第 5 章 二次剩余

本章主要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.

5.1 二次剩余的概念和性质

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, 其核心就是本节的重点——二次剩余和二次互反律.

在 4.3 节中, 我们给出了 n 次剩余的定义. 其中当 $n = 2$ 时, 我们就可以得到二次剩余的定义. 显然, 设 m 是大于 1 的整数, a 是与 m 互素的整数, 若

$$x^2 \equiv a \pmod{m} \tag{5.1.1}$$

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

$$ax^2+bx+c \equiv 0 \pmod{p} \tag{5.1.2}$$

其中 p 是一个奇素数且 $a \not\equiv 0 \pmod{p}$, 即$(a, p)=1$. 所以$(4a, p)=1$. 因此, 方程(5.1.2)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

$$y^2 \equiv d \pmod{p} \tag{5.1.3}$$

如果 $x \equiv x_0 \pmod{p}$是方程(5.1.2)的一个解, 那么任意整数 $y_0 \equiv 2ax_0+b \pmod{p}$就是方程(5.1.3)的解. 反过来, 如果 $y \equiv y_0 \pmod{p}$是方程(5.1.3)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(5.1.2)的一个解.

例 5.1.1 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 $y\equiv 3, 10 \pmod{13}$. 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(5.1.2)的可解性与 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(5.1.2)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

$$x^2\equiv a \pmod{p}, \tag{5.1.4}$$

其中 p 是奇素数.

例 5.1.2 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 5.1.1.

定理 5.1.1 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(5.1.4)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 3.5.1, 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

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

由威尔逊定理$(p\text{-}1)! \equiv -1 \pmod{p}$，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 $p \mid a^{p-1} - 1$. 由定理 3.4.3 有

$$p \mid a^{\frac{p-1}{2}} - 1 \text{或} p \mid a^{\frac{p-1}{2}} + 1.$$

根据(1)的证明，可知 a 是模 p 的二次非剩余的充要条件是

$$p \mid a^{\frac{p-1}{2}} + 1,$$

即

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

证毕.

例 5.1.3 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 5.1.2 中我们已经知道解为 4 和 9.

定理 5.1.2 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

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2 \tag{5.1.5}$$

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

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

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 $1\le i<j\le\frac{p-1}{2}$ 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 5.1.2 很好地验证了这个定理.

习题 5.1

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

1. 设 p 为奇素数, 求-1 是模 p 的二次剩余的充要条件.

5.2 勒让德符号与二次互反律

5.1 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 5.2.1 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 5.2.1　利用例 5.1.2 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 5.1.1 改写如下.

定理 5.2.1*　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 5.2.2　设 p 是奇素数，a, b 都是与 p 互素的整数，我们有

(1) 若 $a\equiv b \pmod{p}$，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

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

由于勒让德符号取值只有 ± 1，且 p 是奇素数，故

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

这一结论有一个推论, 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；

(3) 显然，a^2 是模 p 的二次剩余，所以必有

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

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：

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

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 5.2.3 设 p 是奇素数，我们有

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

例 5.2.2 判断 $x^2\equiv -46 \pmod{17}$是否有解.

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

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.

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 5.2.4（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

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

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

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

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

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

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

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

用反证法，假设存在

$$a_s=p-b_t,$$

则有

$$ak_i\equiv p-ak_j\ (\mathrm{mod}\ p),$$

即

$$ak_i+ak_j\equiv 0\ (\mathrm{mod}\ p),$$

于是

$$k_i+k_j\equiv 0\ (\mathrm{mod}\ p),$$

即有 $p\mid k_i+k_j$.

因为

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

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

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，$a_1, a_2, \cdots, a_l, p-b_1, p-b_2, \cdots, p-b_m$ 这 $\frac{p-1}{2}$ 个整数两两互不相等.

由于

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

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

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

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

则

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

再根据欧拉判别条件，我们有

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

证毕.

例 5.2.3 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 5.2.5 设 p 是奇素数，则有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{若 } p\equiv\pm1\ (\mathrm{mod}\ 8),\\ -1, & \text{若 } p\equiv\pm3\ (\mathrm{mod}\ 8).\end{cases}$$

证明 由高斯引理，考虑

$$2\cdot1,\quad 2\cdot2,\quad 2\cdot3,\quad \cdots,\quad 2\cdot\frac{p-1}{2}$$

模 p 后得到的最小正剩余中大于 $\frac{p}{2}$ 的个数是 m，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 $2k(k=1, 2, \cdots, \frac{p-1}{2})$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$(x_n\ldots x_2x_1 1)_2$，我们有

$$m=(x_n\ldots x_2x_1)_2-(x_n\ldots x_2)_2$$

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

$$p=(x_n\cdots001)_2 \text{ 或 } p=(x_n\cdots111)_2$$

即 $p\equiv\pm1 \pmod 8$.

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

$$p=(x_n\cdots101)_2 \text{ 或 } p=(x_n\cdots011)_2$$

即 $p\equiv\pm3 \pmod 8$, 证毕.

定理 5.2.6 设 p 是奇素数, $(a, 2p) = 1$, 则 $\left(\dfrac{a}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{ak}{p}\right\rfloor}$.

证明 由于当$(a, p)=1$ 时,

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

对 $k = 1, 2, \cdots, \dfrac{p-1}{2}$ 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 $a-1\equiv0 \pmod 2$, 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

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

下面我们给出用于计算勒让德符号的著名的**二次互反律**.

定理 5.2.7 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

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

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 5.2.1(a)所示.

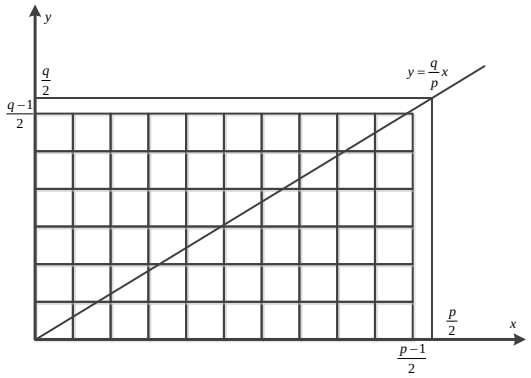

图 5.2.1(a) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

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 5.2.1(b)所示.

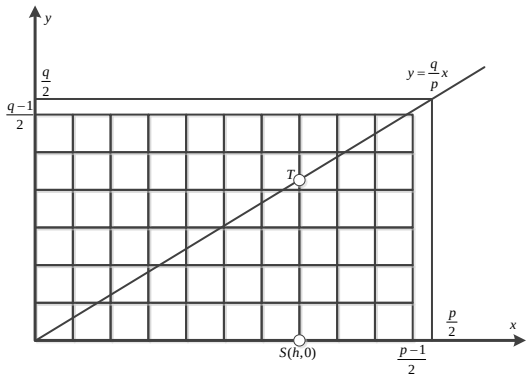

图 5.2.1(b) v 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

则在垂直直线 ST 上，整数点个数为 $\left\lfloor \frac{qh}{p} \right\rfloor$ 为图 5.2.1(c)中实心点的个数.

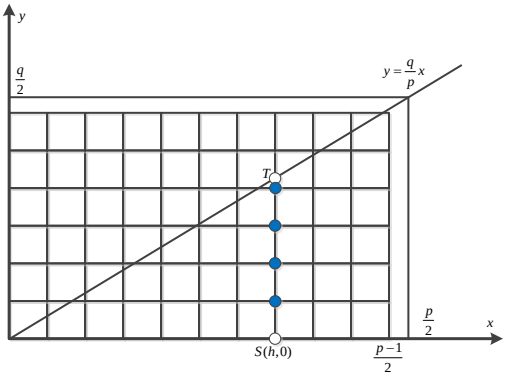

图 5.2.1(c) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

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 5.2.1(d)中的实心点所示.

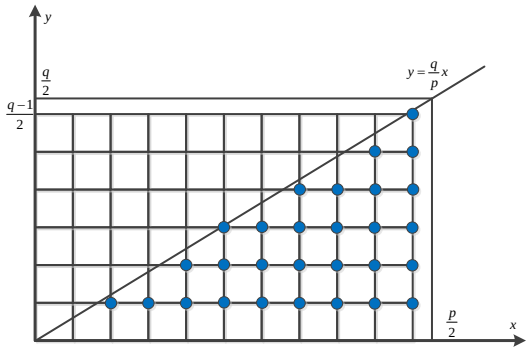

图 5.2.1(d) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

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 $0 \leqslant k \leqslant \frac{q-1}{2}$. 如图 5.2.1(e)所示.

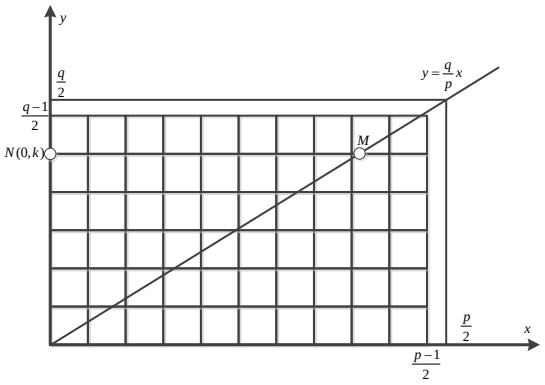

图 5.2.1(e) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

于是，在水平直线 NM 上，整数点个数为 $\left\lfloor \frac{pk}{q} \right\rfloor$，如图 5.2.1(f)中的实心点所示.

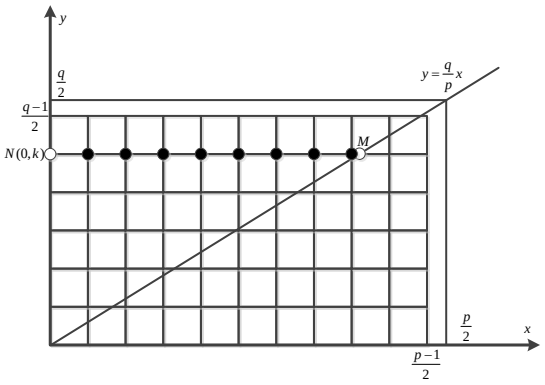

图 5.2.1(f) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

于是，上三角形内的整数点个数为 $\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{pk}{q} \right\rfloor$. 如图 5.2.1(g)中的实心点所示.

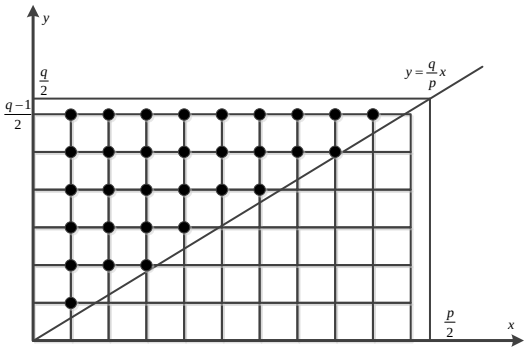

图 5.2.1(g) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

因为对角线上除原点外无整数点，所以长方形内整数点个数为

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

如图 5.2.1(h)中的实心点所示. 证毕.

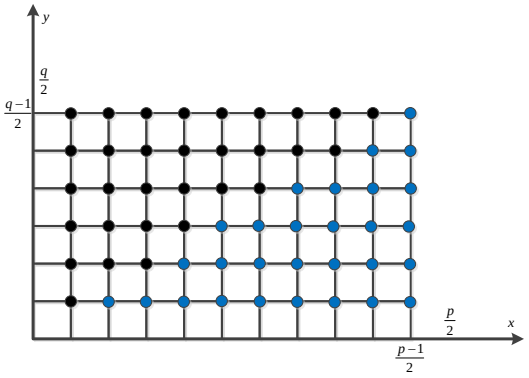

图 5.2.1(h) 长为 $\frac{p}{2}$，宽为 $\frac{q}{2}$ 的长方形内的整数点个数

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 5.2.4 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 5.2.5 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.

下面给出求解勒让德符号的程序流程图，如图 5.2.2 所示.

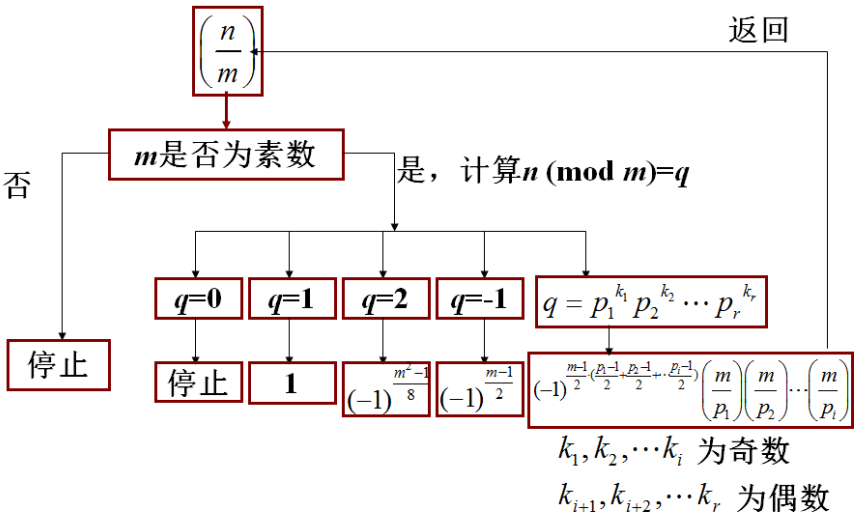

图 5.2.2　计算勒让德符号的流程图

习题 5.2

A 组

1. 求出同余方程 $x^2\equiv 8(\mathrm{mod}\,287)$ 的所有解.

2. 下列各方程有几个解?

(1) $x^2\equiv 19(\mathrm{mod}\,170)$;

(2) $x^2\equiv 38(\mathrm{mod}\,79)$;

(3) $x^2\equiv 76(\mathrm{mod}\,165)$.

3. 判断同余方程 $x^2\equiv 191(\mathrm{mod}\,397)$ 是否有解.

4. 判断同余方程 $x^2\equiv 11(\mathrm{mod}\,511)$ 是否有解.

5. 求解同余方程 $x^2\equiv 2(\mathrm{mod}\,73)$.

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

B 组

1. 求所有奇素数 p, 它以 3 为其二次剩余.
2. 求所有奇素数 p, 它以 5 为其二次剩余.
4. 设 p 是奇素数, 证明 $x^2\equiv 3(\mathrm{mod}\ p)$有解的充要条件是 $p\equiv\pm1(\mathrm{mod}\ 12)$.
5. 证明若 $p\equiv 1(\mathrm{mod}\ 5)$, 则 5 是模 p 的二次剩余.
6. 不解方程, 求满足方程 E: $y^2 = x^3 - 3x + 10(\mathrm{mod}\ 23)$的点的个数.
7. 编程计算勒让德符号.

5.3 雅可比符号

定义 5.3.1 设正奇数 $m = p_1 p_2\cdots p_r$ 是奇素数 p_i $(i = 1, 2, \cdots, r)$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 5.3.1 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 $m=p_1p_2\cdots p_r$，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 5.3.2 设 m 是正奇数，我们有

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

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

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

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

则有

$$\frac{m-1}{2}\equiv\sum_{i=1}^{r}\frac{p_i-1}{2}\ (\mathrm{mod}\,2),$$

于是

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

(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 5.3.3 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 5.3.2 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

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

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 5.3.1 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 5.3.4 素数 $p\equiv 3(\mathrm{mod}\ 4)$，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

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

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.

例 5.3.2 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

$$23^{\frac{7+1}{4}}=23^2\equiv 2^2\equiv 4(\mathrm{mod}\,7),$$

$$23^{\frac{11+1}{4}}=23^3\equiv 1^3\equiv 1(\mathrm{mod}\,11).$$

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 5.3

A 组

1. 利用雅可比符号计算

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

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

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

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

B 组

1. 编写程序实现 2^{200} 位的 Rabin 密码算法加密函数和解密函数.
2. 编程计算雅可比符号.