Introduction to Sets and Logic (MATH 1190)

Instructor: Lili Shen
Email: shenlili@yorku.ca

Department of Mathematics and Statistics
York University

Nov 13, 2014

Quiz announcement

The second quiz will be held on Thursday, Nov 20, 9-10 pm in class. The contents in our lecture notes from Oct 9 to Nov 13 will be covered. Relevant material in textbook is:

- Section 2.1-2.5 (70%),
- Section 4.1 and 4.3 (30%).

Tips for quiz preparation: focus on lecture notes and recommended exercises.

All the rules are the same as Quiz 1. Please check the lecture note on Oct 9 for details.

Number theory

- Number theory is a branch of pure mathematics devoted primarily to the study of the integers.
- The basic notions of this chapter are divisibility and prime numbers.
- Number theory is known as

  "The Queen of Mathematics"

  because of its foundational place and and its wealth of open problems.

Outline

Division

Definition

Let a and b be integers with $a \neq 0$. If

$$\exists c \in \mathbf{Z}(b = ac),$$

then we say

- a divides b, or
- a is a factor of b, or
- a is a divisor of b, or
- b is divisible by a, or
- b is a multiple of a,

and denote it by $a \mid b$. We write $a \nmid b$ if a does not divide b.

As a simple example, $3 \mid 12$ but $3 \nmid 7$.

Properties of divisibility

Theorem

Let a, b, c be integers and $a \neq 0$.

(i) *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

(ii) *If $a \mid b$, then $a \mid bc$ for all integers c.*

(iii) *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Properties of divisibility

Proof.

(i) If $a \mid b$ and $a \mid c$, then there are integers s and t with $b = as$ and $c = at$. Thus

$$b + c = as + at = a(s + t),$$

and it follows that $a \mid (b + c)$.

(ii) If $a \mid b$, then there is an integer s with $b = as$. For any integer c, by

$$bc = asc = a(sc)$$

we have $a \mid bc$.

Properties of divisibility

(iii) If $a \mid b$ and $b \mid c$, then there are integers s and t with $b = as$ and $c = bt$. Thus

$$c = bt = ast = a(st),$$

and consequently $a \mid c$.

$\square$

Properties of divisibility

Corollary

Let a, b, c be integers and $a \neq 0$. If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m, n.

Properties of divisibility

Proof.

If $a \mid b$ and $a \mid c$, then for all integers m, n,

$$a \mid mb \quad \text{and} \quad a \mid nc.$$

It follows that

$$a \mid (mb + nc).$$

$\square$

The division algorithm

The following theorem can be proved using the well-ordering property of nonnegative integers introduced in Section 5.2.

Theorem (The division algorithm)

Let a be an integer and d a positive integer. Then there are unique integers q and r with $0 \leq r < d$, such that

$$a = dq + r.$$

In this case,

- *d is called the divisor;*
- *a is called the dividend;*
- *q is called the quotient;*
- *r is called the remainder.*

The division algorithm

Example

- When 101 is divided by 11, the quotient is 9 and the remainder is 2, i.e.,

$$101 = 11 \cdot 9 + 2.$$

- When -11 is divided by 3, the quotient is -4 and the remainder is 1, i.e.,

$$-11 = 3(-4) + 1.$$

The division algorithm

Remark

- The remainder cannot be negative. Although
$$-11 = 3(-3) - 2,$$
we cannot say the quotient when -11 is divided by 3 is -4 with the remainder -2.
- $d \mid a$ if and only if the remainder is zero when a is divided by d.

Congruence relation

Definition

If a and b are integers and m is a positive integer, then a is congruent to b modulo m, denoted by $a \equiv b \pmod{m}$, if

$$m \mid (a-b).$$

- $a \equiv b \pmod{m}$ is a congruence and m is its modulus (plural moduli).
- $a \equiv b \pmod{m}$ if and only if they have the same remainder when divided by m.
- We write $a \not\equiv b \pmod{m}$ if a is not congruent to b modulo m.

As a simple example, $17 \equiv 5 \pmod{6}$ but $24 \not\equiv 14 \pmod{6}$.

Properties of congruence relations

Theorem

Let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if there is an integer k such that

$$a = b + km.$$

Properties of congruence relations

Proof.

"$\rightarrow$": If $a \equiv b \pmod{m}$, then $m \mid (a - b)$, and thus there is some integer k such that $a - b = km$, i.e., $a = b + km$.

"$\leftarrow$": If $a = b + km$ for some integer k, then $km = a - b$, and it follows that $m \mid (a - b)$, which means $a \equiv b \pmod{m}$. $\square$

Properties of congruence relations

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

and

$$ac \equiv bd \pmod{m}.$$

Properties of congruence relations

Proof.

Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there are integers s and t with $b = a + sm$ and $d = c + tm$. It follows that

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

The conclusion thus follows. $\square$

Examples of congruence relations

Example

From $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$ we have

$$18 \equiv 3 \pmod 5$$

and

$$77 \equiv 2 \pmod 5.$$

Examples of congruence relations

Remark

- It follows immediately from the above theorem that $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{m}$ for any integer c. However, $ac \equiv bc \pmod{m}$ does not imply $a \equiv b \pmod{m}$. For example, $4 \equiv 8 \pmod{4}$ but $2 \not\equiv 4 \pmod{4}$.
- $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ does not imply $a^c \equiv b^d \pmod{m}$. For example, $3 \equiv 3 \pmod{5}$, $1 \equiv 6 \pmod{5}$, but $3^1 \not\equiv 3^6 \pmod{5}$.

Outline

Primes

Definition

A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. Otherwise, p is called composite.

The fundamental theorem of arithmetic

We present the following important fundamental theorem of arithmetic, also called the unique factorization theorem. It can be proved using strong induction introduced in Section 5.2.

Theorem (The fundamental theorem of arithmetic)

Every positive integer greater than 1 *can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.*

In other words, every positive integer greater than 1 *has a unique prime factorization.*

The fundamental theorem of arithmetic

Example

The prime factorizations of some integers are shown below.

- $100 = 2^2 \cdot 5^2$.
- $641 = 641$.
- $999 = 3^3 \cdot 37$.
- $1024 = 2^{10}$.

Trial Division

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Trial Division

Proof.

Suppose that $n = ab$ for some $1 < a < n$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$; otherwise, one would have

$$ab > \sqrt{n} \cdot \sqrt{n} = n,$$

which is a contradiction. Since both a and b divide n, n must have a prime divisor less than or equal to $\sqrt{n}$. $\square$

Trial Division

Example

167 is a prime. Since the only primes not exceeding $\sqrt{167}$ are $2, 3, 5, 7, 11$ (because $13^2 = 169 > 167$), and none of them is a divisor of 167, it follows that 167 is a prime.

The infinitude of primes

Theorem

There are infinitely many primes.

The infinitude of primes

Proof.

Assume that there are only finitely many primes $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 \ldots p_n + 1,$$

then none of the prime numbers $p_1, p_2, \ldots, p_n$ divides Q. Therefore, either Q is a prime number or there is another prime number q that divides Q. Both cases contradict to the assumption that all the prime numbers are in the list $p_1, p_2, \ldots, p_n$. $\square$

Conjectures about primes

Number theory may be the only branch in modern mathematics that allows ordinary people understand

“what the hell are the mathematicians doing?”

There is a list of well-known unsolved problems in mathematics on wikipedia:
`http://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics`
You would be a genius if you understand the meaning of a problem in any section except “Number theory”.

Conjectures about primes

Example (Arbitrarily long arithmetic progressions of primes)

For every positive integer n, there is an arithmetic progression of length n made up entirely of primes.

For example, $3, 7, 11$ is such an arithmetic progression of length 3, and $5, 11, 17, 23, 29$ is such an arithmetic progression of length 5.

This conjecture is solved by Ben Green and Terence Tao in a joint paper

"The primes contain arbitrarily long arithmetic progressions"

in 2004, and is now known as the Green-Tao theorem. Tao was awarded a fields medal in 2006.

Conjectures about primes

Example (Goldbach's Conjecture)

Every even integer greater than 2 is the sum of two primes.

For example, $6 = 3 + 3$, $20 = 3 + 17$, $100 = 17 + 83$, and so on.

Conjectures about primes

In the 20th century, in order to solve this conjecture, the number theorists studied the "$m + n$" problem: to prove that every even integer greater than 2 can be written as the sum of two integers, one of which is the product of at most m primes, and the other is the product of at most n primes. Then the Goldbach's conjecture is exactly "$1 + 1$".

In 1966, Jingrun Chen proved "$1 + 2$": every even integer greater than 2 can be written as the sum of a prime and the product of at most two primes.

However, "$1 + 1$" remains an open problem until now.

Conjectures about primes

Example (The Twin Prime Conjecture)

There are infinitely many twin primes, i.e., pairs of primes of the form $(n, n+2)$.

For example, 3 and 5, 11 and 13, 4967 and 4969.

Conjectures about primes

A prime gap is the difference between two successive prime numbers. The n-th prime gap, denoted by g_n, is the difference between the $(n+1)$-th prime and the n-th prime, i.e.,

$$g_n = p_{n+1} - p_n.$$

The twin prime conjecture asserts exactly that $g_n = 2$ for infinitely many integers n.

Conjectures about primes

The strongest result proved concerning twin primes is that there exists a finite bound for prime gaps. This is proved by Yitang Zhang in his paper

"Bounded gaps between primes"

in 2013, who showed that

"There are infinitely many g_n's that do not exceed 70 million."

The bound "70 million" has been reduced to 246 by refining Zhang's method in April 2014.

Note: In Example 9 on Page 264 of the textbook, "the strongest result proved concerning twin primes is that ..." is an out-of-date information, since this book was published in 2011, two years before the publication of Zhang's work.

Outline

Greatest common divisors

Definition

Let a and b be integers, not both zero.

- The largest integer d such that
$$d \mid a \quad \text{and} \quad d \mid b$$
is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$.
- a and b are called relatively prime if $\gcd(a, b) = 1$.

Examples of greatest common divisors

Example

- Since $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$,

$$\gcd(120, 500) = 2^2 \cdot 5 = 20.$$

- 17 and 22 are relatively prime.

Least common multiples

Definition

The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by both a and b, and is denoted by $\text{lcm}(a, b)$.

Examples of least common multiples

Example

Since $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$,

$$\operatorname{lcm}(120, 500) = 2^3 \cdot 3 \cdot 5^3 = 3000.$$

Least common multiples

Theorem

For positive integers a and b,

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

Least common multiples

Proof.

Let $p_1, p_2, \ldots, p_n$ be the list of prime divisors of a and b, written in the order of nondecreasing size. Then

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n},$$

$$b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n},$$

where $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are nonnegative integers. It follows that

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)},$$

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)}.$$

Least common multiples

Therefore,

$$
\begin{aligned}
&\gcd(a,b)\cdot\operatorname{lcm}(a,b)\\
&= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)+\max(a_n,b_n)}\\
&= p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n}\\
&= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \cdot p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}\\
&= ab.
\end{aligned}
$$

$\square$

The Euclidean Algorithm

Lemma

Let $a = bq + r$, where a, b, q, r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

The Euclidean Algorithm

Proof.

It suffices prove d divides both a and b if and only if d divides both b and r.

"$\to$": If $d \mid a$ and $d \mid b$, then $d \mid (a - bq)$, i.e., $d \mid r$.

"$\leftarrow$": If $d \mid b$ and $d \mid r$, then $d \mid (bq + r)$, i.e., $d \mid a$. $\square$

greatest common divisors as linear combinations

We present the following theorem without a proof (which can be proved using the knowledge of Section 5.2):

Theorem (Bézout)

If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a,b) = sa + tb.$$

Here $sa + tb$ is called a linear combination of a and b.

Examples of greatest common divisors

Example

(i) Find the greatest common divisor $\gcd(108, 300)$.

(ii) Express $\gcd(108, 300)$ as a linear combination of 108 and 300.

Examples of greatest common divisors

Solution.

(i) We use the Euclidean algorithm to find $\gcd(108, 300)$:

$$\begin{aligned} 300 &= 108 \cdot 2 + 84, \\ 108 &= 84 \cdot 1 + 24, \\ 84 &= 24 \cdot 3 + 12, \\ 24 &= 12 \cdot 2. \end{aligned}$$

Therefore, $\gcd(108, 300) = 12$.

Examples of greatest common divisors

(ii)

$$
\begin{aligned}
12 &= 84 - 24 \cdot 3 \\
&= 84 - (108 - 84) \cdot 3 \\
&= 84 \cdot 4 - 108 \cdot 3 \\
&= (300 - 108 \cdot 2) \cdot 4 - 108 \cdot 3 \\
&= 300 \cdot 4 - 108 \cdot 11.
\end{aligned}
$$

$\square$

Examples of greatest common divisors

The solution of (i) in this example can be written in a more intuitive way:

Solution.

(i) We use the Euclidean algorithm to find $\gcd(108, 300)$:

$$\begin{array}{c|c|c|c} 2 & 300 & 108 & 1 \\ & 216 & 84 & \\ \hline 3 & 84 & 24 & 2 \\ & 72 & 24 & \\ \hline & 12 & 0 & \end{array}$$

Therefore, $\gcd(108, 300) = 12$.

Recommended exercises

Section 4.1: 3, 4, 6, 8, 24, 26, 38, 40.

Section 4.3: 3(bcd), 24, 26, 32(c), 33(ab), 40(cdf).