CH 8 - Modular Arithmetics

Luke Lu • 2025-11-05

Basic Modular Arithmetics

🐳 **Info — Congruence and Modular Expression**

Let m be a fixed positive integer. For integers a and b, we say that a is **congruent** to b **modulo** m, and write

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

if and only if $m \mid (a - b)$. For integers a and b such that $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$. We refer to $\equiv$ as **congruence**, and m as its **modulus**.

$$a \equiv b \pmod{m} \Longleftrightarrow m \mid (a - b) \Longleftrightarrow \exists k \in \mathbb{Z}, a - b = km \Longleftrightarrow \exists k \in \mathbb{Z}, a = km + b$$

Examples:

1. $6 \equiv 18 \pmod{12} : 6 - 18 = -12, 12 \mid -12$
2. $73 \equiv 1 \pmod{2} : 13 - 1 = 72, 2 \mid 72$
3. $5 \equiv 1 \pmod{4} : 5 - 1 = 4, 4 \mid 4$
4. $24 \equiv 0 \pmod{24} : 24 - 0 = 24, 24 \mid 24$
5. $-5 \equiv 7 \pmod{12} : -5 - 7 = -12, 12 \mid -12$

🐳 **Info — Equality Properties**

1. Reflexivity: $\forall a \in \mathbb{Z}, a = a$
2. Symmetry: $\forall a, b \in \mathbb{Z}, a = b \Longrightarrow b = a$
3. Transitivity: $\forall a, b, c \in \mathbb{Z}, a = b \land b = c \Longrightarrow a = c$

🐳 **Info — Congruence Relations**

$\forall a, b, c \in \mathbb{Z}$

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m} \land b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

🐳 Info — Basic Modular Operations

$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $\forall n \in \mathbb{N}$, if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$ then

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$
2. $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$
3. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$
4. $a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b_n \pmod{m}$
5. $a_i \equiv b_i \Longrightarrow a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \pmod{m}$
6. $\forall a, b \in \mathbb{Z}$ if $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$
7. $\forall a, b, c \in \mathbb{Z}$, if $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

Proof

$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$ where $a_1 \equiv b_1 \pmod{m}$ and$a_2 \equiv b_2 \pmod{m}$

1. $a_1 + a_2 - b_1 - b_2 = a_1 - b_1 + a_2 - b_2 \pmod{m}$.

   Since $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2$, therefore $m \mid (a_1 - b_1)$ and $m \mid (a_2 - b_2)$.

   By DIC $m \mid (a_1 - b_1 + a_2 - b_2) \equiv m \mid (a_1 + a_2 - (b_1 + b_2))$.

   By definition of Congruence, $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$
2. $a_1 - a_2 - b_1 + b_2 = a_1 - b_1 + a_2 - b_2 \pmod{m}$.

   Since $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, therefore $m \mid (a_1 - b_1)$ and $m \mid (a_2 - b_2)$.

   By DIC $m \mid (a_1 - b_1 - a_2 + b_2) \equiv m \mid (a_1 - a_2 - (b_1 - b_2))$.

   By definition of Congruence, $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$
3. Since $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$,

   therefore $\exists k, l \in \mathbb{Z}$ s.t. $a_1 = km + b_1; a_2 = lm + b_2$.

   $a_1 b_1 - b_1 b_2 = (km + b_1)(lm + b^2) - b_1 b_2 = klm^2 + kmb_2 + b_1 lm + b_1 lm + b_1 b_2$

   $(klm + kb_2 + b_1 l) \cdot m \Longrightarrow m \mid (klm + kb_2 + b_1 l)$.

   Hence, $a_1 a_2 \equiv b_1 b_2 \pmod{m}$

$\square$

Examples:

1. Is $5^9 + 62^{2000} - 14$ divisible by 7

   $5^9 + 62^{2000} - 14 \equiv 0 \pmod{7}$

   $5^9 + 62^{2000} \equiv 0 \pmod{7}$ since $14 \equiv 0 \pmod{7}$

   $(5^2)^4 \cdot 5 + (-1)^{2000} \equiv 0 \pmod{7}$ since $62 \equiv -1 \pmod{7}$ because $62 - (-1) = 63, 7 \mid 63$

   $4^4 \cdot 5 + 1 \equiv 0 \pmod{7}$ since $25 \equiv 4 \pmod{7}$

   $2^2 \cdot 5 + 1 \equiv 0 \pmod{7}$ since $7 \mid (16 - 2)$

   $21 \equiv 0 \pmod{7}$ since $7 \mid 21$

   $\therefore 5^9 + 62^{2000} - 14 \equiv 0 \pmod{7}$ since $7 \mid 5^9 + 62^{2000} - 14$, meaning, $5^9 + 62^{2000} - 14$ is divisible by 7.

2. Illustration of Congruence Divide
   $3 \equiv 27 \pmod{6}$
   $3 \cdot 1 \equiv 3 \cdot 9 \pmod{6}, 1 \not\equiv 9 \pmod{6}$ since $\gcd(3, 6) \neq 1$

Congruence and Remaidners

> 🐳 **Info — Congruent Iff Same Remainder**
>
> $\forall a, b \in \mathbb{Z}, a \equiv b \pmod{m}$ if and only if a and b have the same remainder when divided by m

> 🐳 **Info — Congruent to Remainder**
> $\forall a, b \in \mathbb{Z}$ with $0 \leq b < m, a \equiv b \pmod{m}$ if and only if a has a remainder b when divided by m

Examples:

1. What is the remaidner when $77^{100} \cdot 999 - 6^{83}$ divided by 4?
   $77 \equiv 1 \pmod{4}$
   $999 \equiv -1 \pmod{4}$
   $6 \equiv 2 \pmod{4}$
   $\equiv 1^{100} \cdot -1 - 2^{83} \pmod{7}$
   $\equiv -1 - 2^{82} \cdot 2 \equiv -1 - 2(4)^{41} \equiv -1 - 2(0) \equiv -1 \pmod{4}$

   By CTR $3 \equiv -1 \pmod{4}$, the remainder is 3

> 💡 **Tip — Divisibility by 3**
> For all non-negative integers a, a is divisible by 3 if and only if the sum of the digits in the decimal representation of a is divisible by 3

Proof

Let a be non-negative integer and expressed as

$a = d_k 10^k + d_{k-1} 10^{d-1} + \ldots + d_1 10 + d_0$ where $0 \leq d_i \leq 9$ are the digit $\forall i \in \mathbb{N} \cup \{0\}$

Notice $10 \equiv 1 \pmod{3}$

$a \equiv d_k 1^k + d_{k-1} 1^{d-1} + \ldots + d_1 1^1 + d_0 \pmod{3}$

$a \equiv \sum_{i=0}^{k} d_i \pmod{3}$

Assume a is divisible by 3, then $3 \mid (a - 0) \iff a \equiv 0 \pmod{3}$.

Since $a \equiv \sum_{i=0}^{k} d_i \pmod{3} \overset{\text{by CER}}{\iff} \sum_{i=0}^{k} d_i \equiv 0 \pmod{3}$

Hence $3 \mid \sum_{i=0}^{k} d_i$

$\square$

💡 **Tip — Divisibility by 11**
For all non-negative integers a, $11 \mid a$ if and only if $11 \mid (S_e - S_o)$ where

- S_e is the sum of all even digits of a in the decimal representation
- S_o is the sum of all odd digits of a in the decimal representation

💡 **Tip — Mod 7 or 13**

7. Remove last digit d, subtract $2d$, repeat.
13. Remove last digit d, add $4d$, repeat.

Linear Congruences

🐳 **Info — Definition or Linear Congruences**
A relation of the form

$$ax \equiv c \pmod{m}$$

is called a **linear congruence** in the variable x. A solution to such linear congruence is an integer x_0 s.t.

$$ax_0 \equiv c \pmod{m}$$

🐳 **Info — Linear Congruence Theorem**
For all integers a, c where $a \neq 0$, the linear congruence

$$ax \equiv c \pmod{m}$$

has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$. Moreover, if $x = x_0$ is one particular solution to this congruence, then the set of all solutions is given by

$$\left\{x \in \mathbb{Z} : x \equiv x_0 \left(\operatorname{mod} \frac{m}{d}\right)\right\}$$

or alternatively

$$\left\{x \in \mathbb{Z} : x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d} \pmod{m}\right\}$$

Examples:

1. $4x \equiv 5 \pmod{3}$
   $\gcd(a, m) = \gcd(4, 3) = 1, 1 \mid 5$
   By LCT, there is a solution
   $4x \equiv 5 \equiv 2 \equiv 8 \pmod{3} \Longrightarrow 4x = 8 \Longrightarrow x = 2$
   and $3 \mid (8 - 5)$
   By LCT, all solutions are $\{x \in \mathbb{Z}, x \equiv 2 \pmod{3}\}$.

2. $4x \equiv 8 \pmod{12}$
   $\gcd(a, m) = \gcd(4, 12) = 4, 4 \mid 8$
   By LCT, there is a solution
   $4x \equiv 8 \equiv 4(2) \pmod{12} \Longrightarrow 4x = 8 \Longrightarrow x = 2$
   and $4 \mid 4 \mid (8 - 8)$
   By LCT, all solutions are $\{x \in \mathbb{Z}, x \equiv 2 \pmod{3}\}$
   or $\{x \in \mathbb{Z}, x \equiv 2, 5, 8, 11 \pmod{12}\}$

Non-linear Congruences

💡 **Tip** — Non-linear congruences do not have theorems that directly helps solving. The solutiosn generally are by brute force

Examples:

$x^2 \equiv 6 \pmod{10}$

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$x^2 \pmod{10}$	0	1	2	9	6	5	6	9	4	1

Hence $x \equiv 4, 6 \pmod{10}$

Congruence Classes and Modular Arithmetic

🐳 **Info — Congruence class**

The **congruence class** modulo m of the integer a is the set of integers

$$[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}$$

🐳 **Info — Modular Arithmetic**

We define $\mathbb{Z}_m$ to be the set of m congruence classes

$$\mathbb{Z}_m = \{[0], [1], [2], ..., [m - 1]\}$$

and we define two operations on $\mathbb{Z}_m$, **addition** and **multiplication**, as follows:

$$[a] + [b] = [a + b)]$$

$$[a][b] = [ab]$$

When we apply these operations on the set $\mathbb{Z}_m$, we are doing that is known as **modular arithmetic**

Info — Basic Properties of Congruence Classes

For all $[a] \in \mathbb{Z}_m$

1. $[a] + [0] = [a]$
2. $[a][0] = [0]$
3. $[a] + [-a] = [0]$
4. $[a][1] = [a]$

Example:

Construct a table for $\mathbb{Z}_4$
That is $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$

Addition table

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Multiplicaiton table

$*$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Info — Modular Arithmetic Theorem

For all integers a and c, with a non-zero, the equation

$$[a][x] = [c]$$

in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$, where $d = \gcd(a, m)$. Moreover, when $d \mid c$, there are d solutions, given by

$$[x_0], \left[x_0 + \frac{m}{d}\right], \left[x_0 + 2\frac{m}{d}\right], \ldots, \left[x_0 + (d-1)\frac{m}{d}\right]$$

where $x = [x_0]$ is one particular solution

Info — Inverse to $\mathbb{Z}_m$

Let a be an integer with $1 \leq a \leq m - 1$. The element $[a]$ in $\mathbb{Z}_m$ has a multiplicative inverse if and only if $\gcd(a, m) = 1$. Moreover, when $\gcd(a, m) = 1$, the multiplicative inverse is unique.

🐳 **Info — Inverse to $\mathbb{Z}_p$**

For all prime numbers p and non-zero element $[a]$ $\mathbb{Z}_p$ the multiplicative inverse $[a]^{-}1$ exists and is unique

Examples:

In $\mathbb{Z}_{10}$, solve the following:

1. $[12][x] + [3] = [8] = [2][x] + [3] = [8] \Longrightarrow [2][x] = [5] \overset{\text{by MAT}}{\Longrightarrow}$ No solutions
2. $[15][x] + [7] = [12] = [5][x] = [5] \overset{\text{by MAT}}{\Longrightarrow} [x] = [1]$

   Also by MAT, there are 5 solutions: $\{[1], [3], [5], [7], [9]\}$

🐳 **Info — Fermat's Little Theorem**

For all prime numbers p and integers a not divisible by p, we have

$$a^{p-1} \equiv 1 \pmod{p}$$

💡 **Tip** — Additional Corollaries

1. By FℓT, $[a]^{-}1 = [a]^{p-2}$
2. For all prime numbers p and integers a, we have

$$a^p \equiv a \pmod{p}$$