Math 325K - Lecture 9
Section 4.4 & 4.5

Bo Lin

September 27th, 2018

Outline

- Quotients and remainders.
- Proof by division into cases.
- Proof by contradiction and contraposition.

Definition

As we have seen, if we divide one integer by another one, the result is not always an integer.

Definition

As we have seen, if we divide one integer by another one, the result is not always an integer.

Theorem (Quotient-remainder Theorem)

Given any integer n and positive integer d, there exists a unique pair of integers q and r such that

$$n = dq + r$$

and $0 \leq r < d$.

Definition

As we have seen, if we divide one integer by another one, the result is not always an integer.

Theorem (Quotient-remainder Theorem)

Given any integer n and positive integer d, there exists a unique pair of integers q and r such that

$$n = dq + r$$

and $0 \leq r < d$.

Definition

The unique q above is called the **quotient** *of the division and the unique r above is called the* **remainder** *of the division.*

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n and d:

(a) $n = 20$ *and* $d = 7$;
(b) $n = -8$ *and* $d = 3$;
(c) $n = 4$ *and* $d = 11$.

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n *and* d*:*

(a) $n = 20$ *and* $d = 7$;
(b) $n = -8$ *and* $d = 3$;
(c) $n = 4$ *and* $d = 11$.

Solution

(a) $20 = 7 \cdot 2 + 6$ *and* $0 \leq 6 < 7$, *so* $q = 2$ *and* $r = 6$.

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n and d:

- (a) $n = 20$ *and* $d = 7$;
- (b) $n = -8$ *and* $d = 3$;
- (c) $n = 4$ *and* $d = 11$.

Solution

(a) $20 = 7 \cdot 2 + 6$ *and* $0 \leq 6 < 7$, *so* $q = 2$ *and* $r = 6$.
(b) $-8 = 3 \cdot (-3) + 1$ *and* $0 \leq 1 < 3$, *so* $q = -3$ *and* $r = 1$.

Example: find the quotients and remainders

Example

Find the quotients and remainders for the following pairs of n *and* d*:*

- (a) $n = 20$ *and* $d = 7$;
- (b) $n = -8$ *and* $d = 3$;
- (c) $n = 4$ *and* $d = 11$.

Solution

(a) $20 = 7 \cdot 2 + 6$ *and* $0 \leq 6 < 7$, *so* $q = 2$ *and* $r = 6$.
(b) $-8 = 3 \cdot (-3) + 1$ *and* $0 \leq 1 < 3$, *so* $q = -3$ *and* $r = 1$.
(c) $4 = 11 \cdot 0 + 4$ *and* $0 \leq 4 < 11$, *so* $q = 0$ *and* $r = 4$.

div and mod

Definition

Given any integer n and positive integer d, n div d is the quotient of n divided by d, and n mod d is the remainder of n divided by d.

div and mod

Definition

Given any integer n and positive integer d, n div d is the quotient of n divided by d, and n mod d is the remainder of n divided by d.

Remark

Both n div d and n mod d are uniquely determined and they are always integers. In addition, the latter is always between 0 and $d-1$.

Quantified versions of div and mod

Proposition

For integer n, r and positive integer d with $0 \leq r \leq d-1$,

$$n \textit{ mod } d = r \Leftrightarrow \exists q \in \mathbb{Z} \textit{ such that } n = dq + r.$$

Quantified versions of div and mod

Proposition

For integer n, r and positive integer d with $0 \leq r \leq d - 1$,

$$n \text{ mod } d = r \Leftrightarrow \exists q \in \mathbb{Z} \text{ such that } n = dq + r.$$

Proposition

For integer n, q and positive integer d,

$$n \text{ div } d = q \Leftrightarrow \exists r \in \mathbb{Z} \text{ such that } n = dq + r \wedge 0 \leq r \wedge r \leq d - 1.$$

Divided by 2

Proposition

An integer n is even if and only if the remainder of n divided by 2 is 0. An integer n is odd if and only if the remainder of n divided by 2 is 1.

Divided by 2

Proposition

An integer n is even if and only if the remainder of n divided by 2 is 0. An integer n is odd if and only if the remainder of n divided by 2 is 1.

Proof.

It follows from the definition of even and odd numbers, and the one of remainders. □

The parity property

Now we introduce some results that can be justified by division into cases.

Theorem (The parity property)

Every integer n is either even or odd.

The parity property

Now we introduce some results that can be justified by division into cases.

Theorem (The parity property)

Every integer n is either even or odd.

Proof.

By the Quotient-remainder Theorem, $n = 2 \cdot (n \text{ div } 2) + n \bmod 2$. Since $0 \leq n \bmod 2 < 2$ and it is an integer, $n \bmod 2$ is either 0 or 1. By definition, if it is 0, then n is even; if it is 1, then n is odd. So n is either even or odd. □

The parity of consecutive integers

Theorem

Any two consecutive integers have opposite parity.

The parity of consecutive integers

Theorem

Any two consecutive integers have opposite parity.

Proof.

Let n and $n+1$ be an arbitrary pair of consecutive integers. By the parity property, n is either even or odd. If n is even, then there is an integer k such that $n = 2k$. So $n+1 = 2k+1$ is odd and $n, n+1$ have opposite parity. if n is odd, then there is an integer k such that $n = 2k+1$. So $n+1 = 2k+2 = 2 \cdot (k+1)$ is even, and $n, n+1$ have opposite parity too. Therefore $n, n+1$ always have opposite parity. □

Square of odd integers divided by 8

Proposition

For any odd integer n, *we have* n^2 *mod* $8 = 1$.

Square of odd integers divided by 8

Proposition

For any odd integer n, we have n^2 mod $8 = 1$.

Proof.

Let n be an arbitrary odd integer. By definition, there is an integer k such that $n = 2k + 1$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Since k and $k+1$ are consecutive integers, by the previous theorem, either of them is even, so is their product. There is an integer l such that $k(k+1) = 2l$. Then

$$n^2 = 4k(k+1) + 1 = 8l + 1.$$

By the uniqueness of remainder, n^2 mod $8 = 1$. □

Absolute value

Definition

The **absolute value** *of a real number* x*, denoted by* $|x|$*, is defined as follows:*

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

Absolute value

Definition

The **absolute value** *of a real number* x*, denoted by* $|x|$*, is defined as follows:*

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

Proposition

For $x \in \mathbb{R}$*, we have* $|-x| = |x|$ *and* $|x| \geq x, |x| \geq -x$*.*

Absolute value

Definition

The **absolute value** *of a real number* x*, denoted by* $|x|$*, is defined as follows:*

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

Proposition

For $x \in \mathbb{R}$*, we have* $|-x| = |x|$ *and* $|x| \geq x, |x| \geq -x$*.*

Proof.

Divide into the cases $x > 0, x = 0, x < 0$. □

The triangle inequality

Theorem (Triangle inequality)

For any real numbers x and y, we have that $|x + y| \leq |x| + |y|$.

The triangle inequality

Theorem (Triangle inequality)

For any real numbers x and y, we have that $|x+y| \leq |x| + |y|$.

Proof.

Once again we divide into cases. By definition, $|x+y| = x+y$ or $|x+y| = -(x+y)$. In the first case, we have

$$|x+y| = x+y \leq |x| + y \leq |x| + |y|.$$

In the second case, we have

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

So $|x+y| \leq |x| + |y|$. □

The method of proof by contradiction

Remark

A proof by contradiction consists of the following steps:

- *Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.*
- *Show that this supposition leads logically to a contradiction.*
- *Conclude that the statement to be proved is true.*

The method of proof by contradiction

Remark

A proof by contradiction consists of the following steps:

- *Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true.*
- *Show that this supposition leads logically to a contradiction.*
- *Conclude that the statement to be proved is true.*

Remark

No matter what conclusions we drew during the proof, since in the end we get a contradiction, we cannot claim any result other than the original statement. This is a drawback of proof by contradiction.

Example: no largest integer

Example

Show that there is no largest integer.

Example: no largest integer

Example

Show that there is no largest integer.

Proof.

Suppose there is a largest integer x. Then for any $y \in \mathbb{Z}$, $x \geq y$. Since x is an integer, so is $x + 1$. We take $y = x + 1$, then

$$x \geq y = x + 1,$$

which is a contradiction! Hence our assumption is false and there is no largest integer. □

Sum of rational and irrational numbers

Proposition

The sum of a rational number and an irrational number is irrational.

Sum of rational and irrational numbers

Proposition

The sum of a rational number and an irrational number is irrational.

Proof.

Let r be an arbitrary rational number and s be an arbitrary irrational number. Suppose $r+s$ is rational. Since r is rational, there exist integers a and b with $b \neq 0$ such that $r = \frac{a}{b}$. Since $r+s$ is rational, there exist integers c and d with $d \neq 0$ such that $r+s = \frac{c}{d}$. Then $s = (r+s) - r = c/d - a/b = (bc-ad)/bd$. Since a, b, c, d are integers, so are $bc-ad$ and bd. In addition, since $b \neq 0$ and $d \neq 0$, by the zero product property, $bd \neq 0$. By definition s is also rational, a contradiction! Hence $r+s$ must be irrational. □

The method of proof by contraposition

Recall that the contrapositive of any statement is logically equivalent to itself. So we have the following method of proof by contraposition:

Remark

- *Write the original statement in the form*

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

- *For an arbitrary element $x \in D$, use direct proof to show that if $Q(x)$ is false, then $P(x)$ is false.*

The method of proof by contraposition

Recall that the contrapositive of any statement is logically equivalent to itself. So we have the following method of proof by contraposition:

Remark

- *Write the original statement in the form*

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

- *For an arbitrary element $x \in D$, use direct proof to show that if $Q(x)$ is false, then $P(x)$ is false.*

Example: parity of squares

Example

For any integer n, if n^2 is even, then n is even.

Example: parity of squares

Example

For any integer n, if n^2 is even, then n is even.

Remark

If we try to prove it directly, what can we do? Since n^2 is even, by definition there is an integer k such that $n^2 = 2k$. And then we get stuck here.

Example: parity of squares

Proof.

Let n be an arbitrary integer. Suppose n is not even, then n is odd. By definition, there is an integer k such that $n = 2k + 1$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1.$$

Since k is an integer, so is $2k^2 + 2k$. By definition, n^2 is odd. So n^2 is not even. Hence we also proved the contrapositive that "if n^2 is even, then n is even". □

HW #4 of these sections

Section 4.4 Exercise 2, 8, 21, 25, 35.
Exercises of Section 4.5 will be included in the next assignment.