第4章 同余方程

4.1 同余方程的基本概念
4.2 一次同余方程
4.3 一次同余方程组和中国剩余定理
4.4 模为素数的高次同余方程
4.5 模数为素数幂的同余方程
本章小结

4.1 同余方程的基本概念

4.1 同余方程的基本概念

设 $m, n \in N$ ，多项式 $f(x)=a_n x^n+\cdots+a_1 x+a_0$ ， 其中 $a_i \in Z(i=0,\cdots,n)$ 则 $f(x) \equiv 0 \bmod m$ （1.1）

称为模 m 的同余方程。若 $m \nmid a_n$，则称（1.1）的次数为 n，记为 $\deg f$。

若 $x=c$ 使（1.1）成立，则称之为（1.1）的解。此时与 c 模 m 同余的任一整数也是它的解。不同的解的个数称为它的解数。

显然，考虑（1.1）的解及其解数只需要在模 m 的一个完全剩余系中考虑。

例1.1 求方程 $4x^2+27x-12\equiv 0 \bmod 15$ 的解。

解 在多项式求值时，取完全剩余系为绝对最小完全剩余系时，将使计算简化。在模15的绝对最小完全剩余系 $-7,-6,\cdots,-1,0,1,\cdots,6,7$ 中直接演算知 $x=-6,3$ 是解。解数是2。

例1.2 求$4x^2+27x-9\equiv 0 \bmod 15$的解。

解 直接演算知该方程无解。

因为 $4x^2+27x-9\equiv x^2+3x-6 \bmod 15$， 所以 $4x^2+27x-9\equiv 0 \bmod 15$ 与 $x^2+3x-6\equiv 0 \bmod 15$ 的解和解数相同，但因第2式系数小，直接演算更为简单。一般地有：

定理1.1 （1）若 $f(x)\equiv g(x) \bmod m$ ，则（1.1）的解和解数与 $g(x)\equiv 0 \bmod m$ 相同，称这两个同余方程模 m 等价。

（2）若 $(a,m)=1$，则方程（1.1）的解和解数与方程 $af(x)\equiv 0 \bmod m$ 相同。特别地，当 $(a_n,m)=1$ 时，取 $a\equiv a_n^{-1} \bmod m$，可使（1.1）的首项系数变为1。

证明 简单，略去。

类似地，有同余方程组的概念。

记 $m_1,\cdots,m_k \in N$，$f_1(x),\cdots,f_k(x)$ 都为整系数多项式，则

$$\begin{cases} f_1(x) \equiv 0 \bmod m_1 \\ \cdots \\ f_k(x) \equiv 0 \bmod m_k \end{cases} \tag{1.2}$$

称为同余方程组。

若 $x=c$ 满足（1.2），则称之为（1.2）的解，此时与 c 模 $m=[m_1\cdots m_2]$ 同余的任一整数也是它的解。显然考虑（1.2）的解及解数只需在模 m 的一个完全剩余系中考虑。

4.2 一次同余方程

4.2 一次同余方程

若 $m \nmid a$ ，则方程

$$ax \equiv b \bmod m \quad (2.1)$$

称为一次同余方程。

若（2.1）有解，设为x_0，则存在$q \in Z$ ，使得 $ax_0 = b + qm$ 。

可得

$$(a, m) \mid b \quad (2.2)$$

即（2.2）是（2.1）有解的必要条件。

例如　$4x \equiv 2 \bmod 8$中，$(4,8) = 4 \nmid 2$，该方程一定无解。$3x \equiv 2 \bmod 8$中，$(3,8) = 1 \mid 2$，该方程可能有解，在模8的绝对最小剩余 $-3,-2,-1,0,1,2,3,4$ 中逐一验证知 $x=-2$ 是解，解数为1。$6x \equiv 2 \bmod 8$中，$(6,8) = 2 \mid 2$ ，在模8的绝对最小剩余系中逐一验证知$-1,3$ 是解，解数是2。可见方程（2.1）可能无解，也可能有解，有解时解数可能为1，也可能大于1。

下一定理说（2.2）式也是（2.1）式有解的充分条件。

定理2.1 设 $m \nmid a$，$d=(a,m)$，同余方程（2.1）有解的充要条件是$d \mid b$。在有解时，它的解数为d。又设x_0是

$$\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d} \quad (2.3)$$

的一个解，则（2.1）的 d 个解是 $x_0+\frac{m}{d}t \pmod m$，其中 t 为 $0,1,\cdots,d-1$。

证明 充分性由以下构造方法给出：

第1步： 由 $d|b$，得 $\frac{b}{d}$ 是整数，构造方程（2.3），显然 $(\frac{a}{d},\frac{m}{d})=1$。由第3章定理6.1的推论，（2.3）有解 $x_0 \equiv \frac{b}{d}(\frac{a}{d})^{-1} \bmod \frac{m}{d}$。

第2步： 方程 $ax \equiv b \bmod m$ 的全部解为 $x_0 + t\frac{m}{d}$，其中 $t \in Z$，这是因为 $a(x_0 + t\frac{m}{d}) = ax_0 + tm\frac{a}{d} \equiv ax_0 \bmod m$。又由于 $\frac{a}{d}x_0 \equiv \frac{b}{d} \bmod \frac{m}{d}$，得 $ax_0 \equiv b \bmod m$。所以 $a(x_0 + t\frac{m}{d}) \equiv b \bmod m$。

下面在全部解中求出模m不同余的解。

设$x_1 = x_0 + t_1\frac{m}{d}$，$x_2 = x_0 + t_2\frac{m}{d}$，则$x_1 - x_2 = (t_1 - t_2)\frac{m}{d}$，所以$m \mid x_1 - x_2$当且仅当$d \mid t_1 - t_2$。即$x_1 \not\equiv x_2 \bmod m$当且仅当$t_1 \not\equiv t_2 \bmod d$。所以$t$遍历模$d$的一个完全剩余系（可取为最小非负完全剩余系$0,1,\cdots,d-1$）就可得$ax \equiv b \bmod m$的全部解，即全部解有$d$个。 证毕。

推论 设 $(a, m)=1$，则方程 $ax \equiv b \bmod m$ 有唯一解 $x \equiv ba^{\varphi(m)-1} \bmod m$。

证明 由 $(a, m)=1 \mid b$ 及第3章定理6.1的推论得解。解的唯一性由 $(a, m)=1$ 得。

例2.1 解方程 $20x \equiv 15 \bmod 135$。

解 $d=(20,135)=5$，$5 \mid 15$，所以方程有5个解。构造方程 $4x \equiv 3 \bmod 27$，得解为 $3 \cdot 4^{\varphi(27)-1} \equiv 21 \bmod 27$。所以方程的5个解为 $21+t \cdot 27 \ (t=0,1,2,3,4)$，即 $21, 48, 75, 102, 129$。

4.3 一次同余方程组和中国剩余定理

4.3 一次同余方程组和中国剩余定理

中国剩余定理有2个用途：

（1）已知某个数关于一些两两互素的数的同余类，就可重构这个数。

（2）可将大数用小数表示、大数的运算通过小数实现。

例3.1 Z_{10}中每个数都可从这个数关于2和5（10的两个互素的因子）的同余类重构。比如已知 x关于2和5的同余类分别是[0]和[3]，即$x \bmod 2 \equiv 0, x \bmod 5 \equiv 3$。可知 x是偶数且被5除后余数是3，所以可得8是满足这一关系的唯一的 。

例3.2 假设只能处理5以内的数，则要考虑15以内的数，可将15分解为两个小素数的乘积，$15=3\cdot5$，将1到15之间的数列表表示，表的行号为0-2，列号为0-4，将1到15的数填入表中，使得其所在行号为该数除3得到的余数，列号为该数除5得到的余数。如 $12 \bmod 3=0, 12 \bmod 5=2$，所以12应填在第0行，第2列。如表3.1所示。

表3.1 1到15之间的数

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

用（0, 2）表示12。现在就可处理15以内的数了。

例如求$12\cdot 13\pmod{15}$，13所在的行号1、列号3，将13表示为（1, 3），由$0\cdot 1\equiv 0\bmod 3,\ 2\cdot 3\equiv 1\bmod 5$ 得 $12\cdot 13\pmod{15}$的小数表示是（0, 1），这个位置上的数是6，所以得$12\cdot 13\pmod{15}\equiv 6$。又因$0+1\equiv 1\bmod 3,\ 2+3\equiv 0\bmod 5$，所以12+13的小数表示是（1, 0），这个位置上的数是10，所以$12+13\equiv 10\bmod 15$。

以上两例是中国剩余定理的直观应用, 下面具体介绍定理的内容。

中国剩余定理最早见于《孙子算经》的“物不知数”问题：今有物不知其数，三三数之有二，五五数之有三，七七数之有二，问物有多少？

这一问题用方程组表示为：

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

下面给出解的构造过程。首先将三个余数写成和的形式$2+3+2$，为满足第一个方程，即模3后，后2项消失，给后2项各乘以3，得$2+3\cdot3+2\cdot3$。为满足第二个方程，即模5后，第一、三项消失，给第一、三项各乘以5，得$2\cdot5+3\cdot3+2\cdot3\cdot5$。同理给前2项各乘以7, 得$2\cdot5\cdot7+3\cdot3\cdot7+2\cdot3\cdot5$

然而，将结果带入第一方程，得到 $2\cdot5\cdot7$，为消去 $5\cdot7$，将结果的第一项再乘以 $(5\cdot7)^{-1}\bmod3$，得 $2\cdot5\cdot7\cdot(5\cdot7)^{-1}\bmod3+3\cdot3\cdot7+2\cdot3\cdot5$。类似地，将第二项乘以 $(3\cdot7)^{-1}\bmod5$，第三项乘以 $(3\cdot5)^{-1}\bmod7$，得结果为

$$2\cdot5\cdot7\cdot(5\cdot7)^{-1}\bmod3+3\cdot3\cdot7\cdot(3\cdot7)^{-1}\bmod5+2\cdot3\cdot5\cdot(3\cdot5)^{-1}\bmod7=233$$

又因为$233+k\cdot 3\cdot 5\cdot 7=233+105k$（$k$ 为任一整数）都满足方程组，可取 $k=-2$，得到小于$105\left(=3\cdot 5\cdot 7\right)$的唯一解23，所以方程组的唯一解构造如下：

$$\left[2\cdot 5\cdot 7\cdot (5\cdot 7)^{-1}\bmod 3+3\cdot 3\cdot 7\cdot (3\cdot 7)^{-1}\bmod 5+2\cdot 3\cdot 5\cdot (3\cdot 5)^{-1}\bmod 7\right]\bmod(3\cdot 5\cdot 7)$$

把这种构造法推广到一般形式，就是如下的中国剩余定理。

定理3.1（中国剩余定理） 设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，$M = \prod_{i=1}^{k} m_i$，则一次同余方程组

$$\begin{cases} x \bmod m_1 \equiv a_1 \\ x \bmod m_2 \equiv a_2 \\ \cdots \\ x \bmod m_k \equiv a_k \end{cases} \quad (3.1)$$

对模 M 有唯一解：

$$x \equiv \left(\frac{M}{m_1} e_1 a_1 + \frac{M}{m_2} e_2 a_2 + \cdots + \frac{M}{m_k} e_k a_k \right) \bmod M \quad (3.2)$$

其中 e_i 满足 $\frac{M}{m_i} e_i \equiv 1 \bmod m_i \quad (i = 1, 2, \cdots, k)$。

证明 设 $M_i = M/m_i = \prod_{\substack{\lambda=1 \\ \lambda \neq i}}^{k} m_\lambda \ (i = 1, 2, \cdots, k)$，由 M_i 的定义知 M_i 与 m_i 是互素的，因此 M_i 在模 m_i 下有唯一的乘法逆元，即满足 $\frac{M}{m_i} e_i \equiv 1 \bmod m_i$ 的 e_i 是唯一的。

下面证明对 $\forall i \in \{1, 2, \cdots, k\}$，上述 x 满足 $x \bmod m_i \equiv a_i$ 。

注意到当 $j \neq i$ 时，$m_i \mid M_j$，即 $M_j \equiv 0 \bmod m_i$。所以

$$\left(M_j \times e_j \bmod m_j\right) \bmod m_i \equiv \left(\left(M_j \bmod m_i\right) \times \left(\left(e_j \bmod m_j\right) \bmod m_i\right)\right) \bmod m_i \equiv 0$$

而 $\left(M_i \times \left(e_i \bmod m_i\right)\right) \bmod m_i \equiv \left(M_i \times e_i\right) \bmod m_i \equiv 1$。所以 $x \bmod m_i \equiv a_i$。

下面证明方程组的解是唯一的。设x'是方程组的另一解，即 $x' \equiv a_i \bmod m_i \ (i=1,2,\cdots,k)$。由 $x \equiv a_i \bmod m_i$ 得 $x'-x \equiv 0 \bmod m_i$，即 $m_i \mid (x'-x)$。再根据m_i两两互素，有$M \mid (x'-x)$，即 $x'-x \equiv 0 \bmod M$，所以$x' \bmod M = x \bmod M$ 证毕。

中国剩余定理提供了一个非常有用的特性，即在模 M（$M=\prod_{i=1}^{k} m_i$）下可将大数 由一组小数$(a_1,a_2,\cdots,a_k)$表达，且大数的运算可通过小数实现。表示为：

$$A \leftrightarrow (a_1,a_2,\cdots,a_k)$$

其中$a_i = A \bmod m_i \ (i=1,\cdots,k)$。有以下推论：

推论 如果

$$A \leftrightarrow (a_1, a_2, \cdots, a_k)\ ,\ B \leftrightarrow (b_1, b_2, \cdots, b_k)$$

那么

$$(A+B) \bmod M \leftrightarrow ((a_1+b_1) \bmod m_1, \cdots, (a_k+b_k) \bmod m_k)$$
$$(A-B) \bmod M \leftrightarrow ((a_1-b_1) \bmod m_1, \cdots, (a_k-b_k) \bmod m_k)$$
$$(A\times B) \bmod M \leftrightarrow ((a_1\times b_1) \bmod m_1, \cdots, (a_k\times b_k) \bmod m_k)$$

证明 可由模运算的性质直接得出。 证毕。

定理3.2 设 $m_1,\cdots,m_k$，M，$e_1,\cdots,e_k$ 与定理3.1相同。

$$x=\frac{M}{m_1}e_1x_1+\cdots+\frac{M}{m_k}e_kx_k \quad (3.3)$$

则当 x_i 遍历模 m_i 的完全（简化）剩余系时（$i=1,\cdots,k$），x遍历模 M 的完全（简化）剩余系。

证明 先证完全剩余系的情况，当 x_i 遍历模 m_i的完全剩余系时，x_i有 m_i个取值$(1\text{剟}i\quad k)$，因此 x有 M 个取值。下面证明这M个取值模M两两不同余。设 $x'=\frac{M}{m_1}e_1x_1'+\cdots+\frac{M}{m_k}e_kx_k'$

若 $x\equiv x'\bmod M$，则 $x\equiv x'\bmod m_i$, 从而得 $x_i\equiv x_i'\bmod m_i\ (1\leqslant i\leqslant k)$

再证简化剩余系的情况。由于简化剩余系中的元素是由完全剩余系中与模数互素的元素构成，所以只要证明$(x,M)=1$当且仅当 $(x_i,m_i)=1(1\leqslant i\leqslant k)$。由$(x,M)=1$得 $(x,m_i)=1(1\leqslant i\leqslant k)$否则，若$d=(x,m_i)\neq 1$，则$d\mid x$，$d\mid m_i$ 得$d\mid M$。d是x,M 的公因子，与$(x,M)=1$矛盾。

由$(x,m_i)=1$及（3.3）式得$x \bmod m_i \equiv x_i$，$x_i\in[x]_{m_i}$。由第3章定理3.1得 $(x_i,m_i)=(x,m_i)$，所以$(x_i,m_i)=1$。反之，若 $(x_i,m_i)=1(1\leqslant i\leqslant k)$，则 $x \bmod m_i \equiv x_i$，得 $(x,m_i)=(x_i,m_i)=1$ $(x,M)=1$。

证毕。

例3.1（续） 表4-1的构造：

设$1 \le x \le 15$，求$x \equiv a \bmod 3, x \equiv b \bmod 5$，将$x$填入表的$a$行、$b$列。表建立完成后，数$x$由它的行号$a$和列号$b$表示为$(a,b)$。由$(a,b)$及中国剩余定理可如下恢复：

$$x \equiv \left[a \cdot 5 \cdot \left(5^{-1} \bmod 3\right) + b \cdot 3 \cdot \left(3^{-1} \bmod 5\right)\right] \bmod 15$$

$$\equiv \left[a \cdot 5 \cdot 2 + b \cdot 3 \cdot 2\right] \bmod 15 \equiv \left[10a + 6b\right] \bmod 15$$

例如，$12 \bmod 3 \equiv 0, 12 \bmod 5 \equiv 2;\ 13 \bmod 3 \equiv 1, 13 \bmod 5 \equiv 3$。

所以12位于表中第0行、第2列，13位于表中第1行、第3列。

反之若求表中第0行、第2列的数，将 $a=0, b=2$ 带入

$x \equiv [10a+6b] \bmod 15$ 得 $x=12$。

已知 x 表示为 (a,b)，x的运算可用 (a,b) 实现。设

$x_1=(a_1,b_1),x_2=(a_2,b_2)$，则

$$x_1+x_2=(a_1+a_2,b_1+b_2),\ x_1\cdot x_2=(a_1\cdot a_2,b_1\cdot b_2)$$

例如 $12=(0,\ 2),13=(1,\ 3)$,

$$12+13=(0,\ 2)+(1,\ 3)=(1,\ 0),\ 12\cdot 13=(0,\ 2)\cdot(1,\ 3)=(0,\ 1)$$

所以 $12+13$ 为 10，$12\cdot 13$ 为 6。

例3.2　由以下方程组求 x

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 7 \end{cases}$$

解 $M = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, $M_1 = 105$,$M_2 = 70$, $M_3 = 42$, $M_4 = 30$ 。

易求 $e_1 \equiv M_1^{-1} \bmod 2 \equiv 1$, $e_2 \equiv M_2^{-1} \bmod 3 \equiv 1$, $e_3 \equiv M_3^{-1} \bmod 5 \equiv 3$

$e_4 \equiv M_4^{-1} \bmod 7 \equiv 4$ ，所以

$$x \equiv (105 \times 1 \times 1 + 70 \times 1 \times 2 + 42 \times 3 \times 3 + 30 \times 4 \times 5) \bmod 210 \equiv 173 \bmod 210$$

例3.3 为将 $973 \bmod 1813$ 由模数分别为37和49的两个数表示，可取

$$x = 973 \text{ ，} M = 1813 \text{ ，} \quad m_1 = 37 \text{ ，} \quad m_2 = 49 \text{ 。}$$

由 $a_1 \equiv 973 \bmod m_1 \equiv 11$ ，$a_2 \equiv 973 \bmod m_2 \equiv 42$ ，得 x 在模37和模49下的表达式为 $(11, 42)$。若要求 $973 \bmod 1813 + 678 \bmod 1813$ 可先求出 $678 \leftrightarrow (678 \bmod 37, 678 \bmod 49) = (12, 41)$ ，从而可将以上加法表达为 $((11+12) \bmod 37, (42+41) \bmod 49) = (23, 34)$ 。

例3.4 解方程 $19x \equiv 556 \bmod 1155$。

解 这是一次同余式，可按第2节的方法求解。但因模数1155较大，可按中国剩余定理变成模数较小的同余方程组。由1155=3·5·7·11及第三章定理1.9, 该方程与以下方程组等价。

$$\begin{cases} 19x \equiv 556 \bmod 3 \\ 19x \equiv 556 \bmod 5 \\ 19x \equiv 556 \bmod 7 \\ 19x \equiv 556 \bmod 11 \end{cases} \overset{(1)}{\Leftrightarrow} \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5 \\ 5x \equiv 3 \bmod 7 \\ 8x \equiv 6 \bmod 11 \end{cases} \overset{(2)}{\Leftrightarrow} \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 5 \\ x \equiv 2 \bmod 7 \\ x \equiv 9 \bmod 11 \end{cases}$$

由定理3.1即得 $x \equiv 394 \bmod 1155$。其中第（1）步由定理1.1的（2）得，第（2）步由一元同余式解出 $5x \equiv 3 \bmod 7$ 及 $8x \equiv 6 \bmod 11$得。注意第（1）步中得出的方程组不是定理3.1中的形式，不能直接用定理3.1。

例3.5 解同余方程组 $\begin{cases} x \equiv 3 \bmod 7 \\ 6x \equiv 10 \bmod 8 \end{cases}$。

解 解出一次同余式 $6x \equiv 10 \bmod 8$的解为 $x \equiv 3, 7 \pmod 8$，方程组等价于以下2个方程组：

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 3 \bmod 8 \end{cases} \quad \text{及} \quad \begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 7 \bmod 8 \end{cases}$$

分别由定理3.1得 $x \equiv 3, 31 \pmod{56}$。

注： $x \equiv 3, 7 \pmod 8$表示 $x \equiv 3 \bmod 8, x \equiv 7 \bmod 8$。以后常用这种简单记法。

例3.6 在第3章第6节的例6.2的RSA加密算法中，按照中国剩余定理，可将解密过程简化如下：解密者已知 p,q，计算 $d_p \equiv d \bmod (p-1)$，$d_q \equiv d \bmod (q-1)$，$a_p \equiv c^{d_p} \bmod p$，$a_q \equiv c^d \bmod q$。然后建立方程组

$$\begin{cases} x \equiv a_p \bmod p \\ x \equiv a_q \bmod q \end{cases}$$

由中国剩余定理求出 $x \bmod (pq)$ 即为明文 a。这是因为 $d_p = d + k\varphi(p)$，其中 $k \in N$。

$$a_p \equiv c^{d_p} \bmod p \equiv c^d (a^{\varphi(p)})^k \bmod p \equiv c^d \bmod p \equiv (a \bmod n) \bmod p \equiv a \bmod p$$

同理，$a_q \equiv a \bmod q$，

因此方程组

$$\begin{cases} x \equiv a_p \bmod p \\ x \equiv a_q \bmod q \end{cases}$$

中的 x 即为 a。

$c^d \bmod n$的运行时间是 $O(\log d \cdot \log^2 n)$，若 d与 n同阶，运行时间为 $O(\log^3 n)$。改进后算法的加速比是 $\dfrac{\log^3 n}{2(\log n/2)^3} = 4$

中国剩余定理也用于解高次同余方程（即（1.1）式中 $\deg f \ldots 2$），解法和解数由以下定理给出。

定理3.3 设 $m=m_1\cdots m_k$，其中 $m_i(1\leqslant i\leqslant k)$ 是两两互素的正整数，则同余方程

$$f(x)\equiv 0 \bmod m \quad (3.4)$$

与同余方程组

$$\begin{cases} f(x)\equiv 0 \bmod m_1 \\ \cdots \\ f(x)\equiv 0 \bmod m_k \end{cases} \quad (3.5)$$

等价。设 $\boldsymbol{T}$ 是（3.4）的解数，$\boldsymbol{T}_i$ 是 $f(x)\equiv 0 \bmod m_i\ (1\leqslant i\leqslant k)$ 的解数，则 $T=T_1\cdots T_k$。

证明 设x_0是（3.4）的解，即$f(x_0)\equiv 0 \bmod m$，由第3章定理1.5得$f(x_0)\equiv 0 \bmod m_i\ (1\leqslant i\leqslant k)$，即$x_0$也是（3.5）的解。反之，设$x_0$是（3.5）的解，即$f(x)\equiv 0 \bmod m_i\ (1\leqslant i\leqslant k)$，由第3章定理1.9得$f(x_0)\equiv 0 \bmod [m_1\cdots m_k]\equiv 0 \bmod m$，即$x_0$也是（3.4）的解。

设$f(x)\equiv 0 \bmod m_i$的解是$b_i(1\leqslant i\leqslant k)$，建立方程组

$$\begin{cases} x\equiv b_1 \bmod m_1 \\ \cdots \\ x\equiv b_k \bmod m_k \end{cases} \qquad (3.6)$$

由中国剩余定理得

$$x_0 \equiv \frac{m}{m_1} e_1 b_1 + \cdots + \frac{m}{m_k} e_k b_k \pmod{m} \quad (3.7)$$

由 $x_0 \equiv b_i \bmod m_i$ 得 $f(x_0) \equiv f(b_i) \equiv 0 \bmod m_i$，即 x_0 是式（3.5）的解，因此也是（3.4）的解。

若 $b_i (1 \leqslant i \leqslant k)$ 遍历 $f(x) \equiv 0 \bmod m_i$ 的所有解，则 x_0 遍历 $f(x) \equiv 0 \bmod m$ 的所有解，因此 $T = T_1 \cdots T_k$ 。

证毕。

定理3.3的证明过程即给出了解高次同余方程（3.4）的过程：将 分解成两两互素的数的乘积，建立方程组（3.5），解出（3.5）得一次同余方程组（3.6），由中国剩余定理求出的（3.7）即为原方程（3.4）的解。通常可先将m分解成标准分解式$m=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，取 $m_i=p_i^{\alpha_i}(1\leqslant i\leqslant k)$ 因此一般的高次同余方程的求解就归结为模为素数幂的同余方程的求解。

4.4 模为素数的高次同余方程

4.4 模为素数的高次同余方程

本节考虑同余方程

$$f(x)=a_n x^n+\cdots+a_1 x+a_0\equiv 0 \bmod p \quad (4.1)$$

其中 p 为素数，$a_i\in Z(i=1,\cdots,n)$，$p\nmid a_n$ 。

首先考虑多项式的Eulid除法，有以下结论。

定理4.1 设 $f(x)=a_n x^n+\cdots+a_1 x+a_0$，$g(x)=x^m+\cdots+b_1 x+b_0$，其中 $a_i(1\leqslant i\leqslant n)$，$b_j(1\leqslant j\leqslant m-1)\in Z$，则存在唯一的整系数多项式 $q(x)$ 和 $r(x)$，使得 $f(x)=q(x)g(x)+r(x)$，满足 $\deg r<\deg g$。

证明 分两种情况讨论：

（1） $n<m$ 时，取 $q(x)=0, r(x)=f(x)$ 。

（2） $n\geq m$ 时，对 n 作数学归纳法。

当 $n=m$ 时，因

$$f(x)-a_n g(x)=(a_{n-1}-a_n b_{n-1})x^{n-1}+\cdots+(a_1-a_n b_1)x+(a_0-a_n b_0)$$

取 $q(x)=a_n$ ，$r(x)=f(x)-a_n g(x)$，即得。

假设$n-1(n-1\ldots m)$时结论成立。则n时，由于

$$f(x)-a_n x^{n-m}g(x)=(a_{n-1}-a_n b_{m-1})x^{n-1}+\cdots+$$

$$(a_{n-m}-a_n b_0)x^{n-m}+a_{n-m-1}x^{n-m-1}+\cdots+a_1 x+a_0$$

即 $f(x)-a_n x^{n-m}g(x)$ 是 $n-1$ 次多项式。由归纳假设，存在唯一的整系数多项式 $q_1(x)$ 和 $r_1(x)$，使得

$$f(x)-a_n x^{n-m}g(x)=q_1(x)g(x)+r_1(x)$$ 其中 $\deg r_1<\deg g$，

取 $q(x)=a_n x^{n-m}+q_1(x), r(x)=r_1(x)$即得。唯一性的证明与整数的带余除法类似。

证毕。

定理 4.2 同余方程（4.1）与一个次数不超过 $p-1$ 的同余式模 p 等价。

证明 由多项式Euclid除法，存在唯一的 $q(x)$，$r(x)$，使得 $f(x)\equiv q(x)(x^p-x)+r(x)$，其中 $\deg r<p-1$。由Fermat定理，对任意 x 有 $x^p-x\equiv 0 \bmod p$，所以 $f(x)\equiv r(x) \bmod p$

证毕。

定理的证明过程给出了求（4.1）式的等价式的方法。

定理4.3　若同余方程（4.1）有 k个不同的解 $x \equiv c_i \bmod p\ (1 \leqslant i \leqslant k)$，则存在唯一的整系数多项式 $g_k(x)$，使得 $f(x) \equiv (x-c_1)\cdots(x-c_k)g_k(x) \bmod p$，其中 $g_k(x)$的首项系数为 a_n，$\deg g_k = n-k$　。

证明 对 $f(x)$ 和 $x-c_1$ 用Euclid除法, 存在唯一的 $g_1(x)$, $r_1(x)$, 使得 $f(x)=(x-c_1)g_1(x)+r_1(x)$，其中 $\deg r_1=0$，即 $r_1(x)$ 为常数。由 $f(c_1)\equiv r_1(c_1)\equiv 0 \bmod p$ 得 $r_1(x)\equiv 0 \bmod p$，所以 $f(x)\equiv(x-c_1)g_1(x) \bmod p$。再由 $f(c_2)\equiv(c_2-c_1)g_1(c_2)\equiv 0 \bmod p$ 得 $g_1(c_2)\equiv 0 \bmod p$，对$g_1(x)$与$(x-c_2)$用Euclid除法，得到唯一的$g_2(x)$，满足$g_1(x)\equiv(x-c_2)g_2(x) \bmod p$。如此下去，得到 $g_{k-1}(x)=(x-c_k)g_k(x) \bmod p$。所以$f(x)\equiv(x-c_1)\cdots(x-c_k)g_k(x) \bmod p$，显然$g_k(x)$的首项系数为$a_n$, $\deg g_k=n-k$。

证毕。

定理4.4 同余方程（4.1）的解数不超过它的次数。

证明 反证法。设方程(4.1)的解有 $n+1$个，$x \equiv c_i \bmod p\ (1 \leqslant i \leqslant n+1)$

由定理4.3，存在$g_n(x)$，使得 $f(x) \equiv (x-c_1)\cdots(x-c_n)g_n(x) \bmod p$，

其中$g_n(x)$的首项系数是 a_n，$\deg g_n = 0$，即$g_n(x) \equiv a_n \bmod p$。

由 $f(c_{n+1}) \equiv 0 \bmod p$ 得$(c_{n+1}-c_1)\cdots(c_{n+1}-c_n)g_n(c_{n+1}) \equiv 0 \bmod p$，所以$g_n(c_{n+1}) \equiv 0 \bmod p$，因此$a_n \equiv 0 \bmod p$，与 $p \nmid a_n$矛盾。

证毕。

由反证法可得以下推论：

推论 若同余方程(4.1)的解数大于n，则必有 $p|a_i(1 \leqslant i \leqslant n)$

定理4.5　设 $a_n=1$，同余方程（4.1）恰有 n 个解的充要条件是在模 p 的意义下，x^p-x 能被 $f(x)$ 整除。

证明　由多项式除法，存在唯一的 $q(x)$ 和 $r(x)$，使得 $x^p-x=q(x)f(x)+r(x)$，其中 $\deg r<n$，$\deg q=p-n$。

必要性：若 $f(x)\equiv 0 \bmod p$ 有 n 个解，由Fermat定理知这 n 个解也是 $x^p-x\equiv 0 \bmod p$ 的根，因此也是 $r(x)\equiv 0 \bmod p$ 的根，所以 $r(x)\equiv 0 \bmod p$ 的解数 n 超过它的次数 $\deg r$。由定理4.4的推论，$r(x)\equiv 0 \bmod p$，所以 $x^p-x\equiv q(x)f(x) \bmod p$。

充分性：若 $x^p - x \equiv q(x)f(x) \bmod p$ ，由Fermat定理，对 $\forall x \in \{0, \cdots, p-1\}$，$x^p - x \equiv 0 \bmod p$，因此 $q(x)f(x) \equiv 0 \bmod p$。即 $q(x)f(x) \equiv 0 \bmod p$ 的解数为 p。设 $f(x) \equiv 0 \bmod p$ 的解数为 $k(k \leqslant n)$，$q(x) \equiv 0 \bmod p$ 的解数为 h，则有 $p \leqslant k + h$（因为 $f(x) \equiv 0 \bmod p$ 和 $q(x) \equiv 0 \bmod p$ 可能有相同的解）。但另一方面，由定理4.4得 $k \leqslant n$，$h \leqslant p - n$，所以 $k + h \leqslant n + (p - n) = p$ 所以 $p = k + n$。若 $k < n$，$h \geqslant p - k > p - n = \deg q$，即 $q(x) \equiv 0 \bmod p$ 的解数大于它的次数，矛盾。所以 $k = n$ 。

证毕。

例4.1 判断同余方程 $2x^3+5x^2+6x+1\equiv 0 \bmod 7$ 是否有三个解。

解 因为首相系数为2，不能直接用定理4.5。由定理1.1，该方程与 $4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3 \bmod 7$ 等价，作多项式除法得：$x^7-x=(x^3-x^2+3x-3)(x^3+x^2-2x-2)+7x(x^2-1)$

$x^7-x\equiv(x^3-x^2+3x-3)(x^3+x^2-2x-2) \bmod 7$，即模7下 x^3-x^2+3x-3 整除 x^7-x。所以 $x^3-x^2+3x-3\equiv 0 \bmod 7$ 有3个根，原方程也有3个根。

例4.2 设素数 $p>2$，$p\nmid d$，求同余方程 $x^2-d\equiv 0 \bmod p$ 的解数为2的充要条件。

解 由于 $x^{p-1}-1=(x^2)^{\frac{p-1}{2}}-d^{\frac{p-1}{2}}+d^{\frac{p-1}{2}}-1=(x^2-d)q(x)+d^{\frac{p-1}{2}}-1$。

由定理4.5，解数为2的充要条件是 $d^{\frac{p-1}{2}}-1\equiv 0 \bmod p$。

总结一下，在解同余方程（4.1）时，先去掉系数为p的倍数的项，再按定理4.2找出次数小于等于p的等价方程。

例4.3 求同余方程 $21x^{18}+2x^{15}-x^{10}+4x-3\equiv 0 \bmod 7$ 。

解 去掉系数为7的倍数的项，得 $2x^{15}-x^{10}+4x-3\equiv 0 \bmod 7$ 。

作多项式Euclid除法得

$$2x^{15}-x^{10}+4x-3=(x^7-x)(2x^8-x^3+2x^2)+(-x^4+2x^3+4x-3),$$

因此，等价的同余方程为：$x^4-2x^3-4x+3\equiv 0 \bmod 7$ 。将 $x=0,\pm 1,\pm 2,\pm 3$ 代入知，方程无解。

在定理4.2中求等价的同余方程时，做Euclid除法得 $f(x)=q(x)(x^p-x)+r(x)$。但实际上并不需要知道 $q(x)$，而且次数高时，这种除法很麻烦。事实上可由Euler定理（$x^{p-1}\equiv 1 \bmod p$）直接化简。

例4.4 求同余方程 $3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0 \bmod 5$

解 由Euler定理 $x^4\equiv 1 \bmod 5$。对 x^{14}, $x^{14}\equiv x^{3\cdot 4+2}\equiv (x^4)^3x^2\equiv x^2 \bmod 5$

类似地，得 $x^{13}\equiv x \bmod 5$，$x^{11}\equiv x^3 \bmod 5$，$x^9\equiv x \bmod 5$，$x^6\equiv x^2 \bmod 5$。所以方程等价于 $3x^3+x^2+6x\equiv 0 \bmod 5$。进一步得 $2(3x^3+x^2+6x)\equiv x^3+2x^2+2x\equiv 0 \bmod 5$。将 $x=0,\pm 1,\pm 2$ 代入验证，得方程的解为 $x\equiv 0,1,2 \pmod 5$。

对于化简后得到的等价的同余方程 $r(x) \equiv 0 \bmod p$（其中 $\deg r \leqslant p-1$），没有一般的求解方法，只能是对模 p 的绝对最小剩余系数中的值一一验证。而且还可看出，即使有解，解数也不规则。

4.5 模数为素数幂的同余方程

4.5 模数为素数幂的同余方程

本节考虑形如

$$f(x)\equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \bmod p^{\alpha} \quad (5.1)$$

的方程，其中 $\alpha \ldots 2$ ，p为素数，$p \nmid a_n$ 。

方程的解法是一种递推的方法，先按4.4节求出

$$f(x)\equiv 0 \bmod p \quad (5.2)$$

的解 $x \equiv c \bmod p$ 。

$$f(x)\equiv 0 \bmod p^2 \quad (5.3)$$

的解可设为 $x=c+yp$，其中 y 为待定系数，将 $x=c+yp$ 代入(5.3)可求出 。一直下去，由 $f(x)\equiv 0 \bmod p^{\alpha-1}$ 的解 $x\equiv c \bmod p^{\alpha-1}$，设 $f(x)\equiv 0 \bmod p^{\alpha}$ 的解为 $x\equiv c+yp^{\alpha-1}$，代入 $f(x)\equiv 0 \bmod p^{\alpha}$，确定出待定系数 y，即得 $f(x)\equiv 0 \bmod p^{a}$ 的解。

求 y 的具体过程如下：

由Taylor公式得：

$$f(c+yp^{\alpha-1})=f(c)+f'(c)yp^{\alpha-1}+\frac{f''(c)}{2!}y^2p^{2(\alpha-1)}+\cdots\equiv f(c)+f'(c)yp^{\alpha-1}(\mathrm{mod}\ p^{\alpha})$$

其中 $f'(x)$ 是 $f(x)$ 的导函数。

由 $f(c)+f'(c)yp^{\alpha-1}\equiv 0 \bmod p^{\alpha}$ 得 $p^{\alpha-1}f'(c)y\equiv -f(c) \bmod p^{\alpha}$。

由于 $f(c)\equiv 0 \bmod p^{\alpha-1}$，所以 $\dfrac{f(c)}{p^{\alpha-1}}$ 是整数，方程变为

$$f'(c)y\equiv -\frac{f(c)}{p^{\alpha-1}} \bmod p \quad (5.4)$$

下面分3种情况讨论。

（1） $p \nmid f'(c)$，即 $(f'(c), p)=1$，y有一个解

$$y \equiv -\frac{f(c)}{p^{\alpha-1}}(f'(c))^{-1} \bmod p \text{ 。}$$

（2） $p \nmid f'(c)$，但 $p \nmid \frac{f(c)}{p^{\alpha-1}}$，（5.4）左边为 $0 \bmod p$，右边不为 $0 \bmod p$，因此无解。

（3） $p \nmid f'(c)$ 且 $p \mid \frac{f(c)}{p^{\alpha-1}}$，此时式（5.4）的左右两边都为 $0 \bmod p$，任一 $y \in \{0,1,\cdots,p-1\}$ 都是它的解。

例5.1 解同余方程 $x^3+5x^2+9\equiv 0 \bmod 3^4$ 。

解 设 $f(x)=x^3+5x^2+9$，则 $f'(x)=3x^2+10x$。对同余方程 $x^3+5x^2+9\equiv 0 \bmod 3$，将 $x\equiv 0,\pm 1 (\bmod 3)$ 代入验证知 $x\equiv 0,1 (\bmod 3)$ 是解。

下面求 $x^3+5x^2+9\equiv 0 \bmod 3^2$ 的解。

当 $x\equiv 0 \bmod 3$ 时，$f(0)\equiv 0 \bmod 3^2$，$f'(0)\equiv 0 \bmod 3^2$，方程（5.4）为第3种情况，$y\equiv 0,\pm 1 \pmod 3$都是解，所以 $x^3+5x^2+9\equiv 0 \bmod 3^2$的解是 $x\equiv 0+3y\equiv 0,\pm 3 \pmod{3^2}$ 。

当 $x\equiv 1 \bmod 3$ 时，$f(1)\equiv 6 \bmod 3^2$，$f'(1)\equiv 4 \bmod 3^2$，$3\nmid f'(c)$，方程（5.4）为第1种情况。$4y\equiv -\frac{6}{3} \bmod 3$ ，y 有唯一解 $1 \bmod 3$。所以 $x^3+5x^2+9\equiv 0 \bmod 3^2$的解为 $1+1\cdot 3\equiv 4 \bmod 3^2$。

下面求 $x^3+5x^2+9\equiv 0 \bmod 3^3$ 的解。

按以上方法，相应于 $x\equiv -3 \bmod 3^2$ 的解为 $x\equiv -12,-3,-6 \pmod{3^3}$

相应于 $x\equiv 3 \bmod 3^2$ 的解为 $x\equiv -6,3,12 \pmod{3^3}$。

相应于 $x\equiv 0 \bmod 3^2$, (5.4) 无解, 故原方程无解。

$x\equiv 4 \bmod 3^2$ 相应于 $x\equiv 13 \bmod 3^3$ 的解 。

最后求 $x^3+5x^2+9\equiv 0 \bmod 3^4$ 的解。

按以上方法，可得最后的解为 $x\equiv -21,6,33,-24,3,30,40 \pmod{3^4}$

解同余方程 $f(x)\equiv a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \bmod m$ 的步骤如下：

（1） 写出 m 的标准分解式 $m=\prod_{i=1}^{k} p_i^{\alpha_i}$ 。

（2） 解模为素数幂的每个同余方程 $f(x)\equiv 0 \bmod p_i^{a_1}\ (1\leqslant i\leqslant k)$

这一步归结为求模为素数的同余方程 $f(x)\equiv 0 \bmod p_i$ 。

（3） 建立等价的同余方程组

$$\begin{cases} f(x)\equiv 0 \bmod p_1^{\alpha_1} \\ \cdots \\ f(x)\equiv 0 \bmod p_k^{\alpha_k} \end{cases}$$

由中国剩余定理得 $f(x)\equiv 0 \bmod m$ 的解。

本章小结