2022-2023学年秋季学期

课程名称: 信息安全数学基础

英文名称: Mathematical Foundations for Information Security

授课团队：胡磊、许军、王丽萍、王鹏

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 5 次课] 二次同余式与平方剩余

授课教师：胡磊

授课时间：2022年9月28日

概 要

- 一般二次同余式
- 平方剩余与平方非剩余
- 勒让德符号
- 二次互反律的证明
- 雅可比符号
- 开平方根算法

一般二次同余式

二次同余式的一般形式是 $ax^2+bx+c\equiv 0 \pmod m$ (1)

$$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$$

$$ax^2+bx+c\equiv 0 \pmod m \Leftrightarrow \begin{cases} ax^2+bx+c\equiv 0 \pmod{p_1^{\alpha_1}} \\ \cdots\cdots \\ ax^2+bx+c\equiv 0 \pmod{p_k^{\alpha_k}} \end{cases}$$

故只需讨论模为 p^α 同余式： $ax^2+bx+c\equiv 0 \pmod{p^\alpha}$, (2)

p=2的情形：2进制幂级数方法

讨论模为 p^α 同余式： $ax^2+bx+c\equiv 0 \pmod{p^\alpha}$, (2)

p为奇素数的情形：幂级数方法

当p整除a的时候：幂级数方法

当p不整除a的时候：幂级数方法：起始步骤：模p开平方

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{p^\alpha} \qquad (2ax+b)^2\equiv b^2-4ac \pmod{p^\alpha}$$

$$y=2ax+b \qquad y^2\equiv b^2-4ac \pmod{p^\alpha}$$

特别地，当 p 是奇素数时， $(p,2a)=1$. 上述同余式等价于 (2).

Rabin体制

- N=pq 是RSA模数。加密：将消息适当填充，填充后作运算：

$$c = m^2 \pmod{n}$$

- 解密：用CRT，化成模p和模q，分别开平方，由填充规则确定是哪一个平方根。
- 不知道p和q无法开平方。

模 p 开平方的问题

定义 1 若同余式 $x^2 \equiv a \pmod{m}, \quad (a,m)=1 \quad (3)$ 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 1 1 是模 4 平方剩余， -1 是模 4 平方非剩余.

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

因为 $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1 \pmod{7}$.

模p既约剩余系中有一半的元素为平方元

定理 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 $(p-1)/2$, 且 $(p-1)/2$ 个平方剩余与序列:

$1^2,\ 2^2,\ \ldots,\ (\frac{p-1}{2})^2$ (4) 中的一个数同余，且仅与一个数同余.

证 由定理 1, 平方剩余的个数等于同余式 $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 的解数.

但 $x^{\frac{p-1}{2}} - 1 | x^{p-1} - 1$. 此同余式的解数是 $\frac{p-1}{2}$,

故平方剩余的个数是 $\frac{p-1}{2}$, 而平方非剩余个数是 $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$.

再证明定理的第二部分： 若有两个数模 p 同余,

即存在 $k_1 \neq k_2$ 使得 $k_1^2 \equiv k_2^2 \pmod{p}$, $(k_1 + k_2)(k_1 - k_2) \equiv 0 \pmod{p}$

因此， $p | k_1 + k_2$ 或 $p | k_1 - k_2$. 但 $1 \leq k_1,\ k_2 \leq (p-1)/2$,

$$2 \leq k_1 + k_2 \leq p - 1 < p, \quad |k_1 - k_2| \leq p - 1 < p.$$

从而， $k_1 = k_2$. 矛盾.

椭圆曲线点的嵌入和点的个数

例 4 求满足方程 $E: y^2 = x^3 + x + 1 \pmod 7$ 的所有点.

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

$x = 0,\ y^2 = 1 \pmod 7, \quad y = 1,\ 6 \pmod 7,$

$x = 1,\ y^2 = 3 \pmod 7, \quad$ 无解,

$x = 2,\ y^2 = 4 \pmod 7, \quad y = 2,\ 5 \pmod 7,$

$x = 3,\ y^2 = 3 \pmod 7, \quad$ 无解,

$x = 4,\ y^2 = 6 \pmod 7, \quad$ 无解,

$x = 5,\ y^2 = 5 \pmod 7, \quad$ 无解,

$x = 6,\ y^2 = 6 \pmod 7, \quad$ 无解.

模为奇素数的平方剩余与平方非剩余

讨论模为素数 p 的二次同余式 $x^2 \equiv a \pmod{p}, \quad (a,p)=1.$

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

(ii) a 是模 p 的平方非剩余 $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

并且当 a 是模 p 的平方剩余时, 同余式 (1) 恰有二解.

证：(i) => 由欧拉定理， $a^{(p-1)/2} = x^{p-1} = 1 \pmod{p}$

<= (p-1)/2

等于模p平方剩余的个数

小于等于方程 $x^{(p-1)/2} = 1 \pmod{p}$的解数

小于等于方程的次数(p-1)/2

所以，全部取等号，模p平方剩余的集合等于方程 $x^{(p-1)/2} = 1 \pmod{p}$的解集合

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

(ii) a 是模 p 的平方非剩余 $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

并且当 a 是模 p 的平方剩余时，同余式 (1) 恰有二解.

证 (ii) 因为 p 是奇素数，$(a,p)=1$, 根据欧拉定理，有

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

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

a 是模 p 的平方非剩余的充要条件是 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

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

(ii) a 是模 p 的平方非剩余 $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

并且当 a 是模 p 的平方剩余时，同余式 (1) 恰有二解.

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

(i) 若 a_1, a_2 是模 p 的平方剩余，则 a_1a_2 是模 p 的平方剩余;

(ii) 若 a_1, a_2 是模 p 的平方非剩余，则 a_1a_2 是模 p 的平方剩余;

(iii) 如 a_1 是模 p 平方剩余，a_2 模 p 平方非剩余，则 a_1a_2 是模 p 的平方非剩余.

证 因为 $(a_1a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}}$

所以由定理 1 即得结论.

例 1 判断 137 是否为模 227 平方剩余.

解 根据定理 1, 我们要计算： $137^{(227-1)/2} = 137^{113} \pmod{227}$.

运用模重复平方法.

$$\mathbf{137^{(227-1)/2} = 137^{113} = -1 (mod\ 227)}$$

因此， 137 为模 227 平方非剩余.

勒让德符号

定义 1 设 p 是素数. 定义 **勒让得 (Legendre) 符号** 如下:

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

定理 1 (欧拉判别法则) 对任意整数 a, $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$.

推论 1 设 p 是奇素数, 则 (1) $\left(\frac{1}{p}\right)=1$; (2) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

推论 2 设 p 是奇素数, 那么 $\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{若 } p\equiv 1 \pmod 4;\\ -1, & \text{若 } p\equiv 3 \pmod 4.\end{cases}$

证 若 $p\equiv 1 \pmod 4$, 则 $p=4k+1$, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1$.

$p\equiv 3 \pmod 4$, 则 $p=4k+3$, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=(-1)^{2k+1}=-1$.

定理 2 设 p 是奇素数，则 (i) $\left(\dfrac{a+p}{p}\right)=\left(\dfrac{a}{p}\right)$;

(ii) $\left(\dfrac{ab}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$; (iii) 设 $(a,p)=1$, 则 $\left(\dfrac{a^2}{p}\right)=1$.

证 (i) $x^2\equiv a+p \pmod p$ $\Leftrightarrow$ $x^2\equiv a \pmod p$

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

(ii) 根据欧拉判别法则,

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

因为勒让得符号取值 ±1, 且 p 是奇素数，所以有 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

推论 设 p 是奇素数. 若 $a\equiv b \pmod p$, 则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

证 根据定理2的(i)即得。

引理 (Gauss) 设 p 奇素数. $(a,p)=1$. 若 $a\cdot 1,\ a\cdot 2,\ \ldots,\ a\cdot\dfrac{p-1}{2}$ 中模 p 的最小正剩余大于 $\dfrac{p}{2}$ 的个数是 m, 则 $\left(\dfrac{a}{p}\right)=(-1)^m$.

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

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

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

否则, $ak_i\equiv p-ak_j$, 或 $ak_i+ak_j\equiv 0\ (\mathrm{mod}\ p)$.

因而 $k_i+k_j\equiv 0\,(\mathrm{mod}\,p)$, 这不可能, 因为 $1\le k_i+k_j\le\dfrac{p-1}{2}+\dfrac{p-1}{2}<p$.

这样, $a_1,\ \ldots,\ a_t,\ p-b_1,\ \ldots,\ p-b_m$ 是 $1,\ldots,\dfrac{p-1}{2}$ 的一个排列,

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

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

定理 3 (i) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$. (ii) 若 $(a,2p)=1$, 则 $\left(\frac{a}{p}\right)=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{ak}{p}\right]}$.

证: 因 $ak=p\left[\frac{ak}{p}\right]+r_k,\quad 0<r_k<p$, 对 $k=1,\ \ldots,\ \frac{p-1}{2}$ 求和,

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

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

若 $a=2$, 则 $0\le[\frac{ak}{p}]\le[\frac{p-1}{p}]=0$, 因而 $m\equiv\frac{p^2-1}{8}\pmod 2$;

若 a 为奇数, 则 $m\equiv\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ak}{p}\right]\pmod 2$.

定理 3 (i) $\left(\dfrac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$. (ii) 若 $(a,2p)=1$, 则 $\left(\dfrac{a}{p}\right)=(-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{ak}{p}\right]}$.

推论 设 p 是奇素数，那么

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

证 根据定理 3 (i), 我们有

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

若 $p\equiv\pm1 \pmod 8$, 则存在正整数 k 使得 $p=8k\pm1$. 从而

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

若 $p\equiv\pm3 \pmod 8$, 则存在正整数 k 使得 $p=8k\pm3$. 从而

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=(-1)^{2(4k^2\pm3k)+1}=-1.$$

定理 4 (二次互反律) 若 p, q 是互素奇素数，则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \qquad (9)$$

例 3 2 是模 17 平方剩余； 3 是模 17 平方非剩余.

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

因此， 2 是模 17 平方剩余.

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

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

因此， $\left(\frac{3}{17}\right) = -1$, 3 是模 17 平方非剩余.

例 4 判断同余式 $x^2 \equiv 137 \pmod{227}$ 是否有解.

解 因为 227 是素数,

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

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

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

因此, $\left(\frac{137}{227}\right) = -1$. 同余式 $x^2 \equiv 137 \pmod{227}$ 无解.

例 5 判断 $x^2 \equiv -1 \pmod{365}$ 是否有解，有解时，求出其解数.

解 $365 = 5 \cdot 73$ 不是素数，原同余式等价于：

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

因为 $\left(\frac{-1}{5}\right) = \left(\frac{-1}{73}\right) = 1$, 故同余式组有解. 原同余式有解，解数为 4.

例 6 判断 $x^2 \equiv 2 \pmod{3599}$ 是否有解，有解时求出其解数.

解 $3599 = 59 \cdot 61$ 不是素数，原同余式等价于：

$$\begin{cases} x^2 \equiv 2 \pmod{59}, \\ x^2 \equiv 2 \pmod{61}. \end{cases}$$

因为 $\left(\frac{2}{59}\right) = (-1)^{(59^2-1)/8} = -1$, 故同余式组无解. 原同余式无解.

定理 3 (i) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. (ii) 若 $(a, 2p) = 1$, 则 $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2}\left[\frac{ak}{p}\right]}$.

推论 设 p 是奇素数，那么

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

定理 4 (二次互反律) 若 p, q 是互素奇素数，则

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \qquad (9)$$

例 1 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 $\left(\frac{3}{p}\right)=1$.

根据二次互反律, $\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$.

$$(-1)^{(p-1)/2}=\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4;\\ -1, & \text{当 } p\equiv -1 \pmod 4,\end{cases}$$ 以及 $$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1, & \text{当 } p\equiv 1 \pmod 6;\\ \left(\frac{-1}{3}\right)=-1, & \text{当 } p\equiv -1 \pmod 6\end{cases}$$

故 $\left(\frac{3}{p}\right)=1 \Leftrightarrow \begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 6\end{cases}$ 或 $\begin{cases}p\equiv -1 \pmod 4\\ p\equiv -1 \pmod 6\end{cases}$

这分别等价于 $p\equiv 1 \pmod{12}$, 或 $p\equiv -1 \pmod{12}$.

因此, 3 是模 p 二次剩余的充分必要条件是 $p\equiv \pm 1 \pmod{12}$.

雅可比符号

定义 1 设 $m = p_1 \cdots p_r$ 是奇素数 p_i 的乘积. 对任意整数 a, 定义 **雅可比 (Jacobi) 符号** 为

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

雅可比符号形式上是勒让得符号的推广, 但所蕴含的意义已经不同. 雅可比符号为 -1, 可判断 a 是模 m 平方非剩余; 但雅可比符号为 1, 却不能判断 a 是模 m 平方剩余. 例如, 3 是模 119 平方非剩余, 但

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

定理 1 设 m 是正奇数. 则 (i) $\left(\dfrac{a+m}{m}\right)=\left(\dfrac{a}{m}\right)$;

(ii) $\left(\dfrac{ab}{m}\right)=\left(\dfrac{a}{m}\right)\left(\dfrac{b}{m}\right)$; (iii) 设 $(a,m)=1$, 则 $\left(\dfrac{a^2}{m}\right)=1$.

证 设 $m=p_1\cdots p_r$, 其中 p_i 为奇素数. 根据定义,

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

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

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

引理: 设 $m = p_1 \cdots p_r$ 是奇数. 则

$$\frac{m-1}{2} \equiv \frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \pmod 2;$$

$$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} \pmod 2.$$

证

$$m \equiv (1+2\cdot\frac{p_1-1}{2})\cdots(1+2\cdot\frac{p_r-1}{2}) \equiv 1+2\cdot\left(\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}\right) \pmod 4;$$

$$m^2 \equiv (1+8\cdot\frac{p_1^2-1}{8})\cdots(1+8\cdot\frac{p_r^2-1}{8}) \equiv 1+8\cdot\left(\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}\right) \pmod{16}.$$

所以引理成立. 证毕.

定理 2 设 m 是奇数. 则 (i) $\left(\frac{1}{m}\right)=1$;

(ii) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$; (iii) $\left(\frac{2}{m}\right)\equiv(-1)^{\frac{m^2-1}{8}}$;

证 因为 $m=p_1\cdots p_r$ 是奇数，其中 p_i 是奇素数.

(i) $\left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_r}\right)=1.$

(ii) $\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}=(-1)^{\frac{m-1}{2}}.$

(iii) $\left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)\cdots\left(\frac{2}{p_r}\right)=(-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}}=(-1)^{\frac{m^2-1}{8}}.$

定理 3 设 m, n 都是奇数. 则 $\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right)$.

证 设 $m = p_1 \cdots p_r,\ \ n = q_1 \cdots q_s$.

如果 $(m, n) > 1$, 则 $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0$. 结论成立.

因此, 可设 $(m, n) = 1$.

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{n}{p_i}\right)\prod_{j=1}^{s}\left(\frac{m}{q_j}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\Sigma_{i=1}^{r}\Sigma_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

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

因此, 定理成立. 证毕.

例 1 判断同余式

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

是否有解.

解 不用考虑 563 是否为素数，直接计算雅可比符号.

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

所以原同余式无解.

没有多项式的二次互反律：

没有类似绝对值最小的剩余系：b换成p-b

分数取整，直角坐标系中坐标为分数的点

开平方根算法

设 p 为奇素数. 对任意给定的整数 a, 应用高斯二次互反律 (§4.3 定理 4) 可以快速地判断 a 是否为模 p 平方剩余, 即二次同余式

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

是否有解, 也就是说解的存在性.

现在在有解的情况下, 即 a 满足

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

的情况下, 考虑二次同余式的具体求解.

n阶循环群上开平方算法

△ 当 n 是奇数时，设 $G=\{g, g^2, \cdots, g^{n-1}, g^n=1\}$，对 $\forall 0\le i\le n-1$，令 $2i'\equiv i \pmod n$，即 $i'=\begin{cases}\frac{i}{2} & i\text{偶}\\ \frac{i+n}{2} & i\text{奇}\end{cases}$，则 $g^{i'}=(g^{i'})^2$，而 $g^{i'}=(g^i)^{\frac{n+1}{2}}$

每一个元素的平方根 $g^{i'}$ 存在。例：$F_{2^m}^*$（特征2的有限域）

△ 当 n 是偶数时，设 $n=2m$，g^i 是平方元 $\Leftrightarrow$ i 是偶数。

设 G 是某个乘法无零因子的环的乘法群的子群，由 $(g^m+1)(g^m-1)=g^{2m}-1=0$，知 $g^m=-1$。有 g^i 是平方元 $\Leftrightarrow (g^i)^m=1$

算法想法：

试图寻找奇数 k，使 $a^k=1$，则 $\left(\pm a^{\frac{k+1}{2}}\right)^2=a$。但不一定存在如此的 k。

放宽，寻找奇数 k，偶数 2^l，元素 $B\in G$，s.t. $B^{2^l}a^k=1$，则 $\left(\pm B^{\frac{l}{2}}a^{\frac{k+1}{2}}\right)^2=a$。

算法实现：设 $n=2^s t$，$s\ge 1$，t 为奇数。取 $b\in G$，$b^{\frac{n}{2}}=-1$。令 $B=b^t$，$A=a^t$。

已知 $B^{2^{s-1}}=b^{2^{s-1}t}=b^{\frac{n}{2}}=-1$，$C_1:=A^{2^{s-1}}=a^{2^{s-1}t}=a^{\frac{n}{2}}=1$（设 a 是平方元）。

△ 若 $s=1$，OK.

△ 若 $s\ge 2$，计算 $C_2=A^{2^{s-2}}$，它等于1或-1（因为它的平方 $=a^{2^{s-1}}=1$）。令

$$l_1=\begin{cases}0 & \text{若 } A^{2^{s-2}}=1\\ 1 & \text{若 } A^{2^{s-2}}=-1\end{cases}$$

则 $B^{2^{s-1}l_1}A^{2^{s-2}}=\left(B^{2^{s-1}}\right)^{l_1}\cdot A^{2^{s-2}}=(-1)^{l_1}\cdot A^{2^{s-2}}=1$

若 $s=2$，OK.

△ 若 $s\ge 3$，$B^{2^{s-1}l_1}A^{2^{s-2}}$ 中的所有指数为偶数，且 B 的指数含2的幂次比 A 高1，

计算 $C_3=B^{2^{s-2}l_1}A^{2^{s-3}}$，则 $C_3=1$ 或 -1。令

$$l_2=\begin{cases}0 & C_3=1\\ 1 & C_3=-1\end{cases}$$

则 $B^{2^{s-1}l_2}\cdot B^{2^{s-2}l_1}A^{2^{s-3}}=(-1)^{l_2}\cdot C_3=1$

若 $s=3$，OK.

△ 若 $s\ge 4$，$B^{2^{s-1}l_2+2^{s-2}l_1}A^{2^{s-3}}$ 中的所有指数为偶，且 B 的指数的2幂次比 A 高。

继续上述实现，直至 A 的指数为奇数。

注：对 $G=\mathbb{F}_p^*$，$s=1\Leftrightarrow p\equiv 3 \pmod 4$，算法迭代一步。

例 1 应用上述算法求解同余式 $x^2 \equiv 186 \pmod{401}$.

解 因为 $a = 186 = 2 \cdot 3 \cdot 31$

$$\left(\frac{2}{401}\right) = (-1)^{(401^2-1)/8} = 1, \qquad \left(\frac{3}{401}\right) = (-1)^{\frac{3-1}{2}\frac{401-1}{2}} \left(\frac{401}{3}\right) = \left(\frac{-1}{3}\right) = -1$$

$$\left(\frac{31}{401}\right) = (-1)^{\frac{31-1}{2}\frac{401-1}{2}} \left(\frac{401}{31}\right) = \left(\frac{-2}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right) = (-1)^{\frac{31-1}{2}}(-1)^{\frac{31^2-1}{8}} = -1$$

所以 $\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right)\left(\frac{3}{401}\right)\left(\frac{31}{401}\right) = 1 \cdot (-1) \cdot (-1) = 1.$

故原同余式有解.

$p=401 \quad p-1=400=2^4\cdot 25$

模p平方元 $a=186$，模p非平方元 $b=3$

$A=a^{25}\equiv 98 \pmod p$，$B=b^{25}\equiv 268 \pmod p$

依次计算 $A^2\equiv 381$，$A^4\equiv -1$

$B^2\equiv 45$，$B^4\equiv 20$，$B^8\equiv -1$

因为 $A^4\equiv -1\equiv B^8$，所以

$$A^4B^8=1$$

计算 $A^2B^4\equiv 381\cdot 20\equiv 1$

计算 $AB^2\equiv 98\cdot 45\equiv -1$，所以

$$AB^2\cdot B^8\equiv 1$$

故 $$(a^{13}B^5)^2\equiv a$$

计算 $a^{13}B^5\equiv 98^{13}\cdot 268^5\equiv 304 \pmod p$

例 2 设 p 是形为 $4k+3$ 的素数. 如果 $x^2 \equiv a \pmod{p}$ 有解, 则其解是 $x \equiv \pm a^{(p+1)/4} \pmod{p}$.

解 因为 p 是形为 $4k+3$ 的素数, 所以存在奇数 q 使得 $p-1=2q$.

如果 $x^2 \equiv a \pmod{p}$ 有解, 则 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$,

或者 $a^q \equiv 1 \pmod{p}$

两端同时乘以 a, 得到

$$a^{q+1} \equiv a \pmod{p}.$$

因此, 同余式的解为

$$x \equiv \pm a^{\frac{q+1}{2}} \equiv \pm a^{(p+1)/4} \pmod{p}.$$

例 3 设 $p,\ q$ 是形为 $4k+3$ 的不同素数. 如果整数 a 满足 $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$, 求解同余式 $x^2\equiv a\ (\mathrm{mod}\ pq)$.

解 因为 $x^2\equiv a\ (\mathrm{mod}\ pq)$ 等价于同余式组 $\begin{cases} x^2\equiv a\ \ (\mathrm{mod}\ p) \\ x^2\equiv a\ \ (\mathrm{mod}\ q), \end{cases}$

而同余式 $x^2\equiv a\ (\mathrm{mod}\ p)$ 的解为 $x\equiv\pm a^{(p+1)/4}\ (\mathrm{mod}\ p)$,

同余式 $x^2\equiv a\ (\mathrm{mod}\ q)$ 的解为 $x\equiv\pm a^{(q+1)/4}\ (\mathrm{mod}\ q)$,

原同余式的解为

$$x\equiv\pm(a^{\frac{p+1}{4}}\ (\mathrm{mod}\ p))uq\pm(a^{\frac{q+1}{4}}\ (\mathrm{mod}\ q))vp\ (\mathrm{mod}\ pq)$$

其中整数 $u,\ v$ 分别满足

$$uq\equiv 1\ (\mathrm{mod}\ p),\quad vp\equiv 1\ (\mathrm{mod}\ q).$$