

线性同余方程组解法（模数不互素）

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

其中 $(m_1, m_2) | (b_1 - b_2)$, 我们将 (m_1, m_2) 记作 d .

此方程组可以写作

$$x = m_1 k_1 + b_1 \tag{1}$$

$$x = m_2 k_2 + b_2$$

从而有

$$\begin{aligned} m_1 k_1 + b_1 &= m_2 k_2 + b_2 \\ m_1 k_1 &= (b_2 - b_1) + m_2 k_2 \\ m_1 k_1 &\equiv (b_2 - b_1) \pmod{m_2} \end{aligned} \tag{2}$$

因为 $(m_1, m_2) | (b_1 - b_2)$, 故方程(2)有解. 设 $b = b_2 - b_1$, 有

$$\frac{m_1}{d} k_1 \equiv \frac{b}{d} \pmod{\frac{m_2}{d}} \tag{3}$$

方程(3)有唯一解

$$k_1 \equiv \frac{b}{d} \cdot \left(\frac{m_1}{d}\right)^{-1} \pmod{\frac{m_2}{d}}$$

设 $K = \frac{b}{d} \left(\frac{m_1}{d}\right)^{-1}$, 于是方程(2)的解为

$$k_1 = K + \frac{m_2}{d} \cdot k$$

将其带入方程(1)，有

$$\begin{aligned}x &= m_1 k_1 + b_1 \\&= m_1 \left(K + \frac{m_2}{d} \cdot k \right) + b_1 \\&= m_1 K + b_1 + \frac{m_1 m_2}{d} \cdot k \\&= m_1 K + b_1 + [m_1, m_2] \cdot k\end{aligned}$$

故可得原方程组的解为

$$x \equiv m_1 K + b_1 \pmod{[m_1, m_2]}$$

$$\begin{cases} x \equiv 11 \pmod{36} \\ x \equiv 7 \pmod{40} \end{cases}$$

其中 $(m_1, m_2) = d = 4$.

此方程组可以写作

$$x = 36k_1 + 11 \tag{4}$$

$$x = 40k_2 + 7$$

从而有

$$36k_1 + 11 = 40k_2 + 7$$

$$36k_1 = (7 - 11) + 40k_2$$

$$36k_1 \equiv -4 \pmod{40} \tag{5}$$

从而有

$$\frac{36}{4}k_1 \equiv \frac{-4}{4} \pmod{\frac{40}{4}} \tag{6}$$

方程(3)有唯一解

$$K \equiv 1 \pmod{10}$$

于是方程(2)的解为

$$k_1 = 1 + 10k$$

将其代入方程(1), 有

$$\begin{aligned} x &= 36k_1 + 11 \\ &= 36(1 + 10k) + 11 \\ &= 47 + 360k \end{aligned}$$

故可得原方程组的解为

$$x \equiv 47 \pmod{360}$$