中国剩余定理

定理 $2'$：线性同余方程组

$$\begin{cases} x \equiv c_1 \ (mod \ m_1) \\ x \equiv c_2 \ (mod \ m_2) \\ \vdots \\ x \equiv c_s \ (mod \ m_s) \end{cases} \tag{1}$$

在 $mod \ M = m_1 m_2 \cdots m_s$ 意义下有唯一的解，其中 $m_1, m_2, \cdots, m_s$ 两两互素，$s \geq 2$，

证明：存在性：令 $n_i = \frac{M}{m_i}$

由 $m_1, m_2, \cdots, m_s$ 两两互素，知 $(n_1, m_i) = 1$

对 $1 \leq i \leq s, n_i y_i \equiv 1 \ (mod \ m_i)$ 有唯一解（标注：这里不知道为什么，待解决）

$y_i \equiv n_i^{-1} \ (mod \ m_i)$

可以验证 $x_0 \equiv c_1 n_1 y_1 + c_2 n_2 y_2 + \cdots + c_s n_s y_s \ (mod \ M)$ 满足方程组

例如，由于 $n_2, n_3, \cdots, n_s$ 都被 m_1 整除，故 $x_0 \equiv c_1 n_1 y_1 + 0 + \cdots + 0 \equiv c_1 n_1 y_1 \equiv c_1 \ (mod \ m_1)$

唯一性：假设 x 和 y 都满足这个线性同余方程组，则

$$\begin{cases} x - y \equiv 0 \ (mod \ m_1) \\ x - y \equiv 0 \ (mod \ m_2) \\ \qquad \vdots \\ x - y \equiv 0 \ (mod \ m_s) \end{cases} \tag{2}$$

由 $m_1, m_2, \cdots, m_s$ 两两互素，知 $m_1 m_2 \cdots m_s \mid x - y$

故 $x \equiv y \ (mod \ M)$

例：解同余方程组

$$\begin{cases} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{cases} \tag{3}$$

解： 已知 $c_1 = 2, c_2 = 3, c_3 = 2$

$m_1 = 3, m_2 = 5, m_3 = 7$

$M = 3 \times 5 \times 7 = 105$

$n_1 = 35, n_2 = 21, n_3 = 15$

解

$$\begin{cases} 35y_1 \equiv 1\ (mod\ 3) \\ 21y_2 \equiv 1\ (mod\ 5) \\ 15y_3 \equiv 1\ (mod\ 7) \end{cases} \tag{4}$$

得

$$\begin{cases} y_1 \equiv 2\ (mod\ 3) \\ y_2 \equiv 1\ (mod\ 5) \\ y_3 \equiv 1\ (mod\ 7) \end{cases} \tag{5}$$

$\therefore x_0 \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \equiv 233 \equiv 23\ (mod\ 105)$