# Congruence Theory

NEHS G10 Eve Wang

# Table of Contents

# Where’s Tongyu (Bronze Gudgeon)?

**Throughout this presentation, a hidden Bronze Gudgeon can be found on each slide. Try to spot them all as we go — it might make modular arithmetic a bit more fun! Look carefully... Let’s begin!**

*NOTE: In Mandarien, Bronze Gudgeon pronounce the same as Congruence, both read as “Tongyu”

# Equivalence Relation

# Equivalence relation

A **binary relation** on a set that possesses **reflexivity**, **symmetry**, and **transitivity**.

Example 1.

In the set of real numbers R, the binary relation “=” is an equivalence relation.

**Reflexivity**: For all $a \in R$ , $a = a$

**Symmetry**: For all $a, b \in R$, $a = b \Rightarrow b = a$

**Transitivity**: For all $a, b, c \in R$, $a = b, b = c \Rightarrow a = c$

# Equivalence relation

A **binary relation** on a set that possesses **reflexivity**, **symmetry**, and **transitivity**.

Example 2.

In the set of triangles $T$, the binary relation “$\cong$” (is congruent to) is an equivalence relation.

**Reflexivity**: For all $\Delta A \in T,\ \Delta A \cong \Delta A$

**Symmetry**: For all $\Delta A, \Delta B \in T,\ \Delta A \cong \Delta B \Rightarrow \Delta B \cong \Delta A$

**Transitivity**: For all $\Delta A, \Delta B, \Delta C \in T,$

$$\Delta A \cong \Delta B, \Delta B \cong \Delta C \Rightarrow \Delta A \cong \Delta C$$

# Equivalence relation

Let $S$ be a set, and let $R$ be a binary relation on $S$.
If $R$ satisfies the following properties, then $R$ is an equivalence relation.

**Reflexivity**: For all $a \in S,\ (a, a) \in R$

**Symmetry**: For all $a, b \in S,\ (a, b) \in R \Rightarrow (b, a) \in R$

**Transitivity**:For all $a, b, c \in S,\ (a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$

$$R = \{(x, y) : x^2 = y^2, (x, y) \in R\}$$

$$3^2 = (-3)^2 \Rightarrow (3, -3) \in R$$

$$3^2 \neq 6^2 \Rightarrow (3, 6) \notin R$$

# Equivalence relation

A **binary relation** on a set that possesses **reflexivity**, **symmetry**, and **transitivity**.

Example 3.

In the set of real numbers $R$, consider the binary relation " $>$ ".

**Not Reflexive**: There exists $x \in R$ such that $x > x$ is not true.

**Not Symmetric**: There exists $x, y \in R$ such that $x > y$ holds, but $y > x$ does not hold.

**Transitive**: For all $x, y, z \in R$, if $x > y, y > z \Rightarrow x > z$

**✕ Not an Equivalence Relation!**

# Congruence

# Congruence

Define Congruence Relation: Let $a, b \in Z, n > 0$

iIf $n \mid (a-b)$ , then $a$ and $b$ are said to be congruent modulo $n$, written as $a \equiv b \pmod{n}$

↑ (modulus)

Let $a = q_1 n + r_1,\ b = q_2 n + r_2$

$$a - b = (q_1 - q_2)n + (r_1 - r_2)$$

# Congruence

Define Congruence Relation: Let $a, b \in Z, n > 0$

iIf $n \mid (a-b)$ , then $a$ and $b$ are said to be congruent modulo $n$, written as $a \equiv b \pmod{n}$

(modulus)

If $a \equiv b \pmod{n} \Leftrightarrow a = qn+b, \exists\ q \in Z$

$$\text{Let } a = q_1 n + r, b = q_2 n + r$$

$$a = q_1 n + b - q_2 n$$

$$= (q_1 - q_2) n + b$$

$$= qn + b$$

# Distinguishing “Congruence Relation” and “Modular Operation”

$a \equiv b \pmod{n}$ represents a congruence **relation**. (ex. $5 \equiv 1 \pmod{4}$ )

$a \bmod b$ represents a modular **operation**. (ex.$7 \bmod 3 = 1$ )

# Congruence Is an Equivalence Relation!

In the set of integers $Z$, consider the binary relation " $\equiv$ ".

**Reflexivity**: For all $a \in Z,\ a \equiv a \pmod{n}$

**Symmetry**: For all $a, b \in Z,\ a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

**Transitivity**: For all $a, b, c \in Z,$

$$a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$$

# Some Properties of Congruence

Properties:

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

$c \equiv d \pmod{n}$

Then (1) $a \pm c \equiv b \pm d \pmod{n}$

(2) $ac \equiv bd \pmod{n}$

Examples：$5 \equiv 8 \pmod{3}$

$1 \equiv 4 \pmod{3}$

$6 \equiv 12 \pmod{3}$

(1) $a \pm c \equiv b \pm d \pmod{n}$

$a = nx + b$

$c = ny + d$

$a \pm c = (nx + b) \pm (ny + d)$

$= (b \pm d) \pm n(x + y)$

$\Rightarrow a \pm c \equiv b \pm d \pmod{n}$

# Some Properties of Congruence

Properties:

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

$c \equiv d \pmod{n}$

Then (1) $a \pm c \equiv b \pm d \pmod{n}$

(2) $ac \equiv bd \pmod{n}$

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

Examples：$5 \equiv 8 \pmod{3}$

$1 \equiv 4 \pmod{3}$

$6 \equiv 12 \pmod{3}$

(2) $ac \equiv bd \pmod{n}$

$a = nx+b$

$c = ny+d$

$ac = (nx+b) \cdot (ny+d)$

$= bd + n(by+dx) + n^2xy$

$= bd + n(by+dx+nxy)$

$\Rightarrow ac \equiv bd \pmod{n}$

# Some Properties of Congruence

Property:
If $k \neq 0$ and $ak \equiv bk \pmod{m}$,

then $k$ can be canceled from
both sides only if gcd($k$, $m$)=1.

$$a \equiv b \left( mod \frac{m}{gcd\,(k, m)} \right)$$

*link to *modular inverses*
(to be introduced later)

*for example :*

$8 \equiv 26 \pmod 3$
$4 \equiv 13 \pmod 3$
$\div 2 \quad gcd\,(2, 3) = 1$

$10 \equiv 34 \pmod 8$
$5 \not\equiv 17 \pmod 8$
$5 \equiv 17 \pmod 4$
$\div 2 \quad gcd\,(2, 8) = 2$

# Fun Exercises

# Find Remainders

Example 1. Find the remainder when $2^{90}$ is devided by 11.

# Find Remainders

Example 1. Find the remainder when $2^{90}$ is devided by 11.

$$2^{90} \equiv 4^{45} \equiv 4 \cdot 4^{44} \equiv 4 \cdot 16^{22}$$

$16 \equiv 5\,(mod 11)$ $\equiv 4 \cdot 5^{22} \equiv 4 \cdot 25^{11}$

$25 \equiv 3\,(mod 11)$ $\equiv 4 \cdot 3^{11} \equiv 12 \cdot 3^{10}$

$12 \equiv 1\,(mod 11)$ $\equiv 1 \cdot 9^{5} \equiv 9 \cdot 9^{4} \equiv 9 \cdot 81^{2}$

$81 \equiv 4\,(mod 11)$ $\equiv 9 \cdot 4^{2} \equiv 9 \cdot 5 \equiv 45 \equiv 1\,(mod 11)$

**Method A**

# Find Remainders

Example 1. Find the remainder when $2^{90}$ is devided by 11.

$$2^2 = 4$$

$$2^4 = (2^2)^2 = 4^2 = 16 \equiv 5 (mod 11)$$

$$2^8 \equiv (2^4)^2 \equiv 5^2 \equiv 25 \equiv 3 (mod 11)$$

$$2^{10} = 2^8 \cdot 2^2 \equiv 3 \cdot 4 \equiv 12 \equiv 1 (mod 11)$$

$$2^{90} = \left(2^{10}\right)^9 \equiv 1 \, (mod 11)$$

**Method B**

# Find Remainders

Example 2. Prove that for any positive interger n, $3^{2n+1} + 2^{n+2}$ is a multiple of 7.

$$3^{2n+1} + 2^{n+2} \equiv 3\left(3^2\right)^n + 4 \cdot 2^n$$

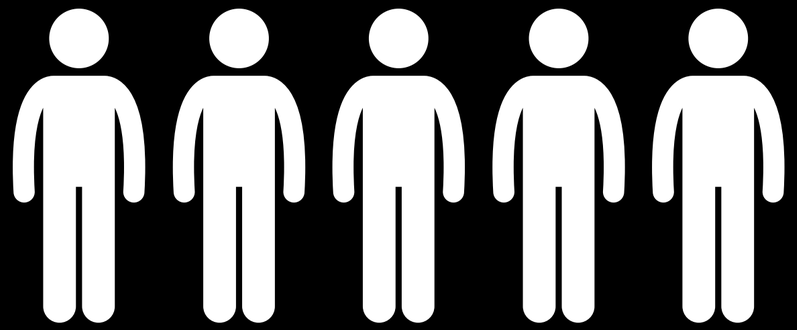
$$\equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 2^n(3+4)$$

$$\equiv 2^n \cdot 0 \equiv 0\,(mod 7)$$

# The Monkey and Coconuts Problem

There are five men and a monkey stranded on a deserted island.

One day, the five men work hard to gather n coconuts from around the island.
They decide to divide the coconuts equally among themselves the next morning.



# The Monkey and Coconuts Problem

At midnight, one man, unable to trust the others, gets up and goes to the coconuts.

To appease the monkey, he gives one coconut to it.
Then he discovers that the remaining coconuts can be divided evenly into five parts.

He hides his one share in a secret place and then goes back to sleep peacefully.

# The Monkey and Coconuts Problem

At midnight, one man, unable to trust the others, gets up and goes to the coconuts.

To appease the monkey, he gives one coconut to it.
Then he discovers that the remaining coconuts can be divided evenly into five parts.

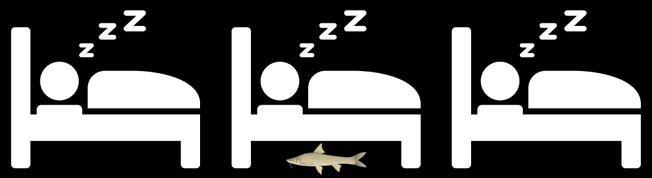
He hides his one share in a secret place and then goes back to sleep peacefully.

# The Monkey and Coconuts Problem

Not long after, another man also woke up.
He did the exact same thing as the first man:

He gave one coconut to the monkey, and found that the remaining coconuts could again be divided evenly into five parts.

He then hid his share in a secret place and went back to sleep.



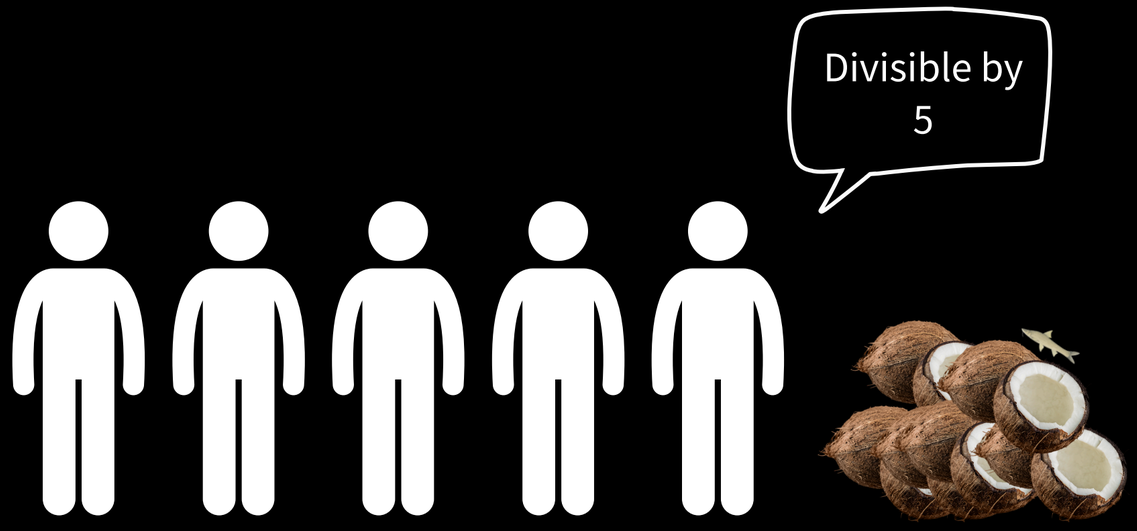
# The Monkey and Coconuts Problem

All of them got up one after another during the night and secretly did the same thing.

# The Monkey and Coconuts Problem

The next morning, when all five men came together to the pile of coconuts, they found that the remaining coconuts could once again be divided evenly into five parts.

Question: What is the smallest possible value of n?



# The Monkey and Coconuts Problem

Let $A = \frac{4}{5}$

First man: $A\left(n-1\right)$

Second man: $A\left(A\left(n-1\right)-1\right) = A^2\left(n-1\right) - A$

Thrid man: $A\left(A^2\left(n-1\right) - A - 1\right) = A^3\left(n-1\right) - A^2 - A$

Fourth man: $A^4\left(n-1\right) - A^3 - A^2 - A$

Fifth man: $A^5\left(n-1\right) - A^4 - A^3 - A^2 - A$

$$= A^5\left(n-1\right) - \frac{A^5 - A}{A-1}$$

$$= A^5\left(n - 1 - \frac{1}{A-1}\right) + \frac{A}{A-1}$$

# The Monkey and Coconuts Problem

$$= A^5 \left( n - 1 - \frac{1}{A-1} \right) + \frac{A}{A-1}$$

$$\left( \frac{4}{5} \right)^5 (n+4) - 4 \equiv 0 \, (mod 5)$$

$$\left( \frac{4}{5} \right)^5 (n+4) \equiv 4 \, (mod 5)$$

$$4 \equiv -1 \, (mod 5)$$

$$\left( \frac{-1}{5} \right)^5 (n+4) \equiv -1 \, (mod 5)$$

$$\frac{n+4}{5^5} \equiv 1 \, (mod 5)$$

$$\frac{n+4}{5^5} = 5k + 1$$

$$n = 5^5 \, (5k+1) - 4$$

$$n_{min} = 5^5 - 4 = 3121$$

# The Monkey and Coconuts Problem

# Chinese Remainder Theorem

# Sunzi Suanjing: “The Problem of Unknown Quantity”

「今有物，不知其數，三三數之賸二，五五數之賸三，七七數之賸二。問物幾何？」

$$x \div 3 \ldots 2$$
$$x \div 5 \ldots 3$$
$$x \div 7 \ldots 2$$
$$x \in Z$$

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Ming dynasty mathematician Cheng Dawei included this problem in his work Suanfa Tongzong (Arithmetic Mastery), and turned it into a poetic verse known as the “Sunzi Riddle Verse”:

**《孫子歌訣》：「三人同行七十稀，五樹梅花廿一支，七子團圓正半月，除百零五便得知」**

$$70 \times 2 \qquad 21 \times 3 \qquad 15 \times 2 \qquad \div 105$$

$$70 \times 2 + 21 \times 3 + 15 \times 2 = 233$$
$$233 \div 105 \ldots 23$$
$$x = 23$$
$$x = 23 + 105k,\ k = 0, 1, 2, 3 \ldots$$

答曰：23

「術曰：三三數之剩二，置一百四十；五五數之剩三，置六十三；七七之數剩二，置三十。 并之得二百三十三。以二百一十減之，即得。 凡三三數之剩一，則置七十；五五數之剩一，則置二十一；七七數之剩一，則置十五。 一百六以上，以一百五減之，即得。」

「三歲孩兒七十稀，五留廿一事尤奇，
七度上元重相會，寒食清明便可知。」

# trial and error

$x \div 3 \ldots 2$ $x = 2, 5, 8, 11, 14, 17, 20, 23, 26\ldots$

$x \div 5 \ldots 3$ $x = 3, 8, 13, 18, 23, 28, 33, 38, 43\ldots$

$x \div 7 \ldots 2$ $x = 2, 9, 16, 23, 30, 37, 44, 51, 58\ldots$

$\Rightarrow x = 23+105k,\ k=0, 1, 2, 3,\ldots$

$105 = \{3, 5, 7\}$

Question: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

let $x = a+b+c$

$$\begin{cases} a \equiv 2 \pmod 3 \\ a \equiv 0 \pmod 5 \\ a \equiv 0 \pmod 7 \end{cases} \qquad \begin{cases} b \equiv 0 \pmod 3 \\ b \equiv 3 \pmod 5 \\ b \equiv 0 \pmod 7 \end{cases} \qquad \begin{cases} c \equiv 0 \pmod 3 \\ c \equiv 0 \pmod 5 \\ c \equiv 2 \pmod 7 \end{cases}$$

$a = 35k_1$ $\qquad$ $b = 21k_2$ $\qquad$ $c = 15k_3$

$3 \mid a-2 = 35k_1 - 2$ $\qquad$ $5 \mid b-3 = 21k_2 - 3$ $\qquad$ $7 \mid c-2 = 15k_3 - 2$

$k_1 = 1$ $\qquad$ $k_2 = 3$ $\qquad$ $k_3 = 2$

$35-2 = 33$ $\qquad$ $63-3 = 60$ $\qquad$ $30-2 = 28$

$\Rightarrow a = 35 \times 1$ $\qquad$ $\Rightarrow b = 21 \times 3$ $\qquad$ $\Rightarrow c = 15 \times 2$

$x = 35\times1 + 21\times3 + 15\times2 = 128$

( 歌訣：$70\times2 + 21\times3 + 15\times2$ )

$k_1=4$

$140\text{-}2 = 138$

$\Rightarrow a=35\times4$

# Chinese Remainder Theorem (C.R.T.)

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \quad \gcd(m,n) = 1$$

Question: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

# Chinese Remainder Theorem (C.R.T.)

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \qquad \gcd(m,n) = 1$$

Question:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

# Chinese Remainder Theorem (C.R.T.)

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \quad \gcd(m,n) = 1$$

Question:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

# Lemma: Bézout's Identity

Recall Bézout's Theorem:

$$if\ (m,n)=d,\ then\ \exists \alpha,\ \beta \in Z$$
$$s.t.\ d=\alpha m+\beta n$$

# Chinese Remainder Theorem (C.R.T.)

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \quad \gcd(m,n) = 1$$

1. $\because (m,n) = 1,$

   $\therefore \exists \alpha, \beta \in Z$ , $s.t.$ $\alpha m + \beta n = 1$ (by Bézout's lemma )

2. let $x = a + b$

$$\begin{cases} a \equiv p \pmod{m} \\ a \equiv 0 \pmod{n} \end{cases} \qquad \begin{cases} b \equiv 0 \pmod{m} \\ b \equiv q \pmod{n} \end{cases}$$

# Chinese Remainder Theorem (C.R.T.)

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \qquad \gcd(m,n) = 1$$

$$\alpha m + \beta n = 1$$

$$p\alpha m + p\beta n = p \Rightarrow \underbrace{p\beta n}_{a} = p - p\alpha m$$

$$q\alpha m + q\beta n = q \Rightarrow \underbrace{q\alpha m}_{b} = q - q\beta n$$

$$\Rightarrow x = a + b = p\beta n + q\alpha m$$

$$x = a + b$$

$$\begin{cases} a \equiv p \pmod{m} \\ a \equiv 0 \pmod{n} \end{cases} \qquad \begin{cases} b \equiv 0 \pmod{m} \\ b \equiv q \pmod{n} \end{cases}$$

*the general solution* : $x = p\beta n + q\alpha m + mnk,\ k \in Z$

# Chinese Remainder Theorem (C.R.T.)

$$\left.\begin{array}{l} x\equiv 2(\mathrm{mod}3) \\ x\equiv 3(\mathrm{mod}5) \end{array}\right] \quad (3,5)=1$$

$$x\equiv 2(\mathrm{mod}7)$$

(Euclidean Algorithm)

$5=3\cdot 1+2$

$3=2\cdot 1+1 \Rightarrow 1=3-2$

$=3-(5-3)$

$=\underset{\alpha}{2}\cdot 3+\underset{\beta}{(-1)}\cdot 5$

$$\begin{cases} x\equiv p(\mathrm{mod}\ m) \\ x\equiv q(\mathrm{mod}\ n) \end{cases} \quad \alpha m+\beta n=1$$

$$\Rightarrow x = p\beta n+q\alpha m$$

$$x = 2\cdot 3\cdot 3+(-1)\cdot 5\cdot 2=8$$

$$\Rightarrow x = 8+15k$$

$$\Rightarrow x\equiv 8(\mathrm{mod}\ 15)$$

# Chinese Remainder Theorem (C.R.T.)

$$\left.\begin{array}{l} x\equiv 8(\mathrm{mod}15) \\ x\equiv 2(\mathrm{mod}7) \end{array}\right]$$

$(15,7)=1$

(Euclidean Algorithm)

$15=7\cdot 2+1$

$\Rightarrow 1=15+(-2)\cdot 7$

$=1\cdot 15+(-2)\cdot 7$

$\alpha \quad \beta$

$$\begin{cases} x\equiv p(\mathrm{mod}\ m) \\ x\equiv q(\mathrm{mod}\ n) \end{cases} \quad \alpha m+\beta n=1$$

$$\Rightarrow x = p\beta n+q\alpha m$$

$$x = 1\cdot 15\cdot 2+(-2)\cdot 7\cdot 8$$

$$\Rightarrow x = -82+105k$$

$$\Rightarrow x = 23+105k$$

# Try It Yourself!

$$\begin{cases} x \equiv p \pmod{m} \\ x \equiv q \pmod{n} \end{cases} \quad \alpha m + \beta n = 1$$

$$\Rightarrow x = p\beta n + q\alpha m$$

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases} \Rightarrow \begin{cases} x \equiv 17 \pmod{35} \\ x \equiv 4 \pmod{11} \end{cases}$$

$$\Rightarrow x \equiv 367 \pmod{385}.$$

# The World of Modular Arithmetic

You can think of mod N as a **finite set** {0, 1, 2, 3,..., n-1}
No matter how you perform modular operations, the result will always fall within this set.

如mod 8 = {0, 1, 2, 3, 4, 5, 6, 7}

(1) A+B ：2+7 mod 8 = 9 mod 8 = 1 (exceeds 7, so it “wraps around”)
(2) A-B：2-7 mod 8 = -5 mod 8 = 3 (exceeds on the negative side, then wraps back)
(3) A×B：2x7 mod 8 = 14 mod 8 = 6 (again, wraps around)
(4) A÷B：2/7 mod 8 ...?

How do we perform division in modular arithmetic?

# Definition of a Group

In algebra, mathematicians must first specify which set they are working with and what operation is being performed on it. For example, we can define addition on integers or multiplication on positive real numbers.
This specification determines the space in which we perform algebraic reasoning.

A group is precisely such a combination of a **set and an operation**.

Formally, a group is a set G equipped with a binary operation +, forming an algebraic structure denoted by (G, +). Here, the operation + is a binary function that takes two elements of G and returns another element of G.

For instance, we usually write +(1, 2) = 3  simply as 1+2=3.

# Definition of a Group

Mathematicians define a group by specifying certain rules. A set G is called a group if it satisfies the following three group axioms:

**Associativity**: For all $a,b,c \in G$, $(ab)c = a(bc)$
**Identity Element**: There exists an element $e \in G$ such that for all $a \in G$, $ae=ea=a$
**Inverse Element**: For every $a \in G$, there exists a unique $b \in G$ such that $ab=e$
We call $b$ the inverse of $a$, and denote it by $b = a^{-1}$

Abelian Group - If, in addition, the operation satisfies the **commutative property**: For all $a,b \in G$, $ab=ba$, then $G$ is called an Abelian group.

# Definition of a Group

**Associativity**: $(ab)c=a(bc)$

**Identity Element**: $e$, $ae=ea=a$

**Inverse Element**: $ab=e$, $b$ it the inverse of $a$, noted as $b= a^{-1}$

**Commutativity**: For all $a,b \in G$, $ab=ba$

**Example: Integers under Addition$(Z,+)$**

**For all $a$, $b$, $\in Z$**

✓ Associativity: $(a+b)+c = a+(b+c)$

✓ Identity Element: $e$ =0 ，$a+e=e+a=a$

✓ Inverse Element: $a+b=e$=0，$b$= -$a$

✓ Commutativity: $a+b=b+a$

Therefore, $(Z,+)$ is a group, and it is Abelian (commutative).

# Definition of a Group

Added the rule of closure (the operation is closed, or the result is defined to stay within the set).

**This rule allows the equation ax = b to be solved for x. Why?**

By the inverse property, $a^{-1}$ exists.

Multiply both sides: $a^{-1}(ax) = a^{-1}b$

By associativity: $(a^{-1}a)x = a^{-1}b$

By the identity property: $ex = a^{-1}b$

Thus, $x = a^{-1}b$

# Definition of a Group

**Example: Real Numbers under Multiplication ($R, \cdot$)**
**For all $a$, $b$, $\in Z$**

**Associativity**: $(ab)c=a(bc)$

**Identity Element**: $e$, $ae=ea=a$

**Inverse Element**: $ab=e$, $b$ it the inverse of $a$, noted as $b=a^{-1}$

✓ Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

✓ Identity Element: $a \cdot e = e \cdot a = a$

✗ All nonzero numbers have inverses (ex. 3*1/3), but 0 has no inverse

**Commutativity**: For all $a,b \in G$, $ab=ba$

Therefore, multiplication of real numbers is not a group.

# Is the Mod N Set a Group?

Let’s go back to the **equivalence relation** we discussed at the beginning.

We have already defined the congruence relation (mod),

and now we can discuss its binary operations.

We will examine whether the **mod N** set forms a group under

addition and under multiplication.

*Note: In this context, the equivalence relation we use is the defined “≡” (congruence), not the ordinary “=” (equality).

mod 8 = {0, 1, 2, 3, 4, 5, 6, 7}

# Is Addition under mod N a Group?

**Associativity**: $(ab)c=a(bc)$

**Identity Element**: $e$, $ae=ea=a$

**Inverse Element**: $ab=e$, $b$ it the inverse of $a$, noted as $b=a^{-1}$

**Commutativity**: For all $a,b \in G$, $ab=ba$

**Addition under mod N(mod N,+), for all $a, b, c \in$ mod N :**

✓ Associativity: $(a+b)+c \equiv a+(b+c)$

✓ Identity Element: $e$ =0, $a+e \equiv e+a \equiv a$

✓ Inverse Element: $a+b \equiv 0$, $a^{-1} \equiv -a \equiv$ N-a

✓ Commutativity: $a+b \equiv b+a$

Therefore, (mod N, +) is a group,

and in fact an Abelian group (commutative group).

# Is Multiplication under mod N a Group?

**Associativity**: $(ab)c=a(bc)$

**Identity Element**: $e$, $ae=ea=a$

**Inverse Element**: $ab=e$, $b$ it the inverse of $a$, noted as $b= a^{-1}$

**Commutativity**: For all $a,b \in G$, $ab=ba$

**Multiplication under mod N(mod N, $\cdot$ ) for all $a, b, c \in$ mod N :**

✓ Associativity: $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c)$

✓ Identity Element: $e$ =1, $a \cdot e \equiv e \cdot a \equiv a$

✓ Inverse Element: $a \cdot b \equiv e \equiv 1$

$a^{-1}$??

✓ Commutativity: $a \cdot b \equiv b \cdot a$

Therefore, the multiplicative set (mod N, $\cdot$ ) is a group,

and it is an Abelian group (commutative).

# Modular Inverse $a^{-1}$

Ordinary division with integers:

$$7 \div 2$$

$$= 7 \times \frac{1}{2}$$

$$= 7 \times 2^{-1}$$

$$(7 \div 2) mod 5$$

$$= \left(7 \times \frac{1}{2}\right) mod 5$$

$$= (7 \times \underline{2^{-1}}) mod 5$$

must be converted into an integer

The result under modular arithmetic must be an integer

(within the mod N set).

# Modular Inverse $a^{-1}$

A modular inverse is similar to the concept of a reciproca:

$$2 \times \frac{1}{2} = 1$$

$$2 \times 3 \equiv 1 \, (mod 5)$$

$$= (7 \times 2^{-1}) mod 5$$

$$= (7 \times 3) mod 5$$

$$= 1$$

2 and 3 are modular inverses (reciprocals) of each other under mod 5.

# Modular Inverse $a^{-1}$

$$a^{-1} \equiv b \, (mod n)$$

$$ab \equiv 1 \, (mod n)$$

$$ab \, mod n = 1$$

# Find the Modular Inverse

$$2^{-1} mod 7 = ?$$

$$(2 \times 4) mod 7 = 1$$

The modular inverse of 2 under mod 7 is 4.

The modular inverse of a number can be different under different mod N.

$$
\begin{aligned}
&(3^{-8} \times 3^{5}) mod 5 \\
&= 3^{-3} mod 5 \\
&= \left(3^{-1}\right)^{3} mod 5 \\
&= 2^{3} mod 5 \\
&= 8 mod 5 \\
&= 3
\end{aligned}
$$

# Modular Inverse $a^{-1}$

Note 1: The modular inverse under mod n must be smaller than n.

$2 \cdot 3 \equiv 1 \pmod 5$ ; $2 \cdot 8 \equiv 1 \pmod 5 \rightarrow$ 3 is the only valid one (the inverse under mod n must be smaller than n)

Note 2: For any a under mod n, the modular inverse $a^{-1}\ \left(1 \leqslant a^{-1} < n\right)$ is unique.

Note 3: The condition for the existence of a modular inverse is: gcd(a, n) = 1

(for example, for $2 \cdot x \equiv 1 \pmod 4$, there is no solution for x)

# Modular Inverse $a^{-1}$

Note 3: The condition for the existence of a modular inverse is: gcd(a, n) = 1

Let $gcd\,(a, n) = d \quad (d > 1)$

Assume $a^{-1} = b$, then $ab \equiv 1\,(mod n)$

which implies $ab = qn + 1$

$$ab - qn = 1$$

Since $d \,|a$ and $d \,|n$

we have $d \,|1$, which is a contradiction.

Therefore, the assumption does not hold.

# Modular Inverse $a^{-1}$

Note 2: The modular inverse of a under mod n is unique.

Assume b and c are both modular inverses of a under mod n:

$$a \cdot b \equiv 1 \pmod{n}$$

$$a \cdot c \equiv 1 \pmod{n}$$

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

Cancelling $a$ on both sides ($a$ and $n$ are coprime , since $a$ has an inverse),

we get $b \equiv c \pmod{n}$

Therefore, the modular inverse is **unique**.

# Modular Inverse $a^{-1}$

When the numbers are large, how can we find the modular inverse?

We can use the **Extended Euclidean Algorithm**.

$\because (m,n) = 1,$

$\therefore \exists \alpha, \beta \in Z \text{ , } s.t. \ \alpha m + \beta n = 1$ (by Bézout's lemma )

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

$\alpha a + \beta n = 1$

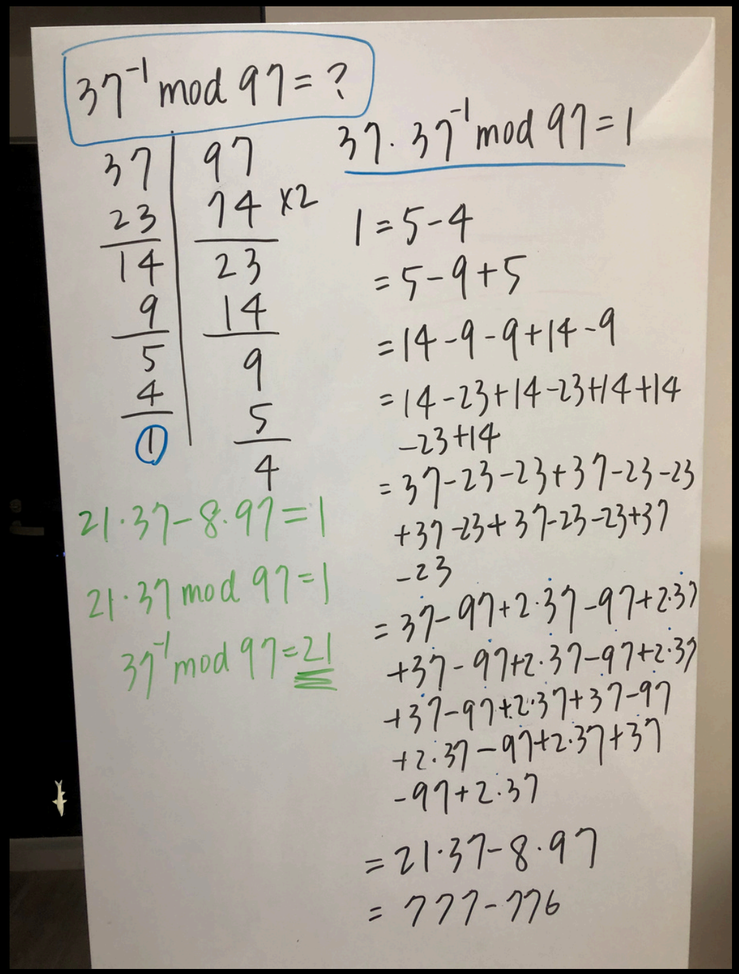
$\alpha a \equiv 1 \pmod{n}$

Therefore, $\alpha$ is the modular inverse element of $a$, i.e. $\alpha = a^{-1}$

$$37^{-1} mod 97 = ?$$

When the numbers are large, how can we find the modular inverse?

We can use the **Extended Euclidean Algorithm**.



# Modular Inverse $a^{-1}$

Take mod 8 as an example:

Addition group under mod 8: {0, 1, 2, 3, 4, 5, 6, 7}

Multiplication group under mod 8: {1, 3, 5, 7}

↑ Inverses (1,1) (3,3) (5,5) (7,7)

Take mod 9 as an example:

Addition group under mod 9: {0, 1, 2, 3, 4, 5, 6, 7, 8}

Multiplication group under mod 9: {1, 2, 4, 5, 7, 8}

↑ Inverses (1,1) (2,5) (4,7) (8,8)

# Modular Inverse $a^{-1}$

Take mod 5 as an example:

Multiplication group under mod 5: {1, 2, 3, 4}

Inverses (1,1) (2,3) (4,4) ↑

For a prime p, the multiplicative group is

{1, 2, 3, ⋯, p−2, p−1}

And every element can be

paired with its inverse.

Take mod 7 as an example:

Multiplication group under mod 7: {1, 2, 3, 4, 5, 6}

Inverses (1,1) (2,4) (3,5) (6,6) ↑

Will there be elements without pairs?

Yes — at the beginning (1) and the

end (p−1).

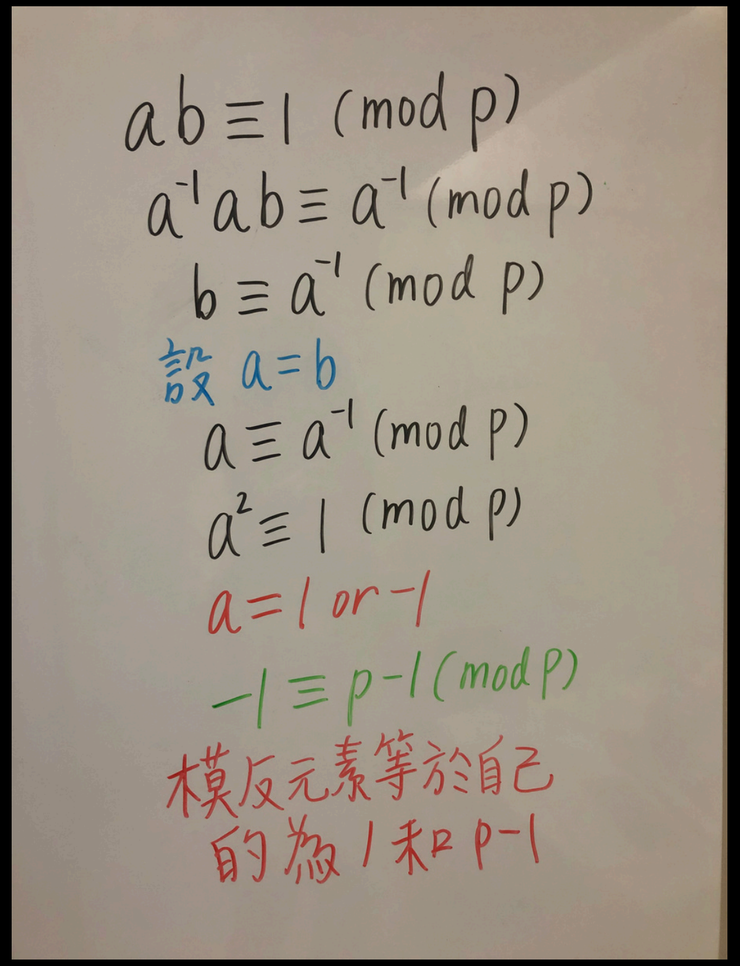
Take mod 11 as an example:

Multiplication group under mod 11: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

Inverses (1,1) (2,6) (3,4) (5,9) (7,8) (10,10) ↑

# Modular Inverse $a^{-1}$

Will there be elements that are not paired with their inverse?



Now let’s try multiplying all the elements together and see the result.

For example, using mod 5,

Multiplicative group mod 5: {1, 2, 3, 4}

↑ Inverses: (1) • (2 • 3) • (4) ≡ 1 • 1 • -1

Using mod 7,

Multiplicative group mod 7: {1, 2, 3, 4, 5, 6}

↑ Inverses: (1) • (2 • 4) • (3 • 5) • (6) ≡ 1 • 1 • 1 • -1

Using mod 11,

Multiplicative group mod 11: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

↑ Inverses: (1) • (2 • 6) • (3 • 4) • (5 • 9) • (7 • 8) • (10)

≡ 1 • 1 • 1 • 1 • 1 • -1

# Wilson's theorem

For a prime p, the multiplicative group is {1, 2, 3,..., p-2, p-1}.

When all elements are multiplied together modulo p, the result is -1.

That is, (p-1)! \mod p = -1.

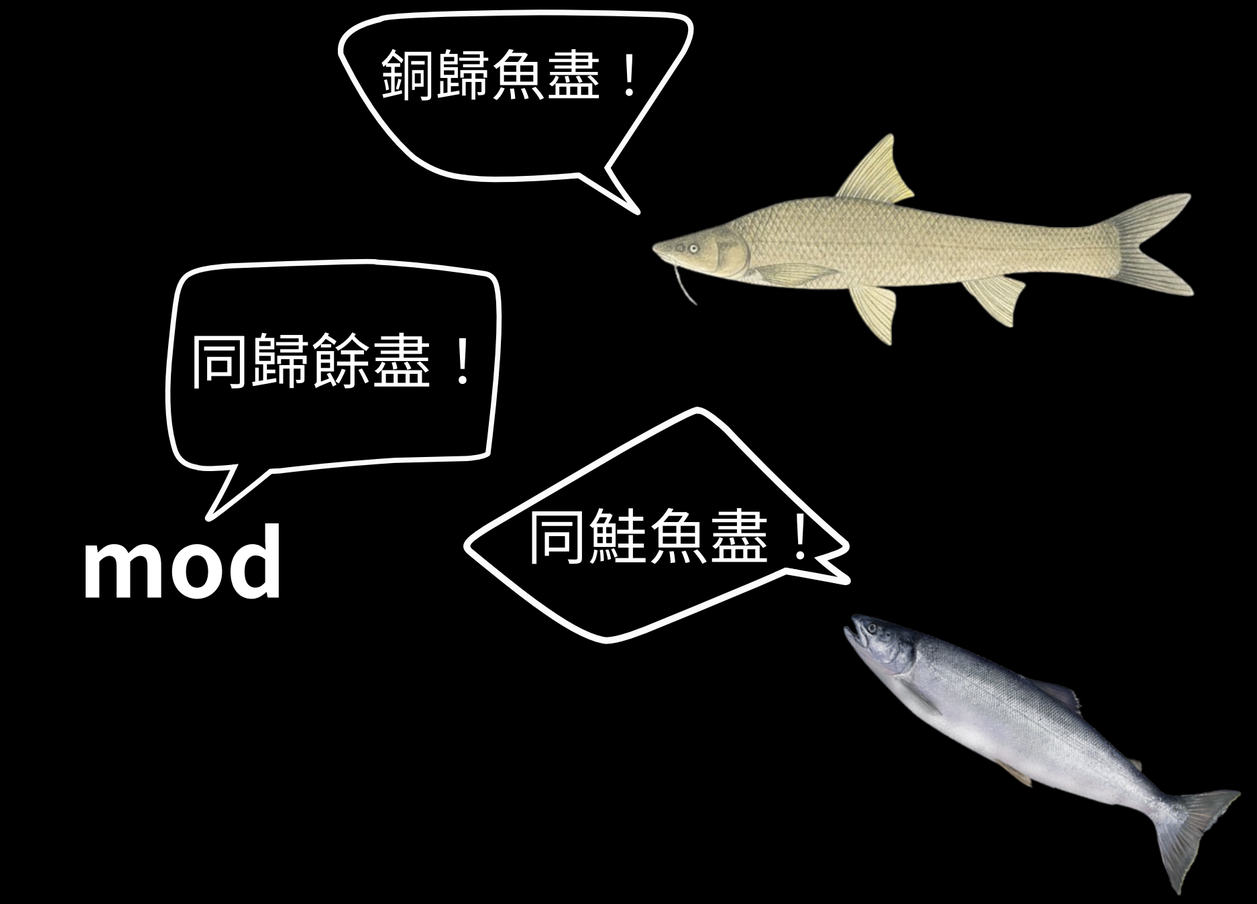
$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

$$p \mid (p-1)! + 1$$

# Applications of Congruence in Everyday Life

- Time and calendar calculations
- Music: the twelve-tone equal temperament (mod 12)
- Cryptography (RSA, key exchange, ⋯)
- Error-correcting codes
- ⋯

# Thanks for listening!



# References


- Bronze Gudgeon — Wikipedia: https://reurl.cc/gG6lV4
- Equivalence Relation — bilibili: https://reurl.cc/xavXYN
- Basic Concept of Congruence — 許介彥: https://reurl.cc/GjplZp
- Modular Inverse & Bézout’s Lemma — 章耕魚: https://reurl.cc/mMyN6j
- Korean Ping Pong Problem & Chinese Remainder Theorem https://reurl.cc/WxNV4O
- Chinese Remainder Theorem: https://reurl.cc/9v3ygv
- Definition of Group and Basic Concepts: https://reurl.cc/9v3QEj
- Modular Inverse — Wikipedia: https://reurl.cc/gG65jp
- Wilson’s Theorem: https://reurl.cc/6vde2y