§1.4 中国剩余定理

Thm4.1 设$(a,m)=d$，则同余方程 $ax\equiv b \pmod m$ 有解的充要条件为 $d|b$，且当 $d|b$ 时，此同余方程模 m 有 d 个解.

证：若 $ax\equiv b \pmod m$ 有解 $x\equiv c\in\mathbb{Z}$，则 $ac\equiv b \pmod m$

$\therefore ac=b+ml \quad (l\in\mathbb{Z})$

$\because d|a \quad d|m \quad \therefore d|ac-ml=b$

若 $d|b$，则 $a=da'$，$b=db'$，$m=dm'$ $\quad (a',m')=1 \quad (a',b',m'\in\mathbb{Z})$

$\therefore ax\equiv b \pmod m$ 等价于 $a'x\equiv b' \pmod{m'}$

$\because (a',m')=1$

$\therefore a'x\equiv b' \pmod{m'}$ 有整数解 $x\equiv c \pmod{m'}$

但模 m' 的一个同余类 $x\equiv c \pmod{m'}$ 等于模 m 的 $d(=\frac{m}{m'})$ 个同余类，$x\equiv c+m'i \pmod m \quad (0\le i\le d-1)$

$\therefore$ 当 $d|b$ 时，同余方程 $ax\equiv b \pmod m$ 的解的个数为 d.

例：解同余方程 $30x\equiv 10 \pmod{34}$

解：$\because (30,34)=2 \quad 2|10$

$\therefore$ 同余方程有解

且等价于 $15x\equiv 5 \pmod{17}$

$\therefore x\equiv \frac{5}{15}\equiv\frac{1}{3}\equiv\frac{18}{3}\equiv 6 \pmod{17}$

$\therefore$ 模34的解有2个 $x\equiv 6, 23 \pmod{34}$

Th4.2 (Lagrange) 设 p 为素数，令 $n\ge 1$，而

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \quad (a_i\in\mathbb{Z}, p\nmid a_n)$$

则同余方程 $f(x)\equiv 0 \pmod p$ 模 p 至多有 n 个解.

证：当 $n=1$ 时，由 Thm4.1 知结论成立.

当 $n\ge 2$ 时，假设结论对 $n-1$ 成立.

设同余方程有 $r+1$ 个不同解 $x\equiv x_0, x_1, \cdots, x_r \pmod p$.

令 $y=x-x_0$，则 $f(x)$ 变成关于 y 的多项式：

$$g(y)=f(y+x_0)=a_n(y+x_0)^n+\cdots+a_1(y+x_0)+a_0.$$

$= a_n y^n + a'_{n-1} y^{n-1} + \cdots + a'_1 y + a'_0 \quad (a'_i \in \mathbb{Z})$

且 $g(y) \equiv 0 \pmod p$ 有 $r+1$ 个模 p 不同解.

$y \equiv 0, x_1 - x_0, x_2 - x_0, \cdots, x_r - x_0 \pmod p$

$\because 0 \equiv g(0) = a'_0 \pmod p$

$\therefore g(y) \equiv a_n y^n + a'_{n-1} y^{n-1} + \cdots + a'_1 y$

$\equiv y(a_n y^{n-1} + a'_{n-1} y^{n-2} + \cdots + a'_1) \pmod p$

由于 $y = x_i - x_0 \ (1 \le i \le r)$ 是 $g(y) \equiv 0 \pmod p$ 的解

从而 $(x_i - x_0) h(x_i - x_0) \equiv g(x_i - x_0) \equiv 0 \pmod p$

其中 $h(y) = a_n y^{n-1} + a'_{n-1} y^{n-2} + \cdots + a'_1$

$\because x_i - x_0 \not\equiv 0 \pmod p$ 可知 $h(x_i - x_0) \equiv 0 \pmod p$

即 $h(y)$ 有 r 个模 p 不同解 $y = x_i - x_0 \pmod p$

但 $h(y)$ 为 $n-1$ 次多项式

由归纳假设, $r \le n-1$, 知 $f(x) \equiv 0 \pmod p$ 的模 p 解数为 $r+1 \le n$.

注: 若 m 不是素数, 则 $f(x) \equiv 0 \pmod m$ 的模 m 解的个数可以多于 $f(x)$ 的次数. 例如: $x^2 \equiv 1 \pmod 8$ 的解有四个: $x \equiv 1, 3, 5, 7 \pmod 8$

Thm 4.5 (中国剩余定理) 设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数, 则对任意整数 $b_1, b_2, \cdots, b_k$, 一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \cdots \\ x \equiv b_k \pmod{m_k} \end{cases} \qquad \langle 7 \rangle$$

必有整数解, 并且全部解形成模 $m_1 m_2 \cdots m_k$ 的一个同余类.

证: 先考虑同余方程组 $\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_j} \quad (2 \le j \le k) \end{cases} \qquad \langle 8 \rangle$

由后 $k-1$ 个同余方程知 x 是 $m_j \ (2 \le j \le k)$ 的公倍数. 因为 $m_j \ (2 \le j \le k)$ 两两互素, 可知 x 是 $M_1 = m_2 m_3 \cdots m_k = \frac{m_1 m_2 \cdots m_k}{m_1}$ 的倍数.

令 $x = M_1 y$, 则同余方程 (8) 等价于 $M_1 y \equiv 1 \pmod{m_1} \qquad \langle 9 \rangle$

$\because y = N_1 \in \mathbb{Z}$ 是 $\langle 9 \rangle$ 的解, 则 $x = M_1 N_1$ 为 (8) 的解.

由 $(M_1, m_1)=1$ 可知，(9) 有解.

类似地，对每个 i $(1\le i\le k)$ 考虑同余方程组

$$\begin{cases} x\equiv 1 \pmod{m_i} \\ x\equiv 0 \pmod{m_j} \end{cases} \quad (1\le j\le k,\ j\ne i) \qquad (10)$$

令 $M_i = \dfrac{m_1 m_2 \cdots m_k}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$.

同余方程 $M_i y \equiv 1 \pmod{m_i}$ 有解 $y = N_i \in \mathbb{Z}$ （$\because (M_i, m_i)=1$）

而 $x = M_i N_i$ 即为 (10) 的解

现考虑整数 $A = b_1 M_1 N_1 + \cdots + b_k M_k N_k$

$\because M_i N_i \equiv 1 \pmod{m_i}$ $\quad M_i N_i \equiv 0 \pmod{m_j}$ $(j\ne i)$

$\therefore A \equiv b_i M_i N_i \equiv b_i \pmod{m_i}$ $\quad (1\le i\le k)$

$\therefore x = A$ 为原方程组的解

进而，若 $x = B$ 是 (7) 的解，则

$B \equiv b_i \equiv A \pmod{m_i}$ $\quad (1\le i\le k)$

则 $A - B \equiv 0 \pmod{m_i}$ $\quad (1\le i\le k)$

$\therefore A - B \equiv 0 \pmod{m_1 m_2 \cdots m_k}$

这表明原方程的全部解是模 $m_1 m_2 \cdots m_k$ 的一个同余类

$a \equiv A \pmod{m_1 m_2 \cdots m_k}$

例：解同余方程组 $\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7 \end{cases}$

解：$m_1=3$ $\quad m_2=5$ $\quad m_3=7$ 两两互素

$M_1 = 5\times 7 = 35$ $\quad M_2 = 3\times 7 = 21$ $\quad M_3 = 3\times 5 = 15$

$b_1 = 2$ $\quad b_2 = 3$ $\quad b_3 = 2$

$M_1 y \equiv 35 y \equiv 1 \pmod 3$ 取 $y = N_1 = 2$ $\quad M_1 N_1 = 70$

从而 $M_1 N_1$ 为 $M_1 = 5\times 7$ 的倍数且模 3 余 1

$M_2 y \equiv 21 y \equiv 1 \pmod 5$ 取 $y = N_2 = 1$ $\quad M_2 N_2 = 21$

$M_3 y \equiv 15 y \equiv 1 \pmod 7$ 取 $y = N_3 = 1$ $\quad M_3 N_3 = 15$

$x \equiv b_1 M_1 N_1 + b_2 M_2 N_2 + b_3 M_3 N_3$

$= 2\times 70 + 3\times 21 + 2\times 15 = 233 \equiv 23 \pmod{105}$

中国剩余定理的应用

1) 当 m 很大时，解同余方程组 $ax \equiv b \pmod m$ 常常困难，但若 $m = m_1 m_2 \cdots m_k$，且 $m_1, \cdots, m_k$ 两两互素，则此同余方程组等价于同余方程组 $ax \equiv b \pmod{m_i}$ $(1 \le i \le k)$，由于 m_i 比 m 小，每个 $ax \equiv b \pmod{m_i}$ 求解较容易，然后利用中国剩余定理.

2) m_i 不互素的时候如何解一元一次同余方程

例如：$\begin{cases} 5x \equiv 7 \pmod{12} & (1) \\ 7x \equiv 1 \pmod{10} & (2) \end{cases}$

$(10, 12) = 2 \ne 1$ 不能直接用中国剩余定理.

但 (1) 等价于 $\begin{cases} 5x \equiv 7 \pmod 3 \\ 5x \equiv 7 \pmod 4 \end{cases}$ 即 $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \end{cases}$

(2) 等价于 $\begin{cases} 7x \equiv 1 \pmod 2 \\ 7x \equiv 1 \pmod 5 \end{cases}$ 即 $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5 \end{cases}$

∴ 原方程组等价于 $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 2 \\ x \equiv 3 \pmod 5 \end{cases}$

由 $x \equiv 3 \pmod 4 \Rightarrow x \equiv 1 \pmod 2$

∴ 原方程组可进一步简化等价为

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

由中国剩余定理：

$$x \equiv b_1 M_1 N_1 + b_2 M_2 N_2 + b_3 M_3 N_3 \equiv 23 \pmod{60}$$

例：求 3^{193} 十进制的最后两位．这相当于求 $x\equiv 3^{193} \pmod{100}$，

$0\le x<100$，这个同余方程可化为方程组

$$\begin{cases} x\equiv 3^{193}\equiv 3 \pmod{4} & (3^2\equiv 1 \pmod{4}) \\ x\equiv 3^{193}\equiv 3^{13}\equiv -2 \pmod{25} & (\varphi(25)=20,\ 3^{20}\equiv 1 \pmod{25}) \end{cases}$$

用中国剩余定理：

$$x\equiv 3\times 25+(-2)\times(-24)=75+48\equiv 23 \pmod{100}.$$

即 $x=23$