decrypt messages encrypted by your classmates using Hill ciphers.
10. Encrypt and decrypt some long messages using a Vigenère cipher one-time pad, sending these messages to a particular classmate.
11. Encrypt some messages using an autokey cipher for your classmates to decrypt.
12. Decrypt some messages that were encrypted using an autokey cipher by your classmates.

Programming Projects

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

1. Encrypt messages using Vigenère ciphers.
2. Decrypt messages that have been encrypted using Vigenère ciphers.
* 3. Given ciphertext encrypted using a Vigenère cipher, run the Kasiski test to determine the key length of the cipher.
4. Given a string of English characters, find the index of coincidence of this string.
** 5. Cryptanalyze ciphertext encrypted using a Vigenère cipher using the Kasiski test, followed by the Friedman test, which uses the index of coincidence to verify the key length, followed by frequency analysis to find each character of the key. Then use the resulting key to recover the original plaintext.
6. Encrypt messages using a Hill cipher.
7. Decrypt messages that were encrypted using a Hill cipher.
* 8. Cryptanalyze messages that were encrypted using a digraphic Hill cipher, by analyzing the frequency of digraphs in the ciphertext.
9. Encrypt messages using a cipher based on an affine transformation. (See the preamble to Exercise 26.)

10. Decrypt messages that were encrypted using an affine transformation.
11. By analyzing the frequency of digraphs in ciphertext, cryptanalyze messages encrypted using a digraphic block cipher based on an affine transformation.
12. Encrypt messages using the autokey cipher.
13. Decrypt messages that were encrypted using the autokey cipher.

8.3 Exponentiation Ciphers

In this section, we discuss a cipher based on modular exponentiation, which was invented in 1978 by Pohlig and Hellman [PoHe78]. We will see that ciphers produced by this system are resistant to cryptanalysis. (This cipher is of more theoretical than practical significance.)

Let p be an odd prime and let e, the enciphering key, be a positive integer with $(e, p-1) = 1$. To encrypt a message, we first translate the letters of the message into numerical equivalents (retaining initial zeros in the two-digit numerical equivalents of letters). We use the same relationship we have used before, as shown in Table 8.9

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numerical Equivalent	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 8.9 *Two-digit numerical equivalents of letters.*

Next, we group the resulting numbers into blocks of $2m$ decimal digits, where $2m$ is the largest positive even integer such that all blocks of numerical equivalents corresponding to m letters (viewed as a single integer with $2m$ decimal digits) are less than p, e.g., if $2525 < p < 252{,}525$, then $m = 2$.

For each plaintext block P, which is an integer with $2m$ decimal digits, we form a ciphertext block C using the relationship

$$C \equiv P^e \pmod{p}, \quad 0 \leq C < p.$$

The ciphertext message consists of these ciphertext blocks, which are integers less than p. Notice that different values of e determine different ciphers, hence e is aptly called the enciphering key. We illustrate the encryption technique with the following example.

Example 8.14. Let the prime to be used as the modulus in the encryption procedure be $p = 2633$, and let the encryption key to be used as the exponent in the modular exponentiation be $e = 29$, so that $(e, p-1) = (29,\ 2632) = 1$. To encrypt the plaintext message

THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER,

we first convert the letters of the message into their numerical equivalents, and then form blocks of length four from these digits, to obtain

1907 0818 0818 0013 0423
0012 1511 0414 0500 1304
2315 1413 0413 1908 0019
0814 1302 0815 0704 1723.

Note that we have added the two digits 23, corresponding to the letter X, at the end of the message to fill out the final block of four digits.

We next translate each plaintext block P into a ciphertext block C using the relationship

$$C \equiv P^{29} \pmod{2633}, \quad 0 \leq C < 2633.$$

For instance, to encrypt the first plaintext block, we compute

$$C \equiv 1907^{29} \equiv 2199 \pmod{2633}.$$

To efficiently carry out the modular exponentiation, we use the algorithm given in Section 4.1. When we encrypt the blocks, we obtain the ciphertext:

2199 1745 1745 1206 2437
2425 1729 1619 0935 0960
1072 1541 1701 1553 0735
2064 1351 1704 1841 1459. ◀

To decrypt a ciphertext block C, we need to know a decryption key, namely an integer d such that $de \equiv 1 \pmod{p-1}$, so that d is an inverse of $e \pmod{p-1}$, which exists because $(e, p-1) = 1$. If we raise the ciphertext block C to the dth power modulo p, we recover your plaintext block P, because

$$C^d \equiv (P^e)^d = P^{ed} \equiv P^{k(p-1)+1} \equiv (P^{p-1})^k P \equiv P \pmod{p},$$

where $de = k(p-1) + 1$, for some integer k, because $de \equiv 1 \pmod{p-1}$. (Note that we have used Fermat's little theorem to see that $P^{p-1} \equiv 1 \pmod{p}$.)

Example 8.15. To decrypt the ciphertext blocks generated using the prime modulus $p = 2633$ and the encryption key $e = 29$, we need an inverse of e modulo $p - 1 = 2632$. An easy computation, as done in Section 4.2, shows that $d = 2269$ is such an inverse. To decrypt the ciphertext block C to define the corresponding plaintext block P, we use the relationship

$$P \equiv C^{2269} \pmod{2633}.$$

For instance, to decrypt the ciphertext block 2199, we have

$$P \equiv 2199^{2269} \equiv 1907 \pmod{2633}.$$

Again, the modular exponentiation is carried out using the algorithm given in Section 4.1. ◀

For each plaintext block P that we encrypt by computing $P^e \pmod{p}$, we use only $O((\log_2 p)^3)$ bit operations, as Theorem 4.9 demonstrates. Before we decrypt, we need to find an inverse d of e modulo $p-1$. This can be done using $O(\log^3 p)$ bit operations (see Exercise 15 of Section 4.2), and this must be done only once. Then to recover the plaintext block P from a ciphertext block C, we simply need to compute the least positive residue of C^d modulo p; we can do this using $O((\log_2 p)^3)$ bit operations. Consequently, the process of encryption and decryption using modular exponentiation can be carried out rapidly.

On the other hand, cyptanalysis of messages encrypted using modular exponentiation generally cannot be accomplished rapidly. To see this, suppose that we know the prime p used as the modulus and, moreover, suppose that we know the plaintext block P corresponding to a ciphertext block C, so that

$$C \equiv P^e \pmod{p}. \tag{8.2}$$

For successful cryptanalysis, we need to find the enciphering key e. This is the discrete logarithm problem, a computationally difficult problem that will be discussed in Chapter 9. Note that when p has more than 200 decimal digits, it is not feasible to solve this problem using a computer.

8.3 Exercises

1. Using the prime $p = 101$ and encryption key $e = 3$, encrypt the message GOOD MORNING using modular exponentiation.
2. Using the prime $p = 2621$ and encryption key $e = 7$, encrypt the message SWEET DREAMS using modular exponentiation.
3. What is the plaintext message that corresponds to the ciphertext 01 09 00 12 12 09 24 10 that is produced using modular exponentiation with modulus $p = 29$ and encryption exponent $e = 5$?
4. What is the plaintext message that corresponds to the ciphertext 1213 0902 0539 1208 1234 1103 1374 that is produced using modular exponentiation with modulus $p = 2591$ and encryption key $e = 13$?
5. Show that the encryption and decryption procedures are identical when encryption is done using modular exponentiation with modulus $p = 31$ and enciphering key $e = 11$.
6. With modulus $p = 29$ and unknown encryption key e, modular exponentiation produces the ciphertext 04 19 19 11 04 24 09 15 15. Cryptanalyze the above cipher, if it is also known that the ciphertext block 24 corresponds to the plaintext letter U (with numerical equivalent 20). (*Hint:* First find the logarithm of 24 to the base 20 modulo 29, using some guesswork.)

8.3 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. Encrypt some messages for your classmates to decrypt using exponentiation ciphers.
2. Decrypt messages encrypted by your classmates using exponentiation ciphers, given the encryption key and prime modulus.

Programming Projects

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

1. Encrypt some messages for your classmates to decrypt using exponentiation ciphers.
2. Decrypt messages encrypted by your classmates using exponentiation ciphers, given the encrypting key and prime modules.

8.4 Public Key Cryptography

The cryptosystems we have discussed so far are all examples of *private key,* or *symmetric* cryptosystems, where the encryption and decryption keys are either the same or can be easily found from each other. For example, in a shift cipher, the encrypting key is an integer k and the corresponding decrypting key is the integer $-k$. In an affine cipher, the encrypting key is a pair (a, b) and the corresponding decrypting key is the pair $(\overline{a}, -\overline{a}b)$, where $\overline{a}$ is an inverse of a modulo 26. In a Hill cipher, the encrypting key is an $n \times n$ matrix $\mathbf{A}$ and the corresponding decrypting key is the $n \times n$ matrix $\overline{\mathbf{A}}$, where $\overline{\mathbf{A}}$ is an inverse of the matrix $\mathbf{A}$ modulo 26. In the Pohlig-Hellman exponentiation cipher, the encrypting key is (e, p), where p is a prime, and the corresponding decrypting key is (d, p), where d is an inverse of e modulo $p - 1$. For the DEA, the encrypting and decrypting keys are exactly the same.

For that reason, if one of the cryptosystems discussed so far is used to establish secure communications within a network, then each pair of communicants must employ an encryption key that is kept secret from the other individuals in the network, because once the encryption key in such a cryptosystem is known, the decryption key can be found using a small amount of computer time. Consequently, to maintain secrecy, the encryption keys must themselves be transmitted over a channel of secure communications.

To avoid assigning a key to each pair of individuals, which must be kept secret from the rest of the network, a new type of cryptosystem, called a *public key* cryptosystem, was invented in the 1970s. In this type of cryptosystem, encrypting keys can be made public, because an unrealistically large amount of computer time is required to find a decrypting transformation from an encrypting transformation. To use a public key cryptosystem to establish secret communications in a network of n individuals, each individual produces a key of the type specified by the cryptosystem, retaining certain private information that went into the construction of the encrypting transformation $E(k)$, obtained from the key

k according to a specified rule. Then a directory of the n keys $k_1, k_2, \ldots, k_n$ is published. When individual i wishes to send a message to individual j, the letters of the message are translated into their numerical equivalents and combined into blocks of specified size. Then, for each plaintext block P a corresponding ciphertext block $C = E_{k_j}(P)$ is computed using the encrypting transformation E_{k_j}. To decrypt the message, individual j applies the decrypting transformation D_{k_j} to each ciphertext block C to find P; that is,

$$D_{k_j}(C) = D_{k_j}(E_{k_j}(P)) = P.$$

Because the decrypting transformation D_{k_j} cannot be found in a realistic amount of time by anyone other than individual j, no unauthorized individuals can decrypt the message, even though they know the key k_j. Furthermore, cryptanalysis of the ciphertext message, even with knowledge of k_j, is extremely infeasible due to the large amount of computer time needed.

Many cryptosystems have been proposed as public key cryptosystems. All but a few have been shown to be unsuitable, by demonstrating that ciphertext messages can be decrypted using a feasible amount of computer time. In this section, we will introduce the most widely used public key cryptosystem, the RSA cryptosystem. In addition, we will introduce several other public key cryptosystems, including the Rabin public key cryptosystem, which we will discuss at the end of this section, and the ElGamal public key cryptosystem, which we will discuss in Chapter 10. The security of these systems rests on the difficulty of two computationally intensive mathematical problems, factoring integers (discussed in Chapter 3) and finding discrete logarithms (to be discussed in Chapter 9). In Section 8.5, we will describe a proposed public key cryptosystem, the knapsack cryptosystem, that turned out not to be suitable as a basis for a public key cryptosystem. (See [MevaVa97] for a comprehensive look at most of the important public key cryptosystems.)

Although public key cryptosystems have many advantages, they are not extensively used for general-purpose encryption. The reason is that encrypting and decrypting in these cryptosystems require too much time and memory on most computers, generally several orders of magnitude more than required for symmetric cryptosystems currently in use. However, public key cryptosystems are used extensively to encrypt keys for symmetric cryptosystems such as DES, so that these keys can be transmitted securely. They are also used in a wide variety of cryptographic protocols, such as in digital signatures (discussed in Section 8.6). They are also particularly useful for applications involving smart cards and electronic commerce.

Also note that in modern cryptography, the cryptosystem used to encrypt messages is publicly known. Consequently, the secrecy of encrypted messages does not depend on the secrecy of the encryption algorithm in use. For symmetric key cryptosystems, the secrecy of messages depends on the secrecy of the encryption key in use and the computational difficulty of finding this key from other information (such as plaintext–ciphertext pairs). For public key cryptosystems, secrecy rests on the secrecy of the decryption key and the computational difficulty of finding this key from the encryption key and other public information (such as plaintext–ciphertext pairs).

The RSA Cryptosystem

The *RSA cryptosystem,* invented by *Ronald Rivest, Adi Shamir, and Leonard Adleman* [RiShAd78] in the 1970s (and patented by them [RiShAd83] in 1983) is a public key cryptosystem based on modular exponentiation, where the keys are pairs (e, n) consisting of an exponent e and a modulus n that is the product of two large primes; that is, $n = pq$, where p and q are large primes, so that $(e, \phi(n)) = 1$. To encrypt a message, we first translate the letters into their numerical equivalents and then form blocks of the largest possible size (with an even number of digits). To encrypt a plaintext block P, we form a ciphertext block C by

$$E(P) = C \equiv P^e \pmod{n}, \quad 0 \leq C < n.$$

The decrypting procedure requires knowledge of an inverse d of e modulo $\phi(n)$, which exists because $(e, \phi(n)) = 1$. To decrypt the ciphertext block C, we find

RONALD RIVEST (b. 1948) received his B.A. from Yale University in 1969 and his Ph.D. in computer science from Stanford University in 1974. He is a professor of computer science at M.I.T., and a cofounder of RSA Data Security, Inc. (now a subsidiary of Security Dynamics), the company that holds the patents on the RSA cryptosystem. Rivest has worked in the areas of machine learning, computer algorithms, and VLSI design. He is one of the authors of a popular textbook on algorithms ([ColeRi01]).

ADI SHAMIR (b. 1952) was born in Tel Aviv, Israel. He received his undergraduate degree from Tel Aviv University in 1972, and his Ph.D. in computer science from the Weizmann Institute of Science in 1977. He held a research assistantship at the University of Warwick for one year, and in 1978 he became an assistant professor at M.I.T. He is now a professor in the Applied Mathematics Department at the Weizmann Institute in Israel, where he formed a group to study computer security. Shamir has made many contributions to cryptography besides coinventing the RSA cryptosystem, including cracking the knapsack cryptosystem proposed as a public cryptosystem by Merkle and Hellman, developing numerous cryptographic protocols, and creative cryptanalysis of DES.

LEONARD ADLEMAN (b. 1945) was born in San Francisco, California. He received his B.S. in mathematics and his Ph.D. in computer science from the University of California, Berkeley, in 1968 and 1976, respectively. He was a member of the mathematics faculty at M.I.T. from 1976 until 1980; during his stay at M.I.T., he helped invent the RSA cryptosystem. In 1980 he was appointed to a position in the computer science department of the University of Southern California, and to a chaired professorship in 1985. Adleman has worked in the areas of computational complexity, computer security, immunology, and molecular biology, in addition to his work in cryptography. He coined the term "computer virus." His recent work on computing using DNA has attracted great interest. Adleman served as the technical adviser for the movie *Sneakers,* in which computer security figured prominently.

$$D(C) \equiv C^d = (P^e)^d = P^{ed} = P^{k\phi(n)+1}$$
$$\equiv (P^{\phi(n)})^k P \equiv P \pmod{n},$$

where $ed = k\phi(n) + 1$ for some integer k, because $ed \equiv 1 \pmod{\phi(n)}$, and by Euler's theorem, we have $P^{\phi(n)} \equiv 1 \pmod{n}$, when $(P, n) = 1$ the (probability that P and n are not relatively prime is extremely small; see Exercise 4 at the end of this section). The pair (d, n) is a decrypting key.

Example 8.16. To illustrate how the RSA cryptosystem works, suppose that the encrypting modulus is the product of the two primes 43 and 59 (which are smaller than the large primes that would actually be used); thus, we have $n = 43 \cdot 59 = 2537$ as the modulus. We take $e = 13$ as the exponent; note that we have $(e, \phi(n)) = (13, 42 \cdot 58) = 1$. To encrypt the message

PUBLIC KEY CRYPTOGRAPHY,

we first translate the letters into their numerical equivalents, and then group these numbers together into blocks of four. We obtain

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

where we have added the dummy letter $X = 23$ at the end of the passage to fill out the final block.

We encrypt each plaintext block into a ciphertext block, using the relationship

$$C \equiv P^{13} \pmod{2537}.$$

For instance, when we encrypt the first plaintext block 1520, we obtain the ciphertext block

$$C \equiv (1520)^{13} \equiv 95 \pmod{2537}.$$

Encrypting all the plaintext blocks, we obtain the ciphertext message

0095 1648 1410 1299
0811 2333 2132 0370
1185 1957 1084.

To decrypt messages that have been encrypted using this RSA cipher, we must find an inverse of $e = 13$ modulo $\phi(2537) = \phi(43 \cdot 59) = 42 \cdot 58 = 2436$. A short computation using the Euclidean algorithm, as done in Section 4.2, shows that $d = 937$ is an inverse of 13 modulo 2436. Consequently, to decrypt the ciphertext block C, we use the relationship

$$P \equiv C^{937} \pmod{2537}, \quad 0 \le P < 2537,$$

which is valid because

$$C^{937} \equiv (P^{13})^{937} \equiv (P^{2436})^5 P \equiv P \pmod{2537}.$$

Note that we have used Euler's theorem to see that

$$P^{\phi(2537)} = P^{2436} \equiv 1 \pmod{2537},$$

when $(P, 2537) = 1$ (which is true for all of the plaintext blocks in this example). ◀

The Security of the RSA Cryptosystem To understand how the RSA cryptosystem fulfills the requirements of a public key cryptosystem, first note that each individual can find two large primes p and q, each with 100 decimal digits, in just a few minutes of computer time. These primes can be found by picking odd integers with 100 digits at random; by the prime number theorem, the probability that such an integer is prime is approximately $2/\log 10^{100}$. Hence, we expect to find a prime after examining an average of $1/(2/\log 10^{100})$, or approximately 115, such integers. To test these randomly chosen odd integers for primality, we use Rabin's probabilistic primality test (discussed in Section 6.2). For each of these 100-digit odd integers we perform Miller's test for 100 bases less than the integer; the probability that a composite integer passes all these tests is less than 10^{-60}. The procedure we have just outlined requires only a few minutes of computer time to find a 100-digit prime, and each individual need do so only twice.

Once the primes p and q have been found, an encrypting exponent e must be chosen such that $(e, \phi(pq)) = 1$. One suggestion for choosing e is to take any prime greater than both p and q. No matter how e is found, it should be true that $2^e > n = pq$, so that it is impossible to recover the plaintext block P, $P \neq 0$ or 1, just by taking the eth root of the integer C with $C \equiv P^e \pmod{n}$, $0 \leq C < n$. As long as $2^e > n$, every message, other than $P = 0$ and 1, is encrypted by exponentiation followed by a reduction modulo n.

We note that the modular exponentiation needed for encrypting messages using the RSA cryptosystem can be done using only a few seconds of computer time when the modulus, exponent, and base in the modular exponentiation have as many as 200 decimal digits. Also, using the Euclidean algorithm, we can rapidly find an inverse d of the encryption exponent e modulo $\phi(n)$ when the primes p and q are known, so that $\phi(n) = \phi(pq) = (p-1)(q-1)$ is known.

To see why knowledge of the encrypting key (e, n) does not easily lead to the decrypting key (d, n), note that to find d, an inverse of e modulo $\phi(n)$, requires that we first find $\phi(n) = \phi(pq) = (p-1)(q-1)$. Note that finding $\phi(n)$ is not easier than factoring the integer n. To see why, note that $p + q = n - \phi(n) + 1$ and $p - q = \sqrt{(p+q)^2 - 4pq} = \sqrt{(p+q)^2 - 4n}$ and that $p = \frac{1}{2}[(p+q) + (p-q)]$ and $q = \frac{1}{2}[(p+q) - (p-q)]$. Consequently, p and q can easily be found when $n = pq$ and $\phi(n) = (p-1)(q-1)$ are known. Note that when p and q both have approximately 100 decimal digits, $n = pq$ has approximately 200 decimal digits. Using the fastest factorization algorithm known, millions of years of computer time are required to factor an integer of this size. Also, if the integer d is known, but $\phi(n)$ is not, then n may also be factored easily, since $ed - 1$ is a multiple of $\phi(n)$ and there are special algorithms for factoring an integer n using any multiple of $\phi(n)$ (see [Mi76]).

It has not been proven that it is impossible to decrypt messages encrypted using the RSA cryptosystem without factoring n, but so far no such method has been discovered.

As yet, all decrypting methods that work in general are equivalent to factoring n and, as we have remarked, factoring large integers seems to be an intractable problem, requiring tremendous amounts of computer time. If no method of decrypting RSA messages without factoring the modulus n is found, the security of the RSA system can be maintained as factoring methods and computational power improve, by increasing the size of the modulus. Unfortunately, messages encrypted using the RSA will become vulnerable to attack when factoring the modulus n becomes feasible. This means that extra care should be taken—for example, by using primes p and q each with several hundred digits—to protect the secrecy of messages that must be kept secret for tens, or hundreds, of years.

Note that a few extra precautions should be taken in choosing the primes p and q to be used in the RSA cryptosystem, to prevent the use of special rapid techniques to factor $n = pq$. For example, both $p - 1$ and $q - 1$ should have large prime factors, $(p - 1, q - 1)$ should be small, and p and q should have decimal expansions differing in length by a few digits.

As we have remarked, the security of the RSA cryptosystem depends on the difficulty of factoring large integers. In particular, for the RSA cryptosystem, once the modulus n has been factored it is easy to find the decrypting transformation from the encrypting transformation. Note, however, that it may be possible to somehow find the decrypting transformation from the encrypting transformation without factoring n, although this seems unlikely at present.

Attacks on Implementations of the RSA Cryptosystem

After 20 years of scrutiny, a variety of attacks on particular implementations of the RSA cryptosystem have been devised. These attacks show that care must be taken when implementing RSA to avoid particular vulnerabilities. Note that no fundamental vulnerability has been found that would make RSA unsuitable for use as a public key cryptosystem. We will describe a variety of these attacks. The interested reader should consult [Bo99].

Encrypting the same plaintext message with different keys can lead to a successful *Hastad broadcast attack*. For example, when the encryption exponent 3 is used by three different people with different encryption moduli to encrypt the same plaintext message, someone who has the three ciphertext messages produced can recover the original plaintext. In general, it is possible to recover a plaintext message from ciphertext produced by encrypting the message using different RSA encryption keys when sufficiently many copies of the message have been encrypted. This type of attach can even succeed if the original message is altered for each recipient in a way that produces linearly related plaintext. To avoid this vulnerability, different random paddings of the message should be encrypted.

We now describe a vulnerability of RSA found by M. Wiener [Wi90]. He showed that the decrypting exponent d of an RSA cryptosystem with encrypting key (e, n) can be efficiently determined if $n = pq$, p and q are primes with $q < p < 2q$, and the decrypting exponent d is less than $n^{1/4}/3$. (In Chapter 12 we will use the theory of continued

fractions to develop this attack.) This result shows that primes p and q that are not too close together should be used to produce the encrypting modulus and a decrypting exponent d that is relatively large should be used. Although it is customary to first select the encryption key in an RSA cipher, we can make the decrypting exponent large by selecting it first, and then using it to compute the encrypting exponent e.

Disclosing partial information about one of the primes that make up the encrypting modulus n leads to another weakness of the RSA cryptosystem. Suppose that $n = pq$ has m digits. Then knowing the initial $m/4$ or the final $m/4$ digits of p allows n to be efficiently factored. For example, when both p and q have 100 decimal digits, if we know the first 50 or the last 50 digits of p, we will be able to factor n. Details of this partial key disclosure attack can be found in [Co97]. A similar result shows that if we know the last $m/4$ digits of the decrypting exponent d, then we can efficiently find d using $O(e \log e)$ operations. This shows that if the encryption exponent e is small, the decryption exponent d can be found if we know the last 1/4 of its digits.

The final type of attack we mention was discovered by Paul Kocher in 1995 when he was an undergraduate at Stanford University. He demonstrated that the decryption exponent in the RSA cryptosystem can be determined by carefully measuring the time required for the system to perform a series of decryptions. This provides information that can be used to determine the decryption key d. Fortunately, it is easy to devise methods to thwart this attack. For a description of this attack, see [TrWa02] and the article by Kocher [Ko96a].

The widespread acceptance and use of the RSA cryptosystem makes in an inviting target for attack. That only minor vulnerabilities have been found has given people confidence in the practical use of this cryptosystem. This fuels the search for vulnerabilities in this popular cryptosystem.

The Rabin Cryptosystem

Michael Rabin [Ra79] discovered a variant of the RSA cryptosystem for which factorization of the modulus n has almost the same computational complexity as obtaining the decrypting transformation from the encrypting transformation. To describe Rabin's cryptosystem let $n = pq$, where p and q are odd primes, and let b be an integer with $0 \leq b < n$. To encrypt the plaintext message P, we form

$$C \equiv P(P + b) \pmod{n}.$$

We will not discuss the decrypting procedure for Rabin ciphers here, because it relies on some concepts that we have not yet developed (see Exercise 49 in Section 11.1). However, we remark that there are four possible values of P for each ciphertext C such that $C \equiv P(P + b) \pmod{n}$, an ambiguity that complicates the decrypting process. When p and q are known, the decrypting procedure for a Rabin cipher can be carried out rapidly because $O(\log\ n)$ bit operations are needed.

Rabin has shown that if there is an algorithm for decrypting in this cryptosystem, without knowledge of the primes p and q, that requires $f(n)$ bit operations, then there is an algorithm for the factorization of n requiring only $2(f(n) + \log n)$ bit

operations. Hence, the process of decrypting messages encrypted with a Rabin cipher without knowledge of p and q is a problem of computational complexity similar to that of factorization. For more information about the Rabin public key cryptosystem, see [MevaVa97].

8.4 Exercises

1. Find the primes p and q if $n = pq = 14{,}647$ and $\phi(n) = 14{,}400$.
2. Find the primes p and q if $n = pq = 4{,}386{,}607$ and $\phi(n) = 4{,}382{,}136$.
3. Suppose a cryptanalyst discovers a message P that is not relatively prime to the enciphering modulus $n = pq$ used in an RSA cipher. Show that the cryptanalyst can factor n.
4. Show that it is extremely unlikely that a message such as that described in Exercise 3 can be discovered. Do this by demonstrating that the probability that a message P is not relatively prime to n is $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$, and if p and q are both larger than 10^{100}, this probability is less than 10^{-99}.
5. What is the ciphertext that is produced when RSA encryption with key $(e, n) = (3,2669)$ is used to encrypt the message BEST WISHES?
6. What is the ciphertext that is produced when RSA encryption with key $(e, n) = (7,2627)$ is used to encrypt the message LIFE IS A DREAM?
7. If the ciphertext message produced by RSA encryption with the key $(e, n) = (13,2747)$ is 2206 0755 0436 1165 1737, what is the plaintext message?
8. If the ciphertext message produced by RSA encryption with the key $(e, n) = (5,2881)$ is 0504 1874 0347 0515 2088 2356 0736 0468, what is the plaintext message?
9. Encrypt the message SELL NOW using the Rabin cipher $C \equiv P(P + 5) \pmod{2573}$.
10. Encrypt the message LEAVE TOWN using the Rabin cipher $C \equiv P(P + 11) \pmod{3901}$.
11. Suppose that Bob, extremely concerned with security, selects an encrypting modulus n, $n = pq$, where p and q are large primes, and two encrypting exponents e_1 and e_2. He asks Alice to double encrypt messages set to him by first encrypting plaintext using the RSA cipher with encryption key (e_1, n) and then encrypting the resulting ciphertext again using the RSA cipher with encryption key (e_2, n). Does Bob gain any extra security by this double encryption? Justify your answer.
12. Suppose that a plaintext message P is not relatively prime to $n = pq$, where p and q are large primes. Is it possible to successfully decrypt the ciphertext produced by encrypting p using RSA encryption with key (e, n)?
13. Suppose that two parties share a common modulus n in the RSA cryptosystem, but have different encrypting exponents. Show that the plaintext of a message sent to each of these two parties encrypted using each of their RSA keys can be recovered from the ciphertext messages.
14. Show that if the encryption exponent 3 is used for the RSA cryptosystem by three different people with different moduli, a plaintext message P encrypted using each of their keys can be recovered from these resulting three ciphertext messages. (*Hint:* Suppose that the moduli in these three keys are n_1, n_2, and n_3. First find a common

solution to the congruences $x_i \equiv P^3 \pmod{n_i}, i = 1, 2, 3$.) (This is an example of a Hastad broadcast attack.)

15. Describe how an RSA cryptosystem works if the encrypting modulus n is the product of three primes, rather than two primes.

16. Suppose that two people have RSA encrypting keys with encrypting moduli n_1 and n_2, respectively, when $n_1 \neq n_2$. Show how you could break the system if $(n_1, n_2) > 1$.

8.4 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. Construct a key for the RSA cipher for inclusion in a directory of encryption keys for the members of your class.
2. For each member of your class, encrypt a message using the RSA cipher with the public keys published in the directory.
3. Decipher the messages sent to you by your classmates that were encrypted using your RSA encryption key.

Programming Projects

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

1. Encrypt messages with an RSA cipher.
2. Decrypt messages that were encrypted using an RSA cipher.

8.5 Knapsack Ciphers

In this section, we discuss cryptosystems based on the knapsack problem. Given a set of positive integers $a_1, a_2, \ldots, a_n$ and an integer S, the *knapsack problem* asks which of these integers, if any, add together to give S. Another way to phrase the knapsack problem is to ask for values of $x_1, x_2, \ldots, x_n$, each either 0 or 1, such that

$$S = a_1x_1 + a_2x_2 + \cdots + a_nx_n. \tag{8.3}$$

We use an example to illustrate the knapsack problem.

Example 8.17. Let $(a_1, a_2, a_3, a_4, a_5) = (2, 7, 8, 11, 12)$ and $S = 21$. By inspection, we see that there are two subsets of these five integers that add together to give 21, namely $21 = 2 + 8 + 11 = 2 + 7 + 12$. Equivalently, there are exactly two solutions to the equation $2x_1 + 7x_2 + 8x_3 + 11x_4 + 12x_5 = 21$, with $x_i = 0$ or 1 for $i = 1, 2, 3, 4, 5$. These solutions are $x_1 = x_3 = x_4 = 1, x_2 = x_5 = 0$, and $x_1 = x_2 = x_5 = 1, x_3 = x_4 = 0$. ◀

To verify that equation (8.3) holds, where each x_i is either 0 or 1, requires that we perform at most n additions. On the other hand, to search by trial and error for solutions of

(8.3) may require that we check all 2^n possibilities for $(x_1, x_2, \ldots, x_n)$. The best method known for finding a solution of the knapsack problem requires $O(2^{n/2})$ bit operations, which makes a computer solution of a general knapsack problem extremely infeasible even when $n = 100$.

Certain values of the integers $a_1, a_2, \ldots, a_n$ make the solution of the knapsack problem much easier than the solution in the general case. For instance, if $a_j = 2^{j-1}$, to solve $S = a_1x_1 + a_2x_2 + \cdots + a_nx_n$, where $x_i = 0$ or 1 for $i = 1, 2, \ldots, n$, simply requires that we find the binary expansion of S. We can also produce easy knapsack problems by choosing the integers $a_1, a_2, \ldots, a_n$ so that the sum of the first $j - 1$ of these integers is always less than the jth integer, that is, so that

$$\sum_{i=1}^{j-1} a_i < a_j, \quad j = 2, 3, \ldots, n.$$

If a sequence of integers $a_1, a_2, \ldots, a_n$ satisfies this inequality, we call the sequence *super-increasing.*

Example 8.18. The sequence 2, 3, 7, 14, 27 is super-increasing because $3 > 2$, $7 > 3 + 2$, $14 > 7 + 3 + 2$, and $27 > 14 + 7 + 3 + 2$. ◀

To see that knapsack problems involving super-increasing sequences are easy to solve, we first consider an example.

Example 8.19. Let us find the integers from the set 2, 3, 7, 14, 27 that have 37 as their sum. First, we note that since $2 + 3 + 7 + 14 < 27$, a sum of integers from this set can only be greater than 27 if the sum contains the integer 27. Hence, if $2x_1 + 3x_2 + 7x_3 + 14x_4 + 27x_5 = 37$ with each $x_i = 0$ or 1, we must have $x_5 = 1$ and $2x_1 + 3x_2 + 7x_3 + 14x_4 = 10$. Because $14 > 10$, x_4 must be 0 and we have $2x_1 + 3x_2 + 7x_3 = 10$. Because $2 + 3 < 7$, we must have $x_3 = 1$ and therefore $2x_1 + 3x_2 = 3$. Obviously, we have $x_2 = 1$ and $x_1 = 0$. The solution is $37 = 3 + 7 + 27$. ◀

In general, to solve knapsack problems for a super-increasing sequence $a_1, a_2, \ldots, a_n$, that is, to find the values of $x_1, x_2, \ldots, x_n$ with $S = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ and $x_i = 0$ or 1 for $i = 1, 2, \ldots, n$ when S is given, we use the following algorithm. First, we find x_n by noting that

$$x_n = \begin{cases} 1 & \text{if } S \geq a_n; \\ 0 & \text{if } S < a_n. \end{cases}$$

Then, we find $x_{n-1}, x_{n-2}, \ldots, x_1$, in succession, using the equations

$$x_j = \begin{cases} 1 & \text{if } S - \sum_{i=j+1}^{n} x_i a_i \geq a_j; \\ 0 & \text{if } S - \sum_{i=j+1}^{n} x_i a_i < a_j, \end{cases}$$

for $j = n - 1, n - 2, \ldots, 1$.

To see that this algorithm works, first note that if $x_n = 0$ when $S \geq a_n$, then $\sum_{i=1}^{n} a_i x_i \leq \sum_{i=1}^{n-1} a_i < a_n \leq S$, contradicting the condition $\sum_{j=1}^{n} a_j x_j = S$. Similarly,

if $x_j = 0$ when $S - \sum_{i=j+1}^{n} x_i a_i \geq a_j$, then $\sum_{i=1}^{n} a_i x_i \leq \sum_{i=1}^{j-1} a_i + \sum_{i=j+1}^{n} x_i a_i < a_j + \sum_{i=j+1}^{n} x_i a_i \leq S$, which is again a contradiction.

Using this algorithm, knapsack problems based on super-increasing sequences can be solved extremely quickly. We now discuss a cryptosystem based on this observation, invented by Merkle and Hellman [MeHe78], that was initially considered a good choice for a public key cryptosystem. (We will comment more about this later in this section.)

The ciphers that we describe here are based on transformed super-increasing sequences. To be specific, let $a_1, a_2, \ldots, a_n$ be super-increasing and let m be a positive integer with $m > 2a_n$. Let w be an integer relatively prime to m with inverse $\overline{w}$ modulo m. We form the sequence $b_1, b_2, \ldots, b_n$, where $b_j \equiv wa_j \pmod{m}$ and $0 \leq b_j < m$. We cannot use this special technique to solve a knapsack problem of the type $S = \sum_{i=1}^{n} b_i x_i$, where S is a positive integer, because the sequence $b_1, b_2, \ldots, b_n$ is not super-increasing. However, when $\overline{w}$ is known, we can find

$$\overline{w}S = \sum_{i=1}^{n} \overline{w} b_i x_i \equiv \sum_{i=1}^{n} a_i x_i \pmod{m}, \tag{8.4}$$

because $\overline{w}b_j \equiv a_j \pmod{m}$. From (8.4), we see that

$$S_0 = \sum_{i=1}^{n} a_i x_i,$$

where S_0 is the least positive residue of $\overline{w}S$ modulo m. We can easily solve the equation

$$S_0 = \sum_{i=1}^{n} a_i x_i,$$

because $a_1, a_2, \ldots, a_n$ is super-increasing. This solves the knapsack problem

$$S = \sum_{i=1}^{n} b_i x_i,$$

because $b_j \equiv wa_j \pmod{m}$ and $0 \leq b_j < m$. We illustrate this procedure with an example.

Example 8.20. The super-increasing sequence $(a_1, a_2, a_3, a_4, a_5) = (3, 5, 9, 20, 44)$ can be transformed into the sequence $(b_1, b_2, b_3, b_4, b_5) = (23, 68, 69, 5, 11)$ by taking $b_j \equiv 67a_j \pmod{89}$, for $j = 1, 2, 3, 4, 5$. To solve the knapsack problem $23x_1 + 68x_2 + 69x_3 + 5x_4 + 11x_5 = 84$, we can multiply both sides of this equation by 4, an inverse of 67 modulo 89, and then reduce modulo 89, to obtain the congruence $3x_1 + 5x_2 + 9x_3 + 20x_4 + 44x_5 \equiv 336 \equiv 69 \pmod{89}$. Because $89 > 3 + 5 + 9 + 20 + 44$, we can conclude that $3x_1 + 5x_2 + 9x_3 + 20x_4 + 44x_5 = 69$. The solution of this easy knapsack problem is $x_5 = x_4 = x_2 = 1$ and $x_3 = x_1 = 0$. Hence, the original knapsack problem has as its solution $68 + 5 + 11 = 84$. ◀

The cryptosystem based on the knapsack problem invented by Merkle and Hellman works as follows. Each individual chooses a super-increasing sequence of positive

Letter	Binary Equivalent	Letter	Binary Equivalent
A	00000	N	01101
B	00001	O	01110
C	00010	P	01111
D	00011	Q	10000
E	00100	R	10001
F	00101	S	10010
G	00110	T	10011
H	00111	U	10100
I	01000	V	10101
J	01001	W	10110
K	01010	X	10111
L	01011	Y	11000
M	01100	Z	11001

Table 8.10 *The binary equivalents of letters.*

integers of a specified length, say N (for example, $a_1, a_2, \ldots, a_N$), as well as a modulus m with $m > 2a_N$ and a multiplier w with $(m, w) = 1$. The transformed sequence $b_1, b_2, \ldots, b_n$ is made public. When someone wishes to send a message P to this individual, the message is first translated into a string of zeros and ones using the binary equivalents of letters, as shown in Table 8.10. This string of zeros and ones is next split into segments of length N (for simplicity, we suppose that the length of the string is divisible by N; if not, we can simply fill out the last block with all ones). For each block, a sum is computed using the sequence $b_1, b_2, \ldots, b_N$: for instance, the block $x_1x_2 \ldots x_N$ gives $S = b_1x_1 + b_2x_2 + \cdots + b_Nx_N$. Finally, the sums generated by each block form the ciphertext message.

We note that to decipher ciphertext generated by the knapsack cipher, without knowledge of m and w, requires that a group of hard knapsack problems of the form

$$S = b_1x_1 + b_2x_2 + \cdots + b_Nx_N \tag{8.5}$$

be solved. On the other hand, when m and w are known, the knapsack problem (8.5) can be transformed into an easy knapsack problem, because

$$\begin{aligned} \overline{w}S &= \overline{w}b_1x_1 + \overline{w}b_2x_2 + \cdots + \overline{w}b_Nx_N \\ &\equiv a_1x_1 + a_2x_2 + \cdots + a_Nx_N \pmod{m}, \end{aligned}$$

in which $\overline{w}b_j \equiv a_j \pmod{m}$, where $\overline{w}$ is an inverse of w modulo m, so that

$$S_0 = a_1x_1 + a_2x_2 + \cdots + a_Nx_N, \tag{8.6}$$

where S_0 is the least positive residue of $\overline{w}S$ modulo m. We have equality in (8.6), because both sides of the equation are positive integers less than m that are congruent modulo m.

We illustrate the encrypting and decrypting procedures of the knapsack cipher with an example. We start with the super-increasing sequence $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) = (2, 11, 14, 29, 58, 119, 241, 480, 959, 1917)$. We take $m = 3837$ as the encrypting modulus, so that $m > 2a_{10}$, and $w = 1001$ as the multiplier, so that $(m, w) = 1$, to transform the super-increasing sequence into the sequence (2002, 3337, 2503, 2170, 503, 172, 3347, 855, 709, 417).

To encrypt the message

REPLY IMMEDIATELY,

we first translate the letters of the message into their five-digit binary equivalents, as shown in Table 8.10, and then group these digits into blocks of ten, to obtain

1000100100 0111101011 1100001000
0110001100 0010000011 0100000000
1001100100 0101111000.

For each block of ten binary digits, we form a sum by adding together the appropriate terms of the sequence (2002, 3337, 2503, 2170, 503, 172, 3347, 855, 709, 417) in the slots corresponding to positions of the block containing a digit equal to 1. This gives us

3360 12986 8686 10042 3629 3337 5530 9529.

For instance, we compute the first sum, 3360, by adding 2002, 503, and 855.

To decrypt, we find the least positive residue modulo 3837 of 23 times each sum, because 23 is an inverse of 1001 modulo 3837, and then we solve the corresponding easy knapsack problem with respect to the original super-increasing sequence (2, 11, 14, 29, 58, 119, 241, 480, 959, 1917). For example, to decrypt the first block, we find that $3360 \cdot 23 \equiv 540 \pmod{3837}$, and then note that $540 = 480 + 58 + 2$. This tells us that the first block of plaintext binary digits is 1000100100.

Knapsack ciphers originally seemed to be excellent candidates for use in public key cryptosystems. However, in 1982 Shamir [Sh84] has shown that they are not satisfactory for public key cryptography. The reason is that there is an efficient algorithm for solving knapsack problems involving sequences $b_1, b_2, \ldots, b_n$ with $b_j \equiv wa_j \pmod{m}$, where w and m are relatively prime positive integers and $a_1, a_2, \ldots, a_n$ is a super-increasing sequence. The algorithm found by Shamir can solve these knapsack problems using only $O(P(n))$ bit operations, where P is a polynomial, instead of requiring exponential time, as is required for known algorithms for general knapsack problems involving sequences of a general nature. Although we will not go into the details of the algorithm found by Shamir here, the reader can find these details by consulting [Od90].

There are several possibilities for altering this cryptosystem to avoid the weakness found by Shamir. One such possibility is to choose a sequence of pairs of relatively prime

integers $(w_1, m_1), (w_2, m_2), \ldots, (w_r, m_r)$, and then form the series of sequences

$$b_j^{(1)} \equiv w_1 a_j \pmod{m_1}$$
$$b_j^{(2)} \equiv w_2 b_j^{(1)} \pmod{m_2}$$
$$\vdots$$
$$b_j^{(r)} \equiv w_r b_j^{(r-1)} \pmod{m_r},$$

for $j = 1, 2, \ldots, n$. We then use the final sequence $b_1^{(r)}, b_2^{(r)}, \ldots, b_n^{(r)}$ as the encrypting sequence. Unfortunately, efficient algorithms have been found for solving knapsack problems involving sequences obtained by iterating modular multiplications with different moduli.

A comprehensive discussion of knapsack ciphers can be found in [Od90]. This article describes knapsack ciphers and their generalizations, and goes on to explain the attacks that have been found for breaking them.

8.5 Exercises

1. Decide whether each of the following sequences is super-increasing.

   a) (3, 5, 9, 19, 40) c) (3, 7, 17, 30, 59)
   b) (2, 6, 10, 15, 36) d) (11, 21, 41, 81, 151)

2. Show that if $a_1, a_2, \ldots, a_n$ is a super-increasing sequence, then $a_j \geq 2^{j-1}$ for $j = 1, 2, \ldots, n$.

3. Show that the sequence $a_1, a_2, \ldots, a_n$ is super-increasing if $a_{j+1} > 2a_j$ for $j = 1, 2, \ldots, n-1$.

4. Find all subsets of the integers 2, 3, 4, 7, 11, 13, 16 that have 18 as their sum.

5. Find the sequence obtained from the super-increasing sequence (1, 3, 5, 10, 20, 41, 81) when modular multiplication is applied with multiplier $w = 17$ and modulus $m = 163$.

6. Encrypt the message BUY NOW using the knapsack cipher based on the sequence obtained from the super-increasing sequence (17, 19, 37, 81, 160), by performing modular multiplication with multiplier $w = 29$ and modulus $m = 331$.

7. Decrypt the ciphertext 402 75 120 325 that was encrypted by the knapsack cipher based on the sequence (306, 374, 233, 19, 259). This sequence is obtained by using modular multiplication with multiplier $w = 17$ and modulus $m = 464$, to transform the super-increasing sequence (18, 22, 41, 83, 179).

8. Find the sequence obtained by applying successively the modular multiplications with multipliers and moduli (7,92), (11,95), and (6,101), respectively, on the super-increasing sequence (3, 4, 8, 17, 33, 67).

9. What process can be employed to decrypt messages that have been encrypted using knapsack ciphers that involve sequences arising from iterating modular multiplications with different moduli?

A *multiplicative knapsack problem* is a problem of the following type: Given positive integers $a_1, a_2, \ldots, a_n$ and a positive integer P, find the subset, or subsets, of these integers with product P, or equivalently, find all solutions of

$$P = a_1^{x_1} a_2^{x_2} \cdots a_n^{x_n},$$

where $x_j = 0$ or 1 for $j = 1, 2, \ldots, n$.

10. Find all products of subsets of the integers 2, 3, 5, 6, 10 equal to 60.

11. Find all products of subsets of the integers 8, 13, 17, 21, 95, 121 equal to 15,960.

12. Show that if the integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime, then the multiplicative knapsack problem $P = a_1^{x_1} a_2^{x_2} \cdots a_n^{x_n}$, $x_j = 0$ or 1 for $j = 1, 2, \ldots, n$ is easily solved from the prime factorizations of the integers $P, a_1, a_2, \ldots, a_n$, and show that if there is a solution, then it is unique.

13. Show that by taking logarithms to the base b modulo m, where $(b, m) = 1$ and $0 < b < m$, the multiplicative knapsack problem

$$P = a_1^{x_1} a_2^{x_2} \cdots a_n^{x_n}$$

is converted into an additive knapsack problem

$$S = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n,$$

where $S, \alpha_1, \alpha_2, \ldots, \alpha_n$ are the logarithms of $P, a_1, a_2, \ldots, a_n$ to the base b modulo m, respectively.

14. Explain how Exercises 12 and 13 can be used to produce ciphers where messages are easily decrypted when the mutually relatively prime integers $a_1, a_2, \ldots, a_n$ are known, but cannot be decrypted quickly when the integers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are known.

8.5 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. Starting with a super-increasing sequence that you have constructed, perform modular multiplication with modulus m and multiplier w to find a sequence to serve as your public key for the knapsack cipher.

2. For each of your classmates, encrypt a message using their public key for the knapsack cipher.

3. Decrypt the messages that were sent to you by classmates.

** 4. Using algorithms described in [Od90], solve knapsack problems based on a sequence obtained by modular multiplication of a super-increasing sequence.

Programming Projects

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

1. Solve knapsack problems by trial and error.

2. Solve knapsack problems involving super-increasing sequences.

3. Encrypt messages using knapsack ciphers.
4. Decrypt messages that were encrypted using knapsack ciphers.
5. Encrypt and decrypt messages using knapsack ciphers involving sequences arising from iterating modular multiplications with different moduli.
6. Solve multiplicative knapsack problems involving sequences of mutually relatively prime integers (see Exercise 14).

8.6 Cryptographic Protocols and Applications

In this section, we describe how cryptosystems can be used in protocols, which are algorithms carried out by two or more parties to achieve a specific goal, and in other cryptographic applications. In particular, we will show how two or more people can exchange encryption keys. We will also explain how messages can be signed using the RSA cryptosystem, and how cryptography can be used to allow people to play poker fairly over a network. Finally, we will show how people can share a secret, so that no one person knows the secret, but a large enough group of people can recover the secret by cooperating. These are only a few of the many examples of protocols and applications that we could discuss; the interested reader should consult [MevaVa97] to learn about additional protocols and applications based on the ideas we have covered in this chapter.

Diffie-Hellman Key Exchange

We will now discuss a protocol that allows two parties to exchange a secret key over an insecure communications link without having shared any information in the past. Exchanging keys is a problem of fundamental importance in cryptography. The method that we will describe was invented by Diffie and Hellman in 1976 (see [DiHe76]) and is called the *Diffie-Hellman key agreement protocol.* The common secret key generated by this protocol can be used as a shared key for a symmetric cryptosystem to be used during a particular communication session by parties who have never met or shared any prior information. It has the property that unauthorized parties cannot discover it in a feasible amount of computer time.

To implement this protocol, we need a large prime p and an integer r such that the least positive residue of r^k runs inclusively through all integers from 1 to $n-1$. (This means that r is a primitive root of p, a concept that we will study in Chapter 9.) Both the large prime p and the integer r are public information.

In this protocol, two parties who want to share a common key each pick a random private value from the set of positive integers between 1 and $p-2$, inclusive. If the two parties select k_1 and k_2, respectively, the first party sends the second party the integer y_1, where

$$y_1 \equiv r^{k_1} \pmod{p}, \quad 0 < y_1 < p,$$

and the second party finds the common key K by computing

$$K \equiv y_1^{k_2} \equiv r^{k_1 k_2} \pmod{p}, \quad 0 < K < p.$$

Similarly, the second party sends the first party the integer y_2, where

$$y_2 \equiv r^{k_2} \pmod{p}, \quad 0 < y_2 < p,$$

and the first party finds the common key K by computing

$$K \equiv y_2^{k_1} \equiv r^{k_1 k_2} \pmod{p}, \quad 0 < K < p.$$

The security of this key agreement protocol depends on the security of determining the secret key K, given the least positive residues of r^{k_1} and r^{k_2} modulo p; that is, it depends on the difficulty of computing what are known as discrete logarithms modulo p (to be discussed in Chapter 9), which is thought to be a computationally difficult problem. It has been shown (see [Ma94]) that breaking this protocol is equivalent to computing discrete logarithms, when certain conditions hold.

In a similar manner, a common key can be shared by any group of n individuals. If these individuals have keys $k_1, k_2, \ldots, k_n$, they can share the common key

$$K = r^{k_1 k_2 \cdots k_n} \pmod{p}.$$

We leave an explicit description of a method used to produce this common key as a problem for the reader.

The topic of key establishment protocols extends far beyond what we have described here. Many different protocols for establishing shared keys have been developed, including protocols that make use of trusted servers for distributing keys. To learn more about this topic, consult Chapter 12 of [MevaVa97].

Digital Signatures

When we receive an electronic message, how do we know that it has come from the supposed sender? We need a *digital signature* that can tell us that the message must have originated with the party who supposedly sent it. We will show that a public key cryptosystem, such as the RSA cryptosystem, can be used to send "signed" messages. When signatures are used, the recipient of a message is sure that the message came from the sender, and can convince an impartial judge that only the sender could be the source of the message. This authentication is needed for electronic mail, electronic banking, and electronic stock market transactions. To see how the RSA cryptosystem can be used to send signed messages, suppose that individual i wishes to send a signed message to individual j. The first thing that individual i does to a plaintext block P is to compute

$$S = D_{k_i}(P) \equiv P^{d_i} \pmod{n_i},$$

where (d_i, n_i) is the decrypting key for individual i, which only individual i knows. Then, if $n_j > n_i$, where (e_j, n_j) is the encryption key for individual j, individual i encrypts S by forming

$$C = E_{k_j}(S) \equiv S^{e_j} \pmod{n_j}, \quad 0 \leq C < n_j.$$

When $n_j < n_i$, individual i splits S into blocks of size less than n_j and encrypts each block using the encrypting transformation E_{k_j}.

For decrypting, individual j first uses the private decrypting transformation D_{k_j} to recover S, because

$$D_{k_j}(C) = D_{k_j}(E_{k_j}(S)) = S.$$

To find the plaintext message P, supposedly sent by individual i, individual j next uses the public encrypting transformation E_{k_i}, because

$$E_{k_i}(S) = E_{k_i}(D_{k_i}(P)) = P.$$

Here, we have used the identity $E_{k_i}(D_{k_i}(P)) = P$, which follows from the fact that

$$E_{k_i}(D_{k_i}(P)) \equiv (P^{d_i})^{e_i} \equiv P^{d_i e_i} \equiv P \pmod{n_i},$$

because

$$d_i e_i \equiv 1 \pmod{\phi(n_i)}.$$

The combination of the plaintext block P and the signed version S convinces individual j that the message actually came from individual i. Also, individual i cannot deny sending the message, because no one other than individual i could have produced the signed message S from the original message P.

Electronic Poker

An amusing application of exponentiation ciphers has been described by Shamir, Rivest, and Adleman [ShRiAd81]. They show that by using exponentiation ciphers, a fair game of poker may be played by two players, communicating via computers. Suppose that Alex and Betty wish to play poker. First, they jointly choose a large prime p. Next, they individually choose secret keys e_1 and e_2, to be used as exponents in modular exponentiation. Let E_{e_1} and E_{e_2} represent the corresponding encrypting transformations, so that

$$E_{e_1}(M) \equiv M^{e_1} \pmod{p}$$
$$E_{e_2}(M) \equiv M^{e_2} \pmod{p},$$

where M is a plaintext message. Let d_1 and d_2 be the respective inverses of e_1 and e_2 modulo p, and let D_{e_1} and D_{e_2} be the corresponding decrypting transformations, so that

$$D_{e_1}(C) \equiv C^{d_1} \pmod{p}$$
$$D_{e_2}(C) \equiv C^{d_2} \pmod{p},$$

where C is a ciphertext message.

Note that encrypting transformations commute, that is,

$$E_{e_1}(E_{e_2}(M)) = E_{e_2}(E_{e_1}(M)),$$

because $(M^{e_2})^{e_1} \equiv (M^{e_1})^{e_2} \pmod{p}$.

To play electronic poker, the deck of cards is represented by the 52 messages

$$M_1 = \text{"TWO OF CLUBS"}$$
$$M_2 = \text{"THREE OF CLUBS"}$$
$$\vdots$$
$$M_{52} = \text{"ACE OF SPADES"}.$$

When Alex and Betty wish to play poker electronically, they use the following sequence of steps. We suppose that Betty is the dealer.

1. Betty uses her encrypting transformation to encipher the 52 messages for the cards. She obtains $E_{e_2}(M_1), E_{e_2}(M_2), \ldots, E_{e_2}(M_{52})$. Betty shuffles the deck, by randomly reordering the encrypted messages. Then she sends the 52 shuffled encrypted messages to Alex.
2. Alex selects, at random, five of the encrypted messages that Betty has sent him. He returns these five messages to Betty and she decrypts them to find her hand, using her decrypted transformation D_{e_2} because $D_{e_2}(E_{e_2}(M)) = M$ for all messages M. Alex cannot determine which cards Betty has, because he cannot decrypt the encrypted messages $E_{e_2}(M_j)$, $j = 1, 2, \ldots, 52$.
3. Alex selects five other encrypted messages at random. Let these messages be C_1, C_2, C_3, C_4, and C_5, where

   $$C_j = E_{e_2}(M_{i_j}),$$

   $j = 1, 2, 3, 4, 5$. Alex sends these five previously encrypted messages using his encrypted transformation. He obtains the five messages

   $$C_j^* = E_{e_i}((C_j) = E_{e_i}(E_{e_2}(M_{i_j})),$$

   $j = 1, 2, 3, 4, 5$. Alex sends these five messages that have been encrypted twice (first by Betty and afterward by Alex) to Betty.
4. Betty uses her decrypted transformation D_{e_2} to find

   $$\begin{aligned} D_{e_2}(C_j^*) &= D_{e_2}(E_{e_1}(E_{e_2}(M_{i_j}))) \\ &= D_{e_2}(E_{e_2}(E_{e_1}(M_{i_j}))) \\ &= E_{e_1}(M_{i_j}), \end{aligned}$$

   because $E_{e_1}(E_{e_2}(M)) = E_{e_2}(E_{e_1}(M))$ and $D_{e_2}(E_{e_2}(M)) = M$ for all messages M. Betty sends the five messages $E_{e_1}(M_{i_j})$ back to Alex.
5. Alex uses his decrypting transformation D_{e_1} to obtain his hand, because

   $$D_{e_1}(E_{e_1}(M_{i_j})) = M_{i_j}.$$

When a game is played where it is necessary to deal additional cards, such as draw poker, the same steps are followed to deal additional cards from the remaining deck. Note that using the procedure we have described, neither player knows the cards in the hand of the other player, and all hands are equally likely for each player. To guarantee

that no cheating has occurred, at the end of the game both players reveal their keys, so that each player can verify that the other player was actually dealt the cards claimed.

A description of a possible weakness in this scheme, and how it may be overcome, may be found in the exercise set of Section 11.1.

Secret Sharing

We now discuss another application of cryptography, namely a method for sharing secrets. Suppose that in a communications network there is some vital, but extremely sensitive, information. If this information is distributed to several individuals, it becomes much more vulnerable to exposure; on the other hand, if this information is lost, there are serious consequences. An example of such information is the *master key* K used for access to the password file in a computer system.

To protect this master key K from both loss and exposure, we construct *shadows* $k_1, k_2, \ldots, k_r$, which are given to r different individuals. We will show that the key K can be produced easily from any s of these shadows, where s is a positive integer less than r, whereas the knowledge of less than s of these shadows does not permit the key K to be found. Because at least s different individuals are needed to find K, the key is not vulnerable to exposure. In addition, the key K is not vulnerable to loss, since any s individuals from the r individuals with shadows can produce K. Schemes with properties we have just described are called *(s, r)-threshold schemes.*

To develop a system that can be used to generate shadows with these properties, we use the Chinese remainder theorem. We choose a prime p greater than the key K and a sequence of pairwise relatively prime integers $m_1, m_2, \ldots, m_r$ that are not divisible by p, such that

$$m_1 < m_2 < \cdots < m_r,$$

and

$$m_1 m_2 \cdots m_s > p m_r m_{r-1} \cdots m_{r-s+2}. \tag{8.7}$$

Note that the inequality (8.7) states that the product of the s smallest of the integers m_j is greater than the product of p and the $s-1$ largest of the integers m_j. From (8.7), we see that if $M = m_1 m_2 \cdots m_s$, then M/p is greater than the product of any set of $s-1$ of the integers m_j.

Now, let t be a nonnegative integer less than M/p that is chosen at random. Let

$$K_0 = K + tp,$$

so that $0 \leq K_0 \leq M-1$ (because $0 \leq K_0 = K + tp < p + tp = (t+1)p \leq (M/p)p = M$).

To produce the shadows $k_1, k_2, \ldots, k_r$, we let k_j be the integer such that

$$k_j \equiv K_0 \pmod{m_j}, \quad 0 \leq k_j < m_j,$$

for $j = 1, 2, \ldots, r$. To see that the master key K can be found by any s individuals from the total of r individuals with shadows, suppose that the s shadows $k_{j_1}, k_{j_2}, \ldots, k_{j_s}$ are available. Using the Chinese remainder theorem, we can easily find the least positive residue of K_0 modulo M_j, where $M_j = m_{j_1} m_{j_2} \cdots m_{j_s}$. Because we know that $0 \leq K_0 < M \leq M_j$, we can determine K_0, and then find $K = K_0 - tp$.

On the other hand, suppose that we know only the $s - 1$ shadows $k_{i_1}, k_{i_2}, \ldots, k_{i_{s-1}}$. By the Chinese remainder theorem, we can determine the least positive residue a of K_0 modulo M_i, where $M_i = m_{i_1} m_{i_2} \cdots m_{i_{s-1}}$. With these shadows, the only information we have about K_0 is that a is the least positive residue of K_0 modulo M_i and $\leq K_0 < M$. Consequently, we only know that

$$K_0 = a + xM_i,$$

where $0 \leq x < M/M_i$. From (8.7), we can conclude that $M/M_i > p$, so that as x ranges through the positive integers less than M/M_i, x takes every value in a full set of residues modulo p. Because $(m_j, p) = 1$ for $j = 1, 2, \ldots, s$, we know that $(M_i, p) = 1$ and, consequently, $a + xM_i$ runs through a full set of residues modulo p as x does. Hence, we see that the knowledge of $s - 1$ shadows is insufficient to determine K_0, as K_0 could be in any of the p congruence classes modulo p.

We use an example to illustrate this threshold scheme.

Example 8.21. Let $K = 4$ be the master key. We will use a (2,3)-threshold scheme of the kind just described, with $p = 7$, $m_1 = 11$, $m_2 = 12$, and $m_3 = 17$, so that $M = m_1 m_2 = 132 > pm_3 = 119$. We pick $t = 14$ randomly from among the positive integers less than $M/p = 132/7$. This gives us

$$K_0 = K + tp = 4 + 14 \cdot 7 = 102.$$

The three shadows k_1, k_2, and k_3 are the least positive residues of K_0 modulo m_1, m_2, and m_3; that is,

$$\begin{aligned} k_1 &\equiv 102 \equiv 3 \pmod{11} \\ k_2 &\equiv 102 \equiv 6 \pmod{12} \\ k_3 &\equiv 102 \equiv 0 \pmod{17}, \end{aligned}$$

so that the three shadows are $k_1 = 3$, $k_2 = 6$, and $k_3 = 0$.

We can recover the master key K from any two of the three shadows. Suppose we know that $k_1 = 3$ and $k_3 = 0$. Using the Chinese remainder theorem, we can determine K_0 modulo $m_1 m_3 = 11 \cdot 17 = 187$; in other words, because $K_0 \equiv 3 \pmod{11}$ and $K_0 \equiv 0 \pmod{17}$, we have $K_0 \equiv 102 \pmod{187}$. Because $0 \leq K_0 < M = 132 < 187$, we know that $K_0 = 102$, and consequently the master key is $K = K_0 - tp = 102 - 14 \cdot 7 = 4$. ◀

For more details on secret sharing schemes, see [MevaVa97].

8.6 Exercises

1. Using the Diffie-Hellman key agreement protocol, find the common key that can be used by two parties with keys $k_1 = 27$ and $k_2 = 31$, when the modulus is $p = 103$ and the base $r = 5$.

2. Using the Diffie-Hellman key agreement protocol, find the common key that can be used by two parties with keys $k_1 = 7$ and $k_2 = 8$, when the modulus is $p = 53$ and the base is $r = 2$.

3. What is the group key K that can be shared by three parties with keys $k_1 = 3, k_2 = 10$, and $k_3 = 5$, using the modulus $p = 601$ and base $r = 7$?

4. What is the group key K that can be shared by four parties with keys $k_1 = 11, k_2 = 12, k_3 = 17$, and $k_4 = 19$, using the modulus $p = 1009$ and base $r = 3$?

* 5. Describe the steps of a protocol that allows n parties to share a common key, as described in the text.

6. Romeo and Juliet have as their RSA keys $(5, 19 \cdot 67)$ and $(3, 11 \cdot 71)$, respectively.
   a) Using the method in the text, what is the signed ciphertext message sent by Romeo to Juliet, when the plaintext message is GOODBYE SWEET LOVE?
   b) Using the method in the text, what is the signed ciphertext message sent by Juliet to Romeo, when the plaintext message is ADIEU FOREVER?

7. Harold and Audrey have as their RSA keys $(3, 23 \cdot 47)$ and $(7, 31 \cdot 59)$, respectively.
   a) Using the method in the text, what is the signed ciphertext sent by Harold to Audrey, when the plaintext message is CHEERS HAROLD?
   b) Using the method in the text, what is the signed ciphertext sent by Audrey to Harold, when the plaintext message is SINCERELY AUDREY?

In Exercises 8 and 9, we present two methods for sending signed messages using the RSA cipher system, avoiding possible changes in block sizes.

* 8. Let H be a fixed integer. Let each individual have two pairs of encrypting keys: $k = (e, n)$ and $k^* = (e, n^*)$ with $n < H < n^*$, where n and n^* are each the product of two primes. Using the RSA cryptosystem, individual i can send a signed message P to individual j by sending $E_{k_j^*}(D_{k_i}(P))$.
   a) Show that it is not necessary to change block sizes when the transformation $E_{k_j^*}$ is applied after D_{k_i} has been applied.
   b) Explain how individual j can recover the plaintext message P, and why no one other than individual i could have sent the message.
   c) Let individual i have encrypting keys $(3, 11 \cdot 71)$ and $(3, 29 \cdot 41)$, so that $781 = 11 \cdot 71 < 1000 < 1189 = 29 \cdot 41$, and let individual j have enciphering keys $(7, 19 \cdot 47)$ and $(7, 31 \cdot 37)$, so that $893 = 19 \cdot 47 < 1000 < 1147 = 31 \cdot 37$. What ciphertext message does individual i send to individual j using the method given at the beginning of this exercise, when the signed plaintext message is HELLO ADAM? What ciphertext message does individual j send to individual i when the signed plaintext message is GOODBYE ALICE?

* 9. a) Show that if individuals i and j have encrypting keys $k_i = (e_i, n_i)$ and $k_j = (e_j, n_j)$, respectively, where both n_i and n_j are products of two distinct primes, then individual

i can send a signed message P to individual j without needing to change the size of blocks, by sending

$$E_{k_j}(D_{k_i}(P)) \text{ if } n_i < n_j$$
$$D_{k_j}(E_{k_i}(P)) \text{ if } n_i < n_j.$$

b) How can individual j recover P?

c) How can individual j guarantee that a message came from individual i?

d) Let $k_i = (11, 47 \cdot 61)$ and $k_j = (13, 43 \cdot 59)$. Using the method described in part (a), what does individual i send to individual j if the message is REGARDS FRED, and what does individual j send to individual i if the message is REGARDS ZELDA?

10. Decompose the master key $K = 5$ into three shadows using a (2,3)-threshold scheme of the type described in the text, with $p = 7$, $m_1 = 11$, $m_2 = 12$, $m_3 = 17$, and $t = 14$, as in Example 8.21.

11. Decompose the master key $K = 3$ into three shadows using a (2,3)-threshold scheme of the type described in the text, with $p = 5$, $m_1 = 8$, $m_2 = 9$, $m_3 = 11$, and $t = 13$.

12. Show how to recover the master key K from each of the three pairs of shadows found in Exercise 10.

13. Show how to recover the master key K from each of the three pairs of shadows found in Exercise 11.

14. Construct a (3,5)-threshold scheme of the type described in the text. Use the scheme to decompose the master key $K = 22$ into five shadows, and show how the master key can be found using one set of three shadows so produced.

8.6 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. Produce a set of common keys using a prime p with more than 100 digits.

2. Produce some signed messages using the RSA cryptosystem and verify that these messages came from the supposed sender.

3. Construct a (4,6)-threshold scheme that decomposes a master key into six shadows. Distribute these shadows to six members of your class, and then select three different groups of four of these six people, reconstructing the key from the four shadows of the people in each group.

Programming Projects

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

1. Produce common keys for individuals in a network.

2. Send signed messages using an RSA cipher and the method described in the text.

3. Send signed messages using an RSA cipher and the method in Exercise 8.
4. Send signed messages using an RSA cipher and the method in Exercise 9.
* 5. Play electronic poker using encryption via modular exponentiation.
6. Find the shadows in a threshold scheme of the type described in the text.
7. Recover the master key from a set of shadows.