Discrete Mathematics

Chapter 4.4

Direct Proof and Counterexample IV

The Quotient-Remainder Theorem

Hisham Ihshaish - Birzeit University

Based on Susanna S. Epp, Discrete Mathematics with Applications, 4th ed., Section 4.4

Chapter 4.4

Division into cases and the quotient-remainder theorem

In this session:

- **Part 1: The quotient-remainder theorem**
- Part 2: div and mod, and applications
- Part 3: Representing integers using quotient-remainder
- Part 4: Absolute value

Division with a remainder - the idea

From elementary school: when you divide 11 by 4, you get a quotient of 2 and a remainder of 3.

Long division

$$\begin{array}{r} 2 \quad \leftarrow \text{quotient} \\ 4\,)\,11 \\ \underline{\;8\;} \\ 3 \quad \leftarrow \text{remainder} \end{array}$$

Or: 11 equals 2 groups of 4, with 3 left over.

As an equation

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

(quotient = 2, remainder = 3)

The remainder (3) is less than the divisor (4) - if it were not, another group of 4 could be separated off.

In general: given any integer n and any positive divisor d, we can write $n = dq + r$ with $0 \le r < d$.

The quotient-remainder theorem

Theorem 4.4.1 (the quotient-remainder theorem)

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

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

Examples.

$54 = 4 \cdot 13 + 2$	$q = 13$	$r = 2$
$-54 = 4 \cdot (-14) + 2$	$q = -14$	$r = 2$
$54 = 70 \cdot 0 + 54$	$q = 0$	$r = 54$

Notice in the second example: when n is negative, q must be negative enough so that r is still in [0, d).

Chapter 4.4

Division into cases and the quotient-remainder theorem

In this session:

- Part 1: The quotient-remainder theorem
- **Part 2: div and mod, and applications**
- Part 3: Representing integers using quotient-remainder
- Part 4: Absolute value

div and mod

Definition

Given an integer n and a positive integer d,

n div d = the integer quotient when n is divided by d,

n mod d = the non-negative integer remainder when n is divided by d.

Symbolically: $n \text{ div } d = q$ and $n \bmod d = r \iff n = dq + r$, with q, r integers and $0 \le r < d$.

Examples.

32 div 9 = 3 **32 mod 9 = 5**

(because $32 = 9 \cdot 3 + 5$)

In programming languages

C, C++, Java :	/	and	%
Python :	//	and	%
Pascal :	div	and	mod
.NET :	/	and	mod

Warning: in C and Java, the % operator does NOT match "mod" when n is negative - it can return a negative result.

Application 1: day of the week, one year from today

Today is Tuesday. Neither this year nor next year is a leap year. What day of the week is it 1 year from today?

Step 1. How many days in a year (non-leap)?

365 days.

Step 2. How many full weeks fit in 365 days, and how many days are left over?

$365 \text{ div } 7 = 52$ *(52 full weeks)*

$365 \bmod 7 = 1$ *(1 extra day)*

So $365 = 7 \cdot 52 + 1$.

Step 3. Conclusion.

After 364 days (52 full weeks) the day is again Tuesday.

After 365 days the day is **Wednesday.**

Application 2: Valentine's day computation

Today is Thursday, 16 October 2014. Which day of the week is Valentine's day - 14 February 2015?

Step 1. Count the days from 16 Oct 2014 to 14 Feb 2015.

Remaining days in October (16 → 31):	**15**
Days in November:	**30**
Days in December:	**31**
Days in January:	**31**
Days in February (1 → 14):	**14**
Total:	**121 days**

Step 2. $121 \text{ div } 7 = 17, \quad 121 \bmod 7 = 2.$ *So 121 days = 17 weeks + 2 days.*

Step 3. After 17 full weeks the day is still Thursday. Adding 2 more days: **Saturday.**

Application 3: solving a problem with mod

Suppose m is an integer with m mod 11 = 6. What is 4m mod 11 ?

Solution.

Translate the hypothesis: $m \bmod 11 = 6 \iff m = 11q + 6$ for some integer q.

Multiply by 4: $4m = 4(11q + 6) = 44q + 24$

Rewrite 24 as a multiple of 11 plus a remainder: $24 = 22 + 2 = 11 \cdot 2 + 2$

Substitute: $4m = 44q + 22 + 2 = 11(4q + 2) + 2$

Note 4q + 2 is an integer, and $0 \le 2 < 11$.

Therefore $\mathbf{4m \bmod 11 = 2.}$ ■

Chapter 4.4

Division into cases and the quotient-remainder theorem

In this session:

- Part 1: The quotient-remainder theorem
- Part 2: div and mod, and applications
- **Part 3: Representing integers using quotient-remainder**
- Part 4: Absolute value

Representing integers - parity

Apply the quotient-remainder theorem with d = 2.

For every integer n there exist unique integers q and r with

$$n = 2q + r \quad \text{with} \quad 0 \le r < 2.$$

The only non-negative integers less than 2 are 0 and 1, so r = 0 or r = 1:

If r = 0:

$$n = 2q$$

n is EVEN.

(Arabic: زوجي)

If r = 1:

$$n = 2q + 1$$

n is ODD.

(Arabic: فردي)

Parity property: every integer is either even or odd - but not both.

Theorem 4.4.2 - parity of consecutive integers

Any two consecutive integers have opposite parity - one is even and the other is odd.

Proof (by division into cases).

Suppose m and m + 1 are two consecutive integers. By the parity property, m is even or m is odd.

Case 1. m is even.

$m = 2k$ for some integer k.

Then $m + 1 = 2k + 1$,

which is odd (by definition of odd).

So m even, m+1 odd. ✓

Case 2. m is odd.

$m = 2k + 1$ for some integer k.

Then $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$,

and k + 1 is an integer; so m + 1 is even.

So m odd, m+1 even. ✓

In either case, one of m and m + 1 is even and the other is odd. ▪

The “divide into cases” proof method

Generalising what we just did:

Method of proof by division into cases

To prove a statement of the form

$$\text{“If } A_1 \text{ or } A_2 \text{ or } \ldots \text{ or } A_n, \text{ then } C\text{”},$$

prove all of the following:

$$\text{If } A_1, \text{ then } C. \qquad \text{If } A_2, \text{ then } C. \qquad \ldots \qquad \text{If } A_n, \text{ then } C.$$

Then C is true regardless of which A_i happens to be the case.

Where do the cases come from?

Most often: the quotient-remainder theorem. With d = 2, d = 3, d = 4 ... we get 2, 3, 4 cases for any integer.

Cases must be EXHAUSTIVE (cover every possibility).

Representations - integers modulo 4

Apply the quotient-remainder theorem with d = 4.

For every integer n there exist unique integers q and r with

$$n = 4q + r \quad \text{with} \quad 0 \le r < 4.$$

So $r \in \{0, 1, 2, 3\}$, and every integer can be written in exactly one of these four forms:

$n = 4q$ *(divisible by 4)*	$n = 4q + 1$ *(odd, leaves 1)*
$n = 4q + 2$ *(even, leaves 2)*	$n = 4q + 3$ *(odd, leaves 3)*

Note. Cases 4q and 4q+2 are the EVEN integers; cases 4q+1 and 4q+3 are the ODD integers.

Theorem 4.4.3 - square of any odd integer = 8m + 1

For every odd integer n, there exists an integer m such that $n^2 = 8m + 1$.

Proof (by division into cases on n mod 4).

Any odd integer n has the form $n = 4q + 1$ or $n = 4q + 3$ for some integer q.

Case 1. $n = 4q + 1$.

$$n^2 = (4q + 1)^2$$
$$= 16q^2 + 8q + 1$$
$$= \mathbf{8(2q^2 + q) + 1}$$

Let $m = 2q^2 + q$ (an integer).

Then $n^2 = 8m + 1$. ✓

Case 2. $n = 4q + 3$.

$$n^2 = (4q + 3)^2$$
$$= 16q^2 + 24q + 9$$
$$= 16q^2 + 24q + 8 + 1$$
$$= \mathbf{8(2q^2 + 3q + 1) + 1}$$

Let $m = 2q^2 + 3q + 1$ (an integer).

Then $n^2 = 8m + 1$. ✓

Congruence modulo

Definition

For integers A, B and a positive integer C,

$$A \equiv B \pmod{C} \quad \Leftrightarrow \quad C \mid (A - B).$$

Read: "A is congruent to B modulo C". (Arabic: توافق بمقياس)

Example 1.

$26 \equiv 11 \pmod{5}$

because $5 \mid (26 - 11) = 5 \mid 15$. ✓

Example 2.

$a \equiv 3 \pmod{2}$

means $2 \mid (a - 3)$, i.e. a is odd.

Quick check. Given $x \equiv -2 \pmod{2}$, which of these are valid x?

26	✓	−49	✗	−44	✓	−23	✗
$2 \mid (26-(-2)) = 2 \mid 28$ ✓		$2 \nmid (-49-(-2)) = -47$ ✗		$2 \mid (-44-(-2)) = -42$ ✓		$2 \nmid (-23-(-2)) = -21$ ✗	

Chapter 4.4

Division into cases and the quotient-remainder theorem

In this session:

- Part 1: The quotient-remainder theorem
- Part 2: div and mod, and applications
- Part 3: Representing integers using quotient-remainder
- **Part 4: Absolute value**

Absolute value

Definition

For any real number x,

$$|x| = x \quad \text{if } x \geq 0$$

$$|x| = -x \quad \text{if } x < 0$$

Examples: $|2| = 2$, $|-2| = 2$, $|0| = 0$.

Lemma 4.4.4

For all real numbers r,

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

(Both bounds are tight.)

Proof of Lemma 4.4.4 (by cases on the sign of r):

Case 1. $r \geq 0$.

$|r| = r$, so $r \leq |r|$.

$|r| \geq 0 \Rightarrow -|r| \leq 0 \leq r$.

Hence $-|r| \leq r \leq |r|$. ✓

Case 2. $r < 0$.

$|r| = -r$, so $-|r| = r$.

Also $r < 0 < |r|$, so $r < |r|$.

Hence $-|r| \leq r \leq |r|$. ✓

Theorem 4.4.6 - the triangle inequality

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

Proof (by division into cases on the sign of x + y).

Case 1. $x + y \ge 0$.

$|x + y| = x + y$ (by definition).

By Lemma 4.4.4:

$x \le |x|$ and $y \le |y|$.

Add the inequalities:

$x + y \le |x| + |y|$.

Therefore: $|x + y| \le |x| + |y|$. ✓

Case 2. $x + y < 0$.

$|x + y| = -(x + y) = (-x) + (-y)$.

By Lemmas 4.4.4 and 4.4.5:

$-x \le |-x| = |x|$, $-y \le |-y| = |y|$.

Add the inequalities:

$(-x) + (-y) \le |x| + |y|$.

Therefore: $|x + y| \le |x| + |y|$. ✓

In both cases $|x + y| \le |x| + |y|$. ■

Summary - what we covered

Quotient-remainder theorem

- $n = dq + r,\ 0 \le r < d$ - unique q, r
- Foundation of div, mod, modular arithmetic

div and mod

- n div d = q, n mod d = r
- Day-of-the-week, m mod 11 problems
- C/Java's % can return negatives

Representations and proofs

- d = 2: parity (even / odd)
- d = 4: 4q, 4q+1, 4q+2, 4q+3
- T 4.4.2 (consecutive opposite parity)
- T 4.4.3 (odd squared = 8m + 1)

Other tools

- Division-into-cases proof method
- Congruence: $A \equiv B \pmod{C} \Leftrightarrow C \mid (A-B)$
- $|x|$, Lemma 4.4.4, triangle inequality