第 3 章　同余方程

求解同余方程的各种方法对许多密码算法的设计和分析具有重要作用. 本章我们首先介绍同余方程和线性同余方程的基本概念和性质. 然后讨论如何使用中国剩余定理求解线性同余方程组. 接下去讨论二次同余方程的解法——二次剩余理论, 并引入与二次剩余相关的运算函数, 即勒让德符号与雅可比符号. 最后, 我们讨论高次同余方程的解法.

学习本章之后，我们应该能够

- 掌握线性同余方程、线性同余方程组和中国剩余定理的概念与性质，以及相应的求解方法；
- 掌握二次剩余的概念与性质，以及相关的计算方法和应用；
- 掌握勒让德符号和雅可比符号的概念和性质，以及其相关的应用；
- 了解高次同余方程的概念和性质，以及方程的求解方法.

3.1　线性同余方程

上一章我们研究了同余的概念和一些性质， 现在我们开始讨论在模 m 的情况下多项式方程的求解问题.

定义 3.1.1　设多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

其中 $n>0$，$a_i\ (i = 0,1,2,\ldots,n)$是整数，又设 $m>0$，则同余式

$$f(x) \equiv 0 \pmod{m} \tag{3.1.1}$$

称为模 m 的**同余方程**. 若 a_n 不能被 m 整除，则 n 称为 $f(x)$的**次数**，记为 $\deg f(x)$.

若 x_0 满足

$$f(x_0) \equiv 0 \pmod{m},$$

则

$$x \equiv x_0 \pmod{m}$$

叫作同余方程(3.1.1)的**解**. 如果 $y_0 \equiv x_0 \pmod{m}$，那么必然有 $f(y_0) \equiv f(x_0) \equiv 0 \pmod{m}$，所以，同余方程不同的解是指模 m 互不同余的解.

由定义可知， 要求解同余方程(3.1.1)， 只要将 0, 1, …, $m-1$ 逐个代入式(3.1.1)中进行验算即可. 然而，当 m 较大时，巨大的计算量会难以令人满意.

例 3.1.1　求解同余方程 $x^4 + 3x^2 - 2x + 1 \equiv 0 \pmod 5$.

解　求解此模 5 的 4 次同余方程，可将 0, 1, 2, 3, 4 逐个代入，由于

$$2^4 + 3\times 2^2 - 2\times 2 + 1 = 25 \equiv 0 \pmod 5,$$

故 $x \equiv 2 \pmod 5$是该同余方程的解.

□

例 3.1.2 求解同余方程 $x^2 + 1 \equiv 0 \pmod 7$.

解 这是一个模 7 的 2 次同余方程，由于将 0, 1, …, 6 逐个代入方程中均不满足，故此同余方程无解.

□

下面我们讨论线性同余方程（也就是一次同余方程）的求解问题.

定理 3.1.1 设 $m > 1$，并且$(a, m) = 1$，则同余方程

$$ax \equiv b \pmod m \tag{3.1.2}$$

有且仅有一个解$x \equiv ba^{\varphi(m)-1} \pmod m$.

证明 由于 1, 2, …, m 组成一个模 m 的完全剩余系，又$(a, m) = 1$，故 $a, 2a, \ldots, ma$ 也组成一个模 m 的完全剩余系. 所以，其中有且仅有一个数设为 $a \times j$，满足

$$a \times j \equiv b \pmod m,$$

于是$x \equiv j \pmod m$就是式(3.1.2)的唯一解.

因为

$$a^{\varphi(m)} \equiv 1 \pmod m,$$

所以，有

$$a^{\varphi(m)} b \equiv b \pmod m,$$

即

$$a \cdot a^{\varphi(m)-1} b \equiv b \pmod m,$$

故$x \equiv ba^{\varphi(m)-1} \pmod m$是(3.1.2)式的唯一解.

□

由定理 3.1.1 可推出，当 $m > 1$,并且$(a, m) = 1$ 时，$a^{-1} \equiv a^{\varphi(m)-1} \pmod m$.

定理 3.1.2 设 $m > 1$, $(a, m) = d > 1$，则同余方程(3.1.2)有解的充要条件是 $d \mid b$. 并且在(3.1.2)式有解时，它的解的个数为 d，且若$x \equiv x_0 \pmod m$是(3.1.2)式的特解，则它的 d 个解为

$$x \equiv x_0 + \frac{m}{d} t \pmod m,$$

其中$t = 0,1,2, \ldots, d-1$.

证明 先证必要性. 如果(3.1.2)式有解 $x \equiv x_0 \pmod m$，则有

$$m \mid ax_0 - b,$$

又

$$d \mid m,$$

故

$$d \mid ax_0 - b.$$

又因为 $d \mid a$，所以有 $d \mid b$.

再证充分性．如果 $d|b$，则 $\frac{b}{d}$ 为整数，又 $(\frac{a}{d},\frac{m}{d})=1$，根据定理 3.1.1，同余方程

$$\frac{a}{d}x\equiv\frac{b}{d}\pmod{\frac{m}{d}}$$

有唯一解，由定理 2.1.7，这个解必满足同余方程(3.1.2)式，故(3.1.2)式有解.

若 $x\equiv x_0 \pmod{\frac{m}{d}}$ 是同余方程

$$\frac{a}{d}x\equiv\frac{b}{d}\pmod{\frac{m}{d}}$$

的唯一解，则有以下 d 个模 m 不同余的整数

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

是(3.1.2)式的解．由于

$$ax_0\equiv b \pmod m,$$

且显然有

$$at\frac{m}{d}\equiv 0 \pmod m,\ t=0,\ldots,d-1,$$

故

$$a\left(x_0+t\frac{m}{d}\right)\equiv b \pmod m,$$

于是$x\equiv x_0+\frac{m}{d}t \pmod m$是(3.1.2)式的解．又

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

两两模 m 不同余，且对于其他解，均可在以上这 d 个解中找到一数与之模 m 同余，即(3.1.2)式只有 d 个解．定理得证.

□

例 3.1.3　求解一次同余方程 $28x\equiv 21 \pmod{35}$.

解　由于 $d=(28,35)=7$，且显然 21 能被 7 整除，故此同余方程有解.

先求出同余方程

$$4x\equiv 3 \pmod 5$$

的解为 $x\equiv 2 \pmod 5$，所以原同余方程

$$28x\equiv 21 \pmod{35}$$

的一个特解为 $x_0\equiv 2 \pmod{35}$.

于是原同余方程的全部解为

$$x\equiv 2+5t \pmod{35},\ \ t=0,1,\ldots,4,5,6,$$

即 $x\equiv 2,7,12,17,22,27,32 \pmod{35}$.

□

习题 3.1

A 组

1. 求解下列一次同余方程：

   (1) $27x \equiv 12 \pmod{15}$;

   (2) $24x \equiv 6 \pmod{81}$;

   (3) $91x \equiv 26 \pmod{169}$;

   (4) $71x \equiv 32 \pmod{3\,441}$.

2. 确定下面同余式的不同解的个数，无需求出解.

   (1) $72x \equiv 47 \pmod{200}$;

   (2) $4\,183x \equiv 5\,781 \pmod{15\,087}$;

   (3) $1\,537x \equiv 2\,863 \pmod{6\,731}$.

3. 某天文学家知道某颗卫星绕地球运行的周期是 x 小时，x 是整数且小于 24. 如果天文学家注意到卫星从某日 0 时至另外某日 17 时的时间间隔内完成 11 次周期运行，请问卫星的轨道周期是多少小时?

B 组

4. 编程判断同余方程 $ax \equiv b \pmod{m}$是否有解，如果有解，求出所有的解.

5. 设 p 为一个奇素数，k 为一个正整数，证明同余方程 $x^2 \equiv 1 \pmod{p^k}$正好有两个不同余的解，即 $x \equiv \pm 1 \pmod{p^k}$.

6. 如果在一个密码系统中，明文 x 被加密成密文 y，使得 $y \equiv 7x+3 \pmod{26}$，那么由密文 y 解密得到明文 x 的公式是什么?

3.2 线性同余方程组与中国剩余定理

我国古代的一部优秀的数学著作《孙子算经》中，有一类叫作“物不知数”的问题，原文如下：

“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？”

这个问题可以表达如下：现有一未知数，被 3 除余 2，被 5 除余 3，被 7 除余 2，求此未知数. 我国明代数学家程大位(字汝思，号宾渠，1533—1606)在《算法统宗》这部著作中，把解法用一首优美的诗来总结：

三人同行七十稀，五树梅花廿一枝，

七子团圆整半月，除百零五便得知.

这首诗的意思是，将此未知数被 3 除所得的余数乘 70，被 5 除所得的余数乘 21，被 7 除所得的余数乘 15，再将它们求和，将和除以 105，得到的余数即为所求未知数. 于是，以上“物不知数”问题可求解如下：

$$2\times70+3\times21+2\times15=233,$$

将 233 除以 105，余数 23 即为所求.

这个问题为什么可以这样求解？这是不是一种巧合？在这个问题中，我们遇到的是 3 除, 5 除, 7 除，如果用其他的数代替 3, 5, 7，能否有同样类似的解法？著名的中国剩余定理，也称为“孙子定理”等，就是用来解决这类问题的.

这其实就是一个求一次同余方程组的问题，此同余方程组表示如下，注意其中每一行的模数各不相同而且两两互素：

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

我们先来直观的看一下这个问题的解法，这个问题看上去是不好解的，但是如果我们换一个类似的问题，就会感觉好解了，如下：

$$\begin{cases} x\equiv 0 \pmod 3 \\ x\equiv 0 \pmod 5 \\ x\equiv 0 \pmod 7 \end{cases}$$

由同余的概念马上可知道，$3|x$，$5|x$，$7|x$，所以 $3\times5\times7|x$，即 $105|x$，因此方程组的解必为

$$x\equiv 0 \pmod{105}.$$

让我们再换一个稍微复杂的问题

$$\begin{cases} a\equiv 1 \pmod 3 \\ a\equiv 0 \pmod 5 \\ a\equiv 0 \pmod 7 \end{cases}$$

类似于上面问题的思考思路，由第二和第三式知道 $5\times7|a$，即 $35|a$，也就是 a 为 35 的倍数，那么接下来要看 35 的倍数中哪些除以 3 余 1，也就是看 35 的倍数中哪些具有如下的性质

$$35\times n\equiv 1 \pmod 3,$$

很明显 35 与 n 互为模 3 的逆元，35 本身不行，但是 70 就行了（注意这个时候 $n=2$），从而 70 +105 的倍数也行，所以方程组的解必为

$$a\equiv 70 \pmod{105}.$$

同样的道理，我们对方程组

$$\begin{cases} b\equiv 0 \pmod 3 \\ b\equiv 1 \pmod 5 \\ b\equiv 0 \pmod 7 \end{cases}$$

得到解为

$$b\equiv 21 \pmod{105}.$$

对方程组

$$\begin{cases} c \equiv 0 \pmod 3 \\ c \equiv 0 \pmod 5 \\ c \equiv 1 \pmod 7 \end{cases}$$

得到解为

$$c \equiv 15 \pmod{105}.$$

另外，我们很容易观察到：

$$\begin{cases} 2a \equiv 2 \pmod 3 \\ 2a \equiv 0 \pmod 5 \\ 2a \equiv 0 \pmod 7 \end{cases}$$

$$\begin{cases} 3b \equiv 0 \pmod 3 \\ 3b \equiv 3 \pmod 5 \\ 3b \equiv 0 \pmod 7 \end{cases}$$

和

$$\begin{cases} 2c \equiv 0 \pmod 3 \\ 2c \equiv 0 \pmod 5 \\ 2c \equiv 2 \pmod 7 \end{cases}$$

所以，原来方程的解必为

$$x \equiv 2a + 3b + 2c \pmod{105}.$$

前面提及的实际数值解答为

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

□

将此问题推广，我们可给出下面定理.

定理 3.2.1 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，若令

$$m = m_1 m_2 \cdot \cdots \cdot m_k,$$

$$M_i = m_1 m_2 \cdot \cdots \cdot m_{i-1} m_{i+1} \cdot \cdots \cdot m_k,$$

（即 $m = m_i M_i$），$i = 1,2,\ldots,k$

则对任意的整数 b_1，$b_1, \ldots, b_k$，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \tag{3.2.1}$$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod m, \tag{3.2.2}$$

其中

$$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1,2,\ldots,k.$$

证明　由于对任意给定的 i 和 j，若满足 $1\leqslant i, j\leqslant k$ 且 $i\neq j$，则有

$$(m_i, m_j) = 1,$$

故

$$(m_i, M_i) = 1.$$

于是对每一个 M_i，存在一个唯一的 M_i'，$i = 1,2,\ldots,k$，使得

$$M_i'M_i \equiv 1 \pmod{m_i},\quad i = 1,2,\ldots,k.$$

又由 $m = m_iM_i$，得 $m_i \mid M_j$，$i\neq j$，因此

$$M_1'M_1b_1 + M_2'M_2b_2 + \cdots + M_k'M_kb_k \equiv M_i'M_ib_i \equiv b_i \pmod{m_i},\quad i = 1,2,\ldots,k,$$

即(3.2.2)式是同余方程组(3.2.1)的解.

再证明这个解的唯一性．设 x_1, x_2 是满足同余方程组(3.2.1)的任意两个整数，则

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

因为 $m_1, m_2, \ldots, m_k$ 是 k 个两两互素的正整数，根据定理 2.1.9，进而有

$$x_1 \equiv x_2 \pmod{m},$$

即解是唯一的．定理得证.

□

这个定理就是著名的**中国剩余定理**.

例 3.2.1　求解同余方程组

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 6 \pmod{13} \end{cases}$$

解　利用定理 3.2.1，其中 $m_1 = 3$，$m_2 = 5$，$m_3 = 7$，$m_4 = 13$．令 $m = m_1m_2m_3m_4 = 1\,365$，则

$$M_1 = m_2m_3m_4 = 455,\quad M_2 = m_1m_3m_4 = 273,$$
$$M_3 = m_1m_2m_4 = 195,\quad M_4 = m_1m_2m_3 = 105,$$

分别求解同余方程

$$M_i'M_i \equiv 1 \pmod{m_i},\quad i = 1, 2, 3, 4,$$

得

$$M_1' = 2,\quad M_2' = 2,\quad M_3' = 6,\quad M_4' = 1,$$

故此同余方程组的解为

$$x \equiv 2\times455\times1 + 2\times273\times2 + 6\times195\times4 + 1\times105\times6 \equiv 7\,312 \equiv 487 \pmod{1\,365}.$$

□

定理 3.2.2　设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，令

$$m = m_1m_2\cdot\cdots\cdot m_k,$$
$$m = m_iM_i,$$
$$M_i'M_i \equiv 1 \pmod{m_i},\quad i = 1,2,\ldots,k,$$

若 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则

$$M_1'M_1b_1 + M_2'M_2b_2 + \cdots + M_k'M_kb_k$$

遍历模 m 的完全剩余系.

证明 令

$$x_0 = M_1'M_1b_1 + M_2'M_2b_2 + \cdots + M_k'M_kb_k \pmod{m},$$

则当 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系时，x_0 遍历 m 个整数. 下面证明这 m 个整数两两模 m 不同余. 若

$$M_1'M_1b_1 + \cdots + M_k'M_kb_k \equiv M_1'M_1b_1' + \cdots + M_k'M_kb_k' \pmod{m},$$

其中 b_i 和 b_i' 在同一个模 m_i 的完全剩余系中取值，由于 $m_i \mid m$，$m_i \mid M_j$，$i \neq j$，故根据定理 2.1.8 有

$$M_i'M_ib_i \equiv M_i'M_ib_i' \pmod{m_i}, \quad i = 1,2,\ldots,k,$$

又因为

$$M_i'M_i \equiv 1 \pmod{m_i}, \quad i = 1,2,\ldots,k,$$

所以

$$b_i \equiv b_i' \pmod{m_i}, \quad i = 1,2,\ldots,k.$$

由于 b_i 和 b_i' 在同一个模 m_i 的完全剩余系中取值，故只能有

$$b_i = b_i', \quad i = 1,2,\ldots,k.$$

定理得证.

□

以上定理可以看作是定理 2.2.4 的推广.

定理 3.2.3 同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

有解的充要条件是$(m_1, m_2) \mid (b_1 - b_2)$. 如果上述条件成立，则同余方程组模$[m_1, m_2]$有唯一解.

证明 设$(m_1, m_2) = d$，先证必要性. 若 x_0 为同余方程组的解，则有

$$x_0 \equiv b_1 \pmod{d}, \qquad x_0 \equiv b_2 \pmod{d},$$

两式相减得 $b_1 - b_2 \equiv 0 \pmod{d}$，因此 $d \mid b_1 - b_2$.

再证充分性. 若 $d \mid b_1 - b_2$，则因 $x \equiv b_1 \pmod{m_1}$的解可写为

$$x = b_1 + m_1y,$$

将其代入 $x \equiv b_2 \pmod{m_2}$得

$$m_1y \equiv b_2 - b_1 \pmod{m_2}.$$

因为$(m_1, m_2) = d$，$d \mid b_2 - b_1$，故上式有解，即原同余方程组有解.

设原同余方程组有两个解分别为 x_1 和 x_2，则

$$x_1 - x_2 \equiv 0 \pmod{m_1}, \qquad x_1 - x_2 \equiv 0 \pmod{m_2},$$

于是有 $x_1 - x_2 \equiv 0 \pmod{[m_1, m_2]}$，即同余方程组模$[m_1, m_2]$有唯一解.

通过以上述定理可知，对于一次同余方程组

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

其中 $k \geqslant 3$，若$(m_1, m_2) \mid b_1 - b_2$，可先解前面两个方程得

$$x \equiv b_2' \pmod{[m_1, m_2]}.$$

若$([m_1, m_2], m_3) \mid b_2' - b_3$，则可再与后面的 $x \equiv b_3 \pmod{m_3}$联立解出

$$x \equiv b_3' \pmod{[m_1, m_2, m_3]}.$$

依此类推，最后可得唯一解

$$x \equiv b_k' \pmod{[m_1, m_2, \cdots, m_k]}.$$

如果中间有一步出现无解，则原同余方程组无解．定理得证．

□

例 3.2.2 判断方程组

$$\begin{cases} x \equiv 11 \pmod{36} \\ x \equiv 7 \pmod{40} \\ x \equiv 32 \pmod{75} \end{cases}$$

是否有解.

解 $(36, 40) = 4$，$(36, 75) = 3$，$(40, 75) = 5$.

$$b_1 - b_2 = 11 - 7 = 4,$$

$$b_1 - b_3 = 1 - 32 = -21,$$

$$b_2 - b_3 = 7 - 32 = -25.$$

因此方程组肯定有解，因为方程组满足有解条件，即 $4 \mid 4$，$3 \mid -21$，$5 \mid -25$．且解的模数是 $[36, 40, 75]=1\ 800$．这个方程的解为 $x \equiv 407 \pmod{1\ 800}$．有兴趣的读者可以自行练习写出全部求解过程.

□

定理 3.2.4 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，令$m = m_1 m_2 \cdot \cdots \cdot m_k$，则同余方程

$$f(x) \equiv 0 \pmod{m} \tag{3.2.3}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \quad\vdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases} \tag{3.2.4}$$

等价．若用 T_i 表示同余方程

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

的解数（即解的个数），$i=1,2,\ldots,k$，用 T 表示同余方程(3.2.3)的解数，则

$$T=T_1T_2\cdot\cdots\cdot T_k.$$

证明 设 x_0 为同余方程(3.2.3)的解，则

$$f(x_0)\equiv 0 \pmod m.$$

由定理 2.1.8 可知

$$f(x_0)\equiv 0 \pmod{m_i},\quad i=1,2,\ldots,k,$$

即 x_0 亦为同余方程组(3.2.4)的解.

若 x_0 为同余方程组(3.2.4)的解，即

$$f(x_0)\equiv 0 \pmod{m_i},\quad i=1,2,\ldots,k.$$

由定理 2.1.9 可知

$$f(x_0)\equiv 0 \pmod m,$$

即 x_0 亦为同余方程(3.2.3)的解.

设同余方程 $f(x)\equiv 0 \pmod{m_i}$的解为 b_i，$i=1,2,\ldots,k$. 由孙子定理可知同余方程组

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

的解为

$$x\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots+M_k'M_kb_k \pmod m.$$

由于

$$f(x)\equiv f(b_i)\equiv 0 \pmod{m_i},\quad i=1,2,\ldots,k,$$

故 x 亦为同余方程(3.2.3)的解. 于是当 b_i 遍历 $f(x)\equiv 0 \pmod{m_i}$的所有解时，x 遍历同余方程(3.2.3)的所有解. 于是，有$T=T_1T_2\cdot\cdots\cdot T_k$. 定理得证.

□

例 3.2.3 求解同余方程

$$x^4+2x^3+8x+9\equiv 0 \pmod{35}.$$

解 设 $f(x)=x^4+2x^3+8x+9$，由定理 3.2.4 知同余方程 $f(x)\equiv 0 \pmod{35}$等价于同余方程组

$$\begin{cases} f(x)\equiv 0 \pmod 5 \\ f(x)\equiv 0 \pmod 7 \end{cases}$$

用直接验算的方法容易得到 $f(x)\equiv 0 \pmod 5$的解为

$$x\equiv 1,4 \pmod 5,$$

$f(x)\equiv 0 \pmod 7$的解为

$$x\equiv 3,5,6 \pmod 7.$$

由孙子定理，可求出同余方程组

$$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 7 \end{cases}$$

当(b_1, b_2)分别取$(1, 3),\ (1, 5),\ (1, 6),\ (4, 3),\ (4, 5),\ (4, 6)$时的解为

$$x \equiv 21b_1 + 15b_2 \equiv 31, 26, 6, 24, 19, 34 \pmod{35}.$$

这 6 个解即为原同余方程的解.

□

这个定理使我们能够利用孙子定理来解单个的具有较大模数的线性同余方程， 这种方法可能在计算上更有效率.

例 3.2.4 求解 $13x \equiv 71 \pmod{380}$.

解 因为 $380 = 4\times5\times19$，所以它等价于如下方程组

$$\begin{cases} 13x \equiv 71 \pmod 4 \\ 13x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} (4+4+4+1)x \equiv 71 \pmod 4 \\ (5+5+3)x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv 71 \pmod 4 \\ 3x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv 3 \pmod 4 \\ 3x \equiv 1 \pmod 5 \\ 13x \equiv 14 \pmod{19} \end{cases}$$

利用单同余方程式的解法可得到

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod{19} \end{cases}$$

接着应用孙子定理求解即可，最后得到的解为

$$x \equiv 327 \pmod{380}.$$

□

前面讨论的同余方程组问题中， 我们注意到方程组中的每一行的模数都不相同， 而且只有一个待解的未知元. 还有另一类重要的多元线性同余方程组问题， 不同之处在于这类问题中的模数都相同， 而且具有两个或者两个以上的未知元. 这样的问题与我们在线性代数中学过的关于实数和复数的方程组问题非常相像， 而且可以使用很多线性代数中的向量和矩阵的表示及运算方法. 下面通过实例来加深读者对此的理解.

例 3.2.5 在古典的 Hill 密码中， 如果按对加密， 则每一对明文组成的行向量用(x_1, x_2)

来表示，加密后的密文对形成的行向量用(y_1, y_2)来表示，y_1, y_2是由x_1, x_2的线性组合计算而来：

$$\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 8x_1 + 7x_2 \pmod{26} \end{cases}$$

使用矩阵表达即为

$$(y_1, y_2) \equiv (x_1, x_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \pmod{26}.$$

其中的 2 乘 2 阶矩阵被称作密钥，那么如何解密呢，即如何由(y_1, y_2)来计算得到(x_1, x_2)呢？实际上，我们可以采用消元方法来解，先消去未知元x_2解得x_1，然后采用同样的方法，先消去未知元x_1解得x_2．还可以利用逆矩阵的方法，即

$$(x_1, x_2) \equiv (y_1, y_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} \pmod{26},$$

其中

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

我们可以验证一下这个逆矩阵的正确性：

$$\begin{aligned} &\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \\ =&\begin{pmatrix} 11\times 7 + 8\times 23 & 11\times 18 + 8\times 11 \\ 3\times 7 + 7\times 23 & 3\times 18 + 7\times 11 \end{pmatrix} \\ =&\begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix} \\ \equiv&\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26} \end{aligned}$$

两者的乘积是单位矩阵，说明它们互为逆矩阵.

如果明文是$(x_1, x_2) = (9, 20)$，计算过程如下：

$$(9,20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99+60, 72+140) \equiv (3,4) \pmod{26}.$$

则密文为(3, 4)．反过来，接收方收到密文(3, 4)后，希望恢复明文，计算过程如下：

$$(3,4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (21+92, 54+44) \equiv (9,20) \pmod{26},$$

可见的确正确地恢复了明文(9, 20).

□

那么，在模 26 运算下，如何判断矩阵是否可逆，又如何计算可逆矩阵的逆矩阵呢？下

面我们不加证明地给出有关定理.

定理 3.2.5 矩阵 **K** 在模 26 运算下存在可逆矩阵的充分必要条件是(det **K**, **26**) = 1 (det **K** 表示矩阵 **K** 的行列式的值).

定理 3.2.6 如果二阶矩阵

$$K=\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

可逆，则其逆矩阵为

$$K^{-1}=(\det K)^{-1}\begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix} \pmod{26}.$$

习题 3.2

A 组

1. 求解以下同余方程组：

(1) $\begin{cases} x\equiv 9 \pmod{12} \\ x\equiv 6 \pmod{25} \end{cases}$ (2) $\begin{cases} x\equiv 4 \pmod{11} \\ x\equiv 3 \pmod{17} \end{cases}$

(3) $\begin{cases} x\equiv 2 \pmod{9} \\ 3x\equiv 4 \pmod{5} \\ 4x\equiv 3 \pmod{7} \end{cases}$ (4) $\begin{cases} x\equiv 5 \pmod{7} \\ x\equiv 12 \pmod{15} \\ x\equiv 18 \pmod{22} \end{cases}$

2. 求解以下同余方程组（注意不只一个解）：

$$\begin{cases} 2x\equiv 3 \pmod{5} \\ 4x\equiv 2 \pmod{6} \\ 3x\equiv 2 \pmod{7} \end{cases}$$

3. 有总数不满 50 人的一队士兵，一至三报数，最后一人报“一”；一至五报数，最后一人报“二”；一至七报数，最后一人也报“二”. 这队士兵有多少人？

4. 利用转化成联立方程组的方法解 $91x\equiv 419 \pmod{440}$.

5. 求解同余方程$x^2+18x-823\equiv 0 \pmod{1\,800}$.

6. 对于同余方程组

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \end{cases}$$

(1) 证明上述方程组有一个解当且仅当$(m_1, m_2)\mid(a_1-a_2)$；

(2) 证明当上述方程组有解时，该解模$[m_1, m_2]$是唯一的.

B 组

7. 一个数被 3, 5, 7, 11 除所得的余数均为 2, 且为 13 的倍数, 求出符合上述条件的最小正整数.

8. 已知有相邻的 4 个正整数, 它们依次可被 2^2, 3^2, 5^2 及 7^2 整除, 求出符合上述条件的最小一组正整数.

9. 对于同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

(1) 证明上述方程组有一个解当且仅当对于所有的(i, j)都满足$(m_i, m_j) \mid (a_i - a_j)$, 其中 $1 \leqslant i < j \leqslant r$;

(2) 证明当上述方程组有解时, 该解模$[m_1, m_2, \ldots, m_r]$是唯一的.

10. 编程实现中国剩余定理.

11. 已知 Hill 密码中的明文分组长度是 2, 密钥 $\boldsymbol{K}$ 是一个 2 阶可逆方阵. 假设明文 3, 14, 2, 19 所对应的密文是 1, 14, 11, 21, 试求密钥 $\boldsymbol{K}$.

3.3 二次剩余

本节介绍二次同余方程的解法——二次剩余理论. 二次剩余理论在数论中有着深刻的结果, 是现代类域论的雏形, 在椭圆曲线密码学中也有重要的应用. 另外, 二次剩余还应用于 Rabin 公钥密码算法中.

我们在中学学过一元二次方程理论, 我们知道, 对于实系数一元二次方程的根, 存在判别式用于判断它有没有根, 有几个根; 如果有根, 可以用求根公式求出它的全部根. 但是到目前为止, 人们还没有找到具有普遍性的有效方法来求解一般的多项式同余方程. 除了求根方法的问题以外, 还有一个与此有关的问题, 即在没有求出方程的根的时候, 是否存在一个有效的方法来判断方程的可解性, 也就是说判断方程有没有解. 二次同余方程在后面这个问题上有比较丰富的理论, 其核心就是本节的二次剩余和 3.4 节的二次互反律.

设 m 是大于 1 的整数, a 是与 m 互素的整数, 若

$$x^2 \equiv a \pmod{m} \tag{3.3.1}$$

有解, 则 a 叫作模 m 的二**次剩余**, 或**平方剩余**. 否则, a 叫作模 m 的二**次非剩余**, 或**平方非剩余**.

下面关于一般形式的二次同余方程的讨论将使我们看到二次同余方程的可解性与二次剩余的概念是紧密联系在一起的.

考虑下面的二次同余方程

$$ax^2+bx+c\equiv 0 \pmod{p} \tag{3.3.2}$$

其中 p 是一个奇素数且 $a\not\equiv 0(\mathrm{mod}\ p)$，即$(a,p)=1$．所以$(4a,p)=1$．因此，方程(3.3.2)与下面的方程等价

$$4a(ax^2+bx+c)\equiv 0 \pmod{p},$$

即

$$(2ax+b)^2-(b^2-4ac)\equiv 0 \pmod{p},$$

移项后得到

$$(2ax+b)^2\equiv (b^2-4ac) \pmod{p}.$$

现在，令 $y=2ax+b$，$d=b^2-4ac$，则得到

$$y^2\equiv d \pmod{p} \tag{3.3.3}$$

如果 $x\equiv x_0 \pmod{p}$是方程(3.3.2)的一个解，那么任意整数 $y_0\equiv 2ax_0+b \pmod{p}$就是方程(3.3.3)的解．反过来，如果 $y\equiv y_0 \pmod{p}$是方程(3.3.3)的一个解，那么下面的线性同余方程

$$2ax\equiv y_0-b \pmod{p}$$

的解

$$x\equiv x_0=(2a)^{-1}(y_0-b) \pmod{p}$$

就是原方程(3.3.2)的一个解.

例 3.3.1 求解二次同余方程 $5x^2-6x+2\equiv 0 \pmod{13}$.

解 $d=b^2-4ac=36-40=-4$，因此我们需要先解如下的具有简单形式的二次同余方程

$$y^2\equiv -4\equiv 9 \pmod{13},$$

它的解是 $y\equiv 3, 10(\mathrm{mod}\ 13)$．接着需要分别求解两个线性同余方程

$$10x\equiv 9 \pmod{13},$$

和

$$10x\equiv 16 \pmod{13}.$$

由于 10 的逆元是 4，所以这两个方程的解分别为 $x\equiv 10, 12 \pmod{13}$．这两个解就是原方程的解.

□

上面的讨论说明模数为奇素数的一般形式的二次同余方程(3.3.2)的可解性问题与b^2-4ac是否为二次剩余的问题是等价的．根据高次同余方程的理论（参见“3.6 节 高次同余方程”的相关内容）可知，对于一般的模数来说，总可以将方程化为模数为素数幂的联立方程组，同时模数为素数幂的方程的解可以通过模数为素数的方程的解求得，此外模数为 2 的二次同余方程求解非常简单，因此，讨论模数为奇素数的方程(3.3.2)的可解性是至关重要的．相应地，我们将着重讨论模数为奇素数的二次剩余问题，即

$$x^2\equiv a \pmod{p}, \tag{3.3.4}$$

其中 p 是奇素数.

例 3.3.2 求模 13 的二次剩余和二次非剩余.

解 首先, 我们注意到如果 $a \equiv b \pmod{13}$, 那么 a 是模 13 的二次剩余当且仅当 b 是模 13 的二次剩余. 因此, 我们只需要在 1 到 12 的范围内找模 13 的二次剩余. 通过计算得到

$$1^2 \equiv 12^2 \equiv 1 \pmod{13},$$

$$2^2 \equiv 11^2 \equiv 4 \pmod{13},$$

$$3^2 \equiv 10^2 \equiv 9 \pmod{13},$$

$$4^2 \equiv 9^2 \equiv 3 \pmod{13},$$

$$5^2 \equiv 8^2 \equiv 12 \pmod{13},$$

$$6^2 \equiv 7^2 \equiv 10 \pmod{13},$$

所以, 模 13 的二次剩余是 1,3,4,9,10,12. 当然, 模 13 的二次非剩余是 2,5,6,7,8,11.

同理可验证，模 17 的二次剩余是 1, 2, 4, 8, 9, 13, 15, 16, 模 17 的二次非剩余是 3, 5, 6, 7, 10, 11, 12, 14；模 19 的二次剩余是 1, 4, 5, 6, 7, 9, 11, 16, 17, 模 19 的二次非剩余是 2, 3, 8, 10, 12, 13, 14, 15, 18.

□

下面，我们给出二次剩余的**欧拉判别条件**，即定理 3.3.1.

定理 3.3.1 设 p 是奇素数，$(a, p)=1$，则

(1) a 是模 p 的二次剩余的充要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

(2) a 是模 p 的二次非剩余的充要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

并且当 a 是模 p 的二次剩余时，同余方程(3.3.4)恰有二解.

证明 (1) 先证必要性. 若 a 是模 p 的二次剩余，则有整数 x 满足

$$x^2 \equiv a \pmod{p}.$$

因为$(a, p)=1$，所以$(x, p)=1$, 应用欧拉定理，可知

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

再证充分性. 用反证法, 假设满足

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

即 a 不是模 p 的二次剩余. 考虑线性同余方程 $sx \equiv a \pmod{p}$，由定理 3.1.1, 当 s 从 p 的最小正缩系中取值时, 方程 $sx \equiv a \pmod{p}$ 必有唯一解. 亦即 s 取 p 的最小正缩系中的每个元素 i, 必有唯一的 $x=x_i$ 属于 p 的最小正缩系, 使得 $sx \equiv a \pmod{p}$ 成立; 若 a 不是模 p 的二次剩余, 则 $i \neq x_i$, 这样 p 的最小正缩系中的 $p-1$ 个数可以按$<i, x_i>$两两配对相乘, 得到

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p},$$

由威尔逊定理$(p-1)! \equiv -1 \pmod{p}$，所以有

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

这与条件 $a^{(p-1)/2} \equiv 1 \pmod{p}$矛盾. 所以必定存在一个 i, 使得 $i=x_i$, 即 a 是模 p 的二次剩余.

(2) 由于 a 与 p 互素，根据欧拉定理，可知

$$a^{p-1} \equiv 1 \pmod{p},$$

即 $p|a^{p-1}-1$. 由定理 2.4.3 有

$$p|(a^{\frac{p-1}{2}}-1) \text{ 或 } p|(a^{\frac{p-1}{2}}+1).$$

根据(1)的证明，可知 a 是模 p 的二次非剩余的充要条件是

$$p|(a^{\frac{p-1}{2}}+1),$$

即

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

定理得证.

□

例 3.3.3 利用欧拉判别条件判断 2 和 3 是否为模 13 的二次剩余或者二次非剩余.

解 由于

$$2^{\frac{(13-1)}{2}} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13},$$

所以 2 是模 13 的二次非剩余. 而

$$3^{\frac{(13-1)}{2}} = 3^6 = 27^2 \equiv 1^2 \equiv 1 \pmod{13},$$

所以 3 是模 13 的二次剩余. 此时，$x^2 \equiv 3 \pmod{13}$必有两个解，在例 3.3.2 中我们已经知道解为 4 和 9.

□

定理 3.3.2 设 p 是奇素数，则模 p 的缩系中二次剩余与非二次剩余的个数各为 $\frac{p-1}{2}$，且 $\frac{p-1}{2}$ 个二次剩余分别与序列

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2 \tag{3.3.5}$$

中的一个数模 p 同余，且仅与一个数模 p 同余.

证明 取模 p 的绝对值最小的缩系

$$-\frac{p-1}{2},\ -\frac{p-1}{2}+1,\ \cdots,-1,\ 1,\ \cdots,\ \frac{p-1}{2}-1,\ \frac{p-1}{2}$$

来讨论. a 是模 p 的二次剩余当且仅当 a 的值为以下数列

$$\left(-\frac{p-1}{2}\right)^2,\ \left(-\frac{p-1}{2}+1\right)^2,\ \dots,(-1)^2,(1)^2,\dots,\left(\frac{p-1}{2}-1\right)^2,\ \left(\frac{p-1}{2}\right)^2 \pmod p$$

中的某一项, 而$(-i)^2 = i^2 \pmod p$，所以 a 是模 p 的二次剩余当且仅当 a 的值为以下数列

$$(1)^2,\dots,\left(\frac{p-1}{2}-1\right)^2,\ \left(\frac{p-1}{2}\right)^2 \pmod p$$

中的某一项, 又因为 $1\leqslant i<j\leqslant\frac{p-1}{2}$ 时, $i^2 \not\equiv j^2 \pmod p$, 所以模 p 的全部二次剩余即

$$(1)^2,\dots,\left(\frac{p-1}{2}-1\right)^2,\ \left(\frac{p-1}{2}\right)^2 \pmod p$$

共有 $\frac{p-1}{2}$ 个，模 p 的二次非剩余共有$(p-1)-\frac{p-1}{2}=\frac{p-1}{2}$ 个. 定理得证.

□

例 3.3.2 很好地验证了这个定理.

习题 3.3

A 组

1. 求 23, 31, 37, 47 的二次剩余和二次非剩余.
2. 求满足方程 $E: y^2 = x^3 - 3x + 1 \pmod 7$的所有点.
3. 求满足方程 $E: y^2 = x^3 + 3x + 2 \pmod 7$的所有点.
4. 利用欧拉判别条件判断 2 是否为 29 的二次剩余.

B 组

5. 设 p 为奇素数, 证明–1 是模 p 的二次剩余的充要条件.
6. 编写程序使用欧拉判别条件判别输入的 a 是模 p 二次剩余, 或是二次非剩余, 如果是二次剩余，输出 $x^2 \equiv a \pmod p$的两个解.

3.4 勒让德符号与二次互反律

3.4.1 勒让德符号

3.3 节虽然给出了模 p 的二次剩余的欧拉判别条件，但是当 p 比较大时，很难实际应用. 现在我们引入由大数学家勒让德于 1798 年发明的勒让德符号，以此给出一个比较便于实际计算的二次剩余判别方法.

定义 3.4.1 设 p 是奇素数，$(a, p)=1$，定义**勒让德(Legendre)符号**如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若}a\text{是模}p\text{的二次剩余};\\ -1, & \text{若}a\text{是模}p\text{的二次非剩余}.\end{cases}$$

注：$\left(\frac{a}{p}\right)$读作 a 对 p 的勒让德符号.

例 3.4.1　利用例 3.3.2 写出对 13 的勒让德符号.

解　$\left(\frac{1}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{10}{13}\right)=\left(\frac{12}{13}\right)=1$,

$$\left(\frac{2}{13}\right)=\left(\frac{5}{13}\right)=\left(\frac{6}{13}\right)=\left(\frac{7}{13}\right)=\left(\frac{8}{13}\right)=\left(\frac{11}{13}\right)=-1.$$

利用勒让德符号，我们可以将定理 3.3.1 改写如下.

定理 3.4.1*　设 p 是奇素数，a 是与 p 互素的整数，则

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod{p}.$$

显然，我们有$\left(\frac{1}{p}\right)=1$.

进一步，我们可以得出有关勒让德符号的一些性质.

定理 3.4.2　设 p 是奇素数，a, b 都是与 p 互素的整数，我们有

(1) 若 $a\equiv b(\mathrm{mod}\, p)$，则$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(3) $\left(\frac{a^2}{p}\right)=1$.

证明　(1) 因为 $a\equiv b \pmod{p}$，所以同余方程

$$x^2\equiv a \pmod{p}$$

等价于同余方程

$$x^2\equiv b \pmod{p}.$$

因此

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right).$$

(2) 根据欧拉判别条件，我们有

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod{p}, \quad \left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}} \pmod{p}, \quad \left(\frac{ab}{p}\right)\equiv (ab)^{\frac{p-1}{2}} \pmod{p}.$$

因此

$$\left(\frac{ab}{p}\right)\equiv(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\mathrm{mod}\,p).$$

由于勒让德符号取值只有 ± 1，且 p 是奇素数，故

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

（**注：**这一结论有如下的推论 3.4.1）.

(3) 显然，a^2 是模 p 的二次剩余，所以必有

$$\left(\frac{a^2}{p}\right)=1.$$

定理得证.

□

推论 3.4.1 设 p 是奇素数，a, b 都是与 p 互素的整数，那么

a) 若 a, b 均为模 p 的二次剩余，则 ab 也是模 p 的二次剩余；

b) 若 a, b 均为模 p 的二次非剩余，则 ab 是模 p 的二次剩余；

c) 若 a, b 中有一个为模 p 的二次剩余，另一个为模 p 的二次非剩余，则 ab 是模 p 的二次非剩余.

证明 由定理 3.4.2，结论很显然.

□

当 $a=\pm 2^k q_1^{l_1}q_2^{l_2}\cdots q_s^{l_s}$，其中 q_i ($i = 1, 2, \cdots, s$)为不同的奇素数，根据上面的定理，我们有

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^k\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s}.$$

因为 $\left(\frac{1}{p}\right)=1$，所以任给一个与 p 互素的整数 a，计算 $\left(\frac{a}{p}\right)$ 时，只需算出以下三种值：

$$\left(\frac{-1}{p}\right),\ \left(\frac{2}{p}\right),\ \left(\frac{q}{p}\right)(q\text{ 为奇素数}).$$

需要注意的是，这种计算方法依赖于对 a 的因子分解，而目前还没有找到高效的因子分解方法，因此这里的勒让德符号的计算方法对大的模数 p 和整数 a 来说不切实际.

根据欧拉判别条件，显然我们可得出以下定理.

定理 3.4.3 设 p 是奇素数，我们有

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{若 } p\equiv 1(\mathrm{mod}\,4),\\ -1, & \text{若 } p\equiv 3(\mathrm{mod}\,4).\end{cases}$$

例 3.4.2　判断 $x^2 \equiv -46 \pmod{17}$是否有解.

解　$\left(\frac{-46}{17}\right)=\left(\frac{-1}{17}\right)\left(\frac{46}{17}\right)=\left(\frac{46}{17}\right)=\left(\frac{17\times 2+12}{17}\right)=\left(\frac{12}{17}\right)=\left(\frac{3}{17}\right)\left(\frac{2^2}{17}\right)=\left(\frac{3}{17}\right)$,

而$\left(\frac{3}{17}\right)\equiv 3^{\frac{17-1}{2}}=3^8=81^2\equiv -1 \pmod{17}$，所以原方程无解.

□

3.4.2 高斯引理

关于勒让德符号计算，古典数论得出了非常精彩的研究成果. 为此，我们先介绍德国数学家高斯关于二次剩余的**高斯引理**.

定理 3.4.4（高斯引理（二次剩余））　设 p 是奇素数，a 是与 p 互素的整数，如果下列 $\frac{p-1}{2}$ 个整数

$$a\cdot 1,\quad a\cdot 2,\quad a\cdot 3,\quad \cdots,\ a\cdot\frac{p-1}{2}$$

模 p 后得到的最小正剩余中大于 $\frac{p}{2}$ 的个数是 m，则

$$\left(\frac{a}{p}\right)=(-1)^m.$$

证明　设 $a_1, a_2, \cdots, a_l$ 是整数

$$a\cdot 1,\quad a\cdot 2,\quad a\cdot 3,\quad \ldots,\ a\cdot\frac{p-1}{2}$$

模 p 后小于 $\frac{p}{2}$ 的最小正剩余，$b_1, b_2, \cdots, b_m$ 是这些整数模 p 后大于 $\frac{p}{2}$ 的最小正剩余，显然

$$l+m=\frac{p-1}{2},$$

则原来的 $\frac{p-1}{2}$ 个整数之积和相应的最小正剩余之间具有如下关系

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!=\prod_{k=1}^{\frac{p-1}{2}}ak\equiv\prod_{i=1}^{l}a_i\prod_{j=1}^{m}b_j\equiv(-1)^m\prod_{i=1}^{l}a_i\prod_{j=1}^{m}(p-b_j)\pmod{p}.$$

下面证明 $a_1, a_2, \ldots, a_l, p-b_1, p-b_2, \ldots, p-b_m$ 两两互不相等，这只需证明

$$a_s\neq p-b_t,\quad s=1,2,\ldots,l,\quad t=1,2,\ldots,m.$$

用反证法，假设存在

$$a_s=p-b_t,$$

则有

$$ak_i\equiv p-ak_j \pmod{p},$$

即

$$ak_i + ak_j \equiv 0 \pmod{p},$$

于是

$$k_i + k_j \equiv 0 \pmod{p},$$

即有 $p \mid k_i + k_j$.

因为

$$1 \leqslant k_i \leqslant \frac{p-1}{2},\ i = 1, 2, \ldots, \frac{p-1}{2},$$

$$1 \leqslant k_j \leqslant \frac{p-1}{2},\ j = 1, 2, \ldots, \frac{p-1}{2},$$

所以

$$1 \leqslant k_i + k_j \leqslant \frac{p-1}{2} + \frac{p-1}{2} < p,$$

这与 $p \mid k_i + k_j$ 矛盾，故假设不成立. 因此，$a_1, a_2, \ldots, a_l, p - b_1, p - b_2, \ldots, p - b_m$ 这 $\frac{p-1}{2}$ 个整数两两互不相等.

由于

$$1 \leqslant a_s \leqslant \frac{p-1}{2},\ s = 1, 2, \ldots, l,$$

$$1 \leqslant p - b_t \leqslant \frac{p-1}{2},\ t = 1, 2, \ldots, m,$$

故 $a_1, a_2, \ldots, a_l, p - b_1, p - b_2, \ldots, p - b_m$ 这 $\frac{p-1}{2}$ 个整数就是 $1, 2, \ldots, \frac{p-1}{2}$ 的一个排列，于是

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^m \prod_{i=1}^{l} a_i \prod_{j=1}^{m} (p - b_j) = (-1)^m \left(\frac{p-1}{2}\right)! \pmod{p},$$

则

$$a^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}.$$

再根据欧拉判别条件，我们有

$$\left(\frac{a}{p}\right) = (-1)^m.$$

定理得证.

□

例 3.4.3 利用高斯引理判断 5 是否为模 13 的二次剩余.

解 按照高斯引理，我们首先得到(13–1)/2=6 个整数，即 5, 10, 15, 20, 25, 30，模 13 化简得到的最小正剩余为 5, 10, 2, 7, 12, 4，其中三个大于 13/2，所以

$$\left(\frac{5}{13}\right) = (-1)^3 = -1,$$

即 5 不是模 13 的二次剩余.

□

定理 3.4.5 设 p 是奇素数, 则有

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{若 } p \equiv \pm 1 \pmod 8, \\ -1, & \text{若 } p \equiv \pm 3 \pmod 8. \end{cases}$$

证明 由高斯引理, 考虑

$$2\times 1,\ 2\times 2,\ 2\times 3,\ \ldots,\ 2\times\frac{p-1}{2}$$

模 p 后得到的最小正剩余中大于 $\frac{p}{2}$ 的个数是 m, 该数列中最大的数为

$$2\cdot\frac{p-1}{2} = p-1 < p,$$

故不需要考虑模 p 问题. 这些形如 $2k$ (k = 1, 2, …, $\frac{p-1}{2}$)的数, 要满足大于 $\frac{p}{2}$ 且小于 p, 则有

$$\frac{p}{2} < 2k < p,$$

于是

$$m = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor.$$

其中符号$\lfloor x \rfloor$表示对 x 下取整. 我们在 C 语言课程中学过, 对二进制形式的整数右移一个比特, 相当于对它除以 2 后下取整. 我们可以利用这一性质来求 m 的值. 注意到 p 是奇数, 设 p 的二进制表示形式为$(x_n\cdots x_3x_2x_1 1)_2$, 我们有

$$m = (x_n\cdots x_3x_2x_1)_2 - (x_n\cdots x_3x_2)_2$$

当$x_1 = x_2$时, m 二进制表示形式的最后一个比特为 0, 因此 m 为偶数; 若 2 是模 p 的二次剩余, 则此时有

$$p = (x_n\cdots x_4 001)_2 \text{ 或者 } p = (x_n\cdots x_4 111)_2$$

即 $p \equiv \pm 1 \pmod 8$.

当$x_1 \neq x_2$时, m 二进制表示形式的最后一个比特为 1, 因此 m 为奇数; 若 2 是模 p 的二次非剩余, 则此时有

$$p = (x_n\cdots x_4 101)_2 \text{ 或者 } p = (x_n\cdots x_4 011)_2$$

即 $p \equiv \pm 3 \pmod 8$, 定理得证.

□

定理 3.4.6 设 p 是奇素数, $(a, 2p) = 1$, 则$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor}$.

证明 由于当(a, p)=1 时,

$$ak = p\left\lfloor \frac{ak}{p} \right\rfloor + r_k,\quad 0<r_k<p,\quad k = 1, 2, \ldots, \frac{p-1}{2},$$

对 $k = 1, 2, \ldots, \dfrac{p-1}{2}$ 求和，并利用高斯引理的证明中的符号，我们有

$$\begin{aligned} a\frac{p^2-1}{8} &= p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + \sum_{i=1}^{l} a_i + \sum_{j=1}^{m} b_j \\ &= p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + \sum_{i=1}^{l} a_i + \sum_{j=1}^{m} (p - b_j) + 2\sum_{j=1}^{m} b_j - mp \\ &= p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + \frac{p^2-1}{8} - mp + 2\sum_{j=1}^{m} b_j \end{aligned}$$

于是，

$$(a-1)\frac{p^2-1}{8} = p\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor - mp + 2\sum_{j=1}^{m} b_j\ .$$

因为对每个奇素数 p，都有正整数 d 使

$$p = 2d + 1,$$

则有

$$(a-1)\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + m + 2\left(\sum_{j=1}^{m} b_j + d\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor - (d+1)m \right),$$

因此，我们有

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + m \pmod 2.$$

若 a 为奇数，即$(a, 2p) = 1$ 时，有 $a^{-}1 \equiv 0 \pmod 2$，因此有

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor + m \equiv 0 \pmod 2,$$

所以上式中两个加数必然同为奇数或者偶数, 即

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor \pmod 2.$$

再根据高斯引理，可知

$$\left(\frac{a}{p}\right) = (-1)^m = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{ak}{p} \right\rfloor}.$$

定理得证.

□

3.4.3 二次互反律

下面我们给出用于计算勒让德符号的著名的**二次互反律**. 通过引入二次互反律, 可以将模数较大的二次剩余判别问题转换为模数较小的二次剩余判别问题, 从而提高勒让德符号的计算效率.

定理 3.4.7 设 p, q 是奇素数, $p \neq q$, 则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

证明 因为 p, q 是奇素数, 所以

$$(q, 2p) = 1, \quad (p, 2q) = 1,$$

于是分别有

$$\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{h=1}^{\frac{p-1}{2}}\left\lfloor\frac{qh}{p}\right\rfloor}, \qquad \left(\frac{p}{q}\right) = (-1)^{\sum\limits_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{pk}{q}\right\rfloor},$$

因此只需证明

$$\sum_{h=1}^{\frac{p-1}{2}}\left\lfloor\frac{qh}{p}\right\rfloor + \sum_{k=1}^{\frac{q-1}{2}}\left\lfloor\frac{pk}{q}\right\rfloor = \frac{p-1}{2}\cdot\frac{q-1}{2}$$

即可.

考察长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数, 如图 3.4.1 所示.

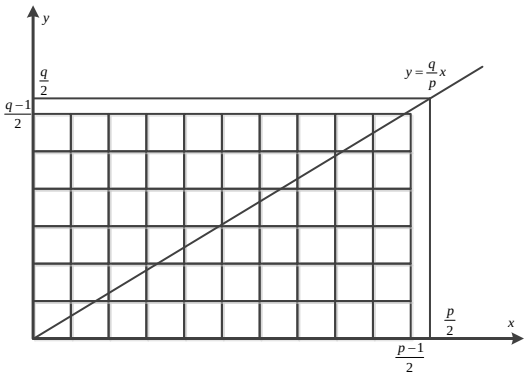

图 3.4.1 长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数（一）

设点 S 的坐标为$(h, 0)$, 点 T 是直线 $x = h$ 与直线 $y = \frac{q}{p}x$ 的交点, 其中 h 为整数, 且 $0 \leqslant h \leqslant \frac{p-1}{2}$. 如图 3.4.2 所示.

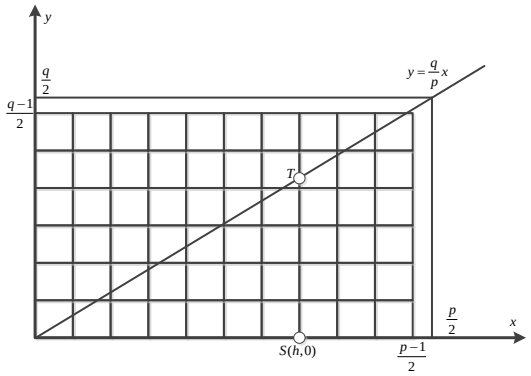

图 3.4.2 长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数（二）

则在垂直直线 ST 上，整数点个数为 $\left\lfloor \frac{qh}{p} \right\rfloor$ 为图 3.4.3 中实心点的个数.

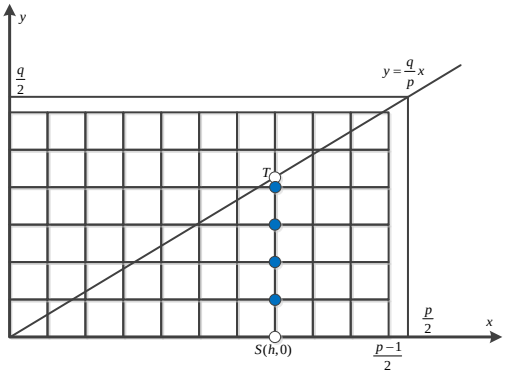

图 3.4.3 长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数（三）

于是，下三角形内的整数点个数为 $\sum_{h=1}^{\frac{p-1}{2}} \left\lfloor \frac{qh}{p} \right\rfloor$，如图 3.4.4 中的实心点所示.

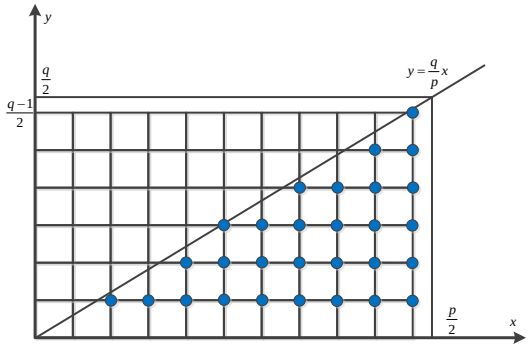

图 3.4.4 长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数（四）

同理，设点 N 的坐标为 $(0, k)$，点 M 是直线 $y=k$ 与直线 $y=\frac{q}{p}x$ 的交点，其中 k 为整数，

且 $0\leqslant k\leqslant\dfrac{q-1}{2}$. 如图 3.4.5 所示.

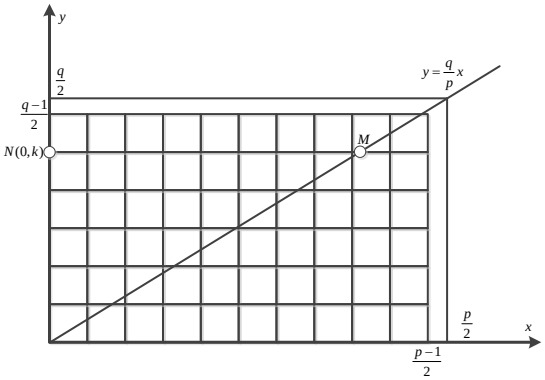

图 3.4.5 长为 $\dfrac{p}{2}$，宽为 $\dfrac{q}{2}$ 的长方形内的整数点个数（五）

于是，在水平直线 NM 上，整数点个数为 $\left\lfloor\dfrac{pk}{q}\right\rfloor$，如图 3.4.6 中的实心点所示.

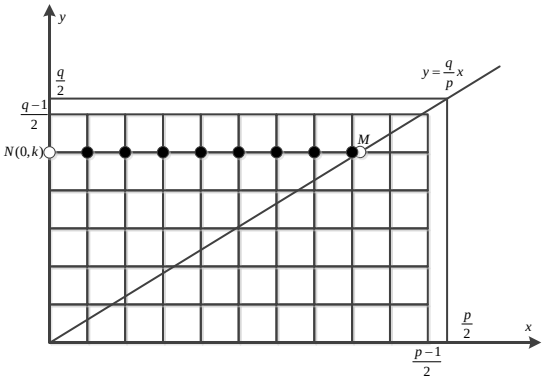

图 3.4.6 长为 $\dfrac{p}{2}$，宽为 $\dfrac{q}{2}$ 的长方形内的整数点个数（六）

于是，上三角形内的整数点个数为 $\sum\limits_{k=1}^{\frac{q-1}{2}}\left\lfloor\dfrac{pk}{q}\right\rfloor$. 如图 3.4.7 中的实心点所示.

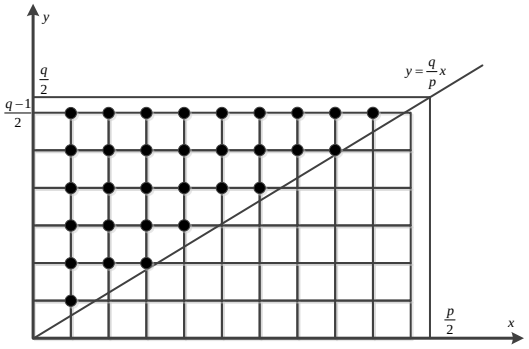

图 3.4.7 长为 $\dfrac{p}{2}$、宽为 $\dfrac{q}{2}$ 的长方形内的整数点个数（七）

因为对角线上除原点外无整数点，所以长方形内的整数点个数为

$$\sum_{h=1}^{\frac{p-1}{2}}\left\lfloor \frac{qh}{p} \right\rfloor+\sum_{k=1}^{\frac{q-1}{2}}\left\lfloor \frac{pk}{q} \right\rfloor=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

如图 3.4.8 中的实心点所示. 定理得证.

□

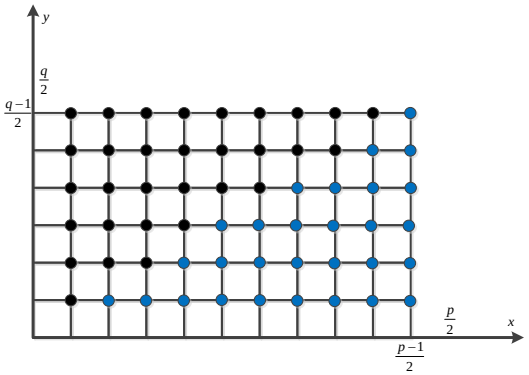

图 3.4.8 长为 $\frac{p}{2}$、宽为 $\frac{q}{2}$ 的长方形内的整数点个数（八）

在实际应用中，我们有时也把二次互反律写为如下形式：

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

二次互反律漂亮地解决了勒让德符号的计算问题，从而在实际上解决了二次剩余的判别问题，是古典数论最优美的研究成果之一. 历史上，欧拉和勒让德都曾经提出过二次互反律的猜想，但第一个严格的证明是由高斯在 1796 年做出的. 高斯曾把二次互反律誉为算术理论中的宝石，“数论之酵母”. 目前人们已经找到了二次互反律的二百多种证明方法，对二次互反律的探索研究极大地推动了数论的发展.

此外，在现代经典的代数数论中，类域论的相关深刻结果也被看作为二次互反律的延伸.

例 3.4.4 3 是否为模 17 的二次剩余?

解 由二次互反律，有

$$\left(\frac{3}{17}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{17-1}{2}}\left(\frac{17}{3}\right)=\left(\frac{17}{3}\right)=\left(\frac{-1}{3}\right)=(-1)^{\frac{3-1}{2}}=-1,$$

故 3 是模 17 的二次非剩余.

□

例 3.4.5 同余方程

$$x^2\equiv 137 \pmod{227}$$

是否有解?

解 因为 227 为素数，则

$$\left(\frac{137}{227}\right)=\left(\frac{-90}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2\cdot 3^2\cdot 5}{227}\right)=-\left(\frac{2}{227}\right)\left(\frac{5}{227}\right),$$

而

$$\left(\frac{2}{227}\right)=(-1)^{\frac{227^2-1}{8}}=(-1)^{\frac{226\cdot 228}{8}}=-1,$$

又由二次互反律，有

$$\left(\frac{5}{227}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{227-1}{2}}\left(\frac{227}{5}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1,$$

因此，

$$\left(\frac{137}{227}\right)=-1,$$

即原同余方程无解.

□

下面，我们总结性地给出求解勒让德符号的程序流程图，如图 3.4.9 所示.

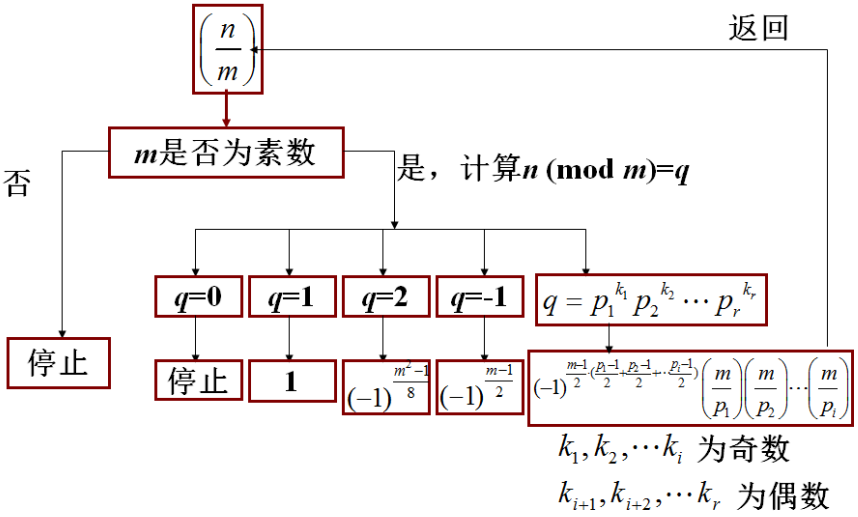

图 3.4.9　计算勒让德符号的流程图

习题 3.4

A 组

1. 求出同余方程 $x^2\equiv 8 \pmod{287}$ 的所有解.

2. 下列各方程有几个解?

(1) $x^2\equiv 19 \pmod{170}$;

(2) $x^2\equiv 38 \pmod{79}$;

(3) $x^2\equiv 76 \pmod{165}$.

3. 判断同余方程 $x^2 \equiv 191 \pmod{397}$ 是否有解.

4. 判断同余方程 $x^2 \equiv 11 \pmod{511}$ 是否有解.

5. 求解同余方程 $x^2 \equiv 2 \pmod{73}$.

6. 是否存在正整数 n 使得 n^2-3 是 313 的倍数?

7. 计算以下勒让德符号：

(1) $\left(\frac{17}{37}\right)$;

(2) $\left(\frac{151}{373}\right)$;

(3) $\left(\frac{191}{397}\right)$;

(4) $\left(\frac{911}{2003}\right)$;

(5) $\left(\frac{37}{20040803}\right)$.

8. 计算勒让德符号 $\left(\frac{7}{11}\right)$：

(1) 使用欧拉判别条件;

(2) 使用高斯引理.

9. 证明如果 p 是奇素数, 则

$$\left(\frac{-2}{p}\right)=\begin{cases}1, & \text{若 } p \equiv 1 \text{ 或} 3 \pmod 8,\\ -1, & \text{若 } p \equiv -1 \text{ 或} -3 \pmod 8.\end{cases}$$

10. 证明如果 p 是奇素数, 则

$$\left(\frac{-3}{p}\right)=\begin{cases}1, & \text{若 } p \equiv 1 \pmod 6,\\ -1, & \text{若 } p \equiv -1 \pmod 6.\end{cases}$$

B 组

11. 求所有奇素数 p, 它以 3 为其二次剩余.

12. 求所有奇素数 p, 它以 5 为其二次剩余.

13. 设 p 是奇素数, 证明 $x^2 \equiv 3 \pmod p$ 有解的充要条件是 $p \equiv \pm 1 \pmod{12}$.

14. 证明有无穷多个形式为 $4k+1$ 的素数.

15. 证明若 $p \equiv 1 \pmod 5$, 则 5 是模 p 的二次剩余, 其中 p 是奇素数.

16. 不解方程, 求满足方程 $E: y^2 = x^3 - 3x + 10 \pmod{23}$ 的点的个数.

17. 编写程序使用欧拉判别条件计算勒让德符号.

18. 编写程序使用高斯引理计算勒让德符号.

19. 编写程序使用二次互反律计算勒让德符号.

3.5 雅可比符号

在勒让德符号的计算中要求 p 为素数. 此外，在使用二次互反律时，也要求 $a = q$ 为素数. 为弱化这些条件，雅可比于 1837 年引入另外一种二次剩余判定符号——雅可比(Jacobi)符号.

定义 3.5.1 设正奇数 $m = p_1 p_2 \cdots p_r$ 是奇素数 p_i $(i = 1, 2, \ldots, r)$的乘积, 定义**雅可比(Jacobi)符号**如下：

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

从形式上看，雅可比符号只是将勒让德符号中的素数 p 推广到了正奇数 m，但其意义就不相同了. 我们知道，若 a 对 p 的勒让德符号为 1，则可知 a 是模 p 的二次剩余，但当 a 对 m 的雅可比符号为 1 时，却不能判断 a 是否是模 m 的二次剩余. 例如，3 是模 119 的二次非剩余，但

$$\left(\frac{3}{119}\right)=\left(\frac{3}{7}\right)\left(\frac{3}{17}\right)=-\left(\frac{1}{3}\right)\left(\frac{-1}{3}\right)=(-1)(-1)=1.$$

下面我们来分析雅可比符号的一些性质.

显然，我们有$\left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_r}\right)=1.$

定理 3.5.1 设 m 是正奇数，a, b 都是与 m 互素的整数，我们有

(1) 若 $a \equiv b(\mathrm{mod}\, m)$，则$\left(\frac{a}{m}\right)=\left(\frac{b}{m}\right)$；

(2) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$；

(3) $\left(\frac{a^2}{m}\right)=1.$

证明 设 $m = p_1 p_2 \cdots p_r$，其中 p_i $(i = 1, 2, \cdots, r)$是奇素数.

(1) 因为 $a \equiv b(\mathrm{mod}\, p)$，所以

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right)=\left(\frac{b}{m}\right).$$

(2)

$$\begin{aligned}\left(\frac{ab}{m}\right)&=\left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right)\\&=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\end{aligned}$$

(3)

$$\left(\frac{a^2}{m}\right)=\left(\frac{a^2}{p_1}\right)\left(\frac{a^2}{p_2}\right)\cdots\left(\frac{a^2}{p_r}\right)=1.$$

定理得证.

□

定理 3.5.2 设 m 是正奇数，我们有

(1) $\left(\dfrac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$；

(2) $\left(\dfrac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

证明 设 $m=p_1p_2\cdots p_r$，其中 p_i $(i=1,2,\cdots,r)$是奇素数.

(1) 因为

$$m=\prod_{i=1}^{r}p_i=\prod_{i=1}^{r}(1+p_i-1)\equiv 1+\sum_{i=1}^{r}(p_i-1)\pmod 4,$$

则有

$$\frac{m-1}{2}\equiv\sum_{i=1}^{r}\frac{p_i-1}{2}\pmod 2,$$

于是

$$\left(\frac{-1}{m}\right)=\prod_{i=1}^{r}\left(\frac{-1}{p_i}\right)=(-1)^{\sum\limits_{i=1}^{r}\frac{p_i-1}{2}}=(-1)^{\frac{m-1}{2}}.$$

(2) 因为

$$m^2=\prod_{i=1}^{r}p_i^2=\prod_{i=1}^{r}(1+p_i^2-1)\equiv 1+\sum_{i=1}^{r}(p_i^2-1)\pmod{16},$$

则有

$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2-1}{8} \pmod 2,$$

于是

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{r}\left(\frac{2}{p_i}\right) = (-1)^{\sum_{i=1}^{r}\frac{p_i^2-1}{8}} = (-1)^{\frac{m^2-1}{8}}.$$

定理得证.

□

定理 3.5.3 设 m, n 是互素的正奇数，则

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

证明 设 $m = p_1p_2\cdots p_r$， $n = q_1q_2\cdots q_s$， 其中 p_i $(i = 1, 2, \cdots, r)$, q_j $(j = 1, 2, \cdots, s)$都是奇素数，则

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{j=1}^{s}\left(\frac{m}{q_j}\right)\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)\\ &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)\\ &= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\end{aligned}$$

由定理 3.5.2 中的证明可知

$$\sum_{i=1}^{r}\frac{p_i-1}{2} \equiv \frac{m-1}{2} \pmod 2,$$

则

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2} \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2,$$

所以

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

定理得证.

□

在实际应用中，我们有时也可把上式写为如下形式：

$$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right).$$

通过上面这些定理， 我们发现雅可比符号具有和勒让德符号一样的计算法则， 于是当 m 为正奇数时，不必再把 m 分解成素因子的乘积，所以计算起来更方便.

例 3.5.1 同余方程

$$x^2 \equiv 286 \pmod{563}$$

是否有解?

解 我们用辗转相除法求得(286, 563) = 1, 于是不必考虑 563 是否为素数即可计算雅可比符号, 即

$$\left(\frac{286}{563}\right)=\left(\frac{2}{563}\right)\left(\frac{143}{563}\right)=(-1)^{\frac{563^2-1}{8}}(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right)=\left(\frac{-9}{143}\right)=\left(\frac{-1}{143}\right)=-1,$$

所以原同余方程无解.

□

实际上, 由雅可比符号的定义, 我们很容易证明, 当 a 是模 m 的二次剩余时, 则有 $\left(\frac{a}{m}\right)=1$ 必然成立, 所以, 当 $\left(\frac{a}{m}\right)=-1$ 时, a 一定是模 m 的二次非剩余. 但是, 正如前面所述, $\left(\frac{a}{m}\right)=1$ 不一定能说明 a 是模 m 的二次剩余.

通俗地讲, 前面的讨论都是关于如何判断一个整数是否具有模 p (或者 m) 的平方根问题的, 在这一节的最后我们针对一种特殊情况给出明确的求平方根的计算公式.

定理 3.5.4 素数 $p \equiv 3 \pmod 4$, 且 a 为模 p 的二次剩余, 则 $\pm a^{\frac{p+1}{4}}$ 为 a 的模 p 平方根.

证明 由欧拉判别条件可以推得

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}}a \equiv 1a = a \pmod p$$

且 $\pm a^{\frac{p+1}{4}}$ 是仅有的两个解, 即 $\pm a^{\frac{p+1}{4}}$ 为 a 的模 p 平方根. 定理得证.

□

例 3.5.2 Rabin 公钥密码算法中, 由明文 x 按下式计算密文

$$y = x^2 \bmod 77,$$

相应的, 我们借用平方根符号, 可以将解密过程表示为

$$x = \sqrt{y} \bmod 77.$$

如果密文为 $y = 23$, 为了解密我们需要先求 23 对模 7 和模 11 的平方根. 因为 7 和 11 都是符合上面定理题设的素数, 所以, 我们利用公式得到这两个平方根

$$23^{\frac{7+1}{4}} = 23^2 \equiv 2^2 \equiv 4 \pmod 7,$$

$$23^{\frac{11+1}{4}} = 23^3 \equiv 1^3 \equiv 1 \pmod{11}.$$

再利用中国剩余定理计算得到明文的四个可能值，x=10, 32, 45, 67.

注：由于该密码算法的加密过程本身是一个多对一的函数， 所以解密过程必然得到多个解，因此，在实际使用的时候，需要额外的冗余信息来保证恢复到正确的那一个明文.

□

习题 3.5

A 组

1. 计算以下雅可比符号：

(1) $\left(\frac{51}{71}\right)$;

(2) $\left(\frac{35}{97}\right)$;

(3) $\left(\frac{313}{401}\right)$;

(4) $\left(\frac{165}{503}\right)$;

(5) $\left(\frac{1009}{2307}\right)$.

2. 同余方程 $x^2 \equiv 2663 \pmod{3299}$ 是否有解?

3. 同余方程 $x^2 \equiv 10001 \pmod{20003}$ 是否有解?

B 组

4. 设 n 为无平方因子正奇数，证明存在一个整数 a 使得 $(a, n) = 1$ 且 $\left(\frac{a}{n}\right) = -1$.

5. 证明若正整数 b 不被奇素数 p 整除，则

$$\left(\frac{b}{p}\right)+\left(\frac{2b}{p}\right)+\left(\frac{3b}{p}\right)+\cdots+\left(\frac{(p-1)b}{p}\right)=0.$$

6. 编写程序实现 2^{200} 位的 Rabin 密码算法加密函数和解密函数.

7. 编写程序计算雅可比符号.

*3.6 高次同余方程

我们知道，任一大于 1 的整数 m 均有标准分解式:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1,2,\ldots,s,$$

其中 $p_i < p_j$（$i<j$）是素数. 于是，由定理 3.2.4 可知，欲解 $f(x) \equiv 0 \pmod{m}$，只需求解同余方程组

$$\begin{cases} f(x)\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x)\equiv 0 \pmod{p_2^{\alpha_2}} \\ \quad\vdots \\ f(x)\equiv 0 \pmod{p_s^{\alpha_s}} \end{cases}$$

所以，我们先来讨论 p 为素数时，同余方程

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod{p^\alpha} \tag{3.6.1}$$

的求解方法，其中 α 为正整数，且 a_n 不能被 p^α 整除.

定理 3.6.1 设 $x\equiv x_1 \pmod p$是同余方程

$$f(x)\equiv 0 \pmod p \tag{3.6.2}$$

的一个解，且满足($f'(x_1)$, p) = 1，则同余方程(3.6.1)有解

$$x\equiv x_\alpha \pmod{p^\alpha}.$$

其中 x_α 由以下关系式递归得到：

$$\begin{cases} x_i\equiv x_{i-1}+p^{i-1}t_{i-1} & \pmod{p^i} \\ t_{i-1}\equiv -\dfrac{f(x_{i-1})}{p^{i-1}}\left(\left(f'(x_1)\right)^{-1} \pmod p\right) & \pmod p \end{cases}$$

i = 2, 3, …, α . 这里， $f'(x)=\sum_{i=1}^{n} ia_ix^{i-1}$ 表示 $f(x)$的导函数.

证明 用数学归纳法.

(1) 当 α = 2 时，根据假设条件，同余方程(3.6.2)的所有解为

$$x=x_1+pt_1,\quad t_1=0,\ \pm 1,\ \pm 2,\ \cdots.$$

于是，我们考虑关于 t_1 的同余方程

$$f(x_1+pt_1)\equiv 0 \pmod{p^2}.$$

由泰勒公式，有

$$f(x_1)+pt_1f'(x_1)\equiv 0 \pmod{p^2},$$

又因为 $f(x_1)\equiv 0 \pmod p$，所以上述同余方程可写为

$$t_1f'(x_1)\equiv -\frac{f(x_1)}{p} \pmod p .$$

由($f'(x_1)$, p) = 1，根据定理 3.1.2，此同余方程的唯一解为

$$t_1\equiv -\frac{f(x_1)}{p}\left(\left(f'(x_1)\right)^{-1} \pmod p\right) \pmod p \quad .$$

故

$$x\equiv x_2\equiv x_1+pt_1 \pmod{p^2}$$

是同余方程 $f(x)\equiv 0 \pmod{p^2}$的解.

(2) 当 $\alpha\geqslant 3$ 时，假设对 $i-1$ $(3\leqslant i\leqslant\alpha)$ 成立，即同余方程

$$f(x)\equiv 0 \pmod{p^{i-1}}$$

有解

$$x = x_{i-1} + p^{i-1}t_{i-1},\ t_{i-1} = 0,\ \pm 1,\ \pm 2,\ \cdots.$$

于是，我们考虑关于t_{i-1}的同余方程

$$f(x_{i-1} + p^{i-1}t_{i-1}) \equiv 0 \pmod{p^i}.$$

由泰勒公式及 $p^{2(i-1)} \geqslant p^i$，可知

$$f(x_{i-1}) + p^{i-1}t_{i-1}f'(x_{i-1}) \equiv 0 \pmod{p^i},$$

因为 $f(x_{i-1}) \equiv 0 \pmod{p^{i-1}}$，所以上述同余方程可写为

$$t_{i-1}f'(x_{i-1}) \equiv -\frac{f(x_{i-1})}{p^{i-1}} \pmod{p}.$$

又 $f'(x_{i-1}) \equiv f'(x_{i-2}) \equiv \cdots \equiv f'(x_1) \pmod{p}$，进而有

$$(f'(x_{i-1}), p) = \cdots = (f'(x_1), p) = 1,$$

再根据定理 3.1.2，此同余方程的唯一解为

$$\begin{aligned} t_{i-1} &\equiv -\frac{f(x_{i-1})}{p^{i-1}}\left((f'(x_{i-1}))^{-1} \pmod{p}\right) \\ &\equiv -\frac{f(x_{i-1})}{p^{i-1}}\left((f'(x_1))^{-1} \pmod{p}\right) \pmod{p} \end{aligned}$$

故

$$x \equiv x_i \equiv x_{i-1} + p^{i-1}t_{i-1} \pmod{p^i}$$

是同余方程$f(x)\equiv 0 \pmod{p^i}$的解.

于是，根据数学归纳法，定理得证.

□

例 3.6.1 求解同余方程

$$f(x) = x^4 + 7x + 4 \equiv 0 \pmod{27}.$$

解 写出$f(x)$的导函数，即

$$f'(x) = 4x^3 + 7.$$

通过直接验算，可知同余方程

$$f(x)\equiv 0 \pmod{3}$$

有一解

$$x_1 \equiv 1 \pmod{3}.$$

于是，有

$$f'(x_1) \equiv -1 \pmod 3,$$

进而

$$\left(f'(x_1)\right)^{-1} \equiv -1 \pmod 3.$$

依次计算如下:

$$\begin{cases} t_1 \equiv -\dfrac{f(x_1)}{3}\left(\left(f'(x_1)\right)^{-1} \pmod 3\right) \equiv 1 \pmod 3 \\ x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod 9 \end{cases}$$

$$\begin{cases} t_2 \equiv -\dfrac{f(x_2)}{3^2}\left(\left(f'(x_1)\right)^{-1} \pmod 3\right) \equiv 2 \pmod 3 \\ x_3 \equiv x_2 + 3^2 t_2 \equiv 22 \pmod{27} \end{cases}$$

所以，原同余方程的解为

$$x_3 \equiv 22 \pmod{27}.$$

□

现在我们重点讨论模 p 的同余方程

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p \tag{3.6.3}$$

的求解方法，其中 a_n 不能被 p 整除.

在此之前，我们先引入多项式的辗转相除法，或称多项式的欧几里得除法.

定理 3.6.2 设

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

为 n 次整系数多项式,

$$g(x) = x^m + b_{m-1}x^{n-1} + \cdots + b_1 x + b_0$$

为 m 次首一（最高项系数为 1）整系数多项式，其中 $m \geqslant 1$，则存在整系数多项式 $q(x)$和 $r(x)$使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$.

证明 我们可分两种情况讨论.

(1) 若 $n < m$，可取 $q(x) = 0$，$r(x) = f(x)$使结论成立.

(2) 若 $n \geqslant m$，可对 $f(x)$的次数 n 作数学归纳法.

当 $n = m$ 时，有

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

因此，取 $q(x) = a_n$，$r(x) = f(x) - a_n g(x)$可使结论成立.

假设当 $n = k - 1$ 时，结论成立，其中 $k - 1 \geqslant m$.

当 $n = k$ 时，则有

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

显然 $f(x) - a_n x^{n-m} g(x)$是次数小于等于 $n-1$ 的多项式，对其运用归纳假设或情况(1)，可知存

在整系数多项式 $q_1(x)$和 $r_1(x)$使得

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

其中 $\deg r_1(x) < \deg g(x)$. 因此，取 $q(x) = a_n x^{n-m} + q_1(x)$，$r(x) = r_1(x)$可使结论成立.

根据数学归纳法原理，可知结论成立，于是定理得证.

□

定理 3.6.3 同余方程(3.6.3)与一个次数小于 p 的模 p 的同余方程等价.

证明 由定理 3.6.2 可知，存在整系数多项式 $q(x)$和 $r(x)$使得

$$f(x) = (x^p - x)q(x) + r(x),$$

其中 $\deg r(x) < p$. 根据费马小定理，对任意整数 x 都有

$$x^p - x \equiv 0 \pmod{p}.$$

于是同余方程

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

等价于同余方程

$$r(x) \equiv 0 \pmod{p}.$$

定理得证.

□

定理 3.6.4 同余方程(3.6.3)最多有 n 个解.

证明 可对 $f(x)$的次数 n 作数学归纳法.

当 $n = 1$ 时，一次同余方程为

$$a_1 x + a_0 \equiv 0 \pmod{p},$$

由于 a_1 不能被 p 整除，即$(a_1, p) = 1$，故同余方程恰有一个解，结论成立.

假设定理对次数为 $n - 1$ $(n \geqslant 2)$的同余方程成立，即次数为 $n - 1$ 的同余方程最多有 $n - 1$ 个解. 下面证明同余方程(3.6.3)最多有 n 个解.

根据定理 3.6.3 可知，同余方程(3.6.3)与一个次数小于 p 的模 p 的同余方程等价，所以不妨设 $n \leqslant p - 1$. 用反证法，假设同余方程(3.6.3) 有 $n + 1$ 个解，设它们为

$$x \equiv x_i \pmod{p}, \quad i = 0, 1, \cdots, n.$$

由于

$$f(x) - f(x_0) = \sum_{k=1}^{n} a_k (x^k - x_0^k) = (x - x_0)g(x),$$

显然，$g(x)$是首项系数为 a_n 的 $n - 1$ 次整系数多项式，根据归纳假设，可知

$$g(x) \equiv 0 \pmod{p}$$

是 $n - 1$ 次同余方程，至多有 $n - 1$ 个解. 而由于

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p}$$

当 $k > 0$ 时，$x_k - x_0 \equiv 0 \pmod{p}$不成立，故 $n-1$ 次同余方程 $g(x) \equiv 0 \pmod{p}$有 n 个解，推出矛盾. 于是假设不成立，定理得证.

□

定理 3.6.4 通常被称为**拉格朗日(Lagrange)定理**.

定理 3.6.5 如果同余方程

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod p$$

的解的个数大于 n，则 $p\mid a_i$，$i=0,1,\ldots,n$.

证明 用反证法. 假设存在某些系数不能被 p 整除，若这些系数的下标最大的为 k，$k\leqslant n$，则原同余方程可写为

$$f(x)\equiv a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0\equiv 0 \pmod p.$$

根据上面的定理可知，此同余方程最多有 k 个解，与所给条件矛盾，故假设不成立. 定理得证.

□

定理 3.6.6 如果同余方程(3.6.3)有 k 个不同的解

$$x\equiv x_i \pmod p,\quad i=1,2,\ldots,k,\ 1\leqslant k\leqslant n,$$

则对任意整数 x，均有

$$f(x)\equiv (x-x_1)(x-x_2)\cdots(x-x_k)f_k(x) \pmod p,$$

其中 $f_k(x)$是首项系数为 a_n 的 $n-k$ 次多项式.

证明 由定理 3.6.2 可知，存在整系数多项式 $f_1(x)$和 $r(x)$使得

$$f(x)=(x-x_1)f_1(x)+r(x),\quad \deg r(x)<\deg(x-x_1).$$

显然，$f_1(x)$是首项系数为 a_n 的 $n-1$ 次多项式. 由于 $\deg(x-x_1)=1$，故 $r(x)=r$ 为整数，又因为 $f(x_1)\equiv 0 \pmod p$，所以有 $r\equiv 0 \pmod p$，即

$$f(x)=(x-x_1)f_1(x) \pmod p.$$

又因为 $f(x_i)\equiv 0 \pmod p$，并且 x_i 与 x_1 模 p 不同余，其中 $i=2,3,\ldots,k$，于是可知

$$f_1(x_i)\equiv 0 \pmod p,\ i=2,3,\ldots,k.$$

同理，对多项式 $f_1(x)$可找到多项式 $f_2(x)$使得

$$\begin{cases} f_1(x)\equiv (x-x_2)f_2(x) & \pmod p \\ f_2(x_i)\equiv 0 & \pmod p \end{cases}$$

其中 $i=3,4,\ldots,k$. 依此类推，可得

$$f_{k-1}(x)\equiv (x-x_k)f_k(x) \pmod p.$$

于是，有

$$f(x)\equiv (x-x_1)\cdots(x-x_k)f_k(x) \pmod p,$$

定理得证.

□

定理 3.6.7 对于素数 p 与正整数 n，$n\leqslant p$，同余方程

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0 \pmod p$$

有 n 个解的充要条件是 x^p-x 被 $f(x)$除所得余式的所有系数均能被 p 整除.

证明 由定理 3.6.2 可知，存在整系数多项式 $q(x)$和 $r(x)$，使得

$$x^p - x = f(x)q(x) + r(x),$$

其中 $r(x)$的次数小于 n，$q(x)$的次数为 $p - n$.

现在证明必要性．若原同余方程有 n 个解，则根据费马小定理，这 n 个解都是

$$x^p - x \equiv 0 \pmod{p}$$

的解，显然这 n 个解也都是

$$r(x) \equiv 0 \pmod{p}$$

的解．由于 $r(x)$的次数小于 n，故由定理 3.6.5 可知，$r(x)$的所有系数均能被 p 整除.

再来证明充分性．若 $r(x)$的所有系数均能被 p 整除，则显然有

$$r(x) \equiv 0 \pmod{p}.$$

又由费马小定理，可知对任意整数有

$$x^p - x \equiv 0 \pmod{p}.$$

因此，对任意整数有

$$f(x)q(x) \equiv 0 \pmod{p},$$

即它有 p 个不同的解

$$x \equiv 0, 1, \ldots, p - 1 \pmod{p}.$$

假设 $f(x) \equiv 0 \pmod{p}$的解数小于 n，则 $q(x) \equiv 0 \pmod{p}$的解数小于等于 $p - n$，故

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

的解数小于 p，推出了矛盾．所以 $f(x) \equiv 0 \pmod{p}$的解数为 n．定理得证.

□

例 3.6.2 判断同余方程

$$2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod{7}$$

解的个数.

解 先将多项式化为首项系数为 1．由于 $4\times2 \equiv 1 \pmod{7}$，故我们有

$$4(2x^3 + 5x^2 + 6x + 1) \equiv x^3 - x^2 + 3x - 3 \equiv 0 \pmod{7}.$$

根据多项式的辗转相除法，可得

$$x^7 - x = x(x^3 + x^2 - 2x - 2)(x^3 - x^2 + 3x - 3) + 7x(x^2 - 1).$$

由上面定理可知原同余方程有 3 个解.

□

习题 3.6

A 组

1. 求解同余方程

(1) $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$;

(2) $x^3 + 5x^2 + 9 \equiv 0 \pmod{27}$.

2. 证明同余方程

$$2x^3 - x^2 + 3x + 11 \equiv 0 \pmod 5$$

有 3 个解.

3. 如下各个方程有几个解？

$$x^2-1 \equiv 0 \pmod{168};$$

$$x^2+1 \equiv 0 \pmod{70};$$

$$x^2+ x+1 \equiv 0 \pmod{91};$$

$$x^3+1 \equiv 0 \pmod{140}.$$

B 组

4. 举例说明对模数为合数的情况，拉格朗日定理一般不成立.