



1. 剩余系：模 m 的剩余系： C_0, C_1, \dots, C_{m-1} ，下标代表着模 m 余几。
2. 完全剩余系：从每个模 m 的剩余系中选一个，且这些数两两不互质。完全剩余系的个数为 m 。
例： $m=5$ 的完全剩余系： $0, 1, 2, 3, 4; -5, 1, 2, 3, 4$ 。
3. 非负最小完全剩余系。
例： $m=5$: $0, 1, 2, 3, 4$; $m=9$: $0, 1, 2, 3, 4, 5, 6, 7, 8$ 。
4. 简化剩余系(缩系)。
个数为 $\varphi(m)$ 。
求法：求 $m=8$ 。
 $m=8$ 的完全剩余系： $0, 1, 2, 3, 4, 5, 6, 7$ 。其中与 8 互素的有 $1, 3, 5, 7$ 。
还能列举多个，但个数始终为 $\varphi(m)$ 。
5. 如果一个剩余类中有一个数与 m 互质，那么该剩余类中所有的数都与 m 互质
- b. 平方剩余与平方非剩余
模 $p=7$ 时。
 $1^2 \equiv 1 \pmod{7}, 2^2 \equiv 4 \pmod{7}, 3^2 \equiv 2 \pmod{7}, 4^2 \equiv 2 \pmod{7}, 5^2 \equiv 4 \pmod{7},$
 $6^2 \equiv 1 \pmod{7}$ 。
故模 7 的平方剩余是 $1, 2, 4$ ，平方非剩余是 $3, 5, 6$ 。

7. 求逆元：

$ax \equiv 1 \pmod{p}$ ， a 就是 x 的逆元，记为 x^{-1}

例：求 $a=5, p=14$ 的逆元。

$$5x \equiv 1 \pmod{14}.$$

$$14 - 5 \times 2 = 4$$

$$5 - 4 \times 1 = 1$$

代入 $4 = 14 - 5 \times 2$, $5 - (14 - 5 \times 2) \times 1 = 1$, 即 $5 \times 3 - 14 = 1$. 故逆元为3.

例： $a=5, p=18$

$$5x \equiv 1 \pmod{18}$$

$$3 = 18 - 3 \times 5$$

$$2 = 5 - 1 \times 3$$

$$1 = 3 - 1 \times 2$$

$$1 = 3 - 1 \times (5 - 1 \times 3) = 2 \times 3 - 1 \times 5$$

$$= 2 \times (18 - 3 \times 5) - 1 \times 5$$

$$= 2 \times 18 - 7 \times 5$$

故逆元为-7, $(-7) + 18 = 1$

补充：求形如 $ax \equiv n \pmod{p}$ 的式子。

例： $3x \equiv 4 \pmod{5}$.

① 先求逆元 x^{-1}

$$2 = 5 - 3 \times 1$$

$$1 = 3 - 2 \times 1$$

$$= 3 - (5 - 3 \times 1) = 3 \times 2 - 5$$

故逆元为2.

② 求 $x^{-1} \cdot n$

$$x^{-1} \cdot n = 2 \times 4 = 8.$$

③ 求 $x^{-1} \cdot n \% p$

$$8 \% 5 = 3$$

故 $3x \equiv 4 \pmod{5} \Rightarrow x = 3$

8. 欧拉定理:

若 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$

例: $3^4 \equiv ? \pmod{5}$.

$\varphi(5) = 4$, 且 $(3, 5) = 1$, 故 $3^{6(5)} \equiv 1 \pmod{5}$. 即 $3^4 \equiv 1 \pmod{5}$

9. 指数与原根.

设 $m > 1$, 若 $(a, m) = 1$, 则使得 $a^e \equiv 1 \pmod{m}$ 成立的最小正整数 e 叫作 a 对模 m 的指数(或阶).
记作 $\text{ord}_m(a)$. 若 a 的指数 e 等于 $\varphi(m)$, 则 a 叫作模 m 的原根

例: $a=2, m=7$.

$2^e \equiv 1 \pmod{7}$, 得 $e=3$. 故 3 是 2 对模 7 的指数($\text{ord}_7(2)=3$).

$\varphi(7) = 7 - 1 = 6 \neq 3$, 故 2 不是模 7 的原根

10. 指数的性质:

设 $m > 1$, $(a, m) = 1$, d 为正整数, 则 $a^d \equiv 1 \pmod{m} \Leftrightarrow \text{ord}_m(a) | d$. 即 $d = ne$, n 为正整数

例: $2^e \equiv 1 \pmod{7}$, $e=3$

$$2^{ne} \equiv 1 \pmod{7}, \text{ 即 } 2^3, 2^6, 2^9, 2^{12} \equiv 1 \pmod{7}$$

11. 费马小定理:

设 p 为素数, 则对于每个整数 a , 有 $a^p \equiv a \pmod{p}$

例: 设 $p=3$, $a=2$, $2^3 \equiv 2 \pmod{3}$

设 $p=5$, $a=4$, $4^5 \equiv 4 \pmod{5}$

12. 威尔逊定理

设 p 是一个素数, 则 $(p-1)! \equiv -1 \pmod{p}$

例: $p=5$, $(5-1)! \equiv -1 \pmod{5}$, $4! \equiv -1 \pmod{5}$

模素数(非素数)原根的查找

一、模的是素数

定理: 设 P 为奇素数, $P-1$ 的所有不同素因数是 q_1, \dots, q_s , 则 g 是模 P 原根的充要条件: $g^{\frac{P-1}{q_i}} \not\equiv 1 \pmod{P}$

例: 求模 $P=17$ 的所有原根.

$P-1 = 16 = 2^4$, 故 $P-1$ 的素因数为 2. 只要判断 $g^{\frac{P-1}{2}} \not\equiv 1 \pmod{P}$, 即 $g^8 \not\equiv 1 \pmod{17}$.

取 $g = 2, 3, 4, \dots$ ($g, P) = 1$

$$2^8 = (2^4)^2 \equiv 1 \pmod{17}$$

$$3^8 = (3^4)^2 \equiv 16 \pmod{17}$$

故 3 是最小原根, 所有原根为 $3^k \pmod{17}$, k 为与 16 互质的数 (3, 5, 7, 9, 11, 13, 15) 共 7 个.

二、模的是非素数：

例：求模 $P=81$ 的所有原根。

81不是素数，是形如 P^α 的数，要先求模 P' 的原根。（书 P82 定理 5.2.3, 5.2.4），即求到了 P^α 的原根。

$81 = 3^4$ ，先求模 3 的原根。

3 是素数， $3-1=2$ 。验证 $9^{\frac{1}{2}} \not\equiv 1 \pmod{3}$ ，且 $(3, 9)=1$ 的 9 有 1, 2。 $1 \equiv 1 \pmod{3}$, $2 \not\equiv 1 \pmod{3}$ 。
故 2 是 3 的原根，也是 3^2 的原根，更是 $3^4, 3^{2^2}$ 的原根。

模 81 的所有原根即 $3^k \pmod{81}$ ， k 是与 80 互质的所有数。

例6. 求解一次同余方程 $60x \equiv 7 \pmod{37}$.

$$\text{(1)} (37, 60)$$

$$60 = 37 \times 1 + 23$$

$$37 = 23 \times 1 + 14$$

$$23 = 14 \times 1 + 9$$

$$14 = 9 \times 1 + 5$$

$$9 = 5 \times 1 + 4$$

$$5 = 4 \times 1 + 1 \quad (\text{解到余数为1止})$$

$$1 = 5 - 4 \times 1$$

$$= 5 - (9 - 5 \times 1) = 2 \times 5 - 9 \times 1$$

$$= 2 \times (14 - 9 \times 1) - 9 \times 1$$

$$= 2 \times 14 - 3 \times 9$$

$$= 2 \times 14 - 3 \times (23 - 14 \times 1)$$

$$= 5 \times 14 - 3 \times 23$$

$$= 5 \times (37 - 23 \times 1) - 3 \times 23 = 5 \times 37 - 8 \times 23$$

$$\begin{aligned} & 5 \times 37 - 8 \times 23 \\ & = 5 \times 37 - 8 \times (60 - 37 \times 1) \\ & = 13 \times 37 - 8 \times 60 \\ & \text{故逆元为}-8. \\ & -8 \times 7 = -56 \\ & -56 \% 37 = 18 \end{aligned}$$

利用扩展的欧几里得算法得 $60^{-1} \equiv -8 \pmod{37}$
故该同余方程的解为 $x \equiv -56 \equiv 18 \pmod{37}$

例7. 2004年9月8日是周三，问 2^{2005} 天后是周几？

①先求 $2^e \equiv 1 \pmod{7}$ ，即 $\text{ord}_7(2)$ 是几。

得 $e=3$ 。

$$2^{2005} = (2^3)^{668} \times 2$$

$2^3 \equiv 1 \pmod{7}$ ，则 $(2^3)^{668} \equiv 1 \pmod{7}$ 。

故 $2^{2005} \equiv 2 \pmod{7}$ ， 2^{2005} 天后是周五

1. 中国剩余定理.

设 m_1, m_2, \dots, m_k 两两互素，则对任意 k 个整数 b_1, b_2, \dots, b_k ，下列同余方程

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

必有解 x ，且解 $x = M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 + \dots + M_k M_k^{-1} b_k$.

其中 $M = m_1 m_2 \dots m_k$, $M_i = m_{i+1} \cdot m_{i+2} \dots m_k$ (即除了 m_i 外其余 m 相乘), M_i^{-1} 是使得 $M_i \cdot M_i^{-1} \equiv 1 \pmod{m_i}$ 的数

例. $\begin{cases} 7x \equiv 5 \pmod{18} \\ 13x \equiv 2 \pmod{15} \end{cases}$

解. $18 = 2 \times 9$, $15 = 3 \times 5$. 故方程写为

故 $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{9} \\ x \equiv 4 \pmod{5} \end{cases}$

$$\begin{array}{c} \left\{ \begin{array}{l} 7x \equiv 5 \pmod{2} \\ 7x \equiv 5 \pmod{9} \end{array} \right. \xrightarrow{\text{求解}} \left\{ \begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{9} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x \equiv 2 \pmod{9} \\ x \equiv 2 \pmod{3} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{9} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{array} \right. \\ -2 \end{array}$$

$$m = 2 \times 9 \times 5 = 90, M_1 = 45, M_2 = 10, M_3 = 18, \text{ 能 } 45M_1^{-1} \equiv 1 \pmod{2}, 10M_2^{-1} \equiv 1 \pmod{9}, 18M_3^{-1} \equiv 1 \pmod{5}$$

$$\text{得 } M_1^{-1} \equiv 1 \pmod{2}, M_2^{-1} \equiv 1 \pmod{9}, M_3^{-1} \equiv 2 \pmod{5}$$

$$\text{故 } x \equiv 45b_1 + 10b_2 + 36b_3 \pmod{90}$$

$$\equiv 209 \pmod{90} \equiv 29 \pmod{90}$$

$$x \equiv M_1 M_1^{-1} b_1 + M_2 M_2^{-1} b_2 + \dots \pmod{m}$$

2. 模重复平方算法：计算（例如 $b^n \pmod{m}$ ）。

例：计算 $12996^{227} \pmod{37909}$

① 将指数 227 写成二进制。 $227 = 128 + b^4 + 32 + 2 + 1 = 2^0 + 2^1 + 2^5 + 2^6 + 2^7$

② 将各项系数写出， $1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7$ 系数为 (11000111)

③ 将 12996^{227} 拆分， $12996^{227} = (12996^{2^0}) \cdot (12996^{2^1}) \cdot (12996^{2^5}) \cdot (12996^{2^6}) \cdot (12996^{2^7})$

④ 令 $a=1$ ，若二进制式第一个系数为 1，则计算 $a_0 \equiv a \cdot b \pmod{m}$ ，否则 $a_0 = a$ ， $b_{k-1} = b^{2^{k-1}} = b^2 \cdot b_{k-2}$

例：计算 $501^{13} \pmod{667}$

$$13 = 1 + 2^2 + 2^3 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3, (1011).$$

(1) $n_0=1$, $a_0=a \cdot b \equiv 501$, $b_1=b^2 \equiv 209 \pmod{667}$.

(2) $n_1=0$, $a_1=a_0 \equiv 501$, $b_2=b_1^2 \equiv 326 \pmod{667}$.

(3) $n_2=1$, $a_2=a_1 \cdot b_2 \equiv 578$, $b_3=b_2^2 \equiv 223 \pmod{667}$

(4) $n_3=1$, $a_3=a_2 \cdot b_3 \equiv 163 \pmod{667}$,

故 $501^{13} \equiv 163 \pmod{667}$.

3. 二次同余式

① 欧拉判别条件：设 P 为奇素数， $(a, P) = 1$ ，则 a 是模 P 的平方剩余的条件是 $a^{\frac{P-1}{2}} \equiv 1 \pmod{P}$ ，平方非剩余的条件是 $a^{\frac{P-1}{2}} \equiv -1 \pmod{P}$ 。 $\left(\frac{a}{P}\right) = 1, \left(\frac{a}{P}\right) = -1, x^2 \equiv a \pmod{P}$ 有解/无解。

4. 勒让得符号

① $\left(\frac{a}{P}\right) = \begin{cases} 1, & \text{若 } a \text{ 是模 } P \text{ 的平方剩余, } x^2 \equiv a \pmod{P} \text{ 有解} \\ -1, & \text{若 } a \text{ 是模 } P \text{ 的平方非剩余, } x^2 \equiv a \pmod{P} \text{ 无解} \\ 0, & P | a. \end{cases}$

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

$$③ \text{若 } P \text{ 为奇素数, } \begin{cases} \left(\frac{1}{P}\right) = 1 \\ \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}} \end{cases}$$

$$④ \left(\frac{a+p}{P}\right) = \left(\frac{a}{P}\right)$$

$$⑤ \left(\frac{a \cdot b}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right)$$

$$⑥ \text{若 } (a, P) = 1, \text{ 则 } \left(\frac{a^2}{P}\right) = 1.$$

$$⑦ \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$$

⑧ 二次互反律：

$$\text{若 } P, q \text{ 为互素奇素数, 则 } \left(\frac{q}{P}\right) = (-1)^{\frac{(P-1)(q-1)}{4}} \cdot \left(\frac{P}{q}\right).$$

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

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

$$\left(\frac{1}{P}\right) = 1$$

例 判断 $x^2 \equiv 13 \pmod{227}$ 是否有解.

$$\left(\frac{13}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right) \cdot \left(\frac{90}{227}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{2 \cdot 3^2 \cdot 5}{227}\right) = (-1) \cdot \left(\frac{2}{227}\right) \cdot \left(\frac{5}{227}\right).$$

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

$$\left(\frac{5}{227}\right) = (-1)^{\frac{4 \times 226}{4}} \left(\frac{227}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2 - 1}{8}} = -1$$

$$\text{故 } \left(\frac{13}{227}\right) = (-1) \cdot (-1) \cdot (-1) = -1$$

4. 群

1. 判断群的几个步骤
群 G 中结合法满足以下三个条件.

① 结合律: $\forall a, b \in G$, 有 $(ab)c = a(bc)$.

② 单位元: (得本身) 设非空集合中有一个元素 e , 使得 $\forall a \in G$, 都有 $ea = ae = a$ e 即为 S 中的单位元.

③ 可逆性: (得逆元): $\forall a \in G$, 都存在 $a' \in G$, 有 $aa' = a'a = e$, a' 记为 a^{-1}

2. 加群和乘群:

G 中结合法写作乘法时叫乘群, 加法称加群.

3. 群中元素个数称为群 G 的阶, $|G|$, $|G|$ 有限叫有限群, 无限叫无限群

4. 交换群: 若 G 中结合法还满足交换律的群

5. 子群:

H 为群 G 的子集合, 若对于群 G 的结合法, H 成为一个群, 则 H 称为群 G 的子群.

6. 判断子群:

对 $\forall a, b \in H$, 有 $ab^{-1} \in H$, 则 H 是群 G 的一个子群

7. 循环群中元素的阶:

设循环群 $|G|=n$, 对任意元素 $g=a^k \in G$, ($k \in \mathbb{Z}$), $|g|$ 满足

$$|\alpha^k| = \frac{n}{\text{gcd}(n, k)}, \text{ 当 } G \text{ 为有限循环群}$$

$$\begin{cases} k=0 \text{ 时, 阶为 } 1, \text{ 否则 } |\alpha^k| = \infty \end{cases}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}$$

8. 循环群中生成元的个数.

循环群的阶 $|G|=n$, 则生成元的个数为 $\varphi(n)$, 生成元为与 n 互质的数

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}$$

例: 求循环群 \mathbb{Z}_6 的元素的阶和生成元个数.

$\mathbb{Z}_6 = \langle 1 \rangle$. 模 6 加法群, 群中元素为 $\{0, 1, 2, 3, 4, 5\}$, $|G|=6$. $\varphi(6)=2$. 故生成元为 1, 5, 共 2 个.

元素 0 为单位元, 阶为 1

$$1: (1, 6) = 1, \frac{6}{1} = 6$$

$$2: (2, 6) = 2, \frac{6}{2} = 3$$

$$3: (3, 6) = 3, \frac{6}{3} = 2$$

$$4: (4, 6) = 2, \frac{6}{2} = 3$$

$$5: (5, 6) = 1, \frac{6}{1} = 6$$

$$|\alpha^k| = \frac{n}{\text{gcd}(n, k)}$$

例: 证明: 群 G 是交换群的充要条件是 $\forall a, b \in G$, 有 $(ab)^2 = a^2b^2$.

必要性: $ab = ba$. $(ab)^2 = abab = aabb = a^2b^2$, 故 $(ab)^2 = a^2b^2$.

充分性: $(ab)^2 = a^2b^2$, 展开: $abab = aabb \Rightarrow a^{-1}ababb^{-1} = a^{-1}aabb b^{-1} \Rightarrow ba = ab$.

9. 同态基本定理:

G, G' 为群, f 为 G 到 G' 的一个映射, $\forall a, b \in G$, 有 $f(ab) = f(a)f(b)$, f 叫作 G 到 G' 的一个同态.

10. 置换:

例 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 2 & 6 & 1 \end{pmatrix}$, 计算 $\sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1^{-1}$

$\sigma_1\sigma_2$ 从右到左作用, $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{pmatrix}$, $\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 6 & 1 & 5 \end{pmatrix}$.

σ_1^{-1} : 找第一行数字对应的第二行数字对应的第几行数字.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

环

1. 判定条件：对于一个具有两种结合法的非空集合 R , 若以下条件成立.

① R 对于加法构成一个交换群

结合律
单位元
可逆性
交换律

(对于加法来说的)

② 结合律: $\forall a, b, c \in R, (ab)c = a(bc)$

③ 分配律: $\forall a, b, c \in R, (a+b)c = ac+bc, a(cb+c) = ab+ac$ (对乘法来说的分配律)

2. 交换环

若除了满足上面的之外, 还满足 $\forall a, b \in R$, 有 $ab = ba$.

3. 零因子环

设 R 是环, R 中非零元 a 称为左零因子, 若存在非零元 $b \in R$, 使得 $ab = 0$, a 称为零因子,
若同时存在左零因子和右零因子, R 则为零因子环.

4. 整环

整环
有单位元
无零因子.

5. 环同态

$$\begin{cases} \forall a, b \in R, \text{ 有 } f(a+b) = f(a) + f(b) \\ \forall a, b \in R, \text{ 有 } f(ab) = f(a)f(b) \end{cases}$$

6. 多项式欧几里得除法

$$\text{设 } f(x) = x^4 + 3x^3 - 2x^2 + 5x - 1, g(x) = x^2 + 2x - 1$$

①首项相除, $\frac{x^4}{x^2} = x^2$

②乘回 $g(x)$, 并作相减

$$f(x) - x^2 g(x) = x^3 - x^2 + 5x - 1$$

③重复步骤④, 直到相减结果的最高次数小于 $g(x)$. (用相减得到的式子的最高次项除 $g(x)$ 的)

i. $\frac{x^3}{x^2} = x$, $x g(x) = x^3 + 2x^2 - x$.

$$x^3 - x^2 + 5x - 1 - (x^3 + 2x^2 - x) = -3x^2 + 6x - 1$$

ii. $\frac{-3x^2}{x^2} = -3$, $(-3x^2 + 6x - 1) - (-3x^2 - 6x + 3) = 12x - 4$

此时 $12x - 4$ 的次数小于 $g(x)$. 停止.

$$x^4 + 3x^3 - 2x^2 + 5x - 1 = (x^2 + x - 3)(x^2 + 2x - 1) + (12x - 4)$$

欧几里得与拓展欧几里得算法

$$(121, 169)$$

$$169 = 1 \times 121 + 48$$

$$121 = 2 \times 48 + 25$$

$$48 = 1 \times 25 + 23$$

$$25 = 1 \times 23 + 2$$

$$23 = 11 \times 2 + 1$$

$$2 = 2 \times 1 + 0$$

$$\text{故 } (121, 169) = 1$$

$$1 = 23 - 11 \times 2$$

$$= 23 - 11 \times (25 - 1 \times 23)$$

$$= -11 \times 25 + 12 \times 23$$

$$= -11 \times 25 + 12 \times (48 - 1 \times 25)$$

$$= 12 \times 48 - 23 \times 25$$

$$= 12 \times 48 - 23 \times (121 - 2 \times 48)$$

$$= 58 \times 48 - 23 \times 121$$

$$= 58 \times (169 - 1 \times 121) - 23 \times 121$$

$$= 58 \times 169 - 81 \times 121$$

$$\text{故 } S = -81, \quad t = 58$$

模重复平方算法:

$$312^{13} \pmod{667}$$

$$13 = 8 + 4 + 1 = 1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$$

$$\text{系数}(1011), \text{令 } a_1 = 1, b_1 = 312.$$

$$\text{当 } n_0 = 1, \quad a_0 = ab = 312 \pmod{667}, \quad b_0 = b^2 = 129 \pmod{667}$$

$$n_1 = 0, \quad a_1 = a_0 = 312 \pmod{667}, \quad b_1 = b_0^2 = 110 \pmod{667}.$$

$$n_2 = 1, \quad a_2 = a_1 b_1 = 303 \pmod{667}, \quad b_2 = b_1^2 = 94 \pmod{667}$$

$$n_3 = 1, \quad a_3 = a_2 b_2 = 468 \pmod{667}$$

$$\text{故 } 312^{13} \equiv 468 \pmod{667}.$$

中国剩余定理:

$$\begin{cases} 7x \equiv 5 \pmod{18} \\ 13x \equiv 2 \pmod{15} \end{cases} \Rightarrow \begin{cases} 7x \equiv 5 \pmod{2} \\ 7x \equiv 5 \pmod{9} \end{cases} \Rightarrow \begin{cases} X \equiv 1 \pmod{2} \\ X \equiv 2 \pmod{9} \end{cases} \Rightarrow \begin{cases} X \equiv 1 \pmod{2} \\ X \equiv 2 \pmod{3} \\ X \equiv 4 \pmod{5} \end{cases}$$

求 $P=53$ 的原根.

$$53-1=52=2^2 \times 13, \text{ 故因数为 } 2, 13.$$

$$\text{证 } g^{\frac{52}{2}} \not\equiv 1 \pmod{53} = g^{26} \not\equiv 1 \pmod{53}$$

$$\text{证 } g^{\frac{52}{13}} \not\equiv 1 \pmod{53} = g^4 \not\equiv 1 \pmod{53}$$

$$\text{令 } g=2, 3, \dots$$

$$2^{2b} \equiv -1 \pmod{53}$$

故最小原根为 2, 所有原根为 $2^k \pmod{53}$

k 与 52 互质的数总个数为 $\varphi(\varphi(53))$

$$m = 2 \times 9 \times 5 = 90 \quad M_1 = 45 \quad M_2 = 10 \quad M_3 = 18.$$

$$45M_1^{-1} \equiv 1 \pmod{2} \quad 10M_2^{-1} \equiv 1 \pmod{9} \quad 18M_3^{-1} \equiv 1 \pmod{5}.$$

$$M_1^{-1} \equiv 1 \pmod{2} \quad M_2^{-1} \equiv 1 \pmod{9} \quad M_3^{-1} \equiv 2 \pmod{5}.$$

$$X \equiv 1 \cdot 45 \times 1 + 2 \times 1 \times 10 + 4 \times 18 \times 2 \pmod{90}$$

$$\equiv 209 \pmod{90}$$

$$\equiv 19 \pmod{90}.$$

求 $P=17$ 的原根

$$P-1 = 16 = 2^4, P-1 \text{ 的素因数为 } 2, \frac{16}{2} = 8.$$

只要证 $g^8 \not\equiv 1 \pmod{17}$, 则 g 是最小原根.

令 $g = 2, 3, 4, \dots$

$$2^8 = (2^4)^2 \equiv 1 \pmod{17}$$

$$(3^8) \equiv (3^4)^2 \equiv 1 \pmod{17}, \text{ 故 } 3 \text{ 是最小原根.}$$

故 $\forall n$ 的所有原根为 $3^k \pmod{17}$, k 是与 16 互质的数.

$$\text{故有 } \varphi(\varphi(17)) \quad \varphi(16) = \varphi(2^4) = \varphi(2^4) - \varphi(2^3) = 8.$$

$$x^2 \equiv 13 \pmod{227}$$

$$\left(\frac{13}{227}\right) = \left(\frac{-90}{227}\right) = \left(\frac{-1}{227}\right) \left(\frac{90}{227}\right) = (-1)^{\frac{227-1}{2}} \cdot \left(\frac{2 \times 3 \times 5}{227}\right)$$

$$(-1)^{113} = (-1) \cdot \left(\frac{2}{227}\right) = (-1)^{\frac{227-1}{8}} = 1$$

$$\begin{aligned} \left(\frac{3}{227}\right) &= 1 & \left(\frac{5}{227}\right) &= (-1)^{\frac{227-4}{8}} \cdot \left(\frac{227}{5}\right) \\ &= \left(\frac{2}{5}\right) = (-1)^{\frac{5-1}{8}} = -1 \end{aligned}$$

$$\text{故 } \left(\frac{13}{227}\right) = -1, \text{ 故 } x^2 \equiv 13 \pmod{227} \text{ 无解.}$$