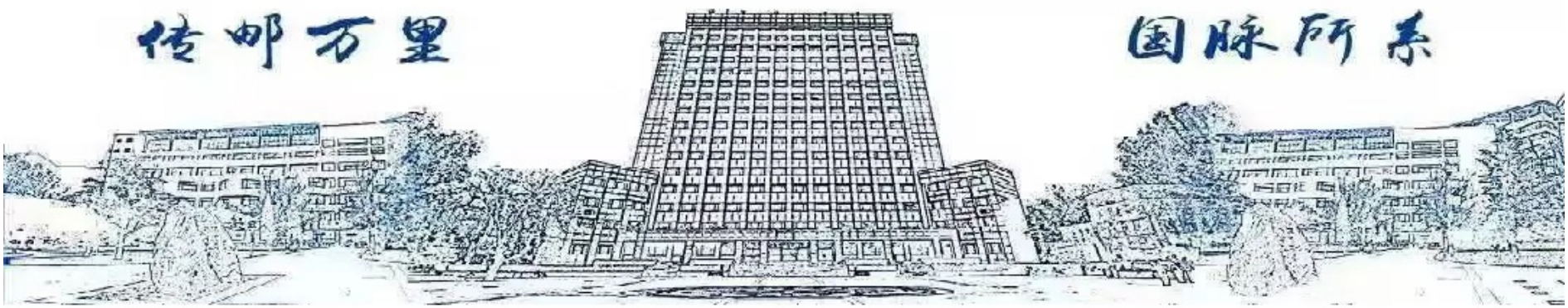
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

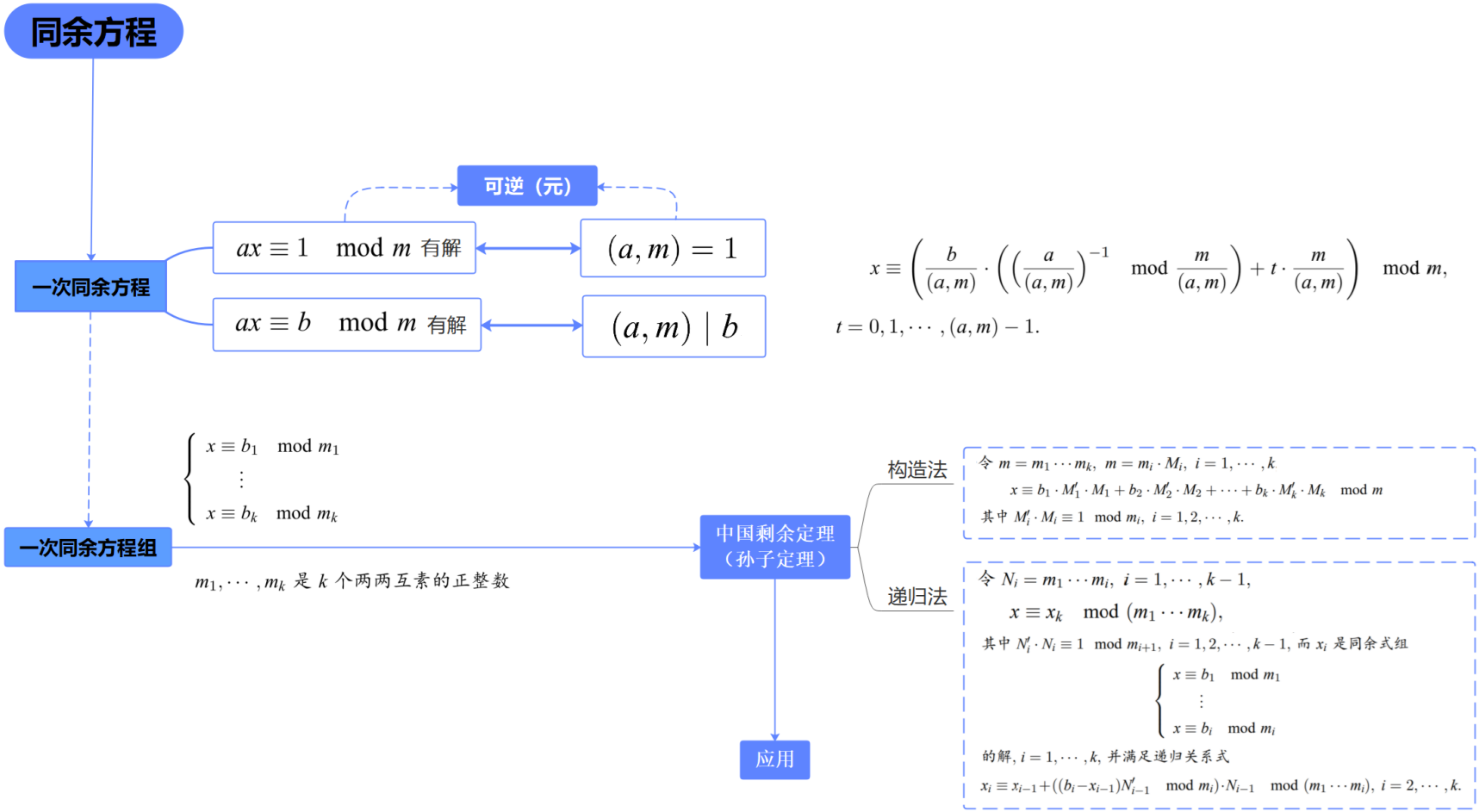
—— 同余方程 (2)

信数课题组

北京邮电大学



上次课回顾


同余方程
一次同余方程
可逆（元）
$ax \equiv 1 \mod m$ 有解
$(a,m)=1$
$ax \equiv b \mod m$ 有解
$(a,m) \mid b$
$x \equiv \left(\frac{b}{(a,m)} \cdot \left(\left(\frac{a}{(a,m)}\right)^{-1} \mod \frac{m}{(a,m)}\right) + t \cdot \frac{m}{(a,m)}\right) \mod m,$
$t = 0, 1, \cdots, (a,m)-1.$
一次同余方程组
$\begin{cases} x \equiv b_1 \mod m_1 \\ \vdots \\ x \equiv b_k \mod m_k \end{cases}$
$m_1, \cdots, m_k$ 是 k 个两两互素的正整数
中国剩余定理（孙子定理）
构造法
令 $m = m_1 \cdots m_k$, $m = m_i \cdot M_i$, $i = 1, \cdots, k$
$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$
其中 $M_i' \cdot M_i \equiv 1 \mod m_i$, $i = 1, 2, \cdots, k$.
递归法
令 $N_i = m_1 \cdots m_i$, $i = 1, \cdots, k-1$,
$x \equiv x_k \mod (m_1 \cdots m_k)$,
其中 $N_i' \cdot N_i \equiv 1 \mod m_{i+1}$, $i = 1, 2, \cdots, k-1$, 而 x_i 是同余式组
$\begin{cases} x \equiv b_1 \mod m_1 \\ \vdots \\ x \equiv b_i \mod m_i \end{cases}$
的解, $i = 1, \cdots, k$, 并满足递归关系式
$x_i \equiv x_{i-1} + ((b_i - x_{i-1}) N_{i-1}' \mod m_i) \cdot N_{i-1} \mod (m_1 \cdots m_i)$, $i = 2, \cdots, k$.
应用

目录

目录

二次同余方程的一般形式是

$$ax^2 + bx + c \equiv 0 \mod m,$$

其中 $a \not\equiv 0 \mod m$.

二次同余方程的一般形式是

$$ax^2 + bx + c \equiv 0 \mod m,$$

其中 $a \not\equiv 0 \mod m$.

因为正整数 m 有素因数分解式 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 所以二次同余方程等价于同余方程组

$$\begin{cases} ax^2 + bx + c \equiv 0 \mod p_1^{\alpha_1}, \\ \vdots \\ ax^2 + bx + c \equiv 0 \mod p_k^{\alpha_k}. \end{cases}$$

因此, 只需讨论模为素数幂 p^α 的同余方程

$$ax^2 + bx + c \equiv 0 \mod p^\alpha, \quad p \nmid a.$$

二次同余方程的一般形式是

$$ax^2 + bx + c \equiv 0 \mod m,$$

其中 $a \not\equiv 0 \mod m$.

因为正整数 m 有素因数分解式 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 所以二次同余方程

等价于同余方程组
$$\begin{cases} ax^2 + bx + c \equiv 0 \mod p_1^{\alpha_1}, \\ \vdots \\ ax^2 + bx + c \equiv 0 \mod p_k^{\alpha_k}. \end{cases}$$

因此, 只需讨论模为素数幂 p^α 的同余方程

$$ax^2 + bx + c \equiv 0 \mod p^\alpha, \quad p \nmid a.$$

两端同乘以 $4a$, 得到 $4a^2x^2 + 4abx + 4ac \equiv 0 \mod p^\alpha$, 即 $(2ax+b)^2 \equiv b^2 - 4ac \mod p^\alpha$. 令 $y = 2ax + b$, 有 $y^2 \equiv b^2 - 4ac \mod p^\alpha$.

二次同余方程的一般形式是

$$ax^2 + bx + c \equiv 0 \mod m,$$

其中 $a \not\equiv 0 \mod m$.

因为正整数 m 有素因数分解式 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 所以二次同余方程

等价于同余方程组
$$\begin{cases} ax^2 + bx + c \equiv 0 \mod p_1^{\alpha_1}, \\ \vdots \\ ax^2 + bx + c \equiv 0 \mod p_k^{\alpha_k}. \end{cases}$$

因此, 只需讨论模为素数幂 p^α 的同余方程

$$ax^2 + bx + c \equiv 0 \mod p^\alpha, \quad p \nmid a.$$

两端同乘以 $4a$, 得到 $4a^2x^2 + 4abx + 4ac \equiv 0 \mod p^\alpha$, 即 $(2ax+b)^2 \equiv b^2 - 4ac \mod p^\alpha$. 令 $y = 2ax + b$, 有 $y^2 \equiv b^2 - 4ac \mod p^\alpha$.

特别地, 当 p 是奇素数时, $(2a, p) = 1$. 同余方程 $y^2 \equiv b^2 - 4ac \mod p^\alpha$ 等价于同余方程 $ax^2 + bx + c \equiv 0 \mod p^\alpha, \quad p \nmid a$.

定义 3.3.1

设 m 是正整数, 若同余方程

$$x^2 \equiv a \mod m, \quad (a, m) = 1$$

有解, 则 a 叫做模 m 的**平方剩余** (或**二次剩余**); 否则, a 叫做模 m 的**平方非剩余** (或**二次非剩余**).

定义 3.3.1

设 m 是正整数, 若同余方程

$$x^2 \equiv a \mod m, \quad (a, m) = 1$$

有解, 则 a 叫做模 m 的**平方剩余** (或**二次剩余**); 否则, a 叫做模 m 的**平方非剩余** (或**二次非剩余**).

例 3.3.1 1 是模 3 平方剩余, -1 是模 3 平方非剩余.

定义 3.3.1

设 m 是正整数, 若同余方程

$$x^2 \equiv a \mod m, \quad (a, m) = 1$$

有解, 则 a 叫做模 m 的**平方剩余** (或**二次剩余**); 否则, a 叫做模 m 的**平方非剩余** (或**二次非剩余**).

例 3.3.1 1 是模 3 平方剩余, -1 是模 3 平方非剩余.

例 3.3.2 $1, 2, 4$ 是模 7 平方剩余, $-1, 3, 5$ 是模 7 平方非剩余. 因为

$$1^2 \equiv 1 \mod 7, \ 2^2 \equiv 4 \mod 7, \ 3^2 \equiv 2 \mod 7,$$
$$4^2 \equiv 2 \mod 7, \ 5^2 \equiv 4 \mod 7, \ 6^2 \equiv 1 \mod 7.$$

定义 3.3.1

设 m 是正整数, 若同余方程

$$x^2 \equiv a \mod m, \quad (a, m) = 1$$

有解, 则 a 叫做模 m 的**平方剩余** (或**二次剩余**); 否则, a 叫做模 m 的**平方非剩余** (或**二次非剩余**).

例 3.3.1 1 是模 3 平方剩余, -1 是模 3 平方非剩余.

例 3.3.2 $1, 2, 4$ 是模 7 平方剩余, $-1, 3, 5$ 是模 7 平方非剩余. 因为

$$1^2 \equiv 1 \mod 7, \ 2^2 \equiv 4 \mod 7, \ 3^2 \equiv 2 \mod 7,$$
$$4^2 \equiv 2 \mod 7, \ 5^2 \equiv 4 \mod 7, \ 6^2 \equiv 1 \mod 7.$$

例 3.3.3 $-1, 1, 2, 3, 4, 9, 10$ 是模 13 平方剩余, $5, 6, 7, 8, 11$ 是模 13 平方非剩余. 因为

$$1^2 \equiv 12^2 \equiv 1 \mod 13, 2^2 \equiv 11^2 \equiv 4 \mod 13, 3^2 \equiv 10^2 \equiv 9 \mod 13,$$
$$4^2 \equiv 9^2 \equiv 3 \mod 13, 5^2 \equiv 8^2 \equiv -1 \mod 13, 6^2 \equiv 7^2 \equiv 10 \mod 13.$$

例 3.3.4 求满足方程 $E:\ y^2 = x^3 + x + 1 \mod 7$ 的所有整数点 (x, y).

例 3.3.4 求满足方程 $E: y^2 = x^3 + x + 1 \mod 7$ 的所有整数点 (x, y).

解：对 $x = 0, 1, 2, 3, 4, 5, 6,$ 分别求出 y.

$$
\begin{aligned}
&x = 0,\ y^2 = 1 \mod 7,\ y = 1, 6 \mod 7,\\
&x = 1,\ y^2 = 3 \mod 7,\ \text{无解},\\
&x = 2,\ y^2 = 4 \mod 7,\ y = 2, 5 \mod 7,\\
&x = 3,\ y^2 = 3 \mod 7,\ \text{无解},\\
&x = 4,\ y^2 = 6 \mod 7,\ \text{无解},\\
&x = 5,\ y^2 = 5 \mod 7,\ \text{无解},\\
&x = 6,\ y^2 = 6 \mod 7,\ \text{无解}.
\end{aligned}
$$

例 3.3.4 求满足方程 $E:\ y^2 = x^3 + x + 1 \mod 7$ 的所有整数点 (x, y).

解：对 $x = 0, 1, 2, 3, 4, 5, 6,$ 分别求出 y.

$$
\begin{aligned}
&x = 0,\ y^2 = 1 \mod 7,\ y = 1, 6 \mod 7,\\
&x = 1,\ y^2 = 3 \mod 7,\ \text{无解},\\
&x = 2,\ y^2 = 4 \mod 7,\ y = 2, 5 \mod 7,\\
&x = 3,\ y^2 = 3 \mod 7,\ \text{无解},\\
&x = 4,\ y^2 = 6 \mod 7,\ \text{无解},\\
&x = 5,\ y^2 = 5 \mod 7,\ \text{无解},\\
&x = 6,\ y^2 = 6 \mod 7,\ \text{无解}.
\end{aligned}
$$

共有 4 个点 $(0, 1), (0, 6), (2, 2), (2, 5)$.

例 3.3.5 求满足方程 $E:\ y^2 = x^3 + x + 2 \mod 7$ 的所有整数点 (x, y).

例 3.3.5 求满足方程 $E: y^2 = x^3 + x + 2 \mod 7$ 的所有整数点 (x, y).

解：对 $x = 0, 1, 2, 3, 4, 5, 6,$ 分别求出 y.

$$
\begin{aligned}
&x = 0,\ y^2 = 2 \mod 7, y = 3, 4 \mod 7,\\
&x = 1,\ y^2 = 4 \mod 7, y = 2, 5 \mod 7,\\
&x = 2,\ y^2 = 5 \mod 7, \text{无解},\\
&x = 3,\ y^2 = 4 \mod 7, y = 2, 5 \mod 7,\\
&x = 4,\ y^2 = 0 \mod 7, y = 0 \mod 7,\\
&x = 5,\ y^2 = 6 \mod 7, \text{无解},\\
&x = 6,\ y^2 = 0 \mod 7, y = 0 \mod 7.
\end{aligned}
$$

例 3.3.5 求满足方程 $E:\ y^2 = x^3 + x + 2 \mod 7$ 的所有整数点 (x, y).

解：对 $x = 0, 1, 2, 3, 4, 5, 6,$ 分别求出 y.

$$
\begin{aligned}
&x = 0,\ y^2 = 2 \mod 7, y = 3, 4 \mod 7,\\
&x = 1,\ y^2 = 4 \mod 7, y = 2, 5 \mod 7,\\
&x = 2,\ y^2 = 5 \mod 7, \text{无解},\\
&x = 3,\ y^2 = 4 \mod 7, y = 2, 5 \mod 7,\\
&x = 4,\ y^2 = 0 \mod 7, y = 0 \mod 7,\\
&x = 5,\ y^2 = 6 \mod 7, \text{无解},\\
&x = 6,\ y^2 = 0 \mod 7, y = 0 \mod 7.
\end{aligned}
$$

共有 8 个点 $(0, 3), (0, 4), (1, 2), (1, 5), (3, 2), (3, 5), (4, 0), (6, 0)$.

下面讨论如何判断同余方程 $x^2 \equiv a \mod m, (a,m) = 1$ 有解.

首先考虑模为素数 p 的二次同余方程 $x^2 \equiv a \mod p, (a,p) = 1$.

定理 3.3.1 (欧拉判别条件)

设 p 是奇素数, $(a,p) = 1$, 则

(i) a 是模 p 的平方剩余的充要条件是

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

(ii) a 是模 p 的平方非剩余的充要条件是

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

并且当 a 是模 p 的平方剩余时, 同余式 $x^2 \equiv a \mod p$ 恰有二解.

下面讨论如何判断同余方程 $x^2 \equiv a \mod m, (a,m) = 1$ 有解.

首先考虑模为素数 p 的二次同余方程 $x^2 \equiv a \mod p, (a,p) = 1$.

定理 3.3.1 (欧拉判别条件)

设 p 是奇素数, $(a,p) = 1$, 则

(i) a 是模 p 的平方剩余的充要条件是

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

(ii) a 是模 p 的平方非剩余的充要条件是

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

并且当 a 是模 p 的平方剩余时, 同余式 $x^2 \equiv a \mod p$ 恰有二解.

证: (i) 因为 p 是奇素数, 所以有表达式

$$\begin{aligned} x^p - x &= x\left((x^2)^{\frac{p-1}{2}} - a^{\frac{p-1}{2}}\right) + \left(a^{\frac{p-1}{2}} - 1\right)x \\ &= xq(x) \cdot (x^2 - a) + \left(a^{\frac{p-1}{2}} - 1\right)x, \end{aligned} \tag{3.3.1}$$

其中 $q(x)$ 是关于 x 的整系数多项式.

根据定理 2.2.14 (费马小定理), 对于任意的 x, 有 $x^p - x \equiv 0 \mod p$.

若 a 是模 p 的平方剩余, 即存在某个 x_0 使得 $x_0^2 \equiv a \mod p$, 其中 $(x_0, p) = 1$, 则

$$0 \equiv x_0^p - x_0 \equiv (x_0^2 - a)x_0 q(x_0) + \left(a^{\frac{p-1}{2}} - 1\right)x_0 \equiv \left(a^{\frac{p-1}{2}} - 1\right)x_0 \mod p,$$

而 $(x_0, p) = 1$, 所以 $a^{\frac{p-1}{2}} \equiv 1 \mod p$ 成立.

根据定理 2.2.14 (费马小定理), 对于任意的 x, 有 $x^p - x \equiv 0 \mod p$.

若 a 是模 p 的平方剩余, 即存在某个 x_0 使得 $x_0^2 \equiv a \mod p$, 其中 $(x_0, p) = 1$, 则

$$0 \equiv x_0^p - x_0 \equiv (x_0^2 - a)x_0 q(x_0) + \left(a^{\frac{p-1}{2}} - 1\right)x_0 \equiv \left(a^{\frac{p-1}{2}} - 1\right)x_0 \mod p,$$

而 $(x_0, p) = 1$, 所以 $a^{\frac{p-1}{2}} \equiv 1 \mod p$ 成立.

同时, 易知 $p - x_0$ 是同余方程 $x^2 \equiv a \mod p$, $(a, p) = 1$ 的另外一个解, 且仅有此二解. 事实上, 若存在第三个解 a_1, 则 a_1 也满足同余方程 $x^2 - a \equiv (x - x_0)(x - p + x_0) \equiv 0 \mod p$, 其中 $a_1 \not\equiv x_0 \mod p$ 且 $a_1 \not\equiv p - x_0 \mod p$, 矛盾! 所以该同余方程有且仅有此二解.

根据定理 2.2.14 (费马小定理), 对于任意的 x, 有 $x^p - x \equiv 0 \mod p$.

若 a 是模 p 的平方剩余, 即存在某个 x_0 使得 $x_0^2 \equiv a \mod p$, 其中 $(x_0, p) = 1$, 则

$$0 \equiv x_0^p - x_0 \equiv (x_0^2 - a)x_0 q(x_0) + \left(a^{\frac{p-1}{2}} - 1\right)x_0 \equiv \left(a^{\frac{p-1}{2}} - 1\right)x_0 \mod p,$$

而 $(x_0, p) = 1$, 所以 $a^{\frac{p-1}{2}} \equiv 1 \mod p$ 成立.

同时, 易知 $p - x_0$ 是同余方程 $x^2 \equiv a \mod p$, $(a, p) = 1$ 的另外一个解, 且仅有此二解. 事实上, 若存在第三个解 a_1, 则 a_1 也满足同余方程 $x^2 - a \equiv (x - x_0)(x - p + x_0) \equiv 0 \mod p$, 其中 $a_1 \not\equiv x_0 \mod p$ 且 $a_1 \not\equiv p - x_0 \mod p$, 矛盾! 所以该同余方程有且仅有此二解.

反过来, 若 $a^{\frac{p-1}{2}} \equiv 1 \mod p$ 成立, 则由式 (3.3.1) 知, $x^p - x \equiv (x^2 - a)xq(x) \mod p$. 根据定理 2.2.14 (费马小定理) 知, $x^p - x \equiv 0 \mod p$ 有 p 个不同的解, 而 $q(x)$ 是次数为 $p - 3$ 的多项式, 故 $q(x) \equiv 0 \mod p$ 最多有 $p - 3$ 个不同的解 (见后面的定理 3.4.4). 所以同余方程 $x^2 \equiv a \mod p$ 一定有解, 即 a 是模 p 的平方剩余.

(ii) 因为 p 是奇素数, $(a,p)=1$, 根据定理 2.2.13 (欧拉定理), 有

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

再根据定理 1.2.10, 有 $p \mid a^{\frac{p-1}{2}}+1$ 或 $p \mid a^{\frac{p-1}{2}}-1$.

因此, 由上述结论 (i) 知, a 是模 p 的平方非剩余的充要条件是

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

(ii) 因为 p 是奇素数, $(a,p)=1$, 根据定理 2.2.13 (欧拉定理), 有

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

再根据定理 1.2.10, 有 $p \mid a^{\frac{p-1}{2}}+1$ 或 $p \mid a^{\frac{p-1}{2}}-1$.

因此, 由上述结论 (i) 知, a 是模 p 的平方非剩余的充要条件是

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

例 3.3.6　判断 211 是否为模 2027 平方剩余.

解：根据定理 3.3.1，我们计算：$211^{\frac{2027-1}{2}}=211^{1013} \mod 2027$.

运用模重复平方计算法. 设 $m=2027, b=211$, 令 $a=1$, 将 1013 写成二进制, $1013=1+2^2+2^4+2^5+2^6+2^7+2^8+2^9$.

(1) $n_0=1$, 计算 $a_0=a\cdot b^{n_0}\equiv 211 \mod 2027$, $b_1=b^2\equiv 1954 \mod 2027$.

(2) $n_1=0$, 计算 $a_1=a_0\cdot b_1^{n_1}\equiv 211 \mod 2027$, $b_2=b_1^2\equiv 1275 \mod 2027$.

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2^{n_2} \equiv 1461 \mod 2027,\ b_3 = b_2^2 \equiv 1998 \mod 2027.$$

(4) $n_3 = 0$, 计算

$$a_3 = a_2 \cdot b_3^{n_3} \equiv 1461 \mod 2027,\ b_4 = b_3^2 \equiv 841 \mod 2027.$$

(5) $n_4 = 1$, 计算

$$a_4 = a_3 \cdot b_4^{n_4} \equiv 339 \mod 2027,\ b_5 = b_4^2 \equiv 1885 \mod 2027.$$

(6) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5^{n_5} \equiv 510 \mod 2027,\ b_6 = b_5^2 \equiv 1921 \mod 2027.$$

(7) $n_6 = 1$, 计算

$$a_6 = a_5 \cdot b_6^{n_6} \equiv 669 \mod 2027,\ b_7 = b_6^2 \equiv 1101 \mod 2027.$$

(8) $n_7 = 1$, 计算

$$a_7 = a_6 \cdot b_7^{n_7} \equiv 768 \mod 2027,\ b_8 = b_7^2 \equiv 55 \mod 2027.$$

(9) $n_8 = 1$, 计算

$$a_8 = a_7 \cdot b_8^{n_8} \equiv 1700 \mod 2027,\ b_9 = b_8^2 \equiv 998 \mod 2027.$$

(10) $n_9 = 1$, 计算

$$a_9 = a_8 \cdot b_9^{n_9} \equiv 1461 \mod 2027,\ b_3 = b_2^2 \equiv 1998 \mod 2027.$$

因此, 221 为模 2027 平方剩余.

(10) $n_9 = 1$, 计算

$$a_9 = a_8 \cdot b_9^{n_9} \equiv 1461 \mod 2027,\ b_3 = b_2^2 \equiv 1998 \mod 2027.$$

因此, 221 为模 2027 平方剩余.

推论 3.3.1

设 p 是奇素数, $(a_1, p) = 1, (a_2, p) = 1$, 则

(i) 若 a_1, a_2 都是模 p 的平方剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方剩余.

(ii) 若 a_1, a_2 都是模 p 的平方非剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方剩余.

(iii) 若 a_1 是模 p 的平方剩余, a_2 是模 p 的平方非剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方非剩余.

(10) $n_9 = 1$, 计算

$$a_9 = a_8 \cdot b_9^{n_9} \equiv 1461 \mod 2027,\ b_3 = b_2^2 \equiv 1998 \mod 2027.$$

因此, 221 为模 2027 平方剩余.

推论 3.3.1

设 p 是奇素数, $(a_1, p) = 1, (a_2, p) = 1$, 则

(i) 若 a_1, a_2 都是模 p 的平方剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方剩余.

(ii) 若 a_1, a_2 都是模 p 的平方非剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方剩余.

(iii) 若 a_1 是模 p 的平方剩余, a_2 是模 p 的平方非剩余, 则 $a_1 \cdot a_2$ 是模 p 的平方非剩余.

证：因为

$$(a_1 a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}},$$

所以由定理 3.3.1 即得结论.

定理 3.3.2

设 p 是奇素数, 则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列

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

中的一个数同余, 且仅与一个数同余.

定理 3.3.2

设 p 是奇素数, 则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列

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

中的一个数同余, 且仅与一个数同余.

证：由定理 3.3.1, 平方剩余的个数等于同余式 $x^{\frac{p-1}{2}} \equiv 1 \mod p$ 的解数. 但 $x^{\frac{p-1}{2}} - 1 \mid x^{p-1} - 1$. 由 3.4 节定理 3.4.5 (后面给予证明), 此同余方程的解数恰好是次数 $\frac{p-1}{2}$, 故平方剩余的个数是 $\frac{p-1}{2}$, 而平方非剩余的个数是 $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

定理 3.3.2

设 p 是奇素数, 则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列

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

中的一个数同余, 且仅与一个数同余.

证：由定理 3.3.1, 平方剩余的个数等于同余式 $x^{\frac{p-1}{2}} \equiv 1 \mod p$ 的解数. 但 $x^{\frac{p-1}{2}} - 1 \mid x^{p-1} - 1$. 由 3.4 节定理 3.4.5 (后面给予证明), 此同余方程的解数恰好是次数 $\frac{p-1}{2}$, 故平方剩余的个数是 $\frac{p-1}{2}$, 而平方非剩余的个数是 $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

若 $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ 中有两个数模 p 同余, 即存在 $k_1 \neq k_2$ 使得 $k_1^2 \equiv k_2^2 \mod p$, 则 $(k_1 + k_2)(k_1 - k_2) \equiv 0 \mod p$. 因此 $p \mid k_1 + k_2$ 或 $p \mid k_1 - k_2$. 但 $1 \leqslant k_1, k_2 \leqslant \frac{p-1}{2}$, 故 $2 \leqslant k_1 + k_2 \leqslant p - 1 < p$, $|k_1 - k_2| \leqslant p - 1 < p$. 从而, $k_1 = k_2$, 矛盾.

目录

定理 3.3.1 给出了整数 a 是否式模奇素数 p 二次剩余的判别法则, 但需要作较复杂的运算. 我们希望有一种更简单的判别法则.

定理 3.3.1 给出了整数 a 是否式模奇素数 p 二次剩余的判别法则, 但需要作较复杂的运算. 我们希望有一种更简单的判别法则.

定义 3.3.2

设 p 是素数, 定义**勒让德** (Legendre) **符号**如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 是模 } p \text{ 的平方剩余;}\\ -1, & \text{若 } a \text{ 是模 } p \text{ 的平方非剩余;}\\ 0, & \text{若 } p \mid a.\end{cases}$$

定理 3.3.1 给出了整数 a 是否式模奇素数 p 二次剩余的判别法则, 但需要作较复杂的运算. 我们希望有一种更简单的判别法则.

定义 3.3.2

设 p 是素数, 定义**勒让德** (Legendre) **符号**如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 是模 } p \text{ 的平方剩余;}\\ -1, & \text{若 } a \text{ 是模 } p \text{ 的平方非剩余;}\\ 0, & \text{若 } p \mid a.\end{cases}$$

例 3.3.7 根据例 3.3.3, 我们有

$$\left(\frac{-1}{13}\right)=\left(\frac{1}{13}\right)=\left(\frac{2}{13}\right)=\left(\frac{3}{13}\right)=\left(\frac{4}{13}\right)=\left(\frac{9}{13}\right)=\left(\frac{10}{13}\right)=1,$$

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

利用勒让德符号, 可以将定理 3.3.1 叙述为

定理 3.3.3 (欧拉判别法则)

设 p 是奇素数, 则对任意整数 a, 有

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

利用勒让德符号, 可以将定理 3.3.1 叙述为

定理 3.3.3 (欧拉判别法则)

设 p 是奇素数, 则对任意整数 a, 有

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

证：根据勒让德符号的定义及定理 3.3.1, 有

$$\left(\frac{a}{p}\right) = 1 \iff a \text{ 是模 } p \text{ 平方剩余} \iff a^{\frac{p-1}{2}} \equiv 1 \mod p$$

和

$$\left(\frac{a}{p}\right) = -1 \iff a \text{ 是模 } p \text{ 平方非剩余} \iff a^{\frac{p-1}{2}} \equiv -1 \mod p$$

以及

$$\left(\frac{a}{p}\right) = 0 \iff p \mid a \iff a^{\frac{p-1}{2}} \equiv 0 \mod p.$$

故结论成立.

例 3.3.8 证明 1, 2, 4 是模 7 平方剩余, -1, 3, 5 是模 7 平方非剩余.

证：因为

$$1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 \mod 7,$$

又由于

$$1^{\frac{7-1}{2}} \equiv 1 \mod 7, 4^{\frac{7-1}{2}} \equiv 1 \mod 7, 2^{\frac{7-1}{2}} \equiv 1 \mod 7,$$

即 $x^{\frac{7-1}{2}} \equiv 1 \mod 7$ 有 3 个解, 平方剩余有 $\frac{p-1}{2} = 3$ 个.

且这 3 个平方剩余, 分别为

$$3^2 \equiv 2, 2^2 \equiv 4, 1^2 \equiv 1 \mod 7.$$

根据欧拉判别法则, 可以判断 1 和 -1 是否为模 p 平方剩余, 即

定理 3.3.4

设 p 是奇素数, 则

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

根据欧拉判别法则, 可以判断 1 和 -1 是否为模 p 平方剩余, 即

定理 3.3.4

设 p 是奇素数, 则

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

证：分别令 $a=1$ 和 $a=-1$, 由定理 3.3.3 立得.

推论 3.3.2

设 p 是奇素数, 则

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

根据欧拉判别法则, 可以判断 1 和 -1 是否为模 p 平方剩余, 即

定理 3.3.4

设 p 是奇素数, 则

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

证：分别令 $a=1$ 和 $a=-1$, 由定理 3.3.3 立得.

推论 3.3.2

设 p 是奇素数, 则

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

证：若 $p\equiv 1 \mod 4$, 则存在正整数 k 使得 $p=4k+1$; 若 $p\equiv 3 \mod 4$, 则存在正整数 k 使得 $p=4k+3$. 由 $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ 立得.

例 3.3.9 判断同余方程 $x^2 \equiv -1 \mod 365$ 是否有解. 有解时, 求出其解数.

解：$365 = 5 \cdot 73$ 不是素数, 原同余方程等价于

$$\begin{cases} x^2 \equiv -1 \mod 5, \\ x^2 \equiv -1 \mod 73. \end{cases}$$

例 3.3.9 判断同余方程 $x^2 \equiv -1 \mod 365$ 是否有解. 有解时, 求出其解数.

解：$365 = 5 \cdot 73$ 不是素数, 原同余方程等价于

$$\begin{cases} x^2 \equiv -1 \mod 5, \\ x^2 \equiv -1 \mod 73. \end{cases}$$

因为

$$\left(\frac{-1}{5}\right) = \left(\frac{-1}{73}\right) = 1,$$

故同余方程组有解, 原同余方程有解. 根据中国剩余定理知, 解数为 4.

定理 3.3.5

设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$; (ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

定理 3.3.5

设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$; (ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

证: (i) 因为同余方程 $x^2\equiv a+p \mod p$ 等价于同余方程 $x^2\equiv a \mod p$, 故由定义知, $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$.

定理 3.3.5

设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$; (ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

证: (i) 因为同余方程 $x^2\equiv a+p \mod p$ 等价于同余方程 $x^2\equiv a \mod p$, 故由定义知, $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$.

(ii) 根据欧拉判别法则, 有

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

因为勒让德符号取值为 0, 1 或 -1, 且 p 为奇素数, 故 $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

定理 3.3.5

设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$; (ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

证: (i) 因为同余方程 $x^2\equiv a+p \mod p$ 等价于同余方程 $x^2\equiv a \mod p$, 故由定义知, $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$.

(ii) 根据欧拉判别法则, 有

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

因为勒让德符号取值为 0, 1 或 -1, 且 p 为奇素数, 故 $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) 由 (ii) 立得.

定理 3.3.5

设 p 是奇素数, 则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$; (ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

证: (i) 因为同余方程 $x^2\equiv a+p \mod p$ 等价于同余方程 $x^2\equiv a \mod p$, 故由定义知, $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$.

(ii) 根据欧拉判别法则, 有

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

因为勒让德符号取值为 0, 1 或 -1, 且 p 为奇素数, 故 $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) 由 (ii) 立得.

推论 3.3.3

设 p 是奇素数, 如果整数 a,b 满足 $a\equiv b \mod p$, 则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

对于一个与 p 互素的整数 a, 高斯给出了另一个判别法则, 以判断 a 是否为模 p 二次剩余.

引理 3.3.1 (Gauss 引理)

设 p 是奇素数, a 是整数, $(a,p)=1$. 如果整数 $a\cdot 1, a\cdot 2, \cdots, a\cdot \frac{p-1}{2}$ 中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m, 则 $\left(\frac{a}{p}\right)=(-1)^m$.

对于一个与 p 互素的整数 a, 高斯给出了另一个判别法则, 以判断 a 是否为模 p 二次剩余.

引理 3.3.1 (Gauss 引理)

设 p 是奇素数, a 是整数, $(a,p)=1$. 如果整数 $a\cdot 1, a\cdot 2, \cdots, a\cdot\frac{p-1}{2}$ 中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m, 则 $\left(\frac{a}{p}\right)=(-1)^m$.

证: 设 $a_1,\cdots,a_t$ 是整数 $a\cdot 1, a\cdot 2,\cdots, a\cdot\frac{p-1}{2}$ 模 p 的小于 $\frac{p}{2}$ 的最小正剩余, $b_1,\cdots,b_m$ 是这些整数模 p 的大于 $\frac{p}{2}$ 的最小正剩余, 则

$$\begin{aligned} a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= \prod_{k=1}^{\frac{p-1}{2}}(a\cdot k) \\ &\equiv \prod_{i=1}^{t} a_i \prod_{j=1}^{m} b_j \mod p \\ &\equiv (-1)^m \prod_{i=1}^{t} a_i \prod_{j=1}^{m}(p-b_j) \mod p. \end{aligned}$$

易知 $a_1, \cdots, a_t, p-b_1, \cdots, p-b_m$ 是模 p 两两不同余的.

(若不然, 则有 $a \cdot k_i \equiv p - a \cdot k_j \mod p$, 即 $a \cdot k_i + a \cdot k_j \equiv 0 \mod p$. 因而 $k_i + k_j \equiv 0 \mod p$, 这与 $1 \leqslant k_i + k_j \leqslant \frac{p-1}{2} + \frac{p-1}{2} < p$ 矛盾.)

易知 $a_1, \cdots, a_t, p-b_1, \cdots, p-b_m$ 是模 p 两两不同余的.

(若不然, 则有 $a \cdot k_i \equiv p - a \cdot k_j \mod p$, 即 $a \cdot k_i + a \cdot k_j \equiv 0 \mod p$. 因而 $k_i + k_j \equiv 0 \mod p$, 这与 $1 \leqslant k_i + k_j \leqslant \frac{p-1}{2} + \frac{p-1}{2} < p$ 矛盾.)

又因为 $(a \cdot k, p) = 1,\ k = 1, \cdots, \frac{p-1}{2}$, 所以 $\frac{p-1}{2}$ 个整数 $a_1, \cdots, a_t$, $p-b_1, \cdots, p-b_m$ 是 $1, \cdots, \frac{p-1}{2}$ 的一个排列, 故

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

因此,

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

再根据定理 3.3.3 及 p 是奇素数, 得

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

定理 3.3.6

设 p 是奇素数, 则

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

(ii) 若 $(a, 2p) = 1$, 则 $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$, 其中 $T(a,p) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{a \cdot k}{p}\right]$.

定理 3.3.6

设 p 是奇素数, 则

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

(ii) 若 $(a, 2p) = 1$, 则 $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$, 其中 $T(a,p) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{a\cdot k}{p}\right]$.

证: 因为 $a \cdot k = \left[\frac{a\cdot k}{p}\right] \cdot p + r_k,\ 0 < r_k < p,\ k = 1, \cdots, \frac{p-1}{2}$, 对 $k = 1, \cdots, \frac{p-1}{2}$ 求和, 并记 $T(a,p) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{a\cdot k}{p}\right]$, 有

$$a \cdot \frac{p^2-1}{8} = T(a,p) \cdot p + \sum_{i=1}^{t} a_i + \sum_{j=1}^{m} b_j$$

$$= T(a,p) \cdot p + \sum_{i=1}^{t} a_i + \sum_{j=1}^{m} (p - b_j) + 2\sum_{j=1}^{m} b_j - m \cdot p$$

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

因此, $(a-1)\cdot\frac{p^2-1}{8} \equiv T(a,p)+m \mod 2$.

因此, $(a-1)\cdot\frac{p^2-1}{8} \equiv T(a,p)+m \mod 2$.

若 $a=2$, 则对于 $0 \leqslant k \leqslant \frac{p-1}{2}$, 有 $0 \leqslant \left[\frac{a\cdot k}{p}\right] \leqslant \left[\frac{p-1}{p}\right] = 0$, 从而 $T(a,p)=0$, 故 $m \equiv \frac{p^2-1}{8} \mod 2$; 若 a 为奇数, 则 $m \equiv T(a,p) \mod 2$.

故由引理 3.3.1 知, 结论成立.

因此, $(a-1)\cdot\frac{p^2-1}{8} \equiv T(a,p)+m \mod 2$.

若 $a=2$, 则对于 $0 \leqslant k \leqslant \frac{p-1}{2}$, 有 $0 \leqslant \left[\frac{a\cdot k}{p}\right] \leqslant \left[\frac{p-1}{p}\right] = 0$, 从而 $T(a,p)=0$, 故 $m \equiv \frac{p^2-1}{8} \mod 2$; 若 a 为奇数, 则 $m \equiv T(a,p) \mod 2$.

故由引理 3.3.1 知, 结论成立.

推论 3.3.4

设 p 是奇素数, 则

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

因此, $(a-1)\cdot\frac{p^2-1}{8} \equiv T(a,p)+m \mod 2$.

若 $a=2$, 则对于 $0 \leqslant k \leqslant \frac{p-1}{2}$, 有 $0 \leqslant \left[\frac{a\cdot k}{p}\right] \leqslant \left[\frac{p-1}{p}\right] = 0$, 从而 $T(a,p)=0$, 故 $m \equiv \frac{p^2-1}{8} \mod 2$; 若 a 为奇数, 则 $m \equiv T(a,p) \mod 2$.

故由引理 3.3.1 知, 结论成立.

推论 3.3.4

设 p 是奇素数, 则

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

证：根据定理 3.3.6 (i), 有 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

若 $p \equiv \pm 1 \mod 8$, 则存在正整数 k 使得 $p = 8k \pm 1$, 从而

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm k)} = 1.$$

若 $p \equiv \pm 3 \mod 8$, 则存在正整数 k 使得 $p = 8k \pm 3$, 从而

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2\pm 3k)+1} = -1.$$

例 3.3.10 判断同余方程 $x^2 \equiv 2 \mod 4088459$ 是否有解, 有解时求出其解数.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2\pm 3k)+1} = -1.$$

例 3.3.10 判断同余方程 $x^2 \equiv 2 \mod 4088459$ 是否有解, 有解时求出其解数.

解：$4088459 = 2017 \cdot 2027$ 不是素数, 原同余方程等价于

$$\begin{cases} x^2 \equiv 2 \mod 2017, \\ x^2 \equiv 2 \mod 2027. \end{cases}$$

因为 $\left(\frac{2}{2027}\right) = (-1)^{\frac{2027^2-1}{8}} = -1$, 所以同余方程组无解.

故原同余方程无解.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2\pm 3k)+1} = -1.$$

例 3.3.10 判断同余方程 $x^2 \equiv 2 \mod 4088459$ 是否有解, 有解时求出其解数.

解：$4088459 = 2017 \cdot 2027$ 不是素数, 原同余方程等价于

$$\begin{cases} x^2 \equiv 2 \mod 2017, \\ x^2 \equiv 2 \mod 2027. \end{cases}$$

因为 $\left(\frac{2}{2027}\right) = (-1)^{\frac{2027^2-1}{8}} = -1$, 所以同余方程组无解.

故原同余方程无解.

注：对于模 m 不是素数的情形, 无法直接通过计算勒让得符号判断是否是模 m 平方剩余, 可以转化成等价的模素数的同余方程组并利用中国剩余定理进行判断. 另外, 后续将引入新的概念——雅可比符号 (第 3.3.3 节), 可对模 m 平方非剩余进行判断.

为进一步简化二次剩余判别问题, 设 p, q 为不同的奇素数, 下面给出二次同余方程 $x^2 \equiv q \mod p$ 与 $x^2 \equiv p \mod q$ 之间的联系. 同时, 基于勒让得符号的函数性质、二次互反律以及欧几里德除法, 可以将模数较大的二次剩余判别问题转为模数较小的二次剩余判别问题, 并最后归结为较少的几个情况, 从而通过快速计算判判断 a 是否为模 p 平方剩余.

为进一步简化二次剩余判别问题, 设 p, q 为不同的奇素数, 下面给出二次同余方程 $x^2 \equiv q \mod p$ 与 $x^2 \equiv p \mod q$ 之间的联系. 同时, 基于勒让得符号的函数性质、二次互反律以及欧几里德除法, 可以将模数较大的二次剩余判别问题转为模数较小的二次剩余判别问题, 并最后归结为较少的几个情况, 从而通过快速计算判判断 a 是否为模 p 平方剩余.

定理 3.3.7 (二次互反律)

若 p, q 是互素的奇素数, 则

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

为进一步简化二次剩余判别问题, 设 p, q 为不同的奇素数, 下面给出二次同余方程 $x^2 \equiv q \mod p$ 与 $x^2 \equiv p \mod q$ 之间的联系. 同时, 基于勒让得符号的函数性质、二次互反律以及欧几里德除法, 可以将模数较大的二次剩余判别问题转为模数较小的二次剩余判别问题, 并最后归结为较少的几个情况, 从而通过快速计算判判断 a 是否为模 p 平方剩余.

定理 3.3.7 (二次互反律)

若 p, q 是互素的奇素数, 则

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

相关背景

欧拉和勒让得都曾经提出过二次互反律的猜想, 但第一个给出严格证明的是高斯于 1796 年做出的, 随后他又发现了另外 7 个不同的证明. 在《算数研究》和相关论文中, 高斯称其为“基石”, 并私下誉其为算术理论中的宝石, 是一个黄金定律.

之后, 雅可比、柯西、刘维尔、克罗内克、弗洛贝尼乌斯等也相继给出了新的证明. 至今, 二次互反律已有超过两百个不同的证明.

证：要证明

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

证：要证明

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

因为 $(2,pq)=1$, 根据定理 3.3.6, 有

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

其中 $T(q,p)=\sum\limits_{h=1}^{\frac{p-1}{2}}\left[\frac{q\cdot h}{p}\right]$, $T(p,q)=\sum\limits_{k=1}^{\frac{q-1}{2}}\left[\frac{p\cdot h}{q}\right]$, 所以只需要证明

$$T(q,p)+T(p,q)=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

事实上, 考察长为 $\frac{p}{2}$, 宽为 $\frac{q}{2}$ 的长方形内的整点个数, 如图 3.2 所示.

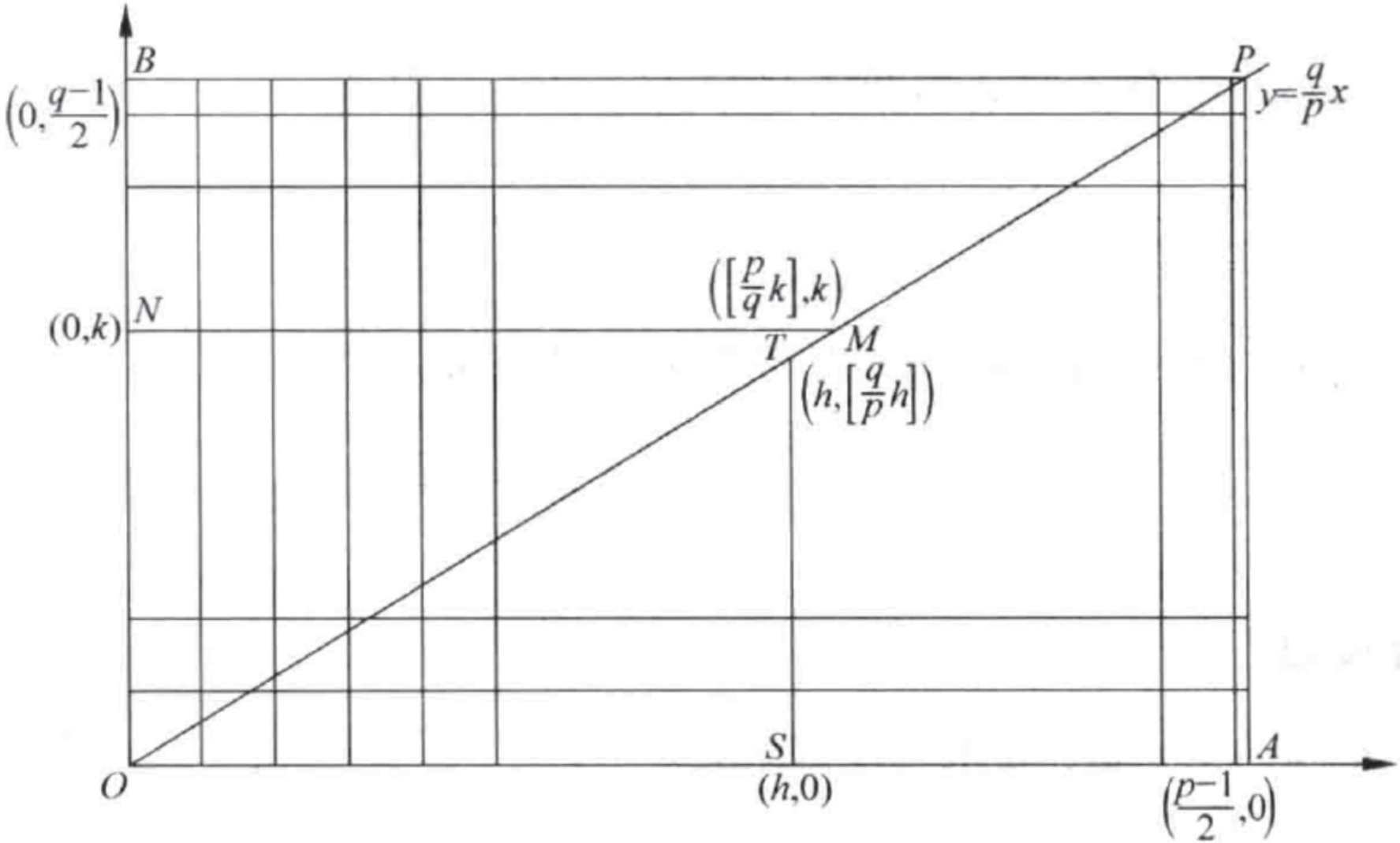
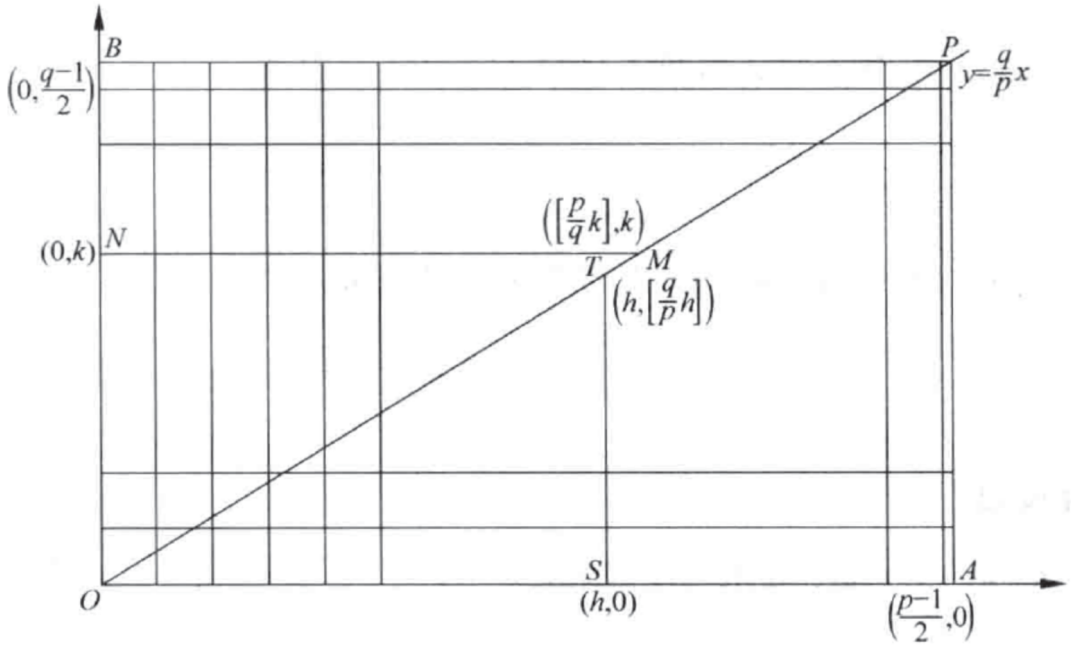
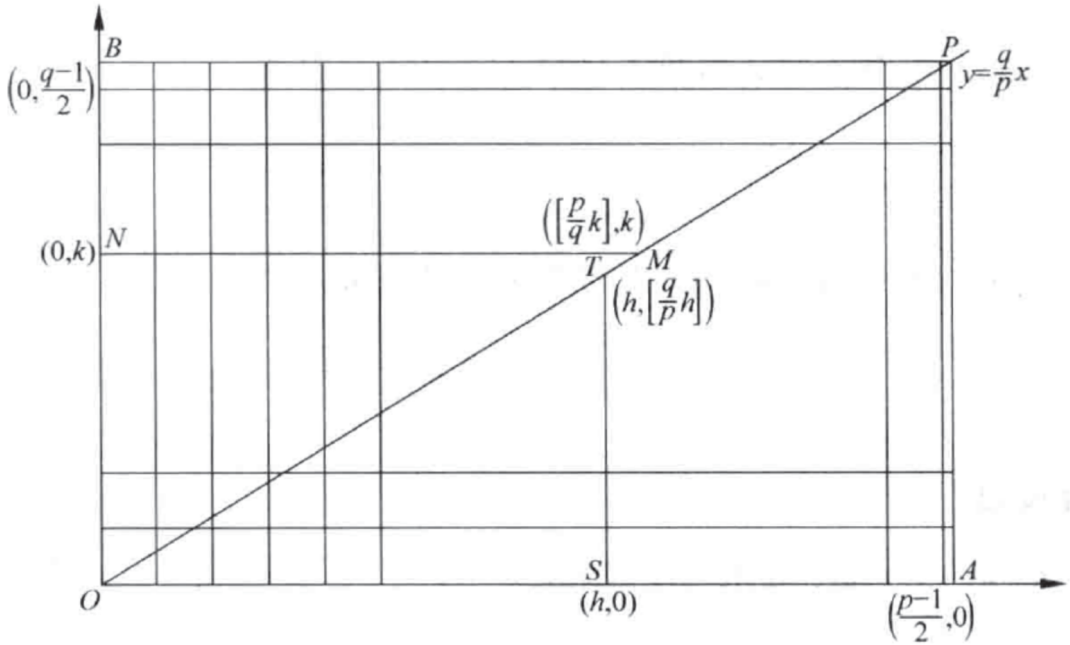


图 3.2 二次互反律的证明


B
$\left(0,\frac{q-1}{2}\right)$
P
$y=\frac{q}{p}x$
$\left(\left[\frac{p}{q}k\right],k\right)$
N
$(0,k)$
T
M
$\left(h,\left[\frac{q}{p}h\right]\right)$
S
A
O
$(h,0)$
$\left(\frac{p-1}{2},0\right)$



垂直直线 ST 上整点个数为 $\left[\frac{q\cdot h}{p}\right]$, 故下三角形内的整点个数为 $T(q,p)$;

垂直直线 NM 上整点个数为 $\left[\frac{p\cdot k}{q}\right]$, 故上三角形内的整点个数为 $T(p,q)$.

而对角线 OP 上无整点, 所以长方形内的整点个数为

$$T(q,p)+T(p,q)=\frac{p-1}{2}\cdot\frac{q-1}{2}.$$

例 3.3.11 证明 2 是模 17 平方剩余, 3 是模 17 平方非剩余.

例 3.3.11 证明 2 是模 17 平方剩余, 3 是模 17 平方非剩余.

证：根据定理 3.3.6, 有

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{2\cdot 18} = 1.$$

因此, 2 是模 17 平方剩余.

例 3.3.11 证明 2 是模 17 平方剩余, 3 是模 17 平方非剩余.

证：根据定理 3.3.6, 有

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{2\cdot 18} = 1.$$

因此, 2 是模 17 平方剩余.

根据二次互反律 (定理 3.3.7),

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

又根据定理 3.3.5,

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

例 3.3.11 证明 2 是模 17 平方剩余, 3 是模 17 平方非剩余.

证：根据定理 3.3.6, 有

$$\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{2\cdot 18} = 1.$$

因此, 2 是模 17 平方剩余.

根据二次互反律 (定理 3.3.7),

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

又根据定理 3.3.5,

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

则有, $\left(\frac{3}{17}\right) = -1$.

因此, 3 是模 17 的平方非剩余.

例 3.3.12 判断同余方程 $x^2 \equiv 1037 \mod 2027$ 是否有解?

例 3.3.12 判断同余方程 $x^2 \equiv 1037 \mod 2027$ 是否有解?

解：根据二次互反律（定理 3.3.7），

$$\left(\frac{1037}{2027}\right) = (-1)^{\frac{1037-1}{2}\cdot\frac{2027-1}{2}}\left(\frac{2027}{1037}\right)$$

根据定理 3.3.5,

$$\begin{aligned}\left(\frac{2027}{1037}\right) = \left(\frac{990}{1037}\right) &= \left(\frac{2}{1037}\right)\left(\frac{3^2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right)\\ &= \left(\frac{2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right).\end{aligned}$$

例 3.3.12 判断同余方程 $x^2 \equiv 1037 \mod 2027$ 是否有解?

解：根据二次互反律（定理 3.3.7），

$$\left(\frac{1037}{2027}\right) = (-1)^{\frac{1037-1}{2}\cdot\frac{2027-1}{2}}\left(\frac{2027}{1037}\right)$$

根据定理 3.3.5,

$$\begin{aligned}\left(\frac{2027}{1037}\right) = \left(\frac{990}{1037}\right) &= \left(\frac{2}{1037}\right)\left(\frac{3^2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right)\\ &= \left(\frac{2}{1037}\right)\left(\frac{5}{1037}\right)\left(\frac{11}{1037}\right).\end{aligned}$$

由定理 3.3.6, 我们有

$$\left(\frac{2}{1037}\right) = (-1)^{\frac{1037^2-1}{8}} = (-1)^{\frac{1038\cdot 1036}{8}} = -1.$$

又有

$$\left(\frac{5}{1037}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

$$\left(\frac{11}{1037}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right) = \left(\frac{3}{11}\right)$$

$$= (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

又有

$$\left(\frac{5}{1037}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

$$\left(\frac{11}{1037}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right) = \left(\frac{3}{11}\right)$$

$$= (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

因此, $\left(\frac{1037}{2027}\right) = 1$.

故同余方程 $x^2 \equiv 1037 \mod 2027$ 有解, 且有二解.

又有

$$\left(\frac{5}{1037}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

$$\left(\frac{11}{1037}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right) = \left(\frac{3}{11}\right)$$

$$= (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

因此, $\left(\frac{1037}{2027}\right) = 1$.

故同余方程 $x^2 \equiv 1037 \mod 2027$ 有解, 且有二解.

例 3.3.13 求所有奇素数 p, 它以 3 为其二次剩余.

又有

$$\left(\frac{5}{1037}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

$$\left(\frac{11}{1037}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right) = \left(\frac{3}{11}\right)$$

$$= (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

因此, $\left(\frac{1037}{2027}\right) = 1$.

故同余方程 $x^2 \equiv 1037 \mod 2027$ 有解, 且有二解.

例 3.3.13　求所有奇素数 p, 它以 3 为其二次剩余.

解：即要求所有奇素数 p, 使得 $\left(\frac{3}{p}\right) = 1$.

又有

$$\left(\frac{5}{1037}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

$$\left(\frac{11}{1037}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{1037-1}{2}}\left(\frac{1037}{11}\right) = \left(\frac{3}{11}\right)$$

$$= (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}}\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = 1.$$

因此, $\left(\frac{1037}{2027}\right) = 1$.

故同余方程 $x^2 \equiv 1037 \mod 2027$ 有解, 且有二解.

例 3.3.13　求所有奇素数 p, 它以 3 为其二次剩余.

解：即要求所有奇素数 p, 使得 $\left(\frac{3}{p}\right) = 1$.

易知, p 是大于 3 的奇素数. 根据二次互反律,

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

因为

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{当 } p \equiv 1 \mod 4 \text{ 时;} \\ -1, & \text{当 } p \equiv -1 \mod 4 \text{ 时.} \end{cases}$$

以及

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1, & \text{当 } p \equiv 1 \mod 6 \text{ 时;} \\ \left(\frac{-1}{3}\right) = -1, & \text{当 } p \equiv -1 \mod 6 \text{ 时.} \end{cases}$$

所以, $\left(\frac{3}{p}\right) = 1$ 的充要条件是

$$\begin{cases} p \equiv 1 \mod 4 \\ p \equiv 1 \mod 6 \end{cases} \text{ 或 } \begin{cases} p \equiv -1 \mod 4 \\ p \equiv -1 \mod 6 \end{cases}$$

这分别等价于

$$p \equiv 1 \mod 12 \text{ 或 } p \equiv -1 \mod 12.$$

因此, 3 是模 p 二次剩余的充要条件是

$$p \equiv \pm 1 \mod 12.$$

本课作业

1. 求出 $p = 5$ 的平方剩余和平方非剩余.
2. 计算 $\left(\frac{13}{89}\right)$.
3. 判断同余方程 $11x^2 \equiv -6 \mod 91$ 是否有解.
4. 求同余方程 $x^2 \equiv 17 \mod 37$ 的解数.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn