第3章　同余方程

在代数里面，一个主要的问题就是解代数方程。而本章所要讨论的正是与解代数方程相类似的问题：求同余方程的解。本章首先讨论一次同余方程和一次同余方程组，之后介绍高次同余方程。对于普通的同余方程本章介绍一般的解法，而对于一次同余方程组，主要介绍著名的孙子定理的求解方法。

本章的内容不仅是初等数论同余理论的核心内容，而且也构成了公共钥匙密码学中多种密码算法的主要内容。

3.1　同余方程和一次同余方程

本节要介绍同余方程的基本概念及一次同余方程。

在本章中，总假定 m 是正整数。

定义 3-1　设 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，称

$$f(x)\equiv 0(\bmod m) \tag{3-1}$$

是关于未知数 x 的模 m 的同余方程，简称为模 m 的同余方程。

若 $a_n\not\equiv 0(\bmod m)$，则称为 n 次同余方程。

定义 3-2　设 x_0 是整数，当 $x=x_0$ 时，式(3-1)成立，则称 x_0 是同余方程(3-1)的解。凡对于模 m 同余的解，被视为同一个解。同余方程(3-1)的解数是指它的关于模 m 互不同余的所有解的个数，也即在模 m 的一个完全剩余系中的解的个数。

由定义 3-2 知，同余方程(3-1)的解数不超过 m。

定理 3-1　下面的结论成立：

(1) 设 $b(x)$是整系数多项式，则同余方程(3-1)与

$$f(x)+b(x)\equiv b(x)(\bmod m)$$

等价。

(2) 设 b 是整数，$(b,m)=1$，则同余方程(3-1)与

$$bf(x)\equiv 0(\bmod m)$$

等价。

(3) 设 m 是素数，$f(x)=g(x)h(x)$，$g(x)$与 $h(x)$都是整系数多项式，又设 x_0 是同余方程(3-1)的解，则 x_0 必是同余方程

$$g(x)\equiv 0(\bmod m)\ \text{或}\ h(x)\equiv 0(\bmod m)$$

的解。

下面，来研究一次同余方程的解。

定理 3-2　设 a、b 是整数，$a\not\equiv 0(\bmod m)$。则同余方程

$$ax\equiv b(\bmod m) \tag{3-2}$$

有解的充要条件是$(a,m)|b$。若有解,则恰有$d=(a,m)$个解。

证 显然,同余方程(3-2)等价于不定方程

$$ax+my=b \tag{3-3}$$

因此,同余方程(3-2)有解的充要条件是$(a,m)|b$可由定理5-2得出(后面会为大家介绍不定方程的知识)。

若同余方程(3-2)有解x_0,则存在y_0,使得x_0与y_0是方程(3-3)的解,此时,方程(3-3)的全部解是

$$\begin{cases} x=x_0+\dfrac{m}{(a,m)}t \\ y=y_0-\dfrac{a}{(a,m)}t \end{cases}, \quad t\in\mathbf{Z} \tag{3-4}$$

由式(3-4)所确定的x都满足方程(3-2)。记$d=(a,m)$,以及

$$t=dq+r, \quad q\in\mathbf{Z}, \quad r=0,1,2,\cdots,d-1$$

则

$$x=x_0+qm+\frac{m}{d}r\equiv x_0+\frac{m}{d}r(\bmod m), \quad 0\leqslant r\leqslant d-1$$

容易验证,当$r=0,1,2,\cdots,d-1$时,相应的解

$$x_0,x_0+\frac{m}{d},x_0+\frac{2m}{d},\cdots,x_0+\frac{(d-1)m}{d}$$

对于模m是两两不同余的,所以同余方程(3-2)恰有d个解。 证毕

在定理的证明中,同时给出了解方程(3-2)的方法,但是,对于具体的方程(3-2),常常可采用不同的方法去解。

例 3-1 设$(a,m)=1$,又设存在整数y,使得$a|b+ym$,则

$$x\equiv\frac{b+ym}{a}(\bmod m)$$

是方程(3-2)的解。

证 直接验算,有

$$ax\equiv b+ym\equiv b(\bmod m)$$

注意:例3-1说明,求方程(3-2)的解可以转化为求方程

$$my\equiv -b(\bmod a) \tag{3-5}$$

的解,这有两个便利之处:第一,将一个对于大模m的同余方程转化为一个对于小模a的同余方程,因此有可能通过对模a的完全剩余系进行逐个验证,以求出方程(3-5)和(3-2)的解;第二,设$m\equiv r(\bmod a)$,$r<a$,则又可继续转化成一个对于更小的模r的同余方程。

例 3-2 解同余方程

$$325x\equiv 20(\bmod 161) \tag{3-6}$$

解 同余方程(3-6)即是

$$3x\equiv 20(\bmod 161)$$

解同余方程

$$161y\equiv -20(\bmod 3)$$

$$2y \equiv 1 \pmod 3$$

得到 $y \equiv 2 \pmod 3$，因此方程(3-6)的解是

$$x \equiv \frac{20 + 2 \times 161}{3} = 114 \pmod{161}$$

例 3-3 设 $a>0$，且$(a, m)=1$，a_1 是 m 对模 a 的最小非负剩余，则同余方程

$$a_1 x \equiv -b\left[\frac{m}{a}\right] \pmod m \tag{3-7}$$

等价于同余方程(3-2)，其中[ ]表示取整。

证 设 x 是(3-2)的解，则由 $m=a\left[\frac{m}{a}\right]+a_1$ 得到

$$a_1 x = \left(m - a\left[\frac{m}{a}\right]\right)x \equiv -ax\left[\frac{m}{a}\right] \equiv -b\left[\frac{m}{a}\right] \pmod m$$

即 x 是同余方程(3-7)的解。但是由假设条件可知同余方程(3-2)与(3-7)都有且只有一个解。所以这两个同余方程等价。

注意：用本例的方法，可以将同余方程(3-2)转化成未知数的系数更小一些的同余方程，从而易于求解。

例 3-4 解同余方程 $6x \equiv 7 \pmod{23}$。

解 由例 3-3，依次得到

$$\begin{aligned} 6x \equiv 7 \pmod{23} &\Leftrightarrow 5x \equiv -7 \times 3 \equiv 2 \pmod{23} \\ &\Leftrightarrow 3x \equiv -2 \times 4 \equiv -8 \pmod{23} \\ &\Leftrightarrow 2x \equiv 8 \times 7 \equiv 10 \pmod{23} \\ &\Leftrightarrow x \equiv 5 \pmod{23} \end{aligned}$$

例 3-5 设$(a,m)=1$，并且有整数 $\delta>0$ 使得

$$a^{\delta} \equiv 1 \pmod m$$

则同余方程(3-2)的解是

$$x \equiv ba^{\delta-1} \pmod m$$

证 直接验证即可。

注意：由例 3-5 及 Euler 定理可知，若$(a,m)=1$，则

$$x \equiv ba^{\varphi(m)-1} \pmod m$$

总是同余方程(3-2)的解。

例 3-6 解同余方程

$$81x^3 + 24x^2 + 5x + 23 \equiv 0 \pmod 7$$

解 原同余方程即是

$$-3x^3 + 3x^2 - 2x + 2 \equiv 0 \pmod 7$$

用 $x=0, \pm1, \pm2, \pm3$ 逐个代入验证，得到它的解是

$$x_1 \equiv 1, x_2 \equiv 2, x_3 \equiv -2 \pmod 7$$

注意：本例使用的是最基本的解同余方程的方法，一般说来，它的计算量太大，不实用。

例 3-7 解同余方程组

$$\begin{cases} 3x+5y \equiv 1 \pmod 7 \\ 2x-3y \equiv 2 \pmod 7 \end{cases} \tag{3-8}$$

解 将式(3-8)的前一式乘以 2 后一式乘以 3 再相减得到

$$19y \equiv -4 \pmod 7$$

$$5y \equiv -4 \pmod 7$$

$$y \equiv 2 \pmod 7$$

再代入式(3-8)的前一式得到

$$3x+10 \equiv 1 \pmod 7$$

$$x \equiv 4 \pmod 7$$

即同余方程组(3-8)的解是 $x \equiv 4, y \equiv 2 \pmod 7$。

例 3-8 设 a_1、a_2 是整数，m_1、m_2 是正整数，证明：同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \tag{3-9}$$

有解的充要条件是

$$a_1 \equiv a_2 \pmod{(m_1, m_2)} \tag{3-10}$$

若有解，则对模$[m_1, m_2]$是唯一的，即若 x_1 与 x_2 都是同余方程组(3-9)的解，则

$$x_1 \equiv x_2 \pmod{[m_1, m_2]} \tag{3-11}$$

证 必要性是显然的。下面证明充分性。

若式(3-10)成立，由定理 3-2，同余方程

$$m_2 y \equiv a_1 - a_2 \pmod{m_1}$$

有解 $y \equiv y_0 \pmod{m_1}$，记 $x_0 = a_2 + m_2 y_0$，则

$$x_0 \equiv a_2 \pmod{m_2}$$

并且

$$x_0 = a_2 + m_2 y_0 \equiv a_2 + a_1 - a_2 \equiv a_1 \pmod{m_1}$$

因此 x_0 是同余方程组的解。

若 x_1 与 x_2 都是方程组(3-9)的解，则

$$x_1 \equiv x_2 \pmod{m_1}, \quad x_1 \equiv x_2 \pmod{m_2}$$

由同余的基本性质，得到式(3-11)。 证毕

3.2 一次同余方程组和孙子定理

本节讨论同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{3-12}$$

在我国古代的孙子算经(纪元前后)里已经提出了这种形式的问题，并且很好地解决了它。孙子算经里提出的问题之一如下：

“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？”“答曰二十三。”

我们设 x 是所求物数，根据题意转化为求解以下问题：

$$x \equiv 2(\mathrm{mod}\ 3),\quad x \equiv 3(\mathrm{mod}\ 5),\quad x \equiv 2(\mathrm{mod}\ 7)$$

定理 3-3（孙子定理） 设 $m_1, m_2, \cdots, m_k$ 是正整数，

$$(m_i, m_j) = 1,\quad 1 \leqslant i, j \leqslant k, i \neq j \tag{3-13}$$

记

$$m = m_1 m_2 \cdots m_k,\quad M_i = \frac{m}{m_i},\quad 1 \leqslant i \leqslant k$$

则存在整数 $M_i'(1 \leqslant i \leqslant k)$，使得

$$M_i M_i' \equiv 1(\mathrm{mod}\ m_i) \tag{3-14}$$

$$M_i M_i' \equiv 0(\mathrm{mod}\ m_j),\quad 1 \leqslant j \leqslant k, i \neq j \tag{3-15}$$

并且

$$x_0 \equiv \sum_{i=1}^{k} a_i M_i M_i'(\mathrm{mod}\ m) \tag{3-16}$$

是同余方程组(3-12)对模 m 的唯一解，即若有 x 使方程组(3-12)成立，则

$$x \equiv x_0(\mathrm{mod}\ m) \tag{3-17}$$

证 由式(3-13)，有$(M_i, m_i)=1$，因此利用辗转相除法可以求出 M_i'与 y_i，使得

$$M_i M_i' + y_i m_i = 1$$

即 M_i'满足式(3-14)和式(3-15)。由式(3-14)与式(3-15)，对于 $1 \leqslant i \leqslant k$，有

$$x_0 \equiv a_i M_i M_i' \equiv a_i(\mathrm{mod}\ m_i),\quad 1 \leqslant i \leqslant k$$

若 x 也使式(3-12)成立，则

$$x \equiv x_0(\mathrm{mod}\ m_i),\quad 1 \leqslant i \leqslant k$$

因此

$$x \equiv x_0(\mathrm{mod}\ [m_1, m_2, \cdots, m_k])$$

但是，由式(3-13)可知$[m_1, m_2, \cdots, m_k]=m$，这就证明了式(3-17)。 证毕

定理 3-4 若 $a_1, a_2, \cdots, a_k$ 分别通过模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则式(3-16)中的 x_0 通过模 $m_1 m_2 \cdots m_k$ 的完全剩余系。

证 令 $x_0 \equiv \sum_{i=1}^{k} a_i M_i M_i'$，则 x_0 通过 $m_1 m_2 \cdots m_k$ 个数。这 m 个数是两两不同余的。这因为若

$$\sum_{i=1}^{k} a_i' M_i M_i' \equiv \sum_{i=1}^{k} a_i'' M_i M_i'(\mathrm{mod}\ m)$$

则

$$a_i' M_i M_i' \equiv a_i'' M_i M_i'(\mathrm{mod}\ m),\quad i = 1, 2, \cdots, k$$

即 $a_i' \equiv a_i''(\mathrm{mod}\ m)$，$i=1,2,\cdots,k$。但 a'、a''是模 m_i 的同一完全剩余系中的二数，故 $a_i'=a_i''$，$i=1,2,\cdots,k$。m 个整数形成模 m 的一个完全剩余系的充分必要条件是两两对模 m 不同余。由此即得定理结论。 证毕

定理 3-5 同余方程组(3-12)有解的充要条件是

$$a_i \equiv a_j (\bmod (m_i, m_j)), \quad 1 \leqslant i, j \leqslant k \tag{3-18}$$

证 必要性是显然的。下面证明充分性。

当 $k=2$ 时,由例 3-8 可知充分性成立。假设充分性当 $k=n$ 时成立。现在证充分性,当 $k=n+1$ 时成立。我们来考虑同余方程组

$$x \equiv a_i (\bmod m_i), \quad 1 \leqslant i \leqslant n+1。$$

由例 3-8,存在 b,使得 $x \equiv b (\bmod [m_n, m_{n+1}])$ 满足同余方程组

$$x \equiv a_n (\bmod m_n), \quad x \equiv a_{n+1} (\bmod m_{n+1})$$

在同余方程组

$$\begin{cases} x \equiv a_1 (\bmod m_1) \\ \quad \vdots \\ x \equiv a_{n-1} (\bmod m_{n-1}) \\ x \equiv b (\bmod [m_n, m_{n+1}]) \end{cases}$$

中,由式(3-18)有

$$a_i \equiv a_j (\bmod (m_i, m_j)), \quad 1 \leqslant i, j \leqslant n-1$$

因此,若能证明

$$a_i \equiv b (\bmod (m_i, [m_n, m_{n+1}])), \quad 1 \leqslant i \leqslant n-1 \tag{3-19}$$

则由归纳假设就可以证明充分性。

由 b 的定义,有

$$a_n \equiv b (\bmod m_n), \quad a_{n+1} \equiv b (\bmod m_{n+1}) \tag{3-20}$$

而且,由于式(3-18)当 $k=n+1$ 时成立,所以,对于 $1 \leqslant i \leqslant n-1$ 有

$$a_i \equiv a_n (\bmod (m_i, m_n)), \quad a_i \equiv a_{n+1} (\bmod (m_i, m_{n+1}))$$

由此及式(3-20)得到,对于 $1 \leqslant i \leqslant n-1$,有

$$a_i \equiv b (\bmod (m_i, m_n)), \quad a_i \equiv b (\bmod (m_i, m_{n+1}))$$

因此

$$a_i \equiv b (\bmod [(m_i, m_n), (m_i, m_{n+1})])$$

由上式及例 1-29,就得到式(3-19)。 证毕

例 3-9 求整数 n,它被 3、5、7 除的余数分别是 1、2、3。

解 n 是同余方程组

$$n \equiv 1 (\bmod 3), \quad n \equiv 2 (\bmod 5), \quad n \equiv 3 (\bmod 7)$$

的解。在孙子定理中,取

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7, \quad m = 3 \times 5 \times 7 = 105$$
$$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15$$
$$M_1' = -1, \quad M_2' = 1, \quad M_3' = 1$$

则

$$n \equiv 1 \times 35 \times (-1) + 2 \times 21 \times 1 + 3 \times 15 \times 1 \equiv 52 (\bmod 105)$$

因此所求的整数为

$$n = 52 + 105t, \quad t \in \mathbf{Z}$$

例 3-10 解“物不知数”问题 $\begin{cases} x\equiv 2(\bmod 3) \\ x\equiv 3(\bmod 5) \\ x\equiv 2(\bmod 7) \end{cases}$

解 已知 $m_1=3, m_2=5, m_3=7$。

故 $m=3\times 5\times 7=105$

$$M_1=35,\quad M_2=21,\quad M_3=15$$
$$M'_1=2,\quad M'_2=1,\quad M'_3=1$$

则

$$x\equiv 35\times 2\times 2+21\times 1\times 3+15\times 1\times 2\equiv 233\equiv 23(\bmod 105)$$

即物品数可能为

$$x=23+105k(k\geqslant 0)$$

3.3 高次同余方程

本节将讨论高次同余方程和它的解数。

定理 3-6 设 $m_1, m_2, \cdots, m_k$ 两两互素，$m=m_1m_2\cdots m_k$，$f(x)$是整系数多项式。则同余方程

$$f(x)\equiv 0(\bmod m) \tag{3-21}$$

与同余方程组

$$\begin{cases} f(x)\equiv 0(\bmod m_1) \\ f(x)\equiv 0(\bmod m_2) \\ \quad\vdots \\ f(x)\equiv 0(\bmod m_k) \end{cases} \tag{3-22}$$

等价。且

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

这里 $T(f;m)$表示同余方程 $f(x)\equiv 0(\bmod m)$的解数。也就是说，解数 $T(f;m)$是 m 的积性函数。

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

$$f(x)\equiv 0(\bmod m)\Leftrightarrow\begin{cases} f(x)\equiv 0(\bmod m_1) \\ f(x)\equiv 0(\bmod m_2) \\ \quad\vdots \\ f(x)\equiv 0(\bmod m_k) \end{cases}$$

即等价性成立。

设方程

$$f(x)\equiv 0(\bmod m_i)$$

的解是 $x\equiv b_i(\bmod m_i)$，$i=1,2,\cdots,k$，则由孙子定理可求得一次同余方程

$$\begin{cases} x \equiv b_1 (\bmod m_1) \\ x \equiv b_2 (\bmod m_2) \\ \quad \vdots \\ x \equiv b_k (\bmod m_k) \end{cases}$$

的解

$$x \equiv M_1 M_1^{-1} b_1 + \cdots + M_k M_k^{-1} b_k (\bmod m)$$

因为

$$f(x) \equiv f(b_i) \equiv 0 \bmod m_i, \quad i = 1, 2, \cdots, k$$

故 x 也是方程(3-21)的解。因此,当 b_i 遍历 $f(x) \equiv 0 (\bmod m_i)$ 的所有解($i = 1, 2, \cdots, k$)时,x 也遍历方程(3-21)的所有解,即方程组(3-22)的解数为

$$T(f; m_1) \cdot T(f; m_2) \cdots T(f; m_k)$$ 证毕

例 3-11 解同余方程 $x^4 + 2x^3 + 8x + 9 = 0 (\bmod 35)$。

解 由定理 3-6 知方程等价于同余方程组

$$\begin{cases} x^4 + 2x^3 + 8x + 9 \equiv 0 (\bmod 5) \\ x^4 + 2x^3 + 8x + 9 \equiv 0 (\bmod 7) \end{cases}$$

即

$$\begin{cases} x^4 + 2x^3 - 2x - 1 \equiv 0 (\bmod 5) ① \\ x^4 + 2x^3 + x + 2 \equiv 0 (\bmod 7) ② \end{cases} \tag{3-23}$$

分别解单个方程:

①的解为 $x \equiv 1, 4 (\bmod 5)$;

②的解为 $x \equiv 3, 5, 6 (\bmod 7)$。

联立二方程的解,得方程组

$$\begin{cases} x \equiv b_1 (\bmod 5) \\ x \equiv b_2 (\bmod 7) \end{cases}$$

其解为

$$\begin{aligned} x &\equiv M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 (\bmod m) \\ &\equiv 7 \times 3 b_1 + 5 \times 3 b_2 (\bmod 35) \end{aligned}$$

其中 $m = 35, M_1 = 7, M_1^{-1} = 3, M_2 = 5, M_2^{-1} = 3$。

对不同的(b_1, b_2),设方程组(3-23)的解为 $x \equiv a (\bmod 35)$。

b_1	1	1	1	4	4	4
b_2	3	5	6	3	5	6
a	31	26	6	24	19	34

注意:解方程组(3-23)的本质原因是求同时满足方程①和方程②的 x,例如方程①的一个解为 $x \equiv 1 (\bmod 5)$,方程②的一个解为 $x \equiv 3 (\bmod 7)$,则二者解的值的集合为

$$A = \{\cdots, -9, -4, 1, 6, 11, 16, 21, 26, 31, 36, \cdots\}$$

$$B = \{\cdots, -11, -4, 3, 10, 17, 24, 31, 38, \cdots\}$$

而其共同解则为集合 A 与 B 的交，即

$$AB = \{\cdots, -4, 31, 66, \cdots\}$$

所以 $x\equiv 31(\bmod 35)$ 是方程组(3-23)两个方程的共同解，从而也就是原方程组的解。

例 3-12 解同余方程

$$x^3 + 3x - 14 \equiv 0(\bmod 45)$$

解 原同余方程等价于同余方程组

$$x^3 + 3x - 14 \equiv 0(\bmod 9) \tag{3-24}$$

$$x^3 + 3x - 14 \equiv 0(\bmod 5) \tag{3-25}$$

先解同余方程(3-24)。容易验证，同余方程 $x^3 + 3x - 14 \equiv 0(\bmod 3)$ 的解是 $x \equiv 2(\bmod 3)$。

令 $x=2+3t$ 并代入方程(3-24)，得到

$$(2 + 3t)^3 + 3(2 + 3t) - 14 \equiv 0(\bmod 9) \tag{3-26}$$

容易看出，这是一个对于任何整数 t 都成立的同余式。所以，方程(3-26)的解是

$$t \equiv 0,1,2(\bmod 3),$$

于是方程(3-24)的解是

$$x \equiv 2,5,8(\bmod 9)$$

再解同余方程(3-25)。用 $x=0,1,2,3,4$ 去验证，得到(3-25)的解是

$$x \equiv 1,2(\bmod 5)$$

因此，原同余方程的解是下面 6 个同余方程组的解：

$$x \equiv a_1(\bmod 9), \quad a_1 = 2,5,8$$

$$x \equiv a_2(\bmod 5), \quad a_2 = 1,2$$

利用孙子定理解这 6 个方程组，记

$$m_1 = 9, m_2 = 5, m = 45, M_1 = 5, M_2 = 9, M_1' = 2, M_2' = -1$$

则

$$x \equiv 10a_1 - 9a_2(\bmod 45)$$

将 a_1 和 a_2 的不同取值代入，得到所求的解：

$$x_1 \equiv 10 \times 2 - 9 \times 1 \equiv 11(\bmod 45)$$

$$x_2 \equiv 10 \times 2 - 9 \times 2 \equiv 2(\bmod 45)$$

$$x_3 \equiv 10 \times 5 - 9 \times 1 \equiv 41(\bmod 45)$$

$$x_4 \equiv 10 \times 5 - 9 \times 2 \equiv 32(\bmod 45)$$

$$x_5 \equiv 10 \times 8 - 9 \times 1 \equiv 26(\bmod 45)$$

$$x_6 \equiv 10 \times 8 - 9 \times 2 \equiv 17(\bmod 45)$$

3.4 模为高次幂的同余方程

定理 3-6 的意义还在于指出了一般同余方程 $f(x)\equiv 0(\bmod m)$ 的求解途径：即先解出每一个同余方程 $f(x)\equiv 0(\bmod m_i)$ 的 t_i 个全部解；然后，求一次同余方程

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

的解；由这样得到的 $t=t_1\cdots t_k$ 个解就是同余方程 $f(x)\equiv 0 \pmod m$ 的全部解。当对某个 j，同余方程 $f(x)\equiv 0 \pmod{m_i}$ 无解，则同余方程 $f(x)\equiv 0 \pmod m$ 也无解。通常，当 $m=p_1^{a_1}\cdots p_k^{a_k}$ 时，取 $m_j=p_j^{a_j}$。这样，一般同余方程的求解就归结为模为素数幂的同余方程的求解。即求解

$$f(x) \equiv 0 \pmod{p^\alpha} \tag{3-27}$$

若 x_0 是同余方程

$$f(x) \equiv 0 \pmod{p^\alpha}$$

的解，则它必是方程

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{3-28}$$

的解，因此，必有与 x_0 相应的方程(3-28)的某个解 x_1，使

$$x_0 \equiv x_1 \pmod{p^{\alpha-1}}, \quad x_0 = x_1 + p^{\alpha-1}t_0$$

此处，t_0 是某个适当的整数。

由此得到提示：可以从方程(3-28)的解中去求方程(3-27)的解。于是现在的问题是，对于方程(3-28)的每个解 x_1，是否必有方程(3-27)的解 x_0 与之对应？若有，如何去确定它？

定义 3-3 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 为整系数多项式，记

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2x + a_1,$$

称 $f'(x)$ 为 $f(x)$ 的导式。

定理 3-7 设 p 是素数，$\alpha\geqslant 2$ 是整数，$f(x)=a_nx^n+\cdots+a_1x+a_0$ 是整系数多项式，又设 x_1 是同余方程(3-28)的一个解。

(1) 若 $f'(x_1)\not\equiv 0 \pmod p$，则存在整数 t，使得

$$x = x_1 + p^{\alpha-1}t \tag{3-29}$$

是同余方程(3-27)的解。

(2) 若 $f'(x_1)\equiv 0 \pmod p$，并且 $f(x_1)\equiv 0 \pmod{p^\alpha}$，则对于 $t=0,1,2,\cdots,p-1$，式(3-29)中的 x 都是方程(3-27)的解。

证 确定式(3-29)中的 t，使 $x_1+p^{\alpha-1}t$ 满足同余方程(3-27)，即要使

$$a_n(x_1 + p^{\alpha-1}t)^n + a_{n-1}(x_1 + p^{\alpha-1}t)^{n-1} + \cdots$$
$$+ a_1(x_1 + p^{\alpha-1}t) + a_0 \equiv 0 \pmod{p^\alpha}$$

即

$$f(x_1) + p^{\alpha-1}tf'(x_1) \equiv 0 \pmod{p^\alpha},$$

$$tf'(x_1) \equiv -\frac{f(x_1)}{p^{\alpha-1}} \pmod p \tag{3-30}$$

下面考虑两种情形。

(1) 若 $f'(x)\not\equiv 0 \pmod p$，则关于 t 的同余方程(3-30)有唯一解 $t\equiv t_0 \pmod p$，即 $t=$