一次同余方程（2）

1. 中国剩余定理

定理如图所示，注意前提互为素数

【定理3.2.1】 设$m_1, m_2, \dots, m_k$是两两互素的正整数. 那么, 对任意整数$b_1, b_2, \dots, b_k$, 一次同余方程组:

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \qquad\cdots \\ x \equiv b_k \pmod{m_k} \end{cases} \qquad (3.2.1)$$

必有解, 且解数为1. 并且有若令

$$M = m_1 m_2 \dots m_k, M_i = M/m_i \ (i=1,2,\dots,k).$$

则同余方程组（3.2.1）的解是

$$x \equiv M_1 M_1^{-1} b_1 + \cdots + M_k M_k^{-1} b_k \pmod{M}. \quad (3.2.2)$$

其中$M_i M_i^{-1} \equiv 1 \pmod{m_i}$ $(i=1,2,\dots,k)$.

2. 例题

【例3.2.1】 解“物不知数”问题. 即解一次同余方程组

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

> 解: 由题目可知，m1 = 3；m2 = 5；m3 = 7；
> 所以 M = m1 * m2 * m3 = 105
> 所以 M1 = M / m1 = 35；M2 = M / m2 = 21；M3 = M / m3 = 15
> 然后我们要求M1，M2，M3的逆元
> 由逆元的定义我们可列出以下式子

$M1 * M1^{-1} \equiv 1(mod m1)$；$M2 * M2^{-1} \equiv 1(mod m2)$；$M3 * M3^{-1} \equiv 1(mod m3)$

> 即35x ≡ 1 （mod 3）；21y ≡ 1（mod 5）；15z ≡ 1（mod 7）
> 化简得2x ≡ 1 （mod 3）；y ≡ 1（mod 5）；z ≡ 1（mod 7）
> 上述式子可直接求得y，z，现在要算x，x可以用欧几里得算法求得
> 所以可以得到M1，M2，M3的逆元
> 最后代入式子 （见上图）可以求得解

3. 例题2

计算$3^{1000}(mod 391)$

2.1.8】, 等价于求解一次同余方程组:

$$\begin{cases} x \equiv 3^{1000} \pmod{17} \\ x \equiv 3^{1000} \pmod{23} \end{cases}.$$

由欧拉定理, $3^{16} \equiv 1 \pmod{17}$, 故

$x \equiv 3^{1000} \pmod{17} \equiv 3^{16\times 62+8} \equiv 3^{8} \equiv 16 \equiv -1.$

由欧拉定理, $3^{22} \equiv 1 \pmod{23}$, 故

$x \equiv 3^{1000} \pmod{23} \equiv 3^{22\times 45+10} \equiv 3^{10} \equiv 8.$

即解一次同余方程组

$$\begin{cases} x \equiv 16 \equiv -1 \pmod{17} \\ x \equiv 8 \pmod{23} \end{cases}.$$

4. 一些性质（可拆分性质）

【定理3.2.2】 设$m_1, m_2, \ldots, m_k$两两互素, M=$m_1 m_2 \ \ldots\ m_k$, $f(x)$是整系数多项式. 则同余方程

$$f(x) \equiv 0 (\bmod M) \quad （3.2.5）$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \ (\bmod m_1) \\ f(x) \equiv 0 \ (\bmod m_2) \\ \qquad \cdots \\ f(x) \equiv 0 \ (\bmod m_k) \end{cases} \qquad （3.2.6）$$

等价. 且

5. 例题3

.

【例3.2.5】（模数$m_1, m_2, \ldots, m_k$不是两两互素）解同余方程组:

$$\begin{cases} x \equiv 3 (\bmod 8) \\ x \equiv 11 (\bmod 20). \\ x \equiv 1 (\bmod 15) \end{cases}$$

解: 这里$m_1 = 8, m_2 = 20, m_3 = 15$不两两互素, 所以不能直接用【定理3.2.1】求解. 容易看出, 本同余方程组的等价方程组为

$$\begin{cases} \quad x \equiv 3 (\bmod 8) \\ \begin{cases} x \equiv 11 (\bmod 4) \\ x \equiv 11 (\bmod 5). \end{cases} \\ \begin{cases} x \equiv 1 (\bmod 5) \\ x \equiv 1 (\bmod 3) \end{cases} \end{cases}$$

中国剩余定理- 扩展

满足第一个方程的x必满足第二个方程, 而第三, 四个方程是一样的. 因此, 原同余方程组和同余方程组

$$\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 3 \end{cases}$$

的解相同.

该同余方程组满足【定理3.2.1】的条件, 其解为

$$x \equiv -29 \pmod{120}$$

【例3.2.6】 解同余方程组

$$\begin{cases} x \equiv 3 \pmod 7 \\ 6x \equiv 10 \pmod 8 \end{cases}.$$

解: 这不是【定理3.2.1】中的同余方程组的形式. 容易得到第二个同余方程有解且解数为2: $x \equiv -1, 3 \pmod 8$.

因此, 原同余方程组的解就是以下两个同余方程组的解:

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv -1 \pmod 8 \end{cases} \qquad (3.2.9)$$

及

$$\begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 3 \pmod 8 \end{cases} \qquad (3.2.10)$$

容易求出, 同余方程组（3.2.9）的解是$x \equiv 31 \pmod{56}$； 同余方程组（3.2.10）的解是$x \equiv 3 \pmod{56}$.