COMP 233 Discrete Mathematics

Chapter 4

Number Theory and Methods of Proof

Topics in this chapter

- Direct Proof and Counterexample I:
  - Introduction
- Direct Proof and Counterexample II:
  - Rational Numbers
- Direct Proof and Counterexample III:
  - Divisibility
- Direct Proof and Counterexample IV:
  - Prime numbers, Division into cases and Quotient-Remainder Theorem
- Proof by contradiction

4.1

Direct Proof and Counterexample I: Introduction

Assumptions:

- Properties of the real numbers (Appendix A) – “basic algebra”
- Logic
- Properties of equality:

    A = A

    If A = B, then B = A.

    If A = B and B = C, then A = C.

- Integers are 0, 1, 2, 3, …, -1, -2, -3, …
- Any sum, difference, or product of integers is an integer.
- most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.

Overview

Complete the following sentences:

An integer ***n* is even** if, and only if n is equal to twice some integer.

$$n = 2k$$

An integer ***n* is odd** if, and only if n is equal to twice some integer plus 1.

$$n=2k+1$$

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

n is prime $\Leftrightarrow$ $\forall$ positive integers r and s, if $n = rs$ then either $r = 1$ and $s = n$ or $r = n$ and $s = 1$.

n is composite $\Leftrightarrow$ $\exists$ positive integers r and s such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

An integer ***n* is prime** if, and only if,

$n > 1$ and the only positive integer divisors of n are 1 and n.

5

- **Even and Odd Integers**
  Use the definitions of *even* and *odd* to justify your answers to the following questions.
  a. Is 0 even?
  b. Is -301 odd?
  c. If a and b are integers, is $6a^2b$ even?
  d. If a and b are integers, is $10a + 8b + 1$ odd?
  e. Is every integer either even or odd?

- **Solution**
  a. Yes, $0 = 2 \cdot 0$.
  b. Yes, $-301 = 2(-151) + 1$.
  c. Yes, $6a^2b = 2(3a^2b)$, and since a and b are integers, so is $6a^2b$ (being a product of integers).
  d. Yes, $10a + 8b + 1 = 2(5a + 4b) + 1$, and since a and b are integers, so is $5a + 4b$ (being a sum of products of integers).
  e. The answer is yes, although the proof is not obvious.

How to (dis)approve statements

Before (dis)approving, write a math statements as a Universal or an Existential Statement:

	Proving	Disapproving
$\exists x \in D \ . \ Q(x)$	One example Constructive Proof	Negate then direct proof
$\forall x \in D \ . \ Q(x)$	**1- Exhaustion** **2- Direct proof**	Counter example

Proving Existential Statements
constructive proofs of existence

- a. Prove the following: ∃ an even integer n that can be written in two ways as a sum of two prime numbers.

- Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers.

- b. Suppose that r and s are integers.
- Prove the following: ∃ an integer k such that
  $22r + 18s = 2k$.
  Let $k = 11r + 9s$.
- Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra.

Proving Universal Statements

The majority of mathematical statements to be proved are universal.

$$\forall x \in D \, . \, P(x) \rightarrow Q(x)$$

One way to prove such statements is called **The Method of Exhaustion**, by listing all cases.

Use the method of exhaustion to prove the following:

$\forall n \in Z$, if n is even and $4 \leq n \leq 12$, then n can be written as a sum of two prime numbers.

$4 = 2 + 2$ $6 = 3 + 3$ $8 = 3 + 5$ $10 = 5 + 5$
$12=5+7$

➔ **This method** is obviously impractical, as we cannot check all possibilities.

Proving a Universal Statement Over a Finite Set

Method of Exhaustion: Prove that every even integer from 2 through 10 can be expressed as a sum of at most 3 perfect squares.

Proof:

$2 = 1^2 + 1^2$

$4 = 2^2$

$6 = 2^2 + 1^2 + 1^2$

$8 = 2^2 + 2^2$

$10 = 3^2 + 1^2$

Note: The method of exhaustion only works for relatively small finite sets.

10

Direct Proofs

Method of Generalizing from the Generic Particular:
If a property can be shown to be true for a particular but arbitrarily chosen element of a set, then it is true for every element of the set.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, $P(x) \rightarrow Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Generalizing from the Generic Particular

suppose *x* is a *particular* but *arbitrarily chosen* element of the set

Step	Visual Result	Algebraic Result
Pick a number.	□	x
Add 5.	□|||||	$x + 5$
Multiply by 4.	□||||| □||||| □||||| □|||||	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	□|| □|| □||||| □|||||	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	□|| □|||||	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.		
					$(2x + 7) - 2x = 7$

Example

Prove that the sum of any two even integers is even.

Formal Restatement: $\forall m,n \in \mathbf{Z}$. Even(m) $\wedge$ Even(n) $\rightarrow$ Even($m + n$)

Starting Point: Suppose m and n are even *[particular but arbitrarily chosen]*

We want to Show: $m+n$ is even

By definition
$m = 2k$
$n = 2j$
For some integers k and j
$m+n = 2k + 2j = 2(k+j)$
Let $r = (k+j)$ is integer, because r is some of integers
Thus: m+n = 2r , that mean m+n is even

[This is what we needed to show.]

Let's Use Direct Proofs!

Question: Is the sum of an even integer plus an odd integer always even? always odd? sometimes even and sometimes odd?

- ∀ integers *x* and *y*, if *x* is even and *y* is odd, then *x* + *y* is odd.
- Assume X is even and Y is odd p.b.a.c
- We want to show that X+Y is odd
- X=2k
- Y = 2j+1
- For some integers k and j
- X+Y = 2k+2j + 1
- = 2(k+j)+1
- M=(k+j) , M is an integer BCZ sum of integers is int.
- X+Y = 2M+1 is an Odd [This is what we needed to show.]

14

Let's Use Direct Proofs!

Question: Is the difference between of an even integer and an odd integer always even? always odd? sometimes even and sometimes odd?

- ∀ integers *x* and *y*, if *x* is even and *y* is odd, then *x* - *y* is odd.
- ∀ Assume X is even and Y is odd p.b.a.c
- ∀ We want to show that X-Y is odd
- ∀ X=2k
- ∀ Y = 2j+1
- ∀ For some integers k and j
- ∀ X-Y = 2k-(2j + 1) = 2k-2j-1
- ∀ = 2(k-j-1)+1 =
- ∀ M=(k-j-1) , M is an integer BCZ some of integers.
- ∀ X-Y = 2M+1 is an Odd [This is what we needed to show.]

15

Prove or disprove?

- If k is odd and m is even, then K^2+m^2 is odd

Class Exercise

Question: If k is an integer, is $2k - 1$ an odd integer?

Reference: An integer is **odd** $\Leftrightarrow$ it can be expressed as 2 times some integer plus 1.

Answer: Yes. Explanation:

Note that $k - 1$ is an integer

because it is a difference of integers. And

$$2(k - 1) + 1 = 2k - 2 + 1$$
$$= 2k - 1$$

Scratch work:

Want: $2k - 1 = 2(\square) + 1$

$\uparrow$ an integer

So we want: $2k - 1 = 2(\square) + 1$

$\Rightarrow 2k - 2 = 2(\square)$

$\Rightarrow 2(k - 1) = 2(\square)$

$\Rightarrow k - 1 = \square$

17

Disproving an Existential Statement

- Show that the following statement is false:
  There is a positive integer n such that $\boldsymbol{n^2 + 3n + 2}$ is prime.
- Proving that the given statement is false is equivalent to proving its negation is true.
- The negation is
  For all positive integers n, $n^2 + 3n + 2$ is not prime.
  Because the negation is universal, it is proved by generalizing from the generic particular.
- ***Claim:*** The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

Disproving an Existential Statement

- **Proof:**
  Suppose n is any *[particular but arbitrarily chosen]* positive integer.
- *[We will show that* $n^2 + 3n + 2$ *is not prime.]*
- We can factor $n^2 + 3n + 2$ to obtain
- $n^2 + 3n + 2 = (n + 1)(n + 2)$.
- We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$).
- Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime.

Directions for Writing Proofs

1. Copy the statement of the theorem to be proved onto your paper.
2. Clearly mark the beginning of your proof with the word "Proof."
3. Write your proof in complete sentences.
4. Make your proof self-contained. *(E.g., introduce all variables)*
5. Give a reason for each assertion in your proof.
6. Include the "little words" that make the logic of your arguments clear. *(E.g., then, thus, therefore, so, hence, because, since, Notice that, etc.)*
7. Make use of definitions but do not include them verbatim in the body of your proof.

Common Proof-Writing Mistakes

1. Arguing from examples.
2. Using the same letter to mean two different things.
3. Jumping to a conclusion/ Assuming what to be proved.
4. .
5. Misuse of the word "if."

21

4.2

Direct Proof and Counterexample II: Rational Numbers

Rational Numbers

Definition: A real number is **rational** if, and only if, it can be written as a ratio of integers with a nonzero denominator.

In symbols :

r is **rational** $\Leftrightarrow \exists$ integers a and b such that $r = a/b$ and $b \neq 0$.

Examples: Identify which of the following numbers are rational. Justify your answers.

1. 43.205

This number is rational: $43.205 = \frac{43205}{1000}$

More Examples

2. $-\frac{6}{5}$ This number is rational: $-\frac{6}{5} = \frac{-6}{5} = \frac{6}{-5}$.

3. 0 This number is rational: $0 = \frac{0}{1}$.

4. 21.34343434...

Let $x = 21.34343434....$
Then $100x = 2134.343434...$
So $100x - x = 2134.343434... - 21.34343434...$, i.e.,
$99x = 2113$. Thus $x = 2113/99$, a rational number.

25

Another Example

Zero Product Property: If any two nonzero real numbers are multiplied, the product is nonzero.

Example: Suppose m and n are nonzero integers. Is $\frac{m}{n} + \frac{n}{m}$ a rational number? Explain.

Solution: By algebra,

$$\frac{m}{n} + \frac{n}{m} = \frac{m^2}{mn} + \frac{n^2}{mn} = \frac{m^2 + n^2}{mn}.$$

Now both $m^2 + n^2$ and mn are integers because products and sums of integers are integers. Also mn is nonzero by the zero product property. Thus $\frac{m}{n} + \frac{n}{m}$ is a rational number.

Zero Product Property: If any two nonzero real numbers are multiplied, the product is nonzero.

26

Example, cont.

True or false? A product of any two rational numbers is a rational number.

(∀ real numbers x and y, if x and y are rational then xy is rational.)

Solution: This is true.

Proof: Suppose x and y are any rational numbers.

[We must show that xy is rational.]

By definition of rational, $x = a/b$ and $y = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Then

$$xy = \frac{a}{b} \cdot \frac{c}{d} \quad \text{by substitution}$$

$$= \frac{ac}{bd} \quad \text{by algebra.}$$

But ac and bd are integers bcoz they are products of integers, and $bd \neq 0$ by the zero product property.

Thus xy is a ratio of integers with a nonzero denominator, and hence xy is rational by definition of rational.

Final Example! (of this group)

True or false? A quotient of any two rational numbers is a rational number.

Solution: This is false.

Counterexample: Consider the numbers 1 and 0. Both are rational because $1 = \frac{1}{1}$ and $0 = \frac{0}{1}$. Then $\frac{1}{0}$ is a quotient of two rational numbers, but it is not even a real number. So it is not a rational number.

28

Theorem 4.2.2

The sum of any two rational numbers is rational.

Proof:

Suppose r and s are rational numbers. *[We must show that $r + s$ is rational.]* Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Thus

$$r + s = \frac{a}{b} + \frac{c}{d} \quad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \quad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers. Also $q \neq 0$ by the zero product property. Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number. *[This is what was to be shown.]*

29

4.3

Direct Proof and Counterexample III: Divisibility

Divisibility

Definition: Given any integers n and d,

d **is a factor of** n
d **is a divisor of** n
d **divides** n
$d \mid n$
n **is divisible by** d
n **is a multiple of** d

$\Leftrightarrow$

n equals d times some integer
$\exists$ an integer k so that $n = d \times k$

These are different ways to describe the relationship

This is the definition

Note: n, d, and k are integers

31

Examples

1. Is 18 divisible by 6?

Answer: Yes, 18 = 6·3.

2. Does 3 divide 15?

Answer: Yes, 15 = 3·5.

3. Does 5 | 30?

Answer: Yes, 30 = 5·6.

4. Is 32 a multiple of 8?

Answer: Yes, 32 = 8·4.

2. Does 12 divide 0?

Answer: Yes, 0 = 12.0.

5. If *d* is any integer, does *d* divide 0?

Answer: Yes, 0 = *d*·0.

32

Examples, continued

Theorm: If a and b are positive integers and $a \mid b$, then $a \leq b$.

6. *Consequence* : Which integers divide 1?

Answer: Only 1 and -1.

7. If m and n are integers, is $10m + 25n$ divisible by 5?

Answer: Yes. $10m + 25n = 5(2m + 5n)$ and $2m + 5n$ is an integer bcz it is a sum of products of integers.

33

Notes

Note: $d \mid n \Leftrightarrow \exists$ an integer k such that $n = dk$.

Thus: $d \nmid n \Leftrightarrow \forall$ integers k, $n \neq dk$

$\Leftrightarrow$ $d \neq 0$ and n/d is not an integer

Example: Does $5 \mid 12$?

Solution: No: 12/5 is not an integer.

- 5/12 is a **number**: (five-twelfths) $5/12 \cong 0.4167$
- $5 \mid 12$ is a **sentence**: "5 divides 12."

34

Transitivity of Divisibility Theorem

The “**transitivity of divisibility**” theorem

∀ integers *a*, *b*, and *c*, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Example

Prove: ∀ integers *a*, *b*, and *c*, if *a* | *b* and *b* | *c*, then *a* | *c*.

(Note: The full proof is on page 174)

Starting point for this proof:

Suppose a, b, and c are [pbac – particular but arbitrarily chosen integers] such that a | b and b | c.

Ending point (what must be shown): *a* | *c*.

Since a|b and b|c *then b= as and c = bt for some integers s and t.*

*T*o show that a|c, we need to show that c = a·(some integer)

We know that c=bt, then we can substitute the expression for b into the equation for c. Thus, c=ast. s and t are integers, so st is an integer. Let st=k, then c=ka. Therefore a|c by definition.

Disproof: To disprove a statement means to show that the statement is false.

Prove or Disprove the following statement:

For all integers a and b, if $a \mid b^2$ then $a \mid b$.

What do you have to do to show that this statement is false?

Answer: Show that the negation of the statement is true.

The negation is:

There exist integers a and b such that a divides b^2 and a does not divide b.

Think about the negation when you look for counterexample.

Counterexample: Let $a = 4$ and $b = 6$. Then $b^2 = 36$, and a divides b^2 because $36 = 4 \cdot 9$. But 4 does not divide 6 because $6/4 = 1½$, which is not an integer.

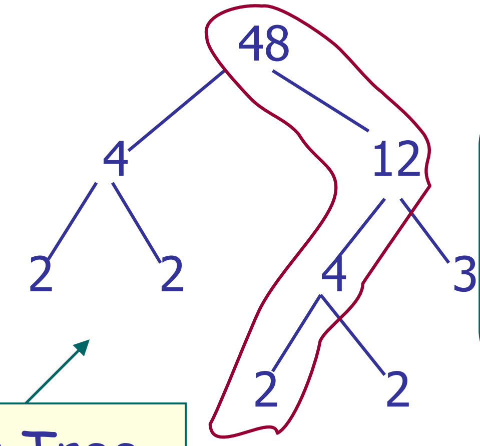
Prime and Composite Numbers

Definition: An integer n is **prime** if, and only if, $n > 1$ and the only positive factors of n are 1 and n.

An integer n is **composite** if, and only if, it is not prime; i.e., $n > 1$ and $n = rs$ for some positive integers r and s where neither r nor s is 1.

Note: An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some positive integers r and s where $1 < r < n$ and $1 < s < n$.

Theorem (Divisibility by a Prime): Given any integer $n > 1$, there is a prime number p so that $p \mid n$.



Factor Tree

Tracing along any other branch would also lead to a prime.

Unique Factorization Theorem

Unique Factorization Theorem for the Integers: Given any integer $n > 1$, either n is prime or n can be written as a product of prime numbers in a way that is unique, except, possibly, for the order in which the numbers are written.

Ex. 1: $500 = 5 \cdot 100 = 5 \cdot 25 \cdot 4 = 5 \cdot 5 \cdot 5 \cdot 2 \cdot 2 = 2 \cdot 5 \cdot 5 \cdot 2 \cdot 5$

$= 2^2 5^3$ ← standard factored form

Ex. 2: $500^3 = (2^2 5^3)^3 = (2^2 5^3)(2^2 5^3)(2^2 5^3) = 2^6 5^9$

39

The standard factored form

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right

Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example

Write 3,300 in standard factored form.

First find all the factors of 3,300. Then

write them in ascending order:

$$3{,}300 = 100 \,.\, 33$$
$$= 4 \,.\, 25 \,.\, 3 \,.\, 11$$
$$= 2 \,.\, 2 \,.\, 5 \,.\, 5 \,.\, 3 \,.\, 11$$
$$= 2^2 \,.\, 3^1 \cdot 5^2 \,.\, 11^1.$$

$$860 = 10 \,.\, 86$$
$$= 2 \,.\, 5 \,.\, 43.2$$
$$= 2^2 \,.\, 5^1 \cdot 43^1.$$

Using Unique Factorization to Solve a Problem

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10$$

Does $17 \mid m$?

Solution:

- Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization of integers theorem).
- But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large).
- Hence 17 must occur as one of the prime factors of *m*, and so $17 \mid m$.

4.4

Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Quotient-Remainder Theorem

For all integers n and positive integers d, there exist unique integers q and r such that

$$n = dq + r \quad \textbf{and} \quad 0 \leq r < d.$$

Quotient-Remainder Theorem

Suppose 14 objects are divided into groups of 3?

x x x   x x x   x x x   x x x   x x

The result is 4 groups of 3 each with 2 left over.

We write

$$\begin{array}{r|l} & \underline{\;4\;} \leftarrow \textit{quotient} \\ 3 & 14 \\ & \underline{12} \\ & \;\;2 \leftarrow \textit{remainder} \end{array}$$

or, $\frac{14}{3} = 4 + \frac{2}{3}$

or, **better**, $14 = 3.4 + 2$

Note: The number left over has to be less than the size of the groups.

45

Quotient-Remainder Theorem

Notice that:

$$\begin{array}{r|l} & \ \ 2 \leftarrow \text{quotient} \\ 4 & \ 11 \\ & \ \ \underline{8} \\ & \ \ 3 \leftarrow \text{remainder} \end{array}$$

$$11 = 2 \cdot 4 + 3.$$

$\uparrow$ 2 groups of 4 $\uparrow$ 3 left over

Examples:

$54 = 4 \cdot 13 + 2$ $q = 13$ $r = 2$

$-54 = 4 \cdot (-14) + 2$ $q = -14$ $r = 2$

$54 = 70 \cdot 0 + 54$ $q = 0$ $r = 54$

Consequences

1. Apply the quotient-remainder theorem with $d = 2$. The result is that there exist unique integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

What are possible values for r?

Answer: $r = 0$ or $r = 1$

Consequence: No matter what integer you start with, it either equals

$$2q + 0\ (= 2q) \quad \text{or} \quad 2q + 1 \quad \text{for some integer } q.$$

even | odd

So: Every integer is either even or odd.

Exercises

Ex: Find q and r if $n = 23$ and $d = 6$.

Answer: $q = 3$ and $r = 5$

Ex: Find q and r if $n = -23$ and $d = 6$.

Answer: $q = -4$ and $r = 1$

Exercises

2. *Similarly*: Given any integer n, apply the quotient-remainder theorem with $d = 3$. The result is that there exist unique integers q and r such that

$$n = 3q + r \quad \text{and} \quad 0 \leq r < 3.$$

What are possible values for r?

Answer: $r = 0$ or $r = 1$ or $r = 2$

Consequence: Given any integer n, there is an integer q so that n can be written in one of the following three forms:

$$n = 3q, \quad n = 3q + 1, \quad n = 3q + 2.$$

3. Similarly for other values of n.

49

div and mod

- **Definition**

Given an integer n and a positive integer d,

$$\begin{aligned} \boldsymbol{n \ div \ d} &= \text{the integer quotient obtained when } n \text{ is divided by } d \text{, and} \\ \boldsymbol{n \ mod \ d} &= \text{the nonnegative integer remainder obtained when } n \text{ is divided by } d. \end{aligned}$$

Symbolically, if n and d are integers and $d > 0$, then

$$n \ div \ d = q \quad \text{and} \quad n \ mod \ d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \leq r < d$.

Examples:

$$32 \text{ div } 9 = 3$$

$$32 \text{ mod } 9 = 5$$

Application of div and mod

Solving a Problem about mod

Suppose m is an integer. If m mod 11 = 6, what is $4m$ mod 11?

$$m = 11q + 6.$$

$$4m = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2.$$

$$4m\ mod\ 11 = 2.$$

Application of div and mod

- Suppose today is Tuesday, what is the day of the week after one year from today.
- Assume not leap.
- Week=7 days
- Year =365 days
- 365 div 7 = 52 365 mod 7 = 1
- 365=7*52+1
- Therefore the day will be Wednsday.

Method of Proof by Division into Cases

Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or ... or A_n, then C," prove all of the following:

$$\begin{aligned}&\text{If } A_1, \text{ then } C,\\&\text{If } A_2, \text{ then } C,\\&\quad\vdots\\&\text{If } A_n, \text{ then } C.\end{aligned}$$

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Any two consecutive integers have opposite parity.

- Proof: Suppose that two *pbac* consecutive integers are given; **m** and **m+1**.
- [We must show that one of **m** and **m+1** is even and that the other is odd.]
- We break the proof into two cases depending on whether m is even or odd.
- Case1(**m** is even): m =2k for some integer k, and so m+1=2k+1, which is odd [by definition of odd]. Hence in this case, one of m and m+1 is even and the other is odd.

Any two consecutive integers have opposite parity.

- **Case 2** (***m is odd***): In this case, m =2k+1 for some integer k, and so
- m+1= (2k+1)+1=2k+2=2(k+1).
- Let c=k+1 is an integer because it is a sum of two integers. m+1=2c
- Therefore, m+1 equals twice some integer, and thus m+1 is even. Hence in this case also, one of m and m+1 is even and the other is odd.
- It follows that regardless of which case actually occurs for the particular m and m+1 that are chosen, one of m and m+1 is even and the other is odd. [This is what was to be shown.]

Recall: Representing Integers using the quotient-remainder theorem

Let d = 4 (Integers Modulo 4)

There exist an integer quotient q and a remainder r such that

$$n = 4q + r \quad \text{and} \quad 0 \leq r < 4.$$

Thus, any integer can be represented as:

$n=4q$ or $n=4q+1$ or $n=4q+2$ or $n=4q+3$

Example

Theorem 4.4.3

The square of any odd integer has the form $8m + 1$ for some integer m.

Proof: $\forall n \in \text{Odd}, \exists\, m \in \mathbf{Z}\ .\ n^2 = 8m + 1.$

Hint: any odd integer can be 4q+1 or 4q+3.

Case 1 (n=4q+1):

$n^2 = 8m + 1 = (4q+1)^2 = 16q^2 + 8q + 1 = 8(\underline{2q^2 + q}) + 1$
Let $(2q^2 + q)$ be an integer m, thus $n^2 = 8m + 1$

Case 2 (4q+3):

$n^2 = 8m + 1 = (4q+3)^2 = 16q^2 + 24q + 8 + 1$
$= 8(\underline{2q^2 + 3q+1}) + 1$
Let $(2q^2 + 3q+1)$ be an integer m, thus $n^2 = 8m + 1$

Overview, cont.

What is the **quotient-remainder** theorem?

For all integers n and positive integers d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \le r < d.$$

$$43 = 8 * 5 + 3$$

What is the **"transitivity of divisibility"** theorem?

$\forall$ integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

58

Disproving a Universal Statement

Most Common Method: Find a counterexample!

Example

Is the following statement true or false? Explain.

$\forall$ real numbers x, if $x^2 > 25$ then $x > 5$.

Solution: The statement is false.

Counterexample:

Let $x = -6$. Then $x^2 = (-6)^2 = 36$, and $36 > -6$ but $-6 \not> 5$.

So (for this x), $x^2 > 25$ and $x \not> 5$.

59

Disproof by Counterexample

$\forall a,b \in \mathbf{R} \;.\; a^2 = b^2 \rightarrow a = b.$

Counterexample:

Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$,
and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.