第5章 二次同余方程

5.1 二次同余方程的概念及二次剩余

由第4章知，解一般模数的二次同余方程可归结为解素数模的二次同余方程：

$$ax^2+bx+c\equiv 0 \bmod p \tag{5.1.1}$$

其中 $p\nmid a$。

由 $p\nmid a$ 得 $(p,a)=1$，$(p,4a)=1$，将式(5.1.1)两边同乘以 $4a$，得

$$4a^2x^2+4abx+4ac\equiv 0 \bmod p$$

$$(2ax+b)^2\equiv b^2-4ac \bmod p$$

做可逆变换 $y=2ax+b$（因为 $(p,2a)=1$），得到式(5.1.1)的等价同余方程：

$$y^2\equiv b^2-4ac \bmod p$$

所以，只需讨论形如 $x^2\equiv d \bmod p$ 的同余方程。当 $p\mid d$ 时，方程只有一个解 $0 \bmod p$，所以下面恒假设 $p\nmid d$。

定义 5.1.1 设素数 $p>2$，$a\in\mathbf{Z}$，$p\nmid a$。如果同余方程

$$x^2\equiv a \bmod p \tag{5.1.2}$$

有解，则称 a 是模 p 的二次剩余，否则称为模 p 的二次非剩余。满足式(5.1.2)的 x 称为 a 的平方根。

例 5.1.1 由 $x^2\equiv 1 \bmod 3$ 得 $x\equiv\pm 1 \bmod 3$，所以1是模3的二次剩余。

$x^2\equiv -1 \bmod 3$ 无解，-1 是模3的二次非剩余。

$x^2\equiv 1 \bmod 5$ 得 $x\equiv\pm 1 \bmod 5$，1是模5的二次剩余。

$x^2\equiv -1 \bmod 5$ 得 $x\equiv\pm 2 \bmod 5$，-1 是模5的二次剩余。

$x^2\equiv 2 \bmod 5$ 无解，2是模5的二次非剩余。

$x^2\equiv -2 \bmod 5$ 无解，-2 是模5的二次非剩余。

已知 p，模 p 的二次剩余和二次非剩余元素的个数由以下定理给出。

定理 5.1.1 在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个二次剩余和 $\frac{p-1}{2}$ 个二次非剩余。若 a 是二次剩余，则方程(5.1.2)有两个解。

证明 取模 p 的绝对最小简化剩余系

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

a 是模 p 的二次剩余，当且仅当 a 与以下 $p-1$ 个值中的一个模 p 同余：

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

但由于$(-j)^2\equiv j^2 \bmod p$，所以 a 是模 p 的二次剩余，当且仅当 a 与以下$\frac{p-1}{2}$个值中的一个模 p 同余：

$$1^2,\cdots,\left(\frac{p-1}{2}-1\right)^2,\left(\frac{p-1}{2}\right)^2 \tag{5.1.3}$$

这$\frac{p-1}{2}$个值中任意两个都不同余。否则设 $i^2\equiv j^2 \bmod p$，则得$(i+j)(i-j)\equiv 0 \bmod p$，所以 $p\mid i+j$ 或 $p\mid i-j$。但 $1\leqslant i,j\leqslant\frac{p-1}{2}$，$2\leqslant i+j\leqslant p-1$，$|i-j|\leqslant p-1$，所以 $i=j$，矛盾。所以式(5.1.3)给出了模 p 的全部二次剩余，其余的 $p-1-\frac{p-1}{2}=\frac{p-1}{2}$个元素是二次非剩余。所以若 a 是二次剩余，a 必为式(5.1.3)中的一项，而且仅为其中一项。

若 $x\equiv i \bmod p$ 是式(5.1.2)的解，则 $x\equiv -i \bmod p$ 也是式(5.1.2)的解，即式(5.1.2)有两个解。 证毕。

由以上证明过程可得如下推论。

推论 设 a 是模 p 的二次剩余，则 a 与 $1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2$ 中的一个且仅与一个模 p 同余。

例 5.1.2 求模 19 的二次剩余。

解 由定理 5.1.1 的推论，求模 19 的二次剩余就是在模 19 的绝对最小简化剩余系 $-9,-8,\cdots,-1,1,2,\cdots,9$ 中求 a，它与 $1^2,2^2,\cdots,9^2$ 中的某一个模 19 同余，如表 5.1.1 所示。

表 5.1.1 模 19 的二次剩余

j	1	2	3	4	5	6	7	8	9
$a\equiv j^2 \bmod 19$	1	4	9	−3	6	−2	−8	7	5

所以模 19 的二次剩余是 $1,-2,-3,4,5,6,7,-8,9$，二次非剩余是 $-1,2,3,-4,-5,-6,-7,8,-9$。

反过来看表 5.1.1，可得每个二次剩余的两个解。例如，6 是二次剩余，它的两个解是 $\pm 5 \bmod 19$。

定理 5.1.2 可直接判断 a 是不是模 p 的二次剩余，可无须在模 p 的绝对最小简化剩余系中逐一验证。

定理 5.1.2 设素数 $p>2$，$p\nmid a$，则 a 是模 p 的二次剩余的充要条件是

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

a 是模 p 的二次非剩余的充要条件是

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

证明 由于

$$x^{p-1}-1=(x^2)^{\frac{p-1}{2}}-a^{\frac{p-1}{2}}+a^{\frac{p-1}{2}}-1=(x^2-a)q(x)+(a^{\frac{p-1}{2}}-1)$$

由定理 4.4.5 得 $x^2-a\equiv 0 \bmod p$ 有两个解(即 a 是模 p 的二次剩余)的充要条件是

$$x^2-a \mid x^p-x=x(x^{p-1}-1)$$

因 $x^2-a\equiv 0 \bmod p$ 没有 0 解,即 x^2-a 没有 x 因子,所以

$$x^2-a \mid x^{p-1}-1$$

等价于

$$a^{\frac{p-1}{2}}-1\equiv 0 \bmod p$$

即

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

又由于

$$\left(a^{\frac{p-1}{2}}+1\right)\left(a^{\frac{p-1}{2}}-1\right)\equiv a^{p-1}-1 \bmod p\equiv 0 \bmod p$$

其中第二个同余式由 Euler 定理得,所以

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

但这两个同余式不能同时成立,否则

$$a^{\frac{p-1}{2}}\equiv -1 \bmod p \quad \text{且} \quad a^{\frac{p-1}{2}}\equiv 1 \bmod p$$

得 $-1\equiv 1 \bmod p$,$2\equiv 0 \bmod p$,矛盾。

所以,a 是模 p 的二次非剩余的充要条件是 $a^{\frac{p-1}{2}}\equiv -1 \bmod p$。　　证毕。

从上述证明过程还可见,如果 a 是模 p 的二次剩余,则

$$a^{\frac{p-1}{2}}-1\equiv 0 \bmod p,\quad x^2-a \mid x^p-x$$

因此 $x^2-a\equiv 0 \bmod p$ 有两个解,这也是定理 5.1.1 的结论。

推论 1　-1 是模 p 的二次剩余的充要条件是 $p\equiv 1 \bmod 4$。

证明　取模 4 的最小非负完全剩余系 0,1,2,3,当且仅当 p 在最小非负完全剩余系中取 1,即 $p\equiv 1 \bmod 4$ 时,满足方程

$$(-1)^{\frac{p-1}{2}}\equiv 1 \bmod p$$

证毕。

推论 2　设素数 $p>2$,$p\nmid a_1$,$p\nmid a_2$,则

(1) 若 a_1、a_2 均为模 p 的二次剩余,则 a_1a_2 也是模 p 的二次剩余。

(2) 若 a_1、a_2 均为模 p 的二次非剩余,则 a_1a_2 是模 p 的二次剩余。

(3) 若 a_1 是模 p 的二次剩余,a_2 是模 p 的二次非剩余,则 a_1a_2 是模 p 的二次非剩余。

证明　因为 $(a_1a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}$,由定理 5.1.2 即得。　　证毕。

例 5.1.3　判断 3 是否为模 17 的二次剩余,7 是否为模 29 的二次剩余。

解　因为

$$3^2\equiv 9 \bmod 17\equiv -8 \bmod 17,\quad 3^4\equiv -4 \bmod 17,\quad 3^8\equiv 16 \bmod 17\equiv -1 \bmod 17$$

所以 3 是模 17 的二次非剩余。

因为

$$7^2 \equiv -9 \bmod 29,\quad 7^3 \equiv -5 \bmod 29,\quad 7^4 \equiv -6 \bmod 29,$$
$$7^7 = 7^3 \cdot 7^4 \equiv 1 \bmod 29,\quad 7^{14} \equiv 1 \bmod 29$$

所以 7 是模 29 的二次剩余。

5.2 Legendre 符号

要判断 a 是否为模 p 的二次剩余，由定理 5.1.1 要逐一检验 a 是否与以下各值中的某一个模 p 同余：

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

或者由定理 5.1.2 计算 $a^{\frac{p-1}{2}} \bmod p$ 的值。当 p 很大时，两个方法都不实用。本节介绍一种简单方法，即求 a 模 p 的 Legendre 符号。

定义 5.2.1 设素数 $p>2$，定义 Legendre 符号如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & a \text{ 是模 } p \text{ 的二次剩余}\\ -1, & a \text{ 是模 } p \text{ 的二次非剩余}\\ 0, & p \mid a\end{cases}$$

所以，要判断 a 是否为模 p 的二次剩余，只需计算 $\left(\frac{a}{p}\right)$ 即可。

定理 5.2.1 Legendre 符号有以下性质。

(1) $\left(\frac{a}{p}\right)=\left(\frac{p+a}{p}\right)$，一般地 $\left(\frac{a}{p}\right)=\left(\frac{a+kp}{p}\right)$，其中 $k \in \mathbf{Z}$。

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

(3) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$，即 Legendre 符号是完全积性的。

(4) 当 $p \nmid a$ 时，$\left(\frac{a^2}{p}\right)=1$。

(5) $\left(\frac{1}{p}\right)=1$，$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$。

证明极简单，略。

由定理 5.2.1 可见，当 a 增加时，$\left(\frac{a}{p}\right)$ 以 p 为周期，若 $a>p$，则总能求出 $q<p$，$(p,q)=1$，使得 $\left(\frac{a}{p}\right)=\left(\frac{q}{p}\right)$。

下面考虑如何求 $\left(\frac{2}{p}\right)$ 及一般形式的 $\left(\frac{q}{p}\right)$，为此需要引入 Gauss 引理。

引理 5.2.1(Gauss 引理) 设素数 $p>2$，$p \nmid a$，如果

$$a \cdot 1, a \cdot 2, \cdots, a \cdot \frac{p-1}{2} \pmod p \tag{5.2.1}$$

中大于 $\frac{p}{2}$ 的元素个数为 n，则

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

证明　在式(5.2.1)的$\frac{p-1}{2}$个数中，当 $i\not\equiv j$ 时，$ai\not\equiv aj \bmod p$，否则由$(a,p)=1$ 得 $i\equiv j \bmod p$。

将式(5.2.1)中大于$\frac{p}{2}$的数记为 $r_1,r_2,\cdots,r_n$，小于$\frac{p}{2}$的数记为 $s_1,s_2,\cdots,s_t$。显然

$$1\leqslant p-r_i<\frac{p}{2}\quad(1\leqslant i\leqslant n)\quad 且\quad p-r_i\not\equiv s_j \bmod p\quad(1\leqslant j\leqslant t)$$

这是因为

$$-\frac{p}{2}<-s_j<0$$

$$-\frac{p}{2}+1<p-r_i-s_j<\frac{p}{2}$$

$$p-r_i-s_j\not\equiv 0 \bmod p$$

所以 $p-r_1,p-r_2,\cdots,p-r_n,s_1,s_2,\cdots,s_t$ 就是 $1,2,\cdots,\frac{p-1}{2}$的一个排列。将式(5.2.1)中的$\frac{p-1}{2}$个数相乘，得

$$\begin{aligned}a^{\frac{p-1}{2}}\cdot\frac{p-1}{2}!&\equiv s_1s_2\cdots s_t\cdot r_1r_2\cdots r_n \bmod p\\&\equiv(-1)^n s_1s_2\cdots s_t(p-r_1)(p-r_2)\cdots(p-r_n) \bmod p\\&\equiv(-1)^n\frac{p-1}{2}! \bmod p\end{aligned}$$

又因为

$$\left(\frac{p-1}{2}!,p\right)=1$$

所以，

$$a^{\frac{p-1}{2}}\equiv(-1)^n \bmod p$$

证毕。

定理 5.2.2　设素数 $p>2$。

(1) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$。

(2) 当$(a,2p)=1$ 时，

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

其中，$T=\sum\limits_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor$。

证明　当 $1\leqslant j\leqslant\frac{p-1}{2}$时，因为

$$ja=p\left\lfloor\frac{ja}{p}\right\rfloor+t_j$$

其中 $0<t_j<p$。对该式两边求和，左边为

$$a\left(1+2+\cdots+\frac{p-1}{2}\right)=a\,\frac{p^2-1}{8}$$

右边为

$$p\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor+\sum_{j=1}^{\frac{p-1}{2}}t_j=pT+\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}r_j$$

$$=pT+\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}(p-r_j)-np+2\sum_{j=1}^{n}r_j$$

由引理 5.2.1 的证明知 $s_1,s_2,\cdots,s_t,p-r_1,p-r_2,\cdots,p-r_n$ 是 $1,2,\cdots,\frac{p-1}{2}$ 的一个排列，

$$\sum_{i=1}^{t}s_i+\sum_{j=1}^{n}(p-r_j)=\frac{p^2-1}{8}$$

得

$$(a-1)\,\frac{p^2-1}{8}=(T-n)p+2\sum_{j=1}^{n}r_j$$

$$(a-1)\,\frac{p^2-1}{8}\equiv(T-n)p \bmod 2\equiv(T-n) \bmod 2\equiv(T+n) \bmod 2$$

当 $a=2$ 时，对于 $1\leqslant j\leqslant\frac{p-1}{2}$，有

$$ja\leqslant p-1,\quad\left\lfloor\frac{ja}{p}\right\rfloor=0$$

所以

$$T=\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor=0$$

所以

$$n\equiv\frac{p^2-1}{8} \bmod 2$$

而当 $(a,2p)=1$ 时，a 必为奇数，$a-1\equiv0 \bmod 2$，所以从上式可得 $T\equiv n \bmod 2$，由引理 5.2.1 即得

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

证毕。

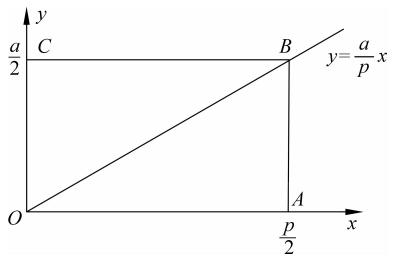

图 5.2.1　T 的几何意义

T 的几何意义如图 5.2.1 所示。

T 表示图 5.2.1 中 x 轴、直线 $x=\frac{p}{2}$、直线 $y=\frac{a}{p}x$ 所围成的 $\triangle OAB$ 内部的整数点的个数，这是因为以下两点：

(1) 线段 AB 上 $x=\frac{p}{2}$，无整数点。线段 OB 上，

因$(a,p)=1$，$p\nmid a$，无整数点。

(2) 当$0<j<\frac{p}{2}$时，线段$x=j$上整数点个数为$\left\lfloor\frac{aj}{p}\right\rfloor$，所以$\triangle OAB$内部整数点个数为

$$\sum_{j=0}^{\frac{p-1}{2}}\left\lfloor\frac{aj}{p}\right\rfloor=T$$

如果$a=q$，其中$q\neq p$且为素数，则有

$$\left(\frac{q}{p}\right)=(-1)^T$$

类似地有

$$\left(\frac{p}{q}\right)=(-1)^S$$

其中，

$$S=\sum_{l=1}^{\frac{q-1}{2}}\left\lfloor\frac{lp}{p}\right\rfloor$$

为图 5.2.1 中$\triangle OCB$内部整数点个数。

而$S+T$是矩形$OABC$内部整数点的个数，因此

$$S+T=\frac{p-1}{2}\frac{q-1}{2}$$

所以有

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{S+T}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

由此可得如下定理。

定理 5.2.3(二次互反律)　设素数p、q均大于 2，$p\neq q$，则

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

或写成

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

二次互反律的意义：$\left(\frac{a}{p}\right)$以p为周期，若$a>p$，则总能找到$q<p$，$(p,q)=1$，使得$\left(\frac{a}{p}\right)=\left(\frac{q}{p}\right)$。由二次互反律知，要求$\left(\frac{q}{p}\right)$，只需求$\left(\frac{p}{q}\right)$，它的周期$q<p$，即所求的 Legendre 符号的周期越来越小，最后变为求形如$\left(\frac{1}{p}\right)$或$\left(\frac{2}{p}\right)$的 Legendre 符号。

例 5.2.1　求$\left(\frac{137}{227}\right)$。

解　227 为素数，

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

其中，

$$\left(\frac{2}{227}\right)=(-1)^{\frac{227^2-1}{8}}=-1,\quad \left(\frac{3^2}{227}\right)=1,\quad \left(\frac{5}{227}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=-1$$

所以$\left(\frac{137}{227}\right)=-1$。这表明同余方程 $x^2\equiv 137 \bmod 227$ 无解。

例 5.2.2 判断以下两个同余方程是否有解。若有解，求出其解数。

(1) $x^2\equiv -1 \bmod 365$。

(2) $x^2\equiv 2 \bmod 3599$。

解

(1) 365 不是素数，$365=5\cdot 73$，所以同余方程与以下同余方程组等价：

$$\begin{cases} x^2\equiv -1 \bmod 5 \\ x^2\equiv -1 \bmod 73 \end{cases}$$

由于$\left(\frac{-1}{5}\right)=1$，$\left(\frac{-1}{73}\right)=1$，同余方程组有解，原方程的解数为 4。

(2) 3599 不是素数，$3599=59\cdot 61$，同余方程等价于以下同余方程组：

$$\begin{cases} x^2\equiv 2 \bmod 59 \\ x^2\equiv 2 \bmod 61 \end{cases}$$

由于$\left(\frac{2}{59}\right)=-1$，所以同余方程组无解，原方程无解。

例 5.2.3 求分别以 3 为其二次剩余和二次非剩余的所有奇素数 p。

解 就是分别求满足$\left(\frac{3}{p}\right)=1$ 和$\left(\frac{3}{p}\right)=-1$ 的奇素数 p。

因为

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

由定理 5.1.2 的推论 1，有

$$(-1)^{\frac{p-1}{2}}=\begin{cases} 1, & p\equiv 1 \bmod 4 \\ -1, & p\equiv -1 \bmod 4 \end{cases}$$

在求$\left(\frac{p}{3}\right)$时，将 $p=3,5,7,11,13,17,19,\cdots$ 逐个代入，可知 $p=7,13,19,\cdots$（即 $p=6k+1, k\in\mathbf{N}$）时为 1，$p=5,11,17,\cdots$（即 $p=6k+5, k\in\mathbf{N}$）时为 -1，所以

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

所以$\left(\frac{3}{p}\right)=1$ 的充要条件是：$p\equiv 1 \bmod 4$ 且 $p\equiv 1 \bmod 6$，即 $p\equiv 1 \bmod 12$；或 $p\equiv -1 \bmod 4$ 且 $p\equiv -1 \bmod 6$，即 $p\equiv -1 \bmod 12$。

而$\left(\frac{3}{p}\right)=-1$ 的充要条件是：$p\equiv 1 \bmod 4$ 且 $p\equiv -1 \bmod 6$；或 $p\equiv -1 \bmod 4$ 且 $p\equiv 1 \bmod 6$。即：$p\equiv 5 \bmod 4$ 且 $p\equiv 5 \bmod 6$；或 $p\equiv -5 \bmod 4$ 且 $p\equiv -5 \bmod 6$。所以 $p\equiv 5 \bmod 12$ 或 $p\equiv -5 \bmod 12$。

例 5.2.4　求分别以 11 为其二次剩余和二次非剩余的所有奇素数 p。

解

$$\left(\frac{11}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right)$$

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1, & p\equiv 1 \bmod 4\\ -1, & p\equiv -1 \bmod 4\end{cases}$$

对模 11 的绝对最小完全剩余系 $\pm1,\pm2,\pm3,\pm4,\pm5$ 中的每个值进行计算，可得

$$\left(\frac{p}{11}\right)=\begin{cases}1, & p\equiv 1,-2,3,4,5 \pmod{11}\\ -1, & p\equiv -1,2,-3,-4,-5 \pmod{11}\end{cases}$$

由同余方程组

$$\begin{cases}p\equiv a_1 \bmod 4\\ p\equiv a_2 \bmod 11\end{cases}$$

得 $p\equiv(-11a_1+12a_2) \bmod 44$。

$\left(\frac{11}{p}\right)=1$ 当且仅当 $a_1=1,a_2=1,-2,3,4,5$；或 $a_1=-1,a_2=-1,2,-3,-4,-5$。所以 $p\equiv\pm1,\pm5,\pm7,\pm9,\pm19 \pmod{44}$。

同理，$\left(\frac{11}{p}\right)=-1$ 当且仅当 $a_1=1,a_2=-1,2,-3,-4,-5$；或 $a_1=-1,a_2=1,-2,3,4,5$。所以 $p=\pm3,\pm13,\pm15,\pm17,\pm21 \pmod{44}$。

例 5.2.5　证明满足 $p\equiv1 \bmod 4$ 的素数有无穷多个。

证明　用反证法。假设满足条件的素数有有限个，它们构成的集合记为 $A=\{p_1,p_2,\cdots,p_k\}$，构造 $P=1+(2p_1p_2\cdots p_k)^2$，满足 $P\equiv1 \bmod 4$，P 不是素数，否则 $P\in A$，不可能。

设 p 是 P 的素因子，则

$$\left(\frac{-1}{p}\right)=\left(\frac{-1+P}{p}\right)=\left(\frac{2(p_1p_2\cdots p_k)^2}{p}\right)=1$$

由定理 5.1.2 的推论 1 可知 $p\equiv1 \bmod 4$，所以 $p\in A$。由 $p\mid P$，$p\mid(2p_1p_2\cdots p_k)^2$ 可得

$$p\mid(P-(2p_1p_2\cdots p_k)^2)=1$$

矛盾。　证毕。

5.3　Jacobi 符号

在求 Legendre 符号 $\left(\frac{a}{p}\right)$ 时，需要求出 a 的素因数分解，然后再用 Legendre 符号的性质和二次互反律来求解，但当 a 很大时计算复杂。为了避免这种复杂的计算，引入 Jacobi 符号。

定义 5.3.1　设 $P=p_1p_2\cdots p_s$，其中 $p_j(1\leqslant j\leqslant s)$ 是素数，定义

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_s}\right)$$

其中 $\left(\frac{a}{p_j}\right)(1\leqslant j\leqslant s)$ 是模 p_j 的 Legendre 符号。称 $\left(\frac{a}{P}\right)$ 为 Jacobi 符号。

由定义 5.3.1 及 Legendre 符号的性质，容易推出 Jacobi 符号有以下性质。

定理 5.3.1

(1) $\left(\frac{1}{P}\right)=1$。

(2) $\left(\frac{a}{P}\right)=\begin{cases}0, & (a,P)>1\\ \pm 1, & (a,P)=1\end{cases}$。

(3) $\left(\frac{a}{P}\right)=\left(\frac{a+P}{P}\right)$。

(4) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$。

(5) $\left(\frac{a}{P_1P_2}\right)=\left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$。

(6) 当 $(a,P)=1$ 时，$\left(\frac{a^2}{P}\right)=\left(\frac{a}{P^2}\right)=1$。

为了进一步得到 Jacobi 符号的其他性质，需要以下引理。

引理 5.3.1 设 $a_j\equiv 1 \bmod m(1\leqslant j\leqslant s)$，$a=a_1a_2\cdots a_s$，则

$$\frac{a-1}{m}\equiv\frac{a_1-1}{m}+\frac{a_2-1}{m}+\cdots+\frac{a_s-1}{m} \mod m$$

证明 对 s 用归纳法。

$s=2$ 时，

$$a-1=a_1a_2-1=(a_1-1)+(a_2-1)+(a_1-1)(a_2-1)$$

由 $a_j\equiv 1 \bmod m$，知 $a\equiv 1 \bmod m$，所以

$$\frac{a-1}{m}\equiv\frac{a_1-1}{m}+\frac{a_2-1}{m}+\frac{(a_1-1)(a_2-1)}{m} \mod m$$

$$\equiv\frac{a_1-1}{m}+\frac{a_2-1}{m} \mod m$$

其中，第 3 项中 $m^2\mid(a_1-1)(a_2-1)$。

设 $s=k$ 时，结论成立。

当 $s=k+1$ 时，

$$a=(a_1a_2\cdots a_k)a_{k+1}$$

$$\frac{a-1}{m}\equiv\frac{a_1a_2\cdots a_k-1}{m}+\frac{a_{k+1}-1}{m} \mod m$$

$$\equiv\left(\frac{a_1-1}{m}+\frac{a_2-1}{m}+\cdots+\frac{a_k-1}{m}\right)+\frac{a_{k+1}-1}{m} \mod m$$

证毕。

定理 5.3.2 $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$，$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$。

证明 设 $P=p_1p_2\cdots p_s$，则

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_s}\right)=(-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_s-1}{2}}=(-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\cdots+\frac{p_s-1}{2}}$$

在引理 5.3.1 中，取 $m=2$，$a_j=p_j(1\leqslant j\leqslant s)$，得