同餘 (Congruence)

一. Def Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, a and b are said to be "congruent modulo n"

if $n \mid a-b$ (n 整除 $a-b$) denoted by $a \equiv b \pmod{n}$ ($a \bmod n = b \bmod n$)

ex. $38 \equiv 14 \pmod{12}$, $38 \bmod 12 = 2$, $14 \bmod 12 = 2 \Leftrightarrow 12 \mid 38-14$

二. 性質

① $a \equiv a \pmod{n}$ (Reflexivity 反身性)

② If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$ (symmetry 對稱性)

③ If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$ (transivity 遞移性)

Let $a \equiv b \pmod{n}$, $a_1 \equiv b_1 \pmod{n}$, $a_2 \equiv b_2 \pmod{n}$

④ $a+k \equiv b+k \pmod{n}$ $\forall k \in \mathbb{Z}$

⑤ $k \cdot a \equiv k \cdot b \pmod{n}$ $\forall k \in \mathbb{Z}$

⑥ $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$

⑦ $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$

⑧ $a^k \equiv b^k \pmod{n}$ $\forall k \in \mathbb{N} \cup \{0\}$

三. 乘法模反元素. we set $\mathbb{Z}_n = 1, 2, 3, \cdots, n-1$

Def: Let $n \in \mathbb{N}$, $a \in \mathbb{Z}_n$, We say that $b \in \mathbb{Z}_n$ be "inverse of a under modular n"

if $a \cdot b \equiv 1 \pmod{n}$, denoted by $b \equiv a^{-1} \pmod{n}$. Remark: a, b 互為 inverse

ex. $3x \equiv 1 \pmod{7}$, $x = 5$ ※

Bézout's lemma:

$ax+by = m \Rightarrow m$ 是 $\gcd(a,b) \times n$, $n \in \mathbb{Z}$

Let $a, b \in \mathbb{Z}$, then $\exists\, x, y \in \mathbb{Z}$ s.t. $ax+by = \gcd(a,b) = d$

← 最大公因數

Pf. Let $S = \{ax+by \mid x, y \in \mathbb{Z}, ax+by > 0\} \Rightarrow S \subseteq \mathbb{N}$ (子集合) and $S \neq \phi$

$\exists\, m \in S$ s.t. $\forall c \in S$, $m \le c$ (Well-Ordered Principle)

Let $d = \gcd(a,b)$

2種證明

① d divides m, d 整除 m; Since $d \mid a$ and $d \mid b$, $d \mid ax+by$ $\forall x, y \in \mathbb{Z}$

$d \mid m$

$\Rightarrow d \mid ax$, $d \mid by$, $d \mid ax+by$

② m divides a suppose that $a = mq + r$, $0 < |r| < m$ ← 假設不整除

write $m = ax+by$ for some $x, y \in \mathbb{Z}$ Then $r = a - qm$

$\Rightarrow r = a - q(ax+by) = (1-qx)a + (-qy)b$ 矛盾 $\because r \in S$ but we set $m \in S$ and $m < r$ but we set $|r| < m$

假設 $|r| < m$ but 證出 $r \in S$, 但 m 已是 S 中最小的 so $r = 0 \Rightarrow m \mid a$

prop: Let $a \in \mathbb{Z}, n \in \mathbb{N}$ (s.t. 使得) (if only if)

"Multiplicative inverse of a under modul n" EXIST iff 'a' is a relatively prime of n pf. "$\Leftarrow$" By Bézout's Lemma.

$\exists\, x, y \in \mathbb{Z}$ s.t. $ax+ny = \gcd(a,n) \Rightarrow ax+ny=1 \Leftrightarrow ax \equiv 1 \pmod n$

"$\Rightarrow$" By assumption

$\exists\, x \in \mathbb{Z}$ s.t. $ax \equiv 1 \pmod n \Rightarrow \exists\, y \in \mathbb{Z}$ s.t. $ax+ny=1$

p.f. Let $d = \gcd(a,n)$ suppose that $d>1$ $\underbrace{\frac{a}{d}x+\frac{n}{d}y}_{\in \mathbb{Z}} = \underbrace{\frac{1}{d}}_{\notin \mathbb{Z}}$ 矛盾

so $d=1$ $\Rightarrow \gcd(a,n)=1$ ↗ n 質數 (1) ↘ a, n 可能為合數 (2)

---

(1) Fermat's Little Theorem:

Let $a \in \mathbb{Z}$, p is pime the $a^{p-1} \equiv 1 \pmod p \Rightarrow a \cdot a^{p-2} \equiv 1 \pmod p$

pf. Let $b = a-1$, then $(b+1)^p = C^p_0 b^p + \underbrace{C^p_1 b^{p-1} + \cdots}_{\bmod p = 0} + C^p_p \cdot 1$

$(b+1)^p \pmod p = b^p + 1$ $(\forall i \in \{1, 2, \cdots p-1\},\ C^p_i \equiv 0 \pmod p)$

$\equiv [(b-1)^p + 1] + 1 \pmod p \equiv \cdots \equiv (b-b)^p + (b+1) \pmod p$

$\equiv a \pmod p$

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

(2) Extend Euclidean Algorithm (Recall: Euclidean Algorithm (輾轉相除法))

Ex. $\gcd(23, 9)$: 由上到下, 再到上

$23 = 9 \times 2 + 5$	$\Rightarrow 5 = 23 + 9(-2)$	$1 = 5 + (4)(-1)$
$9 = 5 \times 1 + 4$	$\Rightarrow 4 = 9 + 5(-1)$	$1 = 5 + [9 + 5 \times (-1)] \times (-1)$
$5 = 4 \times 1 + 1$	$\Rightarrow 1 = 5 + 4(-1)$	$1 = 9 \times (-1) + 5 \times 2$
		$1 = 9 \times (-1) + [23 + 9(-2)](2)$
		$1 = 23 \times 2 + 9(-5)$

$\Rightarrow 23 \cdot \underline{2} \equiv 1 \pmod 9$

補充 $\boxed{\text{歐拉定理: } a^{\varphi(n)} \equiv 1 \pmod n}$

中国餘數定理 (Chinese Remainder Thm)

Recall: System of linear equations.

$$(S)\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = y_1 \\ a_{21}x_1 + \cdots + a_{2n}x = y_2 \\ \vdots \\ a_{nn}x_1 \cdots\cdots + a_{nn}x_n = y_n \end{cases}$$

一元線性同餘方程組

$$(S):\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Let $M = m_1 \cdot m_2 \cdots m_n$ and $M_i = M/m_i \ \forall i \in \{1, \dots, n\}$

If $\gcd(m_i, m_j) = 1 \ \forall 1 \le i < j \le n$ then $x = \sum_{i=1}^{n} a_i t_i M_i$, $t_i \equiv M_i^{-1} \pmod{m_i}$

$M_i t_i \equiv 1 \pmod{m_i}$

---

ex.

$$(S):\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases}$$

a_i m_i

$M = 2\cdot3\cdot5$; $M_1 = 15$, $M_2 = 10$, $M_3 = 6$

$t_1 = 1$, $t_2 = 1$, $t_3 = 1$

$\Rightarrow X = 34$

Pf: $\because \gcd(m_i, m_j) = 1 \ \forall 1 \le i < j \le n$

$\therefore M_i, m_i$ are co-prime $\Rightarrow t_i \equiv M_i \pmod{m_i}$ exit.

Let $i \in \{i, \dots, n\}$, then $a_i \cdot \underbrace{t_i \cdot M_i}_{\equiv 1} \equiv a_i \cdot 1 \pmod{m_i}$

$\forall j \in \{1, 2, \dots, n\} \setminus \{i\}$ 對於所有 $j \ne i$

$a_j \cdot t_j M_j \equiv 0 \pmod{m_i}$ $\because M_j \mid m_i$

$x = a_i t_i M_i + \sum_{j \ne i} a_j t_j M_j \Rightarrow \boxed{X \equiv a_i \pmod{m_i}}$