جامعة بيرزيت
BIRZEIT UNIVERSITY

FACULTY OF ENGINEERING AND TECHNOLOGY

COMPUTER SCIENCE DEPARTMENT

COMP233
Discrete Mathematics

CHAPTER 4

Elementary Number Theory and Methods of Proof

Number Theory

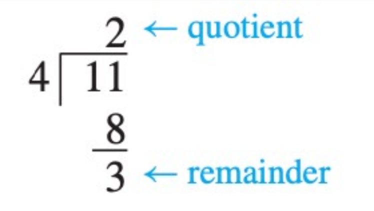
- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Number Theory

- Direct Proof and Counterexamples
- Rational Numbers
- Divisibility
- Division into Cases and the Quotient-Remainder Theorem

Introduction

- When you divide 11 by 4, you get a quotient of 2 and a remainder of 3.



- Another way to say this is that 11 equals 2 groups of 4 with 3 left over:

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

The Quotient-Remainder Theorem

- Given any integer n and positive integer d, there exist unique integers q and r such that

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

- If n is positive, the quotient-remainder theorem can be illustrated on the number line as follows:

Examples

- For each of the following values of n and d, find integers q and r such that

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

1. $n = 54, \ d = 4$

   $54 = 4 \cdot 13 + 2$; *hence* $q = 13$ *and* $r = 2$.

2. $n = -54, \ d = 4$

   $-54 = 4 \cdot (-14) + 2$; *hence* $q = -14$ *and* $r = 2$.

3. $n = 54, \ d = 70$

   $54 = 70 \cdot 0 + 54$; *hence* $q = 0$ *and* $r = 54$.

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

div and mod

- Given an integer n and a positive integer d,
  - $\boldsymbol{n\ div\ d}$ = *the integer quotient obtained when n is divided by d, and*
  - $\boldsymbol{n\ mod\ d}$ = *the nonnegative integer remainder obtained when n is divided by d.*

- Symbolically, if n and d are integers and $d > 0$, then
  $n\ div\ d = q$ and $n\ mod\ d = r \leftrightarrow n = dq + r$

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

div and mod

- $n \bmod d$ equals one of the integers from 0 through $d - 1$ (since the remainder of the division of n by d must be one of these integers).

- A necessary and sufficient condition for an integer n to be divisible by an integer d is that $n \bmod d = 0$.

Calculating div and mod

- You can also use a calculator to compute values of div and mod:

- To compute $n\ div\ d$ for a nonnegative integer n and a positive integer d, you just divide n by d and ignore the part of the answer to the right of the decimal point.
- To find $n\ mod\ d$, you can use the fact that

$$\text{if } n = dq + r, \text{ then } r = n - dq$$

Thus

$$n = d \cdot (n\ div\ d) + n\ mod\ d$$

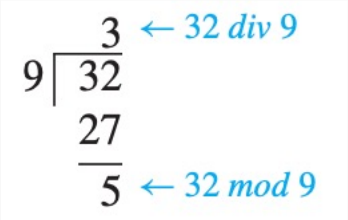
and so

$$n\ mod\ d = n - d \cdot (n\ div\ d)$$

Computing div and mod

- Compute $32\ div\ 9$ and $32\ mod\ 9$ by hand.

- Performing the division by hand gives the following results:



Computing div and mod – cont.

- Compute $32\ div\ 9$ and $32\ mod\ 9$ with a calculator.

- If you use a four-function calculator to divide 32 by 9, you obtain an expression like 3.555555556.

- Discarding the fractional part gives $32\ div\ 9\ =\ 3$.

- And so,

$$32\ mod\ 9\ =\ 32\ -\ 9 \cdot (32\ div\ 9)\ =\ 32\ -\ 27\ =\ 5$$

Computing the Day of the Week

- Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

- There are 365 days in a year that is not a leap year, and each week has 7 days.
- $365\ div\ 7 = 52$ and $365\ mod\ 7 = 1$

- Thus 52 weeks, or 364 days, from today will be a Tuesday
- 365 days from today will be 1 day later, namely Wednesday.

Solving a Problem about mod

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

- Because $m \ mod \ 11 = 6$, the remainder obtained when m is divided by 11 is 6.
- This means that there is some integer q so that
$$m = 11q + 6$$
- Thus $4m = 44q + 24$
$$= 44q + 22 + 2$$
$$= 11(4q + 2) + 2$$
- Since $4q + 2$ is an integer (because products and sums of integers are integers) and since $2 < 11$, the remainder obtained when $4m$ is divided by 11 is 2. Therefore,
$$4m \ mod \ 11 = 2$$

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

Representations of Integers

Any integer must be either odd or even

- We have previously stated that this statement is true. However, at the time when we learned how to represent even and odd integers, we did not know enough to prove it.

- Now we do.

Representations of Integers

- Let n be any integer, and consider what happens when n is divided by 2.
- By the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

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

- But the only integers that satisfy $0 \leq r < 2$ are $r = 0$ and $r = 1$.
- It follows that given any integer n, there exists an integer q with

$$n = 2q + 0 \qquad \text{or} \qquad n = 2q + 1.$$

- In the case that $n = 2q + 0 = 2q$, n is even. In the case that $n = 2q + 1$, n is odd.
- Hence n is either even or odd, and, because of the uniqueness of q and r, n cannot be both even and odd.

Parity

- The **parity** of an integer is its attribute of being even or odd.

- Thus, it can be said that 6 and 14 have the same parity, since both are even.
- And 7 and 15 have the same parity, since both are odd.
- Whereas 7 and 14 have opposite parity, since 7 is odd and 14 is even.

- The **parity property** is the fact that an integer is either even or odd.

Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one is even, and the other is odd.

- Suppose that two particular but arbitrarily chosen consecutive integers are given; call them m and $m + 1$.
- We must show that one of m and $m + 1$ is even and that the other is odd.

- By the parity property, either m is even, or m is odd. We break the proof into two cases depending on whether m is even or odd.

Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one is even, and the other is odd.

- **Case 1: $\boldsymbol{m}$ is even:**

  In this case, $m = 2k$ 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.

Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one is even, and the other is odd.

- **Case 2: $\boldsymbol{m}$ is odd:**

  In this case, $m = 2k + 1$ for some integer k,

  and so, $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$.

  But $k + 1$ is an integer because it is a sum of two integers.

  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.

Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one 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.
- And this is what was to be shown.

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

Proof by Division into Cases

- The division into cases in a proof is like the transfer of control for an **if-then-else** statement in a computer program.

- If m is even, control transfers to case 1; if not, control transfers to case 2.
- For any given integer, only one of the cases will apply.
- You must consider both cases, however, to obtain a proof that is valid for an arbitrarily given integer whether even or not.

- There are times when division into more than two cases is called for.

Method of Proof by Division into Cases

- Suppose that at some stage of developing a proof, you know that a statement of the form

$$A_1 \text{ or } A_2 \text{ or } A_3 \text{ or } \ldots \text{ or } A_n$$

is true, and suppose you want to deduce a conclusion C.

- To prove a statement of the form "If A_1 or A_2 or A_3 or … or A_n, then C," prove all of the following:

If A_1, then C,

If A_2, then C,

…

If A_n, then C.

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

Representations of Integers Modulo 4

- Show that any integer can be written in one of the four forms

$$n = 4q \text{ or } n = 4q + 1 \text{ or } n = 4q + 2 \text{ or } n = 4q + 3$$

for some integer q.

- Given any integer n, apply the quotient-remainder theorem to n with $d = 4$.
- This implies that there exist an integer quotient q and a remainder r such that

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

- But the only nonnegative remainders *r* that are less than 4 are 0, 1, 2, and 3.
- Hence

$$n = 4q \text{ or } n = 4q + 1 \text{ or } n = 4q + 2 \text{ or } n = 4q + 3$$

for some integer q.

The Square of an Odd Integer

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

- Suppose n is a particular but arbitrarily chosen odd integer.
- By the quotient-remainder theorem, n can be written in one of the forms

  $$n = 4q \text{ or } n = 4q + 1 \text{ or } n = 4q + 2 \text{ or } n = 4q + 3$$

  for some integer q.
- Since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

  $$4q + 1 \text{ or } 4q + 3$$

  for some integer q.

The Square of an Odd Integer

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

- **Case 1 ($\boldsymbol{n = 4q + 1}$ for some integer $\boldsymbol{q}$):**

Since $n = 4q + 1$,

$n^2 = (4q + 1)2$ by substitution

$= (4q + 1)(4q + 1)$ by definition of square

$= 16q^2 + 8q + 1$

$= 8(2q^2 + q) + 1$ by the laws of algebra

Let $m = 2q^2 + q$. Then m is an integer since the sums and products of integers are integers.

Thus, substituting,

$n^2 = 8m + 1$ where m is an integer.

The Square of an Odd Integer

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

- **Case 2 ($\boldsymbol{n = 4q + 3}$ for some integer $\boldsymbol{q}$):**

Since $n = 4q + 3$,

$n^2 = (4q + 3)^2$ by substitution

$= (4q + 3)(4q + 3)$ by definition of square

$= 16q^2 + 24q + 9$

$= 16q^2 + 24q + (8 + 1)$

$= 8(2q^2 + 3q + 1) + 1$ by the laws of algebra

Let $m = 2q^2 + 3q + 1$. Then m is an integer since the sums and products of integers are integers.

Thus, substituting,

$n^2 = 8m + 1$ where m is an integer.

The Square of an Odd Integer

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

- Cases 1 and 2 show that given any odd integer, whether of the form

  $4q + 1$ or $4q + 3$,

  $n^2 = 8m + 1$ for some integer m.

- And this is what we needed to show.

Division into Cases and the Quotient-Remainder Theorem

- The Quotient-Remainder Theorem
- div and mod
- Representation of Integers
- Division into Cases
- Absolute Value and the Triangle Inequality

Absolute Value and the Triangle Inequality

- For any real number x, the absolute value of x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & if\ x \geq 0 \\ -x & if\ x < 0 \end{cases}$$

- The ***triangle inequality*** says that the absolute value of the sum of two numbers is less than or equal to the sum of their absolute values.

- To prove the triangle inequality, we need to prove two lemmas first.

Lemmas?

- A **lemma** is a statement that does not have much intrinsic interest but is helpful in deriving other results.

- We will prove the following two lemmas:

  Lemma 1: For all real numbers r, $-|r| \leq r \leq |r|$

  Lemma 2: For all real numbers r, $|-r| = |r|$

Lemma 1: For all real numbers r, $-|r| \leq r \leq |r|$

- Suppose r is any real number. We divide into cases according to whether $r \geq 0$ or $r < 0$.

- **Case 1 ($\boldsymbol{r \geq 0}$):**

  In this case, by definition of absolute value, $|r| = r$.

  Also, since r is positive and $-|r|$ is negative, $-|r| < r$.

  Thus it is true that $-|r| \leq r \leq |r|$.

Lemma 1: For all real numbers r, $-|r| \leq r \leq |r|$

- **Case 2 ($r < 0$):**

  In this case, by definition of absolute value, $|r| = -r$.

  Multiplying both sides by -1 gives that $-|r| = r$.

  Also, since r is negative and $|r|$ is positive, $r < |r|$.

  Thus it is also true in this case that $-|r| \leq r \leq |r|$.

- Hence, in either case,

$$-|r| \leq r \leq |r|$$

- as was to be shown.

Lemma 2: For all real numbers r, $|-r| = |r|$

- Suppose r is any real number.

  if $r > 0$, then $-r < 0$,

  and if $r < 0$, then $-r > 0$.

- Thus,

$$|-r| = \begin{cases} -r & if\ -r > 0 \\ 0 & if\ r = 0 \\ -(-r) & if\ -r < 0 \end{cases}$$

by definition of absolute value

Lemma 2: For all real numbers r, $|-r| = |r|$

- Suppose r is any real number.

  if $r > 0$, then $-r < 0$,

  and if $r < 0$, then $-r > 0$.

- Thus,

$$|-r| = \begin{cases} -r & if\ -r > 0 \\ 0 & if\ r = 0 \\ r & if\ -r < 0 \end{cases}$$

because $-(-r) = r$

Lemma 2: For all real numbers r, $|-r| = |r|$

- Suppose r is any real number.

  if $r > 0$, then $-r < 0$,

  and if $r < 0$, then $-r > 0$.

- Thus,

$$|-r| = \begin{cases} -r & if\ r < 0 \\ 0 & if\ r = 0 \\ r & if - r < 0 \end{cases}$$

because when $-r > 0, r < 0$

Lemma 2: For all real numbers r, $|-r| = |r|$

- Suppose r is any real number.

  if $r > 0$, then $-r < 0$,

  and if $r < 0$, then $-r > 0$.

- Thus,

$$|-r| = \begin{cases} -r & if\ r < 0 \\ 0 & if\ r = 0 \\ r & if r > 0 \end{cases}$$

because when $-r < 0, r > 0$

Lemma 2: For all real numbers r, $|-r| = |r|$

- Suppose r is any real number.

  if $r > 0$, then $-r < 0$,

  and if $r < 0$, then $-r > 0$.

- Thus,

$$|-r| = \begin{cases} r & if\ r \geq 0 \\ -r & if\ r < 0 \end{cases}$$ by reformatting the previous result

$$= |r|$$ by definition of absolute value

The Triangle Inequality

- For all real numbers x and y, $|x + y| \leq |x| + |y|$.

- Suppose x and y, are any real numbers.
- **Case 1 ($\boldsymbol{x + y \geq 0}$):** In this case, $|x + y| = x + y$

  By the first lemma, $x \leq |x|$ and $y \leq |y|$

  Hence, $|x + y| = x + y \leq |x| + |y|$

The Triangle Inequality

- For all real numbers x and y, $|x + y| \leq |x| + |y|$.

- Suppose x and y, are any real numbers.
- **Case 2 ($\boldsymbol{x + y < 0}$):** In this case, $|x + y| = -(x + y) = (-x) + (-y)$

  By the first and second lemmas, $-x \leq |-x| = |x|$ and $-y \leq |-y| = |y|$

  It follows that $|x + y| = (-x) + (-y) \leq |x| + |y|$

- Hence in both cases $|x + y| \leq |x| + |y|$, as was to be shown.