

初等数论

第四章 二次剩余

卢伟

Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院

1. 模为素数的二次同余方程一解的存在性

下面考虑模为素数的二次同余方程：

$$ay^2 + by + c \equiv 0 \pmod{p}$$

其中 $p \nmid a$.

如果 p 为 2 的话，很容易验证这个方程是否有解(将 0 和 1 直接代入检查是否成立即可)，所以我们下面讨论时都假设 $p > 2$.

$p \nmid a \implies p \nmid 4a$ ，所以上述二次同余方程和

$$ay^2 + by + c \equiv 0 \pmod{p}$$

等价(即解相同)，而此式也就是：

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

这样，我们就一般考虑形如：

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

的同余方程.

设素数 $p > 2$ ，如果 $x^2 \equiv a \pmod{p}$ 有解，则称 a 是一个模 p 的平方剩余(二次剩余). 否则，称 a 是一个模 p 的平方非剩余(二次非剩余).

比如, $1^2 \equiv 1 \pmod{3}$, 所以1是模3的平方剩余

0,1,2都不能使得 $x^2 \equiv -1 \pmod{3}$ 成立, 所以-1是一个模3的平方非剩余

$2^2 \equiv 4 \pmod{7}$, 所以4是模7的平方剩余

$4^2 \equiv 2 \pmod{7}$, 所以2是模7的平方剩余

0,1,2,3,4,5,6 均不能使得 $x^2 \equiv 5 \pmod{7}$ 成立, 所以5是模7的平方非剩余.

对方程 $x^2 \equiv a \pmod{p}$, 如果 $p|a$, 假设这个方程有解 x_0 的话, 即 $p|(x_0^2 - a)$, 就有 $p|x_0^2$, 从而 $p|x_0$;

因为否则的话, 就是 $(p, x_0) = 1$, 假设 $x_0 = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, 从而 $p \neq p_i, i = 1, 2, \cdots, s$, 并且 $x_0^2 = p_1^{2a_1} p_2^{2a_2} \cdots p_s^{2a_s}$, 从而 $(p, x_0^2) = 1$,

也就是说如果 $p|a$, 则同余方程 $x^2 \equiv a \pmod{p}$ 只有唯一解 $x \equiv 0 \pmod{p}$. 所以我们下面讨论中都假设 $(a, p) = 1 : x^2 \equiv a \pmod{p}$

定理

在模 p 的一个简化剩余系中, 恰有 $\frac{p-1}{2}$ 个模 p 二次剩余, 恰有 $\frac{p-1}{2}$ 个模 p 二次非剩余; 如果 a 是模 p 二次剩余的话, $x^2 \equiv a \pmod{p}$ ($(a, p) = 1$) 的解数为2.

证明: 以简化剩余系 $\mathcal{A} = \{1, 2, 3, \dots, p-2, p-1\}$ 来考虑(其他简化剩余系类似), 我们要看看 a 从这个集合取值时, 其中有多少个是二次剩余.

而要看 a 取值后是否是二次剩余也就是看在模 p 的任意一个完全剩余系中是否有元素 x , 使得 $x^2 \equiv a \pmod{p}$ 成立, 我们只需要看完全剩余

系 $\mathcal{B} = \{-\frac{p-1}{2}, -\frac{p-1}{2} + 1, -\frac{p-1}{2} + 2, \dots, -1, 0, 1, 2, \dots, \frac{p-1}{2} - 1, \frac{p-1}{2}\}$ 即可, 这些数字中, 0肯定不是方程的解,

所以只需要考虑 $\mathcal{C} = \{-\frac{p-1}{2}, -\frac{p-1}{2} + 1, -\frac{p-1}{2} + 2, \dots, -1, 1, 2, \dots, \frac{p-1}{2} - 1, \frac{p-1}{2}\}$ 这些数即可.

j 从 \mathcal{C} 中任意取值都有 $(-j)^2 \equiv j^2 \pmod{p}$ (j^2 的值在模 p 意义下自然在集合 \mathcal{A} 内), 这样 a 是模 p 二次剩余当且仅当 $a \equiv 1^2 \pmod{p}$, 或 $a \equiv 2^2 \pmod{p}$, 或 $a \equiv 3^2 \pmod{p}$, \dots , 或 $a \equiv \frac{p-1}{2}^2 \pmod{p}$, 也就是说 \mathcal{A} 中有可能成为二次剩余的数至多是 $\frac{p-1}{2}$ 个, 如果这些平方的结果两两不同余, 就意味着 \mathcal{A} 中确实是二次剩余的数有 $\frac{p-1}{2}$ 个.

证明(续):

而当 $1 \leq i, j \leq \frac{p-1}{2} (i \neq j)$ 时, $i^2 \not\equiv j^2 \pmod{p}$ (否则 $p|(i-j)$ 或 $p|(i+j)$, 不可能), 所以这也就给出了模 p 的全部二次剩余, 一共 $\frac{p-1}{2}$ 个. 简化剩余系中剩下的 $\frac{p-1}{2}$ 个数也就是模 p 的二次非剩余了.

根据这个分析, 当 a 是模 p 的二次剩余时, 在 $1 \sim \frac{p-1}{2}$ 之间一定有一个且仅有一个 i 使得 $i^2 \equiv a \pmod{p}$ 成立.

这样 $x^2 \equiv a \pmod{p}$ 的解就是 $x \equiv \pm i \pmod{p}$, 解数为 2.



比如求 $p = 11$ 的二次剩余和二次非剩余:

$$\mathcal{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\mathcal{C} = \{1, 2, 3, 4, 5\}$$

| j | 1 | 2 | 3 | 4 | 5 |
|-------------------------|---|---|---|---|---|
| $d \equiv j^2 \pmod{p}$ | 1 | 4 | 9 | 5 | 3 |

所以, $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ 中 $1, 3, 4, 5, 9$ 是二次剩余, $2, 6, 7, 8, 10$ 是二次非剩余.

根据这个表还可以看出 $x^2 \equiv 9 \pmod{p}$ 的解是 $\pm 3 \pmod{11}$.

定理

a 是模 p 的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

a 是模 p 的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

证明：先说明 $\forall a, s.t., (a, p) = 1$, 则 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 与 $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ 有且只有一个成立：

这是因为我们有

$$(a, p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}$$

从而

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

即

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

这样要么

$$p \mid (a^{\frac{p-1}{2}} - 1) \quad (i.e., a^{\frac{p-1}{2}} \equiv 1 \pmod{p})$$

要么

$$p \mid (a^{\frac{p-1}{2}} + 1) \quad (i.e., a^{\frac{p-1}{2}} \equiv -1 \pmod{p})$$

证明(续1):

这就是说

$p|(a^{\frac{p-1}{2}} - 1)$ 和 $p|(a^{\frac{p-1}{2}} + 1)$ 至少有一个成立.

但二者不能同时成立, 这是因为: 设 t 为任意整数, 如果同时有 $p|(t-1), p|(t+1)$, 则有 $t = kp + 1 = k'p - 1$, 即有 $p|(k' - k) = 2$, 从而 $p|k' - k| = 2$, 但我们已经假设了 p 是 ≥ 3 的素数, 所以等式 $p|k' - k| = 2$ 不可能成立.

这样我们知道, 对于任意的 $a, p \nmid a: a^{\frac{p-1}{2}} \equiv -1 \pmod p$ 与 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ 有且仅有一个成立, 所以如果我们能够证明“ a 是模 p 的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$ ”, 那么自然有“ a 是模 p 的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod p$ ”

证明(续2):

先证明必要性" \implies ":

如果 a 是模 p 的二次剩余, 则必有 x_0 使得 $x_0^2 \equiv a \pmod{p}$ 成立, 因而有 $x_0^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$ 成立, 又

$$p \nmid a \implies p \nmid x_0$$

(否则就有 $p \mid x_0^2$)

$$p \nmid x_0 \implies x_0^{p-1} \equiv 1 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

下证充分性" \impliedby ":

如果 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 这时必有 $p \nmid a$, 否则 $p \mid a^{\frac{p-1}{2}}$. 从而 $(p, a) = 1$, 即 a 是模 p 的一个简化剩余.

任取整数 $c (\neq 0)$, $-\frac{p-1}{2} \leq c \leq \frac{p-1}{2}$, 考虑同余式 $cx \equiv a \pmod{p}$,

我们知道如果 x 遍历简化剩余

系 $\mathcal{A} = \{-\frac{p-1}{2}, -\frac{p-1}{2} + 1, -\frac{p-1}{2} + 2, \dots, -1, 1, 2, \dots, \frac{p-1}{2} - 1, \frac{p-1}{2}\}$, 则 cx 也会遍历模 p 的一个简化剩余系.

这就意味着在集合 \mathcal{A} 中存在唯一一个元素(记作 x_e)使得 $cx_e \equiv a \pmod{p}$.

证明(续3):

如果 a 不是二次剩余的话, 则有 $x_e \neq c$.

而 $c(\neq 0)$ 可以取 $-\frac{p-1}{2} \sim \frac{p-1}{2}$ 的任意数。这样可以

将 $\{-\frac{p-1}{2}, -\frac{p-1}{2} + 1, -\frac{p-1}{2} + 2, \dots, -1, 1, 2, \dots, \frac{p-1}{2} - 1, \frac{p-1}{2}\}$ 的 $p-1$ 个数按照 c, x_c 分为一对对, 每一对都满足 $cx_c \equiv a \pmod{p}$, 从而:

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

另外,

$$1 \equiv 1 \pmod{p}$$

$$2 \equiv 2 \pmod{p}$$

...

$$\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{p}$$

$$\frac{p-1}{2} + 1 \equiv -\frac{p-1}{2} \pmod{p}$$

$$\frac{p-1}{2} + 2 \equiv -\frac{p-3}{2} \pmod{p}$$

...

$$p-1 \equiv -1 \pmod{p}$$

证明(续4):

所以有:

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \left(-\frac{p-3}{2}\right) \cdots (-1) \pmod{p} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

由于已知条件

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

从而

$$(p-1)! \equiv 1 \pmod{p}$$

而由Wilson定理:

$$(p-1)! \equiv -1 \pmod{p},$$

所以 $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 与已知条件矛盾, 故 a 是模 p 的二次剩余. \diamond

这个结论被称为**欧拉判别条件**

示例：判别137是否是模227的二次剩余
根据欧拉判别条件，需要计算：

$$137^{\frac{227-1}{2}} \bmod 227$$

即 $137^{113} \bmod 227$

这可以通过模重复平方算法得出，最后可得：

$$137^{\frac{227-1}{2}} \equiv -1 \bmod 227$$

故137是模227的平方非剩余.

二次剩余小结

考虑模素数二次同余方程：

$$x^2 \equiv a \pmod{p} \quad ((a, p) = 1)$$

1. **定义：**二次(平方)剩余，二次(平方)非剩余
2. **定理：**在模 p 的一个简化剩余系中，恰有 $\frac{p-1}{2}$ 个模 p 二次剩余，恰有 $\frac{p-1}{2}$ 个模 p 二次非剩余；如果 a 是模 p 二次剩余的话， $x^2 \equiv a \pmod{p} \quad ((a, p) = 1)$ 的解数为2.
3. **欧拉判别条件：**
 a 是模 p 的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
 a 是模 p 的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

根据这个结论：

$a = -1$ 是模 p 二次剩余的充要条件是

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

左边数字的值只能是 ± 1 ，如果它为 -1 的话不可能与 1 同余，所以只可能为 1 才能同余，而要 $(-1)^{\frac{p-1}{2}} = 1$ ，等价于 $\frac{p-1}{2} = 2k$ ，等价于 $p = 4k + 1$ ，即 $p \equiv 1 \pmod{4}$ 。

即： $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

所以我们有： -1 是模 p 二次剩余的充要条件是 $p \equiv 1 \pmod{4}$ 。

比如同余方程 $x^2 \equiv -1 \pmod{61}$ 的解数为 2 ，这是因为 $p = 61$ 为素数，且 $61 = 4 \times 15 + 1$ ，所以 -1 是模 61 的二次剩余，即解数为 2 。

示例:

判断同余方程 $x^2 \equiv 16 \pmod{51}$ 的解数.

由于 $51 = 3 \times 17$, 同余方程

$$x^2 \equiv 16 \pmod{51} \quad (1)$$

和同余方程组

$$\begin{cases} x^2 \equiv 16 \pmod{3} \\ x^2 \equiv 16 \pmod{17} \end{cases} \quad (2)$$

等价, 考虑(1)的解数, 只需考虑(2)的解数。

同余方程组(2)又等价于

$$\begin{cases} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv -1 \pmod{17} \end{cases} \quad (2')$$

可使用欧拉判别法判断1是模3的二次剩余(从而第一个同余方程有2个解, 可以检查分别是 $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{3}$),
-1是模17的二次剩余(从而第二个同余方程有2个解, 可以检查分别是 $x \equiv 4 \pmod{17}$, $x \equiv 13 \pmod{17}$), 把它们组合在一起就构成4个同余方程:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{17} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 13 \pmod{17} \end{cases}$$

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{17} \end{cases} \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 13 \pmod{17} \end{cases}$$

它们每个都有一个解, 所以原来的同余方程(1)有4个解.

示例:

判断同余方程 $x^2 \equiv -63 \pmod{187}$ 的解数.

类似上例, 可以判断与之等价的同余方程组:

$$\begin{cases} x^2 \equiv -63 \pmod{11} \\ x^2 \equiv -63 \pmod{17} \end{cases}$$

这个同余方程组等价于:

$$\begin{cases} x^2 \equiv 3 \pmod{11} \\ x^2 \equiv 5 \pmod{17} \end{cases} \quad (2)$$

检查 $\{1, 2, 3, 4, 5, 6, 7, 8, -1, -2, -3, -4, -5, -6, -7, -8\}$, 每个的平方都不与5同余, 所以 $x^2 \equiv 5 \pmod{17}$ 无解, 从而, 原同余方程无解。

定理

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

- 如果 a_1, a_2 都是模 p 的二次剩余, 则 $a_1 a_2$ 也是;
这是因为 $(a_1 a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} a_2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
- 如果 a_1, a_2 都是模 p 的二次非剩余, 则 $a_1 a_2$ 是模 p 的二次剩余;
理由同上
- 如果 a_1, a_2 一个是模 p 的二次剩余, 一个是模 p 的二次非剩余, 则 $a_1 a_2$ 是模 p 的二次非剩余.
这是因为 $(a_1 a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} a_2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

2. 勒让德(Legendre)符号

设 p 是素数, 定义Legendre符号如下:

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

比如

$$0^2 \equiv 0 \pmod{5}, 1^2 \equiv 1 \pmod{5}, 2^2 \equiv 4 \pmod{5}, 3^2 \equiv 4 \pmod{5}, 4^2 \equiv 1 \pmod{5}$$

由此

$$\left(\frac{1}{5}\right) = 1, \left(\frac{4}{5}\right) = 1$$

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

$$\left(\frac{5}{5}\right) = 0$$

$$\left(\frac{a}{p}\right) = 1 \iff a \text{ 是模 } p \text{ 的二次剩余};$$

$$\left(\frac{a}{p}\right) = -1 \iff a \text{ 是模 } p \text{ 的二次非剩余}.$$

根据二次剩余的欧拉判别条件:

a 是模 p 的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

a 是模 p 的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

有: $(\frac{a}{p}) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, 以及 $(\frac{a}{p}) = -1 \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

这也就是说, 如果 p 是奇数, $a \in \mathbb{Z}$, 则:

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

使用此式可以帮助我们计算勒让德符号, 比如:

$$\because 2^{\frac{17-1}{2}} \equiv 1 \pmod{17} \quad \therefore (\frac{2}{17}) = 1$$

即2是模17的二次剩余

$$\because 3^{\frac{17-1}{2}} \equiv -1 \pmod{17} \quad \therefore (\frac{3}{17}) = -1$$

即3是模17的二次非剩余

再如, 设 p 是奇素数:

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

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

对于奇素数 p , 可能的情况有两种:

$$p \equiv 1 \pmod{4}, \quad p \equiv 3 \pmod{4}$$

对于前者, 有 $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$, 从而

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

对于后者, 有 $(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$ 从而

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

从而

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

设 p 是奇素数:

- $(\frac{a+p}{p}) = (\frac{a}{p})$

这是因为下面的两个同余式等价(一个的解也是另外一个的解)

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

这就意味着 a 是模 p 的二次剩余当且仅当 $a + p$ 是模 p 的二次剩余.

类似的, $(\frac{a+kp}{p}) = (\frac{a}{p})$

- $a \equiv b \pmod{p} \implies (\frac{a}{p}) = (\frac{b}{p})$

这是因为

$$a = kp + b \implies (\frac{a}{p}) = (\frac{kp + b}{p}) = (\frac{b}{p})$$

- $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

这是因为

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$$

- $(a, p) = 1 \implies (\frac{a^2}{p}) = 1$

由上一条即得. (如果 $p|a$ 的话, $(\frac{a^2}{p}) = 0$)

根据以上结论, 再由算术基本定理, 我们知道只要能够计算 $(\frac{-1}{p}), (\frac{2}{p}), (\frac{q}{p})$, 我们就能够计算任意的 $(\frac{a}{p})$

引理 (Gauss引理)

设 p 是奇素数, $(a, p) = 1, 1 \leq j \leq \frac{p-1}{2}, t_j = (a \cdot j \bmod p)$ (即 $0 < t_j < p$), 以 m 表示这 $\frac{p-1}{2}$ 个 t_j 中大于 $\frac{p}{2}$ 的 t_j 的个数, 则 $(\frac{a}{p}) = (-1)^m$

事实上, 因为 $p \nmid a$, 对任意的 $1 \leq j < i \leq \frac{p-1}{2}$, 有 $p \nmid [(j \pm i)a]$, 即

$$t_j \not\equiv \pm t_i \pmod{p}$$

以 r_1, r_2, \dots, r_m 表示所有 $t_j (1 \leq j \leq \frac{p-1}{2})$ 中大于 $\frac{p}{2}$ 的数, 以 s_1, s_2, \dots, s_k 表示所有 $t_j (1 \leq j \leq \frac{p-1}{2})$ 中小于 $\frac{p}{2}$ 的数($k + m = \frac{p-1}{2}$), 即:

$$\frac{p}{2} < r_i < p, 1 \leq s_j < \frac{p}{2}$$

从而

$$1 \leq p - r_i < \frac{p}{2}$$

显然有

$$1 \leq p - r_1, p - r_2, \dots, p - r_m < \frac{p}{2}$$

由 $1 \leq j < i < \frac{p}{2}$, $t_j \not\equiv \pm t_i \pmod{p}$ 我们知道

$$s_j \not\equiv p - r_i \pmod{p}, (j = 1, 2, \dots, k, i = 1, 2, \dots, n)$$

从而 $\frac{p-1}{2}$ 个数

$$s_1, s_2, \dots, s_k, p - r_1, p - r_2, \dots, p - r_m$$

恰好是

$$1, 2, 3, \dots, \frac{p-1}{2}$$

的一个排列, 从而

$$t_1 t_2 \cdots t_{\frac{p-1}{2}} \equiv 1a \cdot 2a \cdot \dots \cdot \frac{p-1}{2}a \equiv s_1 s_2 \dots s_k r_1 r_2 \dots r_m$$

$$\equiv (-1)^m s_1 s_2 \dots s_k (p - r_1)(p - r_2) \dots (p - r_m) \equiv (-1)^m 1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2}$$

即得

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

这个结论在数论中被称为**Gauss引理**

Gauss引理的一个直接应用就是计算($\frac{2}{p}$)

$$\bullet \left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

采用Gauss引理中的符号, 取 $a = 2$, 可以看到

$$1 \leq j < \frac{p}{4} \implies 1 \leq t_j = 2j < \frac{p}{2}$$

$$\frac{p}{4} \leq j < \frac{p}{2} \implies \frac{p}{2} \leq t_j = 2j < p$$

所以

$$m = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

从而

$$m = \begin{cases} l & p = 4l + 1 \\ l + 1 & p = 4l + 3 \end{cases}$$

从而

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

此即所证: 当且仅当素数 $p \equiv \pm 1 \pmod{8}$ 时, 2才是模 p 的二次剩余. \diamond

对证明过程的进一步分析, $t_j = (ja \bmod p)$ (i.e., $0 < t_j < p$) 利用符号整数表示就是:

$$ja = p\left[\frac{ja}{p}\right] + t_j, \quad (1 \leq j \leq \frac{p-1}{2})$$

两边对 j 求和得

$$a \sum_{j=1}^{\frac{p-1}{2}} j = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + \sum_{j=1}^{\frac{p-1}{2}} t_j = pT + \sum_{j=1}^{\frac{p-1}{2}} t_j$$

而

$$\sum_{j=1}^{\frac{p-1}{2}} t_j = s_1 + \dots + s_k + r_1 + \dots + r_m$$

$$= s_1 + \dots + s_k + (p-r_1) + \dots + (p-r_m) - mp + 2(r_1 + \dots + r_m) = \sum_{j=1}^{\frac{p-1}{2}} j - mp + 2(r_1 + \dots + r_m)$$

从而

$$a \cdot \frac{\frac{p-1}{2} \cdot (1 + \frac{p-1}{2})}{2} = pT + \frac{\frac{p-1}{2} \cdot (1 + \frac{p-1}{2})}{2} - mp + 2(r_1 + \dots + r_m)$$

$$\frac{p^2-1}{8}(a-1) = p(T-m) + 2(r_1 + \dots + r_m), \text{ i.e., } \frac{p^2-1}{8}(a-1) \equiv T + m \pmod{2}$$

(此处利用等差数列求和公式 $S_n = \frac{n(a_1+a_n)}{2}$)

易见, 当 $a = 2, 1 \leq j \leq \frac{p-1}{2}$ 时, $1 \leq 2j \leq p-1$

$$\left[\frac{2j}{p}\right] = 0$$

从而

$$T = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{2j}{p}\right] = 0$$

从而当 $a = 2$ 时,

$$m \equiv \frac{p^2 - 1}{8} \pmod{2}$$

这样就有

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

当 a 是奇数时:

$a - 1$ 是偶数,

$$\frac{p^2 - 1}{8}(a - 1) \equiv T + m \pmod{2} \implies 0 \equiv T + m \pmod{2}$$

因为 $T + m \equiv T - m \pmod{2}$, 所以有

$$0 \equiv T - m \pmod{2}, \quad \text{i.e., } T \equiv m \pmod{2}$$

即

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right] \equiv m \pmod{2}, \quad \text{i.e., } m = 2k + \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right]$$

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

$$\left(\frac{a}{p} \right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right]}$$

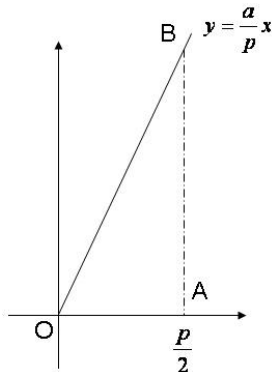
如果 a 也是奇素数(比如记之为 q), 则我们也可以考虑 $\left(\frac{p}{q} \right)$, 同上, 应该有

$$\left(\frac{p}{q} \right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jp}{q} \right]}$$

假设 a 是正数, 继续来看

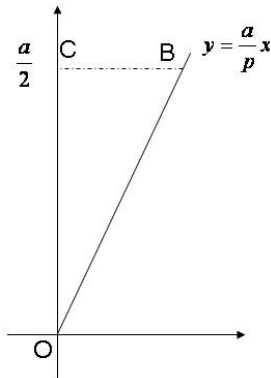
$$T = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right]$$

的意义:



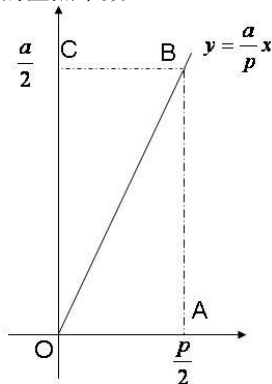
可见, $[\frac{a}{p} \cdot 1], [\frac{a}{p} \cdot 2], \dots, [\frac{a}{p} \cdot \frac{p-1}{2}]$ 分别是 x 取 $1, 2, \dots, \frac{p-1}{2}$ 时对应的竖线上的整点(横纵坐标均为整数)的个数, 而且 AB 上没有整点(因为 $\frac{p}{2}$ 不是整数), OB 上除 O 外无整点(因为 $\frac{a}{p}$ 不是整数), 这样 T 就是三角形 OAB 内部的整点的个数.

如果 a 也是奇素数, 则我们也可以考虑 $(\frac{p}{a})$, 同上, 应该有 $(\frac{p}{a}) = (-1)^{\sum_{j=1}^{\frac{a-1}{2}} [\frac{jp}{a}]}$
 记 $S = \sum_{j=1}^{\frac{a-1}{2}} [\frac{jp}{a}]$, 来看 S 的意义:



可见, $[\frac{p}{a} \cdot 1], [\frac{p}{a} \cdot 2], \dots, [\frac{p}{a} \cdot \frac{a-1}{2}]$ 分别是 y 取 $1, 2, \dots, \frac{a-1}{2}$ 时对应的横线上的整点(横纵坐标均为整数)的个数, 而且 CB 上没有整点(因为 $\frac{a}{2}$ 不是整数), OB 上除 O 外无整点(因为 $\frac{a}{p}$ 不是整数), 这样 S 就是三角形 OCB 内部的整点的个数.

$S + T$ 也就是矩形 $OACB$ 内部的整点个数:



而这个矩形内部的整点个数显然就是 $\frac{p-1}{2} \cdot \frac{a-1}{2}$, 所以,

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

所以 a, p 都是素数时, $(\frac{a}{p}) \cdot (\frac{p}{a}) = (-1)^T \cdot (-1)^S = (-1)^{S+T} = (-1)^{\frac{p-1}{2} \cdot \frac{a-1}{2}}$ 这样 S 就是三角形 OCB 内部的整点的个数. 这就是有用的Gauss二次互反律

定理 (Gauss二次互反律)

$p \neq q$ 均为奇素数, 则

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

根据这个结论, 两个奇素数 p, q :

只要有一个数 $\equiv 1 \pmod{4}$, 就必有 $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$,

当且仅当他们都是形如 $4k+3$ 形式的数时, 才有 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

利用这个结论与 $\left(\frac{2}{p}\right), \left(\frac{-1}{p}\right)$ 相结合可以计算勒让得符号.

计算 $(\frac{137}{227})$

事实上, 227是素数,

$$137 \equiv -90 \pmod{227} \implies \left(\frac{137}{227}\right) = \left(\frac{-90}{227}\right)$$

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

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

$$= (-1) \left(\frac{2}{227}\right) \left(\frac{5}{227}\right) \quad \left(\because p \nmid a \implies \left(\frac{a^2}{p}\right) = 1\right)$$

$$= (-1)(-1) \left(\frac{5}{227}\right) \quad \left(\because 227 = 8 \cdot 8 + 3, \left(\frac{2}{p}\right) = -1 \text{ if } p \equiv \pm 3 \pmod{8}\right)$$

对于 $(\frac{5}{227})$, 因为5模4余1, 所以 $(\frac{5}{227}) = (\frac{227}{5})$,

而 $227 \equiv 2 \pmod{5}$, 所以 $(\frac{227}{5}) = (\frac{2}{5}) = -1 (\because 5 \equiv -3 \pmod{8})$

最终, $(\frac{137}{227}) = -1$

上述计算($\frac{137}{227}$)其实就是相当于判断同余式 $x^2 \equiv 137 \pmod{227}$ 是否有解.

示例: 判断 $x^2 \equiv -1 \pmod{365}$ 是否有解? 有的话, 解数多少?

这时无法直接使用勒让得符号的方法, 因为365不是素数, 所以勒让得符号($\frac{-1}{365}$)没有定义.

但是 $365 = 5 \cdot 73$, 5和73互素,
这时原同余式等价于同余式组

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

这样要判断原同余式的解, 只需要判断这个同余式组的解的情况.

这里5和73都是素数, 所以:

可以使用勒让得符号判断 $x^2 \equiv -1 \pmod{5}$ 有解($\because (\frac{-1}{5}) = 1$),

可以使用勒让得符号判断 $x^2 \equiv -1 \pmod{73}$ 有解($\because (\frac{-1}{73}) = 1$)

所以同余式组有解, 解数为4,

故原同余式有解, 解数为4.

Previously on Quadratic Residue

考虑模素数二次同余方程:

$$x^2 \equiv a \pmod{p} \quad ((a, p) = 1)$$

- **定义:** 如果有解, 则称 a 是一个模 p 的平方剩余(二次剩余). 否则, 称 a 是一个模 p 的平方非剩余(二次非剩余).
- **定理:** 在模 p 的一个简化剩余系中, 恰有 $\frac{p-1}{2}$ 个模 p 二次剩余, 恰有 $\frac{p-1}{2}$ 个模 p 二次非剩余; 如果 a 是模 p 二次剩余的话, $x^2 \equiv a \pmod{p} \quad ((a, p) = 1)$ 的解数为2
- **欧拉判别条件**
 a 是模 p 的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
 a 是模 p 的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

- 勒让得符号:

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

如果 p 是奇数, $a \in \mathbb{Z}$, 则:

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

- $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right), a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), (a, p) = 1 \implies \left(\frac{a^2}{p}\right) = 1$$

- p 是奇素数, $a \in \mathbb{Z}$, 则: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \text{ i.e.,}$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

- $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$ 即: 当且仅当素数 $p \equiv \pm 1 \pmod{8}$ 时, 2 才是模 p 的二次剩余. 或说:

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

- **Gauss 二次互反律** p, q 都是奇数时, $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$, i.e.,
只要有一个数 $\equiv 1 \pmod{4}$, 就必有 $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$,
当且仅当他们都是形如 $4k + 3$ 形式的数时, 才有 $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

3. 雅可比(Jacobi)符号

设 m 是奇素数的乘积, $m = p_1 p_2 \dots p_s, \forall a \in \mathbb{Z}$,

$$\left(\frac{a}{m}\right) \triangleq \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \dots \cdot \left(\frac{a}{p_s}\right)$$

其中 $\left(\frac{a}{p_i}\right)$ 是模 p_i 的勒让得符号. 称 $\left(\frac{a}{m}\right)$ 为雅可比符号.

显然, 根据这个定义, 当 m 本身就是素数时, 雅可比符号就是勒让得符号.

设 m 是奇素数的乘积, $m = p_1 p_2 \dots p_s, \forall a \in \mathbb{Z}$, 则

$$(m, n) > 1, \text{ 则 } \left(\frac{m}{n}\right) = 0, \left(\frac{n}{m}\right) = 0$$

这是因为: 比如 $m = p p_1 p_2 \dots p_s, n = p q_1 q_2 \dots q_t$

则

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p}\right) \left(\frac{m}{q_1}\right) \left(\frac{m}{q_2}\right) \dots \left(\frac{m}{q_t}\right) = 0$$

$\left(\frac{n}{m}\right)$ 类似.

- $(\frac{a+m}{m}) = (\frac{a}{m})$ 事实上,

$$(\frac{a+m}{m}) = (\frac{a+m}{p_1 p_2 \dots p_s}) = (\frac{a+m}{p_1}) \cdot \dots \cdot (\frac{a+m}{p_s}) = (\frac{a}{p_1}) \cdot \dots \cdot (\frac{a}{p_s}) = (\frac{a}{m})$$

类似地, $(\frac{a+km}{m}) = (\frac{a}{m})$

- $(\frac{ab}{m}) = (\frac{a}{m})(\frac{b}{m})$ 理由同上.
- 设 $(a, m) = 1$, 则 $(\frac{a^2}{m}) = 1$
- $(\frac{1}{m}) = 1$

进一步学习之前, 我们看 m 是奇素数的乘积, $m = p_1 p_2 \dots p_s$
从而自然有 $m \equiv p_1 p_2 \dots p_s \pmod{4}$, 即

$$m \equiv (1 + 2 \cdot \frac{p_1 - 1}{2})(1 + 2 \cdot \frac{p_2 - 1}{2}) \dots (1 + 2 \cdot \frac{p_s - 1}{2}) \pmod{4}$$

而

$$(1 + 2 \cdot \frac{p_1 - 1}{2})(1 + 2 \cdot \frac{p_2 - 1}{2}) \dots (1 + 2 \cdot \frac{p_s - 1}{2}) = 1 + 2 \cdot \frac{p_1 - 1}{2} + \dots + 2 \cdot \frac{p_s - 1}{2} + 4 \cdot (\dots)$$

从而

$$m \equiv 1 + 2 \cdot \frac{p_1 - 1}{2} + 2 \cdot \frac{p_2 - 1}{2} + \dots + 2 \cdot \frac{p_s - 1}{2} \pmod{4}$$

所以

$$m - 1 \equiv 2 \cdot (\frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \dots + \frac{p_s - 1}{2}) \pmod{4}$$

$$\frac{m - 1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \dots + \frac{p_s - 1}{2} \pmod{2}$$

即

$$\frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \dots + \frac{p_s - 1}{2} = 2k + \frac{m - 1}{2}$$

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

这是因为

$$\begin{aligned}
 \left(\frac{-1}{m}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_s}\right) \\
 &= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_s-1}{2}} \\
 &= (-1)^{\frac{p_1-1}{2} + \frac{p_2-1}{2} + \frac{p_s-1}{2}} \\
 &= (-1)^{2k + \frac{m-1}{2}} \\
 &= (-1)^{\frac{m-1}{2}}
 \end{aligned}$$

注意到: $(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$, i.e.,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

m 是奇素数的乘积, $m = p_1 p_2 \dots p_s$

从而自然有 $m^2 = p_1^2 p_2^2 \dots p_s^2$, $m^2 \equiv p_1^2 p_2^2 \dots p_s^2 \pmod{16}$, 即

$$m^2 \equiv (1 + 8 \cdot \frac{p_1^2 - 1}{8})(1 + 8 \cdot \frac{p_2^2 - 1}{8}) \dots (1 + 8 \cdot \frac{p_s^2 - 1}{8}) \pmod{16}$$

而

$$(1 + 8 \cdot \frac{p_1^2 - 1}{8})(1 + 8 \cdot \frac{p_2^2 - 1}{8}) \dots (1 + 8 \cdot \frac{p_s^2 - 1}{8}) = 1 + 8 \cdot \frac{p_1^2 - 1}{8} + \dots + 8 \cdot \frac{p_s^2 - 1}{8} + 64 \cdot (\dots)$$

从而

$$m^2 \equiv 1 + 8 \cdot \frac{p_1^2 - 1}{8} + 8 \cdot \frac{p_2^2 - 1}{8} + \dots + 8 \cdot \frac{p_s^2 - 1}{8} \pmod{16}$$

所以

$$\frac{m^2 - 1}{8} \equiv \frac{p_1^2 - 1}{8} + \frac{p_2^2 - 1}{8} + \dots + \frac{p_s^2 - 1}{8} \pmod{2}$$

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

这是因为

$$\begin{aligned}\left(\frac{2}{m}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_s}\right) \\ &= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_s^2-1}{8}} \\ &= (-1)^{\frac{p_1^2-1}{8} + \frac{p_2^2-1}{8} + \frac{p_s^2-1}{8}} \\ &= (-1)^{\frac{m^2-1}{8}}\end{aligned}$$

注意到:

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

即: 当且仅当素数 $p \equiv \pm 1 \pmod{8}$ 时, 2 才是模 p 的二次剩余. 或说:

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

雅克比符号的互反律: m, n 都是奇素数的乘积, $(m, n) = 1$, 则

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

证明: 假设 $m = p_1 p_2 \dots p_s, n = q_1 q_2 \dots q_r$, 其中 p_i, q_j 均为奇素数, 且 $p_i \neq q_j$, 则

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

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

而

$$n = q_1 q_2 \dots q_r \implies \frac{n-1}{2} \equiv \frac{q_1-1}{2} + \frac{q_2-1}{2} + \dots + \frac{q_r-1}{2} \pmod{2}$$

所以

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

注意到:**Gauss二次互反律**: q, p 都是素数时:

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

只要有一个数 $\equiv 1 \pmod{4}$, 就必有 $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

当且仅当它们都是形如 $4k+3$ 形式的数时, 才有 $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

这些性质表明**为了计算雅克比符号(当然包括勒让德符号是它的特殊情形)的值, 并不要求素因数分解式.**

示例: 计算

$$\left(\frac{105}{317}\right) = \left(\frac{307}{105}\right) = \left(\frac{2}{105}\right) = 1$$

可见, 有了雅克比符号后, 大大方便了勒让德符号的计算, 比如 $\left(\frac{105}{317}\right)$, 不必 $\left(\frac{105}{317}\right) = \left(\frac{3}{317}\right)\left(\frac{5}{317}\right)\left(\frac{7}{317}\right)$.

以上的雅克比符号性质虽然都和勒让德符号类似, 但不能掩盖两者之间的本质区别:
雅克比符号 $\left(\frac{n}{m}\right) = 1$ 绝不表示二次同余方程

$$x^2 \equiv n \pmod{m}$$

一定有解

比如: $\left(\frac{3}{119}\right) = 1$, 但 $x^2 \equiv 3 \pmod{9}$ 无解.

同样的, 对雅克比符号来说, 没有性质

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

不存在类似勒让德符号的Gauss引理的性质;

不存在类似: a 是奇数, 则 $\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{aj}{p}\right]}$ 的性质;

等等.

4. 模素数的二次同余方程求解

模素数的二次同余方程的解的存在性判定和具体求解都可以解决. 前面我们知道根据勒让德符号计算可以判定二次同余方程 $x^2 \equiv a \pmod{p}$ 的解的存在与否问题.

那么, 如果判定出来这个方程的解是存在的, 应该怎么求解呢? 下面给出一个一般性的算法. 算法的主要思路是:

- 将 $p-1$ 写成是2的幂和一个奇数的乘积形式, 即 $p-1 = 2^t \cdot s$
- 我们希望能够比较方面的求出方程

$$y^{2^{t-1}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-1}^2$ 的解(事实上, 这个解比较容易写出), 利用这个解能够比较容易地写出

$$y^{2^{t-1}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-2}^2$ 的解;

- 利用

$$y^{2^{t-2}} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^{2^{t-3}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-3}^2$ 的解;

- 利用

$$y^{2^{t-3}} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^{2^{t-4}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-4}^2$ 的解;

-;
- 一般地, 利用

$$y^{2^{t-(k-1)}} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^{2^{t-k}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-k}^2$ 的解;

- 利用

$$y^{2^{t-k}} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^{2^{t-(k+1)}} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_{t-(k+1)}^2$ 的解;

-;
- 利用

$$y^{2^3} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^{2^2} \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_2^2$ 的解;

- 利用

$$y^{2^2} \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y^2 \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_1^2$ 的解;

- 利用

$$y^2 \equiv 1 \pmod{p}$$

的这个解能够比较容易的写出

$$y \equiv 1 \pmod{p}$$

的一个形如 $a^{-1}x_0^2$ 的解;

- 至此, 我们已经得到原方程的一个解, 即 $x_0^2 \equiv a \pmod{p}$

在具体求解之前我们先任意选取模 p 的一个平方非剩余 n , 计算 $b = (n^s \bmod p)$, 从而有

$$b^{2^t} = (n^s)^{2^t} = n^{s \cdot 2^t} = n^{p-1} \equiv 1 \bmod p \quad (\because \text{Euler theorem})$$

$$b^{2^{t-1}} = (n^s)^{2^{t-1}} = n^{s \cdot 2^{t-1}} = n^{\frac{p-1}{2}} \equiv -1 \bmod p \quad (\because \text{square non-residue})$$

给定 $p-1 = 2^t \cdot s$: 方程

$$y^{2^{t-1}} \equiv 1 \bmod p$$

的一个形如 $a^{-1}x_{t-1}^2$ 的解就是:

$$x_{t-1} = (a^{\frac{s+1}{2}} \bmod p)$$

$$(a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv [a^{-1}(a^{\frac{s+1}{2}})^2]^{2^{t-1}} = [a^{-1}a^{s+1}]^{2^{t-1}} = a^{s \cdot 2^{t-1}} \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p$$

下面我们看怎样有这个解找出方程

$$y^{2^{t-2}} \equiv 1 \bmod p$$

的一个形如 $a^{-1}x_{t-2}^2$ 的解:

由于 $(a^{-1}x_{t-1}^2)^{2^{t-1}} \equiv 1 \bmod p$, 而且 $(a^{-1}x_{t-1}^2)^{2^{t-1}} = [(a^{-1}x_{t-1}^2)^{2^{t-2}}]^{2^1}$

所以必定 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$ 或 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$

case 1: 如果 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod p$, 则令 $x_{t-2} = x_{t-1}$, 且有

$$(a^{-1}x_{t-2}^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-2}^2$ 是方程

$$y^{2^{t-2}} \equiv 1 \pmod p$$

的解;

case 2: 如果 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \pmod p$, 则令 $x_{t-2} = x_{t-1} \cdot b$, 且有

$$(a^{-1}x_{t-2}^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2 b^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} (b^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} b^{2^{t-1}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-2}^2$ 是方程

$$y^{2^{t-2}} \equiv 1 \pmod p$$

的解;

亦即: 不论 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod p$ 还是 $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \pmod p$, 我们总能利用方程 $y^{2^{t-1}} \equiv 1 \pmod p$ 计算出方程 $y^{2^{t-2}} \equiv 1 \pmod p$ 的解 $a^{-1}x_{t-2}^2$.

由于 $(a^{-1}x_{t-2}^2)^{2^{t-2}} \equiv 1 \pmod p$, 而且 $(a^{-1}x_{t-2}^2)^{2^{t-2}} = [(a^{-1}x_{t-2}^2)^{2^{t-3}}]^2$
 所以必定 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \pmod p$ 或 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \pmod p$

case 1: 如果 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \pmod p$, 则令 $x_{t-3} = x_{t-2}$, 且有

$$(a^{-1}x_{t-3}^2)^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-3}^2$ 是方程

$$y^{2^{t-3}} \equiv 1 \pmod p$$

的解;

case 2: 如果 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \pmod p$, 则令 $x_{t-3} = x_{t-2} \cdot b^2$, 则 $x_{t-3}^2 = x_{t-2}^2 \cdot b^{2^2}$,
 且有

$$(a^{-1}x_{t-3}^2)^{2^{t-3}} = (a^{-1}x_{t-2}^2 b^{2^2})^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} (b^{2^2})^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} b^{2^{t-1}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-3}^2$ 是方程

$$y^{2^{t-3}} \equiv 1 \pmod p$$

的解;

亦即: 不论 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \pmod p$ 还是 $(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \pmod p$, 我们总能利用
 方程 $y^{2^{t-2}} \equiv 1 \pmod p$ 计算出方程 $y^{2^{t-3}} \equiv 1 \pmod p$ 的解 $a^{-1}x_{t-3}^2$

由于 $(a^{-1}x_{t-3}^2)^{2^{t-3}} \equiv 1 \pmod p$, 而且 $(a^{-1}x_{t-3}^2)^{2^{t-3}} = [(a^{-1}x_{t-3}^2)^{2^{t-4}}]^2$
所以必定 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \pmod p$ 或 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \pmod p$

case 1: 如果 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \pmod p$, 则令 $x_{t-4} = x_{t-3}$, 且有

$$(a^{-1}x_{t-4}^2)^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-4}^2$ 是方程

$$y^{2^{t-4}} \equiv 1 \pmod p$$

的解;

case 2: 如果 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \pmod p$, 则令 $x_{t-4} = x_{t-3} \cdot b^{2^2}$, 则 $x_{t-4}^2 = x_{t-3}^2 \cdot b^{2^3}$,
且有

$$(a^{-1}x_{t-4}^2)^{2^{t-4}} = (a^{-1}x_{t-3}^2 b^{2^3})^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} (b^{2^3})^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} b^{2^{t-1}} \equiv 1 \pmod p$$

即 $a^{-1}x_{t-4}^2$ 是方程

$$y^{2^{t-4}} \equiv 1 \pmod p$$

的解;

亦即: 不论 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \pmod p$ 还是 $(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \pmod p$, 我们总能利用
方程 $y^{2^{t-3}} \equiv 1 \pmod p$ 计算出方程 $y^{2^{t-4}} \equiv 1 \pmod p$ 的解 $a^{-1}x_{t-4}^2$

以此类推，我们总可用一个高次的方程 $y^{2^{t-k}} \equiv 1 \pmod p$ 的解 $a^{-1}x_{t-k}^2$ 计算出一个低次的方程 $y^{2^{t-k-1}} \equiv 1 \pmod p$ 的解 $a^{-1}x_{t-k-1}^2$,

直到最终我们能够用一个高次的方程 $y^{2^3} \equiv 1 \pmod p$ 的解 $a^{-1}x_3^2$ 计算出一个低次的方程 $y^{2^2} \equiv 1 \pmod p$ 的解 $a^{-1}x_2^2$,

能够用一个高次的方程 $y^{2^2} \equiv 1 \pmod p$ 的解 $a^{-1}x_2^2$ 计算出一个低次的方程 $y^2 \equiv 1 \pmod p$ 的解 $a^{-1}x_1^2$,

能够用一个高次的方程 $y^2 \equiv 1 \pmod p$ 的解 $a^{-1}x_1^2$ 计算出一个低次的方程 $y \equiv 1 \pmod p$ 的解 $a^{-1}x_0^2$,
从而 x_0 即为方程 $x^2 \equiv a \pmod p$ 的一个解, 另外一个解为 $x \equiv -x_0 \pmod p$.

示例: 求解 $x^2 \equiv 186 \pmod{401}$

计算 $\left(\frac{186}{401}\right) = 1$, 说明原方程有解.

$$a = 186, p = 401, p - 1 = 2^4 \cdot 25, t = 4, s = 25, a^{-1} 235 \pmod{401}$$

任取一个模 p 的非平方剩余 $n = 3$, 计算 $b = n^s = 3^{25} \equiv 268 \pmod{401}$

计算 $y^{2^{t-1}} \equiv 1 \pmod{p}$ 的解:

$$x_{t-1} = (a^{\frac{s+1}{2}}), \quad x_3 = (186^{\frac{25+1}{2}} \pmod{401}) = 103$$

$$a^{-1} x_3^2 = (235 \cdot 103^2 \pmod{401}) = 98$$

计算 $y^{2^{t-2}} \equiv 1 \pmod{p}$ 的解:

$$\therefore (a^{-1} x_3^2)^{2^{t-2}} \equiv 98^4 \equiv -1 \pmod{401}$$

$$\therefore x_{t-2} = x_{t-1} b, \quad x_2 = (x_3 b \pmod{p}) = (103 \cdot 268 \pmod{401}) = 336$$

$$(a^{-1} x_{t-2}^2 = (235 \cdot 336^2 \pmod{401}) = 400 \equiv -1 \pmod{401}$$

计算 $y^{2^{t-3}} \equiv 1 \pmod{p}$ 的解:

$$\because (a^{-1}x_2^2)^{2^{t-3}} \equiv (-1)^2 \equiv 1 \pmod{401}$$

$$\therefore x_{t-3} = x_{t-2}, \quad x_1 = x_2 = 336$$

$$a^{-1}x_{t-3}^2 = (235 \cdot 336^2 \pmod{401}) = 400 \equiv -1 \pmod{401}$$

计算 $y^{2^{t-4}} \equiv 1 \pmod{p}$, 即 $y \equiv 1 \pmod{p}$ 的解:

$$\because (a^{-1}x_1^2)^{2^{t-4}} \equiv -1 \pmod{401}$$

$$\therefore x_{t-4} = x_{t-3}b^{2^{t-2}}, \quad x_0 = (x_1b^4 \pmod{401}) = (336 \cdot 268^4 \pmod{401}) = 304$$

这就是我们要求的原方程的解: $x \equiv \pm 304 \pmod{401}$.

对于特殊形式的素数 p 不需要像上述那样繁琐的计算, 特别地:

$p = 4k + 3$, p 为素数, k 为任意整数, 已知 $x^2 \equiv a \pmod p$ 有解, 求其解.

因为 $x^2 \equiv a \pmod p$ 有解, 根据欧拉判别准则我们指导下式必定成立:

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

从而

$$a^{\frac{4k+2}{2}} \equiv 1 \pmod p \implies a^{2k+1} \equiv 1 \pmod p$$

从而

$$a^{2k+1} a \equiv a \pmod p$$

即

$$(a^{k+1})^2 \equiv a \pmod p$$

其中 $k + 1 = \frac{p+1}{4}$. 所以原方程的解就是

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p$$

类似地, 如果素数 p 和 q 都是形如 $4k + 3$ 的形式, 且 $x^2 \equiv a \pmod p$, $x^2 \equiv a \pmod q$ 都有解(即 $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, $a^{\frac{q-1}{2}} \equiv 1 \pmod q$ 都成立), 那么二次方程

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

有解, 并且可以通过孙子定理求解同余式组获得:

$$\begin{cases} x \equiv a^{\frac{p+1}{4}} \pmod p \\ x \equiv a^{\frac{q+1}{4}} \pmod q \end{cases}$$
$$\begin{cases} x \equiv -a^{\frac{p+1}{4}} \pmod p \\ x \equiv a^{\frac{q+1}{4}} \pmod q \end{cases}$$
$$\begin{cases} x \equiv a^{\frac{p+1}{4}} \pmod p \\ x \equiv -a^{\frac{q+1}{4}} \pmod q \end{cases}$$
$$\begin{cases} x \equiv -a^{\frac{p+1}{4}} \pmod p \\ x \equiv -a^{\frac{q+1}{4}} \pmod q \end{cases}$$

5. 模为合数的二次同余方程

设 $m = 2^\delta p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, 我们知道对于一个模为合数 m 的二次方程 (a 与 m 互素)

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

他等价于一个同余式组

$$\begin{cases} x^2 \equiv a \pmod{2^\delta} \\ x^2 \equiv a \pmod{p_1^{\alpha_1}} \\ x^2 \equiv a \pmod{p_2^{\alpha_2}} \\ \dots\dots\dots \\ x^2 \equiv a \pmod{p_k^{\alpha_k}} \end{cases}$$

这就是说, 我们需要解决的问题就是: 方程 $x^2 \equiv a \pmod{2^\delta}$ 的判定(与求解), 方程 $x^2 \equiv a \pmod{p^\alpha}$ (a 与 p 互素)的判定(与求解).

定理

方程 $x^2 \equiv a \pmod{p^\alpha}$ (a 与 p 互素) 的判定与求解: $x^2 \equiv a \pmod{p^\alpha}$ 有解 $\iff a$ 为模 p 的二次剩余. 且有解的话, 解数为 2.

" \implies :" 设 $x^2 \equiv a \pmod{p^\alpha}$ 有解 x_1 , 即 $x_1^2 \equiv a \pmod{p^\alpha}$, 从而 $x_1^2 \equiv a \pmod{p}$, 即 a 为模 p 的二次剩余.

" \impliedby :" 设 a 为模 p 的二次剩余, 即存在 $x \equiv x_1 \pmod{p}$ 使得 $x_1^2 \equiv a \pmod{p}$,
 $x_1^2 - a \equiv 0 \pmod{p}$,

取 $f(x) = x^2 - a$, 则上式说明 $f(x) \equiv 0 \pmod{p}$ 有解 x_1 , 从而可以利用这个解对应的求出方程 $f(x) \equiv 0 \pmod{p^2}$ 的解 $x \equiv x_1 + kp \pmod{p^2}$, 其中 k 是 $f'(x_1)k \equiv \frac{-f(x_1)}{p} \pmod{p}$ 的解, 这里得到的 k 的解是唯一的(这是因为 $f'(x_1) = 2x_1$, 2 和 x_1 都与 p 互素, 所以 $(f'(x_1), p) = 1$),

类似的, 利用 $f(x) \equiv 0 \pmod{p^2}$ 的这个解可以唯一的对应 $f(x) \equiv 0 \pmod{p^3}$ 的解, ..., 最终可以利用 $f(x) \equiv 0 \pmod{p}$ 有解 x_1 , 唯一地得到 $f(x) \equiv 0 \pmod{p^\alpha}$ 的解.

我们知道模素数二次同余方程 $x^2 - a \equiv 0 \pmod{p}$ 只有两个解 $x \equiv \pm x_1 \pmod{p}$, 所以二次同余方程 $x^2 - a \equiv 0 \pmod{p^\alpha}$ 也只有两个解(并且可以利用 $\pm x_1$ 求出). \diamond

方程 $x^2 \equiv a \pmod{2^\delta}$ 的判定:

可以看到, 如果 $\delta = 2$: 则

$$x^2 \equiv a \pmod{4} \text{ 有解} \iff a \equiv 1 \pmod{4}$$

这是很显然的: $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9$. 考虑到 $(a, 4) = 1$, 我们得到 $a \equiv 1 \pmod{4}$ 时有解, 且解数为2, 解为 $x \equiv 1 \pmod{4}, x \equiv -1 \pmod{4}$.

当 $\delta \geq 3$ 时: 方程 $x^2 \equiv a \pmod{2^\delta}$ 有解 $\iff a \equiv 1 \pmod{8}$. 且有解的话, 解数为4.

" \implies :" 假设有解 $x \equiv x_1 \pmod{2^\delta}$, 由于 $(a, 2^\delta) = 1$, 所以 a 必定是奇数, 从而 x_1 必定是奇数, 比如 $x_1 = 2l + 1 (l \in \mathbb{Z})$,

从而 $a \equiv (2l + 1)^2 \equiv 1 + 4l(l + 1) \pmod{2^\delta}$,

从而 $a \equiv 1 + 4l(l + 1) \pmod{2^3}$, 即 $a \equiv 1 \pmod{8}$.

" \Leftarrow :" 已知 $a \equiv 1 \pmod{8}$,

当 $\delta = 3$ 时, $2^\delta = 8$: 可以通过检查发现方程 $x^2 \equiv 1 \pmod{8}$ 的解,
 $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 \equiv 1 \pmod{8}, 4^2 = 16 \equiv 0 \pmod{8}, 5^2 = 25 \equiv 1 \pmod{8}, 6^2 = 36 \equiv 4 \pmod{8}, 7^2 = 49 \equiv 1 \pmod{8}$.

可见方程 $x^2 \equiv a \pmod{2^\delta}$ 有解, 且解有4个: $x \equiv 1 \pmod{8}, x \equiv 3 \pmod{8}, x \equiv 5 \pmod{8}, x \equiv 7 \pmod{8}$, 即 $x \equiv \pm 1 \pmod{8}, x \equiv \pm 5 \pmod{8}$, 也就是

$$\{\pm(1 + 4k) : k \in \mathbb{Z}\}$$

当 $\delta = 4$ 时, $2^\delta = 16$: 设 c 是方程 $x^2 \equiv a \pmod{16}$ 的解, 我们知道 c 必定是 $x^2 \equiv a \pmod{8}$ (即 $x^2 \equiv 1 \pmod{8}$) 的解, 所以必有 $x \equiv c \pmod{16} \subset \{\pm(1 + 4k) : k \in \mathbb{Z}\}$, 我们现在关心的是哪些 k 使得 $\pm(1 + 4k)$ 确实是方程 $x^2 \equiv a \pmod{16}$ 的解:

将 $\pm(1 + 4k)$ 代入方程 $x^2 \equiv a \pmod{16}$, 由于 $(1 + 4k)^2 = 1 + 8k + 16k^2$, 从而有 $1 + 8k \equiv a \pmod{16}$, 即 $8k \equiv a - 1 \pmod{16}$, 从而

$$k \equiv \frac{a-1}{8} \pmod{2}, \quad \text{i.e.,} \quad k = 2l + \left(\frac{a-1}{8} \pmod{2}\right), (l \in \mathbb{Z})$$

这样, 方程 $x^2 \equiv a \pmod{16}$ 的解就是(4个):

$$\{\pm(1 + 4 \cdot (2l + (\frac{a-1}{8} \pmod{2})))\} = \{\pm(1 + 8l + 4 \cdot (\frac{a-1}{8} \pmod{2}))\}, l \in \mathbb{Z}.$$

当 $\delta = 5$ 时, $2^\delta = 32$: 设 c 是方程 $x^2 \equiv a \pmod{32}$ 的解, 我们知道 c 必定是 $x^2 \equiv a \pmod{16}$ 的解, 所以必

有 $x \equiv c \pmod{32} \subset \{\pm(1 + 4 \cdot (\frac{a-1}{8} \pmod{2}) + 8l) : k \in \mathbb{Z}\}$, 我们现在关心的是哪些 k 使得 $\pm(1 + 4 \cdot (\frac{a-1}{8} \pmod{2}) + 8l)$ 确实是方程 $x^2 \equiv a \pmod{32}$ 的解:

记 $x_4 = 1 + 4 \cdot (\frac{a-1}{8} \pmod{2})$, 将 $\pm(x_4 + 8l)$ 代入方程 $x^2 \equiv a \pmod{32}$, 由于 $(x_4 + 8l)^2 = x_4^2 + 16x_4l + 64l^2$, 从而有 $x_4^2 + 16x_4l + 64l^2 \equiv a \pmod{32}$, 即 $x_4^2 + 16x_4l \equiv a \pmod{32}$, 即 $x_4^2 + 16l \equiv a \pmod{32}$, 即 $16l \equiv a - x_4^2 \pmod{32}$, 从而

$$l \equiv \frac{a - x_4^2}{16} \pmod{2}, \quad \text{i.e.,} \quad l = 2s + (\frac{a - x_4^2}{16} \pmod{2}), (s \in \mathbb{Z})$$

这样, 方程 $x^2 \equiv a \pmod{32}$ 的解就是(4个):

$$\{\pm(x_4 + 8 \cdot (2s + (\frac{a - x_4^2}{16} \pmod{2})))\} = \{\pm(x_4 + 16s + 8 \cdot (\frac{a - x_4^2}{16} \pmod{2}))\}, s \in \mathbb{Z}.$$

这个过程可以继续下去, 最终求出 $x^2 \equiv a \pmod{2^\delta}$ 的解(4个). \diamond

示例: 求解 $x^2 \equiv 57 \pmod{64}$

$64 = 2^6$, $57 \equiv 1 \pmod{8}$, 所以原同余方程 $x^2 \equiv 57 \pmod{2^6}$ 有解:
从方程 $x^2 \equiv 57 \pmod{2^3}$ 开始: 其解为

$$\pm(1 + 4k), k \in \mathbb{Z}$$

方程 $x^2 \equiv 57 \pmod{2^4}$ 的解: 将 $(1 + 4k)$ 代入 $x^2 \equiv 57 \pmod{2^4}$ 求出 k ,

$$k = 2l + \left(\frac{a-1}{8} \pmod{2}\right) = 2l + 1, \quad \pm(1 + 4(2l + 1)) = \pm(5 + 8l), l \in \mathbb{Z}$$

方程 $x^2 \equiv 57 \pmod{2^5}$ 的解: 将 $(5 + 8l)$ 代入 $x^2 \equiv 57 \pmod{2^5}$ 求出 l ,
 $(5 + 8l)^2 = 25 + 16 \cdot 5l + 64l^2$, 所以 $16 \cdot 5l \equiv a - 25 \pmod{32}$, 即

$$5l \equiv \frac{a-25}{16} \pmod{2}, \quad i.e., l \equiv \frac{a-25}{16} \pmod{2}$$

$$\therefore l = 2s + \left(\frac{a-25}{16} \pmod{2}\right) = 2s, \quad \pm(5 + 8(2s)) = \pm(5 + 16s), s \in \mathbb{Z}$$

方程 $x^2 \equiv 57 \pmod{2^6}$ 的解: 将 $(5 + 16s)$ 代入 $x^2 \equiv 57 \pmod{2^6}$ 求出 s ,
 $(5 + 16s)^2 = 25 + 32 \cdot 5s + 256s^2$, 所以 $32 \cdot 5s \equiv a - 25 \pmod{64}$, 即

$$5s \equiv \frac{a - 25}{32} \pmod{2} \quad i.e., s \equiv \frac{a - 25}{32} \pmod{2},$$

$$\therefore s = 2t + \left(\frac{a - 25}{32} \pmod{2}\right) = 2t + 1, \quad \pm(5 + 16(2t + 1)) = \pm(21 + 32t), t \in \mathbb{Z}$$

$$21 + 32 = 53, -21 \equiv 43 \pmod{64}, -53 \equiv 11 \pmod{64}$$

也就是说, 方程 $x^2 \equiv 57 \pmod{64}$ 的解为 $x \equiv 21 \pmod{64}$, $x \equiv 53 \pmod{64}$, $x \equiv 43 \pmod{64}$,
 $x \equiv 11 \pmod{64}$. \diamond

至此, 关于二次方程我们得到的结论是:

- ① 模素数的二次方程 $x \equiv a \pmod{p}$ 的解的判定与求解;
- ② 模为 2^δ 的二次方程 $x \equiv a \pmod{2^\delta}$ 的解的判定与求解(有解的话, 解数为4, 从 $x^2 \equiv a \pmod{2^3}$ 开始求解);
- ③ 模为 p^α 的二次方程 $x \equiv a \pmod{p^\alpha}$ 的解的判定与求解(有解的话, 解数为2, 从 $x^2 \equiv a \pmod{p}$ 开始求解);
- ④ 模为合数的二次方程 $x^2 \equiv a \pmod{m}$ (a 与 m 互素) 的解的判定与求解(利用2与3).

一次同余方程 $ax \equiv b \pmod{m}$

一次同余方程组-孙子定理.

