Math 2603 - Lecture 8
Section 4.4 & 4.5 Congruences

Bo Lin
(Lecture by Jing Hao)

September 12th, 2019

Congruences

Motivation

In our lives, there are different objects with the same name. For example,

- there is a Thursday in every week;
- there is a moment called "3PM" every day.

It seems that there objects have some property in common.

Motivation

In our lives, there are different objects with the same name. For example,

- there is a Thursday in every week;
- there is a moment called "3PM" every day.

It seems that there objects have some property in common.
In addition, if the time moves forward 10 hours after 3PM, what would be the time? Instead of 13PM, we actually have 1AM.

Motivation

In our lives, there are different objects with the same name. For example,

- there is a Thursday in every week;
- there is a moment called "3PM" every day.

It seems that there objects have some property in common.
In addition, if the time moves forward 10 hours after 3PM, what would be the time? Instead of 13PM, we actually have 1AM.
All these phenomena are related to the **congruence**.

Congruence

Definition

Let $n > 1$ be an integer. given integers a and b, we say that a is congruent to b modulo n and write

$$a \equiv b \pmod{n}$$

if and only if $n \mid (a - b)$.

Congruence

Definition

Let $n > 1$ be an integer. given integers a and b, we say that a is congruent to b modulo n and write

$$a \equiv b \pmod{n}$$

if and only if $n \mid (a - b)$.

Example

$3 \equiv 17 \pmod{7}$, *because* $3 - 17 = -14$, *and* $-14 = 7 \cdot (-2)$ *is divisible by* 7.

Congruence

Definition

Let $n > 1$ be an integer. given integers a and b, we say that a is congruent to b modulo n and write

$$a \equiv b \pmod{n}$$

if and only if $n \mid (a - b)$.

Example

$3 \equiv 17 \pmod{7}$, *because* $3 - 17 = -14$, *and* $-14 = 7 \cdot (-2)$ *is divisible by* 7.
If a and b are integers, then $(4a + 1) \equiv (4b - 3) \pmod{4}$, *because* $(4a + 1) - (4b - 3) = 4a - 4b + 4 = 4(a - b + 1)$ *is a multiple of* 4.

Congruence is an equivalence relation

Proposition

For any integer $n > 1$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof.

Reflexivity: for any $a \in \mathbb{Z}$, $a - a = 0$ is divisible by n.
Symmetry: for $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$, then $a - b$ is divisible by n. Since $b - a = (-1) \cdot (a - b)$, it is also divisible by n.
Transitivity: for $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then there exists integers u, v such that $a - b = nu$ and $b - c = nv$. Then $a - c = nu + nv = n(u + v)$ is divisible by n too. So $a \equiv c \pmod{n}$. □

Congruence classes

Definition

An equivalence class of congruence modulo n is called a **congruence class modulo n.**

Congruence classes

Definition

An equivalence class of congruence modulo n is called a **congruence class modulo** n.

Definition

For $a \in \mathbb{Z}$, the congruence class modulo n of a is denoted $\overline{a}$, which is

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

Example: congruence classes modulo 4

Example

Find all congruence classes modulo 4.

Example: congruence classes modulo 4

Example

Find all congruence classes modulo 4.

Solution

The congruence classes are characterized by the remainder when divided by 4. So there are 4 congruence classes modulo 4 which form a partition of $\mathbb{Z}$:

$$4\mathbb{Z}, 4\mathbb{Z}+1 = \{4x+1 \mid x \in \mathbb{Z}\}, 4\mathbb{Z}+2, 4\mathbb{Z}+3.$$

Example: congruence classes modulo 4

Example

Find all congruence classes modulo 4.

Solution

The congruence classes are characterized by the remainder when divided by 4. So there are 4 congruence classes modulo 4 which form a partition of $\mathbb{Z}$:

$$4\mathbb{Z}, 4\mathbb{Z}+1 = \{4x+1 \mid x \in \mathbb{Z}\}, 4\mathbb{Z}+2, 4\mathbb{Z}+3.$$

Remark

For any positive integer $n > 1$, there are n congruence classes modulo n in $\mathbb{Z}$. They are disjoint and their union is $\mathbb{Z}$.

Equivalent characterizations of congruence

Theorem

Let a, b and $n > 1$ be integers. The following statements are all equivalent:

1. $a \equiv b \pmod{n}$;
2. $n \mid (a - b)$;
3. $a = b + kn$ *for some integer* k;
4. a *and* b *have the same (nonnegative) remainder when divided by* n;
5. $\overline{a} = \overline{b}$.

Arithmetics of congruences

Theorem

Let a, b, c, d *and* $n > 1$ *be integers, and suppose* $a \equiv c \pmod{n}, b \equiv d \pmod{n}$. *Then*

(a) $(a + b) \equiv (c + d) \pmod{n}$;

(b) $ab \equiv cd \pmod{n}$;

(c) $a^m \equiv c^m \pmod{n}$ *for all positive integers* m.

Arithmetics of congruences

Theorem

Let a, b, c, d and $n > 1$ be integers, and suppose $a \equiv c \pmod{n}, b \equiv d \pmod{n}$. Then

(a) $(a + b) \equiv (c + d) \pmod{n}$;

(b) $ab \equiv cd \pmod{n}$;

(c) $a^m \equiv c^m \pmod{n}$ *for all positive integers* m.

Proof.

We only prove (b). Since $a \equiv c \pmod{n}$, there exists an integer s such that $a = c + sn$; since $b \equiv d \pmod{n}$, there exists an integer t such that $b = d + sn$.

Arithmetics of congruences

Theorem

Let a, b, c, d and $n > 1$ be integers, and suppose $a \equiv c \pmod{n}, b \equiv d \pmod{n}$. Then

(a) $(a + b) \equiv (c + d) \pmod{n}$;

(b) $ab \equiv cd \pmod{n}$;

(c) $a^m \equiv c^m \pmod{n}$ *for all positive integers* m.

Proof.

We only prove (b). Since $a \equiv c \pmod{n}$, there exists an integer s such that $a = c + sn$; since $b \equiv d \pmod{n}$, there exists an integer t such that $b = d + sn$. Then

$$ab - cd = (c+sn)(d+tn) - cd = ctn + snd + stn^2 = (ct + ds + stn) \cdot n$$

is a multiple of n, so $ab \equiv cd \pmod{n}$. □

Residues modulo n

Definition

Given integers a and n with $n > 1$, the **residue** *of a modulo n is*

$$a \pmod{n},$$

the nonnegative remainder obtained when a is divided by n.

Residues modulo n

Definition

Given integers a and n with $n > 1$, the **residue** *of a modulo n is*

$$a \pmod{n},$$

the nonnegative remainder obtained when a is divided by n.

Example

$7 \pmod{3} = 1$; $-4 \pmod{6} = 2$.

Equations of congruences

Example

Find all $x \in \mathbb{Z}$ *such that* $3x \equiv 1 \pmod{5}$.

Equations of congruences

Example

Find all $x \in \mathbb{Z}$ such that $3x \equiv 1 \pmod 5$.

Solution

Note that if x is a solution, then any $y \in \overline{x}$ is a solution too. So in fact we are solving for the congruence classes modulo 5.

Equations of congruences

Example

Find all $x \in \mathbb{Z}$ such that $3x \equiv 1 \pmod 5$.

Solution

Note that if x is a solution, then any $y \in \overline{x}$ is a solution too. So in fact we are solving for the congruence classes modulo 5. We have the following table:

x	0	1	2	3	4
$3x$	0	3	6	9	12
$3x \pmod 5$	0	3	$\mathbf{1}$	4	2

Equations of congruences

Example

Find all $x \in \mathbb{Z}$ such that $3x \equiv 1 \pmod 5$.

Solution

Note that if x is a solution, then any $y \in \overline{x}$ is a solution too. So in fact we are solving for the congruence classes modulo 5. We have the following table:

x	0	1	2	3	4
$3x$	0	3	6	9	12
$3x \pmod 5$	0	3	$\mathbf{1}$	4	2

So the answer is $\overline{2} = 5\mathbb{Z} + 2 = \{5y + 2 \mid y \in \mathbb{Z}\}$.

Division of congruences

We note that addition, subtraction and multiplication are commutative with congruence. What about division?

Example

We have $2 \equiv 6 \pmod 4$, *while if we divide both numbers by* 2, $1 \not\equiv 3 \pmod 4$.

Division of congruences

We note that addition, subtraction and multiplication are commutative with congruence. What about division?

Example

We have $2 \equiv 6 \pmod 4$, *while if we divide both numbers by* 2, $1 \not\equiv 3 \pmod 4$.

However, sometimes we can still do division:

Proposition

Let integer $n > 1$ *and* $a, b, c \in \mathbb{Z}$. *If* $ac \equiv bc \pmod n$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \pmod n$.

Division of congruences

Proposition

Let integer $n > 1$ *and* $a, b, c \in \mathbb{Z}$. *If* $ac \equiv bc \pmod{n}$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \pmod{n}$.

Proof.

Since $ac \equiv bc \pmod{n}$, there exists an integer k such that $(a - b)c = ac - bc = kn$.

Division of congruences

Proposition

Let integer $n > 1$ *and* $a, b, c \in \mathbb{Z}$. *If* $ac \equiv bc \pmod{n}$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \pmod{n}$.

Proof.

Since $ac \equiv bc \pmod{n}$, there exists an integer k such that $(a - b)c = ac - bc = kn$. Since $\gcd(c, n) = 1$, by Bezout's Theorem, there exist integers u, v such that $uc + vn = 1$.

Division of congruences

Proposition

Let integer $n > 1$ *and* $a, b, c \in \mathbb{Z}$. *If* $ac \equiv bc \pmod{n}$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \pmod{n}$.

Proof.

Since $ac \equiv bc \pmod{n}$, there exists an integer k such that $(a-b)c = ac - bc = kn$. Since $\gcd(c, n) = 1$, by Bezout's Theorem, there exist integers u, v such that $uc + vn = 1$.Then

$$(a-b) = (a-b)(uc+vn) = u(a-b)c+(a-b)vn = (uk+(a-b)v)n$$

is a multiple of n. □

When $\gcd(a, n) = 1$

Proposition

Let integer $n > 1$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

(a) *there exists an integer s such that $sa \equiv 1 \pmod{n}$;*

(b) *for any $b \in \mathbb{Z}$, the equation $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

When $\gcd(a, n) = 1$

Proposition

Let integer $n > 1$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

(a) *there exists an integer s such that $sa \equiv 1 \pmod{n}$;*

(b) *for any $b \in \mathbb{Z}$, the equation $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

Remark

The congruence class $\overline{s}$ is called the inverse of a modulo n, denoted $a^{-1} \pmod{n}$.

When $\gcd(a, n) = 1$

Proposition

Let integer $n > 1$ and $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$. Then

(a) *there exists an integer s such that $sa \equiv 1 \pmod{n}$;*

(b) *for any $b \in \mathbb{Z}$, the equation $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

Remark

The congruence class $\overline{s}$ is called the inverse of a modulo n, denoted $a^{-1} \pmod{n}$.

Proof.

(a) follows from Bezout's Theorem; in (b), multiplying by s we get $x \equiv sax \equiv sb \pmod{n}$, and $sb \pmod{n}$ is the unique solution. □

Example: congruence equation

Example

Solve $8x \equiv 6 \pmod{15}$.

Example: congruence equation

Example

Solve $8x \equiv 6 \pmod{15}$.

Solution

Since $\gcd(8, 15) = 1$, *we use Euclidean Algorithm to write* $2 \cdot 8 + (-1) \cdot 15 = 1$, *so the inverse of* 8 *modulo* 15 *is* $2 \pmod{15}$.

Example: congruence equation

Example

Solve $8x \equiv 6 \pmod{15}$.

Solution

Since $\gcd(8, 15) = 1$, *we use Euclidean Algorithm to write* $2 \cdot 8 + (-1) \cdot 15 = 1$, *so the inverse of* 8 *modulo* 15 *is* $2 \pmod{15}$. *Then*

$$x \equiv 16x = 2 \cdot 8x \equiv 2 \cdot 6 = 12 \pmod{15}.$$

Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_t$ be pairwisely relatively prime positive integers. Then the system of congruences

$$x \equiv a_i \pmod{m_i} \quad (i = 1, 2, \ldots, t)$$

has a unique solution modulo $M = \prod_{i=1}^{t} m_i$, which is

$$x \equiv \sum_{i=1}^{t} \left(y_i a_i \prod_{j \neq i} m_j \right). \tag{1}$$

Here y_i is an integer such that $y_i \prod_{j \neq i} m_j \equiv 1 \pmod{m_i}$.

Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem)

Let $m_1, m_2, \ldots, m_t$ be pairwisely relatively prime positive integers. Then the system of congruences

$$x \equiv a_i \pmod{m_i} \quad (i = 1, 2, \ldots, t)$$

has a unique solution modulo $M = \prod_{i=1}^{t} m_i$, which is

$$x \equiv \sum_{i=1}^{t} \left(y_i a_i \prod_{j \neq i} m_j \right). \tag{1}$$

Here y_i is an integer such that $y_i \prod_{j \neq i} m_j \equiv 1 \pmod{m_i}$.

Example

Solve the system of congruences

Example: solve congruence equations

Solution

First we compute the inverses:

$$(5 \cdot 7)^{-1} \equiv 2^{-1} \equiv 2 \pmod 3;$$
$$(3 \cdot 7)^{-1} \equiv 1^{-1} \equiv 1 \pmod 5;$$
$$(3 \cdot 5)^{-1} \equiv 1^{-1} \equiv 1 \pmod 7;$$

Second we write x as the sum:

$$\begin{aligned} x &\equiv 2 \cdot 2 \cdot 5 \cdot 7 + 1 \cdot 3 \cdot 3 \cdot 7 + 1 \cdot 2 \cdot 3 \cdot 5 \\ &\equiv 140 + 63 + 30 \equiv 233 \\ &\equiv 23 \pmod{105}. \end{aligned}$$

The Fundamental Theorem of Arithmetics

Theorem

Every integer $n > 1$ can be uniquely written as a product of prime numbers

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s},$$

where $q_1 < q_2 < \cdots < q_s$ are distinct prime numbers and $\alpha_i \in \mathbb{N}$.

The Fundamental Theorem of Arithmetics

Theorem

Every integer $n > 1$ can be uniquely written as a product of prime numbers

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s},$$

where $q_1 < q_2 < \cdots < q_s$ are distinct prime numbers and $\alpha_i \in \mathbb{N}$.

Remark

Since $\gcd(q_i, q_j) = 1$, the integers $q_i^{\alpha_i}$ are pairwisely relatively prime. By Chinese Remainder Theorem, in order to study congruence modulo n, it suffices to study congruence modulo powers of prime numbers. This is a reason why prime numbers are a central topic in number theory.

Applications of congruences

Applications of congruences

Congruences are widely used in our everyday lives.

- Days in a week are modulo 7.

Applications of congruences

Congruences are widely used in our everyday lives.

- Days in a week are modulo 7.
- Time within a day - hours are modulo 12 (or 24), minutes and seconds are modulo 60.

Applications of congruences

Congruences are widely used in our everyday lives.

- Days in a week are modulo 7.
- Time within a day - hours are modulo 12 (or 24), minutes and seconds are modulo 60.
- Codes with check digit - International Standard Book Number (ISBN) is modulo 11 and Universal Product Code (UPC) is modulo 10.

Check digits

In our everyday lives, we need various string of digits, like ID numbers, barcode of grocery items, the number of books and magazines, credit card numbers, and so on. What if the string is sent incorrectly, like two adjacent digits switched or one digit omitted?

Check digits

In our everyday lives, we need various string of digits, like ID numbers, barcode of grocery items, the number of books and magazines, credit card numbers, and so on. What if the string is sent incorrectly, like two adjacent digits switched or one digit omitted?

Remark

Using congruences, we can add some redundant digits such that the new string of digit satisfies some congruence equation. If the string is altered briefly, in most case it does not satisfy the equation anymore, and we can tell that it is wrong. The added digits are called **check digits**.

International Standard Book Number (ISBN)

Since 1968 and until 2007, every book published around the world is identified with a unique 10-digit string, called the *International Standard Book Number* (ISBN for short). The 10 digits are decomposed into 4 parts: country code – publisher code – book code – check digit. It's also called ISBN-10 in order to distinguish with the new version ISBN-13. For example, the latest version of our textbook has ISBN-10 code $0 - 13 - 167995 - 3$.

International Standard Book Number (ISBN)

Since 1968 and until 2007, every book published around the world is identified with a unique 10-digit string, called the *International Standard Book Number* (ISBN for short). The 10 digits are decomposed into 4 parts: country code – publisher code – book code – check digit. It's also called ISBN-10 in order to distinguish with the new version ISBN-13. For example, the latest version of our textbook has ISBN-10 code $0-13-167995-3$.

Definition

Suppose an ISBN-10 code is $x_1x_2\ldots x_{10}$. Then it satisfies

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}.$$

Example: ISBN verification

Example

Show that $0-13-167995-3$ *is a valid ISBN.*

Example: ISBN verification

Example

Show that $0-13-167995-3$ *is a valid ISBN.*

Solution

$$
\begin{aligned}
&1*0+2*1+3*3+4*1+5*6\\
+&6*7+7*9+8*9+9*5+10*3\\
=&0+2+9+4+30+42+63+72+45+30\\
\equiv&4+8+(-2)+(-3)+6+1+8\\
=&22\equiv 0 \pmod{11}.
\end{aligned}
$$

ISBN can identify a single mistake

Proposition

Given any ISBN x, if a single digit of x is altered, or two adjacent distinct digits of x are switched, the new string x' is not a valid ISBN.

ISBN can identify a single mistake

Proposition

Given any ISBN x, if a single digit of x is altered, or two adjacent distinct digits of x are switched, the new string x' is not a valid ISBN.

Proof.

If x_i becomes x_i', then $x_i \not\equiv x_i' \pmod{11}$. Since $\gcd(i, 11) = 1$, $ix_i \not\equiv ix_i' \pmod{11}$, so the sum of x' and x are not congruent modulo 11.

ISBN can identify a single mistake

Proposition

Given any ISBN x, if a single digit of x is altered, or two adjacent distinct digits of x are switched, the new string x' is not a valid ISBN.

Proof.

If x_i becomes x_i', then $x_i \not\equiv x_i' \pmod{11}$. Since $\gcd(i, 11) = 1$, $ix_i \not\equiv ix_i' \pmod{11}$, so the sum of x' and x are not congruent modulo 11.

If x_i and x_{i+1} are distinct and switched. Then in the sum of x, their contribution is $ix_i + (i+1)x_{i+1}$. While in the sum of x', their contribution is $(i+1)x_i + ix_{i+1}$. The difference is $x_i - x_{i+1} \not\equiv 0 \pmod{11}$. □

Universal Product Codes

In North America, a barcode called **Universal Product Code** (UPC for short) appears on almost every item you buy.

Definition

Let $a_1a_2\ldots a_{12}$ be an UPC string. Then a_{12} is the check digit satisfying

$$3a_1+a_2+3a_3+a_4+3a_5+a_6+3a_7+a_8+3a_9+a_{10}+3a_{11}+a_{12} \equiv 0 \pmod{10}$$

Example: verifying a UPC

Verify the UPC on the item shown via doc cam.

HW Assignment #4 - today's sections

Section 4.3 Exercise 4(a)(b), 7, 24.
Section 4.4 Exercise 8, 9(d)(g)(i), 22(b)(c).
Section 4.5 Exercise 4, 10(b), 18(c).