CH 8 - Modular Arithmetics

Luke Lu • 2025-10-27

🐳 **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**.

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

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: $\forall a, b \in \mathbb{Z}, a = b \implies b = a$
3. Transitivity: $\forall a, b, c \in \mathbb{Z}, a = b \land b = c \implies a = c$

🐳 **Info — Congruence Relations**

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

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

🐳 **Info — Modular Arithmetics**

$\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$ 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. $a_i \equiv b_i \implies a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \pmod{m}$
6. $\forall a, b \in \mathbb{Z}$ if $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$

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

$\square$