

Chinese Remainder theorem: (要懂得利用 Euclidean algorithm 求模反元素。
(中國餘數定理)

公式:

$$x \equiv \sum_{i=1}^n a_i M_i y_i \pmod{M}$$

example:

計算軍隊人數，3人為1列，餘2人；

5人為1列，餘3人；7人為1列，

餘2人，請問總共最少有多少人？

Ans.

Assume that total people is x .

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

$$\begin{array}{l} 1. \\ \Rightarrow a_1 = 2 \\ a_2 = 3 \\ a_3 = 2 \end{array}$$

2. 有3個質數: $n = 3$

$$\prod_{i=1}^3 p_i = M = 3 \times 5 \times 7 = 105$$

↓

$$M_1 = \frac{105}{3} = 35$$

3. 求模反元素:

$$(a) M_1 y_1 \equiv 1 \pmod{3}$$

$$M_2 = \frac{105}{5} = 21$$

\Rightarrow Euclidean algorithm:

$$M_3 = \frac{105}{7} = 15$$

$$\begin{array}{r} 35 = 11 \times 3 + 2 \\ 3 = 1 \times 2 + 1 \end{array}$$

$\therefore -1$ 為 35 的
模反元素。

$$y_1 = -1$$

$$\Rightarrow 1 = 3 - 1 \times 2$$

$$= 3 - 1 \times (35 - 11 \times 3)$$

$$= 3 - 35 + 11 \times 3 = (-1) \times 35 + 11 \times 3$$

變數解釋:

$x \rightarrow$ 所要求之數。

$n \rightarrow$ 被質數 mod 的個數。

$a_i \rightarrow x$ 被該質數得出的
餘數。

$$M_i \rightarrow \underbrace{\prod_{j=1}^n \text{prime}_j}_{\text{prime}} \quad \text{用 } M \text{ 代替}$$

$y_i \rightarrow M_i$ 的模反元素。

c)

$$M_2 y_2 \equiv 1 \pmod{5}$$

$$\Rightarrow 21 y_2 \equiv 1 \pmod{5}$$

\Rightarrow 依 Euclidean algorithm 求模反元素：

$$21 = 4 \times 5 + 1$$

$$1 = 21 - 4 \times 5$$

$$= 1 \times 21 + (-4) \times 5$$

$$\therefore y_2 = 1$$

(c)

$$M_3 y_3 \equiv 1 \pmod{7}$$

$$15 y_3 \equiv 1 \pmod{7}$$

\Rightarrow Euclidean algorithm

$$15 = 2 \times 7 + 1$$

$$\Rightarrow 1 = 15 - 2 \times 7$$

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

$$\Rightarrow y_3 = 1$$

Total people:

$$x = \sum_{i=1}^3 a_i M_i y_i$$

$$= 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1$$

$$= -70 + 63 + 30 = 23$$

$$\Rightarrow x \equiv 23 \pmod{M}, M = 3 \times 5 \times 7 = 105$$

\therefore 最少人數為 23 人

如求可能人數：

$$x_{\min} + \left(\prod_{i=1}^n p_i \right) \cdot m, m \in \mathbb{N}$$

這裡定義包含 0。

即：

$$23 + (3 \times 5 \times 7) \cdot m, m \in \mathbb{N}$$

$$\Rightarrow x = 23 + 105m, m \in \mathbb{N}$$

Example: 除數之間不互質，要拆解的情況：

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 8 \pmod{15} \end{cases} \rightsquigarrow \begin{array}{l} 2, 3, 15 \text{ 不互質} \\ 15 \text{ 需拆解。} \end{array}$$

Ans.

$$x \equiv 8 \pmod{\frac{15}{3 \times 5}} \rightarrow \begin{cases} x \equiv 8 \pmod{3} \\ x \equiv 8 \pmod{5} \end{cases} \Rightarrow \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$$

改寫題目：

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \quad a_1 = 1, a_2 = 2, a_3 = 3$$
$$M = 2 \times 3 \times 5 = 30$$
$$M_1 = 15, M_2 = 10, M_3 = 6$$

(a) 求 y_1 :

$$\underline{15} = 17 \times \underline{2} + \underline{1}$$

$$\Rightarrow 1 = 15 - 17 \times 2$$

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

$$\therefore y_1 = 1$$

(b) 求 y_2 :

$$\underline{10} = 3 \times \underline{3} + \underline{1}$$

$$\Rightarrow 1 = 10 - 3 \times 3$$

$$= 1 \times 10 + (-3) \times 3$$

$$\therefore y_2 = 1$$

(c) 求 y_3 :

$$\underline{6} = 1 \times \underline{5} + \underline{1}$$

$$\Rightarrow 1 = 6 - 1 \times 5$$

$$= 1 \times 6 + (-1) \times 5$$

$$\therefore y_3 = 1$$

$$x \equiv 1 \times 15 \times 1 + 2 \times 10 \times 1 + 3 \times 6 \times 1 = 53 \pmod{30}$$

$$\Rightarrow x \equiv 53 \equiv 23 \pmod{30} \#$$

Example: 搭配 Fermat's little theorem 問題：

求最小正整數 $3^{302} \pmod{385}$.

Hint:

Fermat's little theorem :

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

or

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

, a 和 p 互質

Ans. 將 385 分解為 $385 = 5 \times 7 \times 11$

Fermat's little theorem :

$$3^4 \equiv 1 \pmod{5}, 3^6 \equiv 1 \pmod{7}, 3^{10} \equiv 1 \pmod{11}$$

$$\Rightarrow 3^{302} \equiv (3^4)^{75} \cdot 3^2 \equiv 1^{75} \cdot 3^2 \equiv 4 \pmod{5}$$

$$3^{302} \equiv (3^6)^{50} \cdot 3^2 \equiv 1^{50} \cdot 3^2 \equiv 2 \pmod{7}$$

$$3^{302} \equiv (3^{10})^{30} \cdot 3^2 \equiv 1^{30} \cdot 3^2 \equiv 9 \pmod{11}$$

改寫題目：假設 $X = 3^{302}$

即：

$$\begin{cases} X \equiv 4 \pmod{5} \\ X \equiv 2 \pmod{7} \\ X \equiv 9 \pmod{11} \end{cases}$$

$$\begin{aligned} & a_1 = 4, a_2 = 2, a_3 = 9 \\ & M = 5 \times 7 \times 11 = 385 \end{aligned}$$

$$M_1 = 77, M_2 = 55, M_3 = 35$$

2.
(a) 求 y_1 , 即 M_1 的模反元素 =

\Rightarrow Euclidean algorithm:

$$77 = 15 \times \underline{5} + \underline{2}$$

$$5 = 2 \times 2 + 1$$

$$\Rightarrow 1 = 5 - 2 \times 2$$

$$= 5 - 2 \times (77 - 15 \times 5)$$

$$= 5 - 2 \times 77 + 2 \times 15 \times 5$$

$$= (-2) \times 77 + 31 \times 5$$

$$\therefore y_1 = -2$$

(b) 求 y_2 :

$$M_2 = 55 = 6 \times \underline{7} + \underline{6}$$

$$7 = 1 \times 6 + 1$$

$$\Rightarrow 1 = 7 - 1 \times 6$$

$$= 7 - 1 \times (55 - 6 \times 7)$$

$$= (-1) \times 55 + 7 \times 7$$

$$\therefore y_2 = -1$$

(c) 求 y_3 :

$$35 = 3 \times \underline{11} + \underline{2}$$

$$11 = 5 \times 2 + 1$$

$$\Rightarrow 1 = 11 - 5 \times 2$$

$$= 11 - 5(35 - 3 \times 11)$$

$$= (-5) \cdot (35) + 16 \times 11$$

$$\therefore y_3 = -5$$

$$X \equiv \sum_{i=1}^3 a_i M_i Y_i \equiv [4 \times 77 \times (-2)] + [2 \times 55 \times (-1)] + [9 \times 35 \times (-5)]$$

$$\equiv -2301 \equiv 9 \pmod{385}$$



這裡可以看成

$$-2301 + 385m \geq 0, m \in \mathbb{N}$$

$$\Rightarrow \text{猜 } m = 6 \Rightarrow -2301 + 2310 = 9$$

$$3^{302} \pmod{385} = 9 \quad \times$$