第3章 一次同余方程

3.2 一次同余方程组

公元3～4世纪的《孙子算经》的“物不知数”问题: 今有物, 不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?

设物的总数为x, 则x满足

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

称为一次同余方程组.

中国剩余定理-来源

涉及同余方程组的问题在公元1世纪希腊数学家Nicomachus的著作出现过, 然而直到1247年, 秦九韶才在其著作《数书九章》中给出解线性同余方程组的一般方法. 此定理称为中国剩余定理, 或许因为秦九韶等中国数学家对方程组的解做出了贡献. 又因问题在《孙子算经》中提出, 故又称孙子定理.

中国剩余定理

【定理3.2.1】 设$m_1, m_2, \ldots, m_k$是两两互素的正整数. 那么, 对任意整数$b_1, b_2, \ldots, b_k$, 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

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

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

中国剩余定理-证明

先证唯一性, 即若同余方程组（3.2.1）有解 x_1, x_2, 则必有

$$x_1 \equiv x_2 \pmod{M}.$$

这是因为当x_1, x_2均是同余方程组（3.2.1）的解时, 必有

$$x_1 \equiv x_2 \pmod{m_i}, \quad i=1,2,\dots,k.$$

由于$m_1, m_2, \dots, m_k$两两互素, 由同余的性质即知 $x_1 \equiv x_2 \bmod M$, 唯一性成立.

中国剩余定理-证明

下面证由式（3.2.2）给出的

$$c = M_1 M_1^{-1} b_1 + \cdots + M_k M_k^{-1} b_k. \qquad （3.2.4）$$

是同余方程组（3.2.1）的解.

显见, $(m_i, M_i) = 1$, 所以满足式（3.2.3）的M_i^{-1}必存在. 由式（3.2.3）及$m_j | M_i (j \neq i)$知

$$c \equiv M_i M_i^{-1} b_i \equiv b_i \pmod{m_i},\ i=1, 2, \ldots, k.$$

即c是解.

中国剩余定理-例题

【例3.2.1】 解“物不知数”问题. 即解一次同余方程组

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

解: 已知$m_1=3, m_2=5, m_3=7$, 故

$M=3\cdot5\cdot7=105$, $M_1=35, M_2=21$, $M_3=15$.

解方程$M_iM_i^{-1} \equiv 1 \bmod m_i$, 求$M_i^{-1}(i=1,2,3)$:

中国剩余定理-例题

$35M_1^{-1}$≡1(mod 3), 即$2M_1^{-1}$≡1(mod 3), 得M_1^{-1}≡2(mod 3).

$21M_2^{-1}$≡1(mod 5), 即M_2^{-1}≡1(mod 5), 故M_2^{-1}≡1(mod 5).

$15M_3^{-1}$≡1(mod 7), 即M_3^{-1}≡1(mod 7), 故M_3^{-1}≡1(mod 7).

由式（2.2）得解为

$$x \equiv M_1 M_1^{-1} b_1 + \cdots + M_k M_k^{-1} b_k (\mathrm{mod}\, M)$$

≡35×2×2＋21×1×3＋15×1×2(mod 105)

≡233(mod 105)≡23(mod 105).

即物品数可能为$x = 23 + 105k$, (k≥0).

中国剩余定理-应用

【例3.2.3】 计算$3^{1000} \pmod{391}$.

分析: 一个直接的想法就是直接用模重复平方法进行计算. 不过, 注意到391=17×23是合数, $\varphi(391) = \varphi(17 \times 23) = 16 \times 22 = 352$, 由欧拉定理可知$3^{352} \equiv 1 \pmod{391}$, 故

$$3^{1000} \pmod{391} \equiv 3^{296+2\times352} \equiv 3^{296}.$$

但由模重复平方乘法知道, 计算$3^{1000} \pmod{391}$比计算$3^{296} \pmod{391}$只多一个循环.

中国剩余定理-应用

实际上, 令$x \equiv 3^{1000} \pmod{391}$, 由同余的性质【定理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

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

中国剩余定理-应用

由中国剩余定理, $m_1 = 17, m_2 = 23, M = 391, M_1 = 23, M_2 = 17.$

$M_1 M_1^{-1} \equiv 1 \pmod{17}$, 即$23 M_1^{-1} \equiv 1 \pmod{17}$. $M_1^{-1} \equiv 3 \pmod{17}$

$M_2 M_2^{-1} \equiv 1 \pmod{23}$, 即$17 M_2^{-1} \equiv 1 \pmod{23}$. $M_2^{-1} \equiv -4 \pmod{23}$.

方程组的解为 $x \equiv M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 \pmod{M}$, 代入数据并计算得

$x \equiv 23 \times 3 \times 16 + 17 \times 19 \times 8 \pmod{391} \equiv 169.$

也可以是$x \equiv 23 \times 3 \times (-1) + 17 \times 19 \times 8 \pmod{391} \equiv 169.$

还可以是$x \equiv 23 \times 3 \times (-1) + 17 \times (-4) \times 8 \pmod{391} \equiv 169.$

中国剩余定理-小模数

【例3.2.4】 求解方程组

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

解: 方程x≡1(mod 3)的解为A={…, 1, 4, 7, 10, 13, 16, …},
方程x≡5(mod 8)的解为B={…, 5, 13, 21, 29 …}, 而其共同解则为集合A与B的交, 即

A∩B={…, 13, …}.

所以x≡13(mod 24)是方程组的解.

【人物传记】 秦九韶(1202-1261), 字道古, 中国南宋数学家, 出生于中国四川省. 他有十年时间在于成吉思汗率领的蒙古军队作战的前线度过. 根据他的叙述, 他向一位隐士学习了数学. 在前线的日子里, 他研究了一些数学问题. 选取了其中的81个, 将其分为9部分, 写成了《数学九章》. 此书包括了线性同余方程组、中国剩余定理、代数方程、几何图形的面积、线性方程组等.

同余方程的解数

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

$$f(x) \equiv 0 \pmod{M} \quad （3.2.5）$$

与同余方程组

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

等价. 且

$$T(m;\ f) = T(m_1;\ f) \cdot \cdots \cdot T(m_k;\ f).$$

这里$T(m; f)$表示同余方程$f(x) \equiv 0(\mathrm{mod}\ m)$的解数.

证 由同余的性质知, 当$m_1, m_2, \dots, m_k$两两互素时,

$$f(x) \equiv 0 \pmod{M} \quad \begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \qquad \cdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases}$$

设方程

$$f(x) \equiv 0 \pmod{m_i} \qquad （3.2.7）$$

的解是$x \equiv b_i \bmod m_i, (i = 1,2, \dots, k)$, 则由中国剩余定理可求得一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \qquad \cdots \\ x \equiv b_k \pmod{m_k} \end{cases} \qquad （3.2.8）$$

的解为

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

因为

$$f(x) \equiv f(b_i) \equiv 0 (\operatorname{mod} m_i),\ (i = 1,2, \ldots, k).$$

故x也是方程（3.2.5）的解. 因此, 当b_i遍历$f(x) \equiv 0 (\operatorname{mod} m_i)$的所有解$(i = 1,2, \ldots, k)$时, x也遍历方程（3.2.5）的所有解, 即方程组（3.2.6）的解数为

$$T(m_1;\ f) \cdot \cdots \cdot T(m_k;\ f).$$

中国剩余定理- 扩展

【例3.2.4】 解一次同余方程$2^{2011}x \equiv 10 \pmod{77}$

因为$\varphi(77) = 60$, 由欧拉定理可得：$2^{60} \equiv 1 \pmod{77}$, 故

$2^{2011} \equiv 2^{60 \times 33+31} \equiv 2^{31} \pmod{77}$.

由模重复平方计算法的思路可得:

$2 \equiv 2 \pmod{77}$, $2^2 \equiv 4 \pmod{77}$, $2^4 \equiv 16 \pmod{77}$,

$2^8 \equiv 256 \equiv 25 \pmod{77}$, $2^{16} \equiv 625 \equiv 9 \pmod{77}$.

故$2^{31} = 2^{16} \times 2^8 \times 2^4 \times 2^2 \times 2 = 9 \times 25 \times 16 \times 4 \times 2 \equiv 2 \pmod{77}$.

即原同余方程等价于解同余方程$2x \equiv 10 \pmod{77}$.

中国剩余定理- 扩展

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

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

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

$$\begin{cases} x \equiv 3 \pmod 8 \\ \begin{cases} x \equiv 11 \pmod 4 \\ x \equiv 11 \pmod 5 \end{cases}. \\ \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 3 \end{cases} \end{cases}$$

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

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

注意到[8, 20, 15]=120, 所以这也就是原同余方程组的解, 且解数为1

中国剩余定理- 扩展

【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:

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

及

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

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$x \equiv 3 \pmod{56}$.

中国剩余定理- 扩展

【例3.2.7】 求下面同余方程组的解

$$\begin{cases} 3x + y \equiv 7 \pmod{23} & (1) \\ x + 2y \equiv 6 \pmod{23} & (2) \end{cases}$$

解: (1)×2 −(2)得$5x \equiv 8 \pmod{23}$.

因为(5,23)=1|8,方程有解且唯一, 解$5x \equiv 1 \pmod{23}$得$x \equiv 14 \pmod{23}$.

$5x \equiv 8 \pmod{23}$ 的解为x≡20(mod 23).

代入(1)得y≡16(mod23).

作业-3

作业 设a为自己的学号的后5位，求解同余方程组：

$$\begin{cases} ax \equiv 6 \pmod{19} \\ x \equiv a+5 \pmod{23} \end{cases}$$

作业(选做) 求解同余方程：

$$25x \equiv 60 \pmod{85}$$