

$$527 \div 1411 = 0 \text{ 余 } 527$$

一:

1. 由辗转相除法:

$$527 = 0 \times 1411 + 527$$

$$1411 = 2 \times 527 + 357$$

$$527 = 1 \times 357 + 170$$

$$357 = 2 \times 170 + 17$$

$$170 = 10 \times 17 + 0$$

$$\therefore (527, 1411) = 17$$

$$\text{而 } [a, b] = \frac{ab}{(a, b)} = \frac{527 \times 1411}{17} = 43741$$

$$\therefore [527, 1411] = 43741$$

$$2. \quad x^2 \equiv 30 \pmod{41}$$

$$\text{勒让得符号为 } \left(\frac{30}{41}\right) = \left(\frac{2}{41}\right) \left(\frac{5}{41}\right) \left(\frac{3}{41}\right)$$

$$\left(\frac{2}{41}\right) = (-1)^{\frac{41^2-1}{8}} = 1$$

$$(5, 41) = 1$$

$$(3, 41) = 1$$

由二次互反律

$$\left(\frac{5}{41}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{41-1}{2}} \left(\frac{1}{5}\right) = 1$$

$$\left(\frac{3}{41}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{41-1}{2}} \left(\frac{2}{3}\right) = -1$$

$$\therefore \left(\frac{30}{41}\right) = 1 \cdot 1 \cdot (-1) = -1$$

30 不是模 41 平方剩余 原式无解。



扫描全能王 创建

3.

$F_{23}^* = (\mathbb{Z}/23\mathbb{Z})^*$ 为模 23 的简化剩余系

$\varphi(23) = 22$. 因此群阶为 22.

由原根性质, $g, g^2, \dots, g^{\varphi(m)}$ 构成模 m 的一个简化剩余系.

\therefore 23 的原根 $g = 5$ 为一个 F_{23}^* 生成元.

一共有 $\varphi(22) = 10$ 个生成元, 形式为 g^j , $(j, 22) = 1$

$j = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$

\therefore 生成元 g^j 为 5, 10, 20, 17, 11, 21, 19, 15, 7, 14.

4.

求解 $3x \equiv 4 \pmod{5}$, 将 $x = 0, 1, 2, 3, 4$ 代入得

解为 $x \equiv 3 \pmod{5}$

因此原同余式组等价于

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

由 3, 5, 7 两两互素.

可运用中国剩余定理.

$$m = 3 \times 5 \times 7 = 105$$

$$M_1 = 35, M_1' = 2$$

$$M_2 = 21, M_2' = 1$$

$$M_3 = 15, M_3' = 1$$

\therefore 原同余式组解为 $x \equiv 2 \times 35 \times 2 + 3 \times 21 + 4 \times 15 \pmod{105}$

$\therefore x \equiv 53 \pmod{105}$



5.

$$f(x) = 3x^4 + 17x^3 - 5x + 23 \pmod{25}$$

解: 1) $f(x) \equiv 12x^3 + x^2 + 20 \pmod{25}$

2) 验证 $f(x) \equiv 3x^4 + 2x^3 + 3 \pmod{5}$ 的解.

将 $x = 0 - 4$ 代入 解得

$$x_1 \equiv 3 \pmod{5}$$

3) 将 $x = 3 + 5t_1$ 代入 $f(x) \equiv 0 \pmod{25}$

由定理有

$$f(3 + 5t_1) \equiv f(3) + f'(3)5t_1 \equiv 0 \pmod{5^2=25}$$

$$\Rightarrow f(3) \equiv 10 \pmod{25}$$

$$f'(3) \equiv 3 \pmod{25} \quad \text{故化简为}$$

$$10 + 3 \times t_1 \times 5 \equiv 0 \pmod{25}$$

或者 $2 + 3t_1 \equiv 0 \pmod{5}$

解得 $t_1 \equiv 1 \pmod{5}$

\therefore 原式解为 $x \equiv 3 + 5t_1 \equiv 8 \pmod{25}$

$$x \equiv 8 \pmod{25}$$

6.

$$p = (3, 1), \quad x_1 = 3, \quad y_1 = 1 \pmod{a_4 = 5}, \quad a_6 = 3.$$

求 $2p$: $\lambda = \frac{3 \cdot 9 + 5}{2} = \frac{32}{2} = 16.$

$$\therefore x_3 = 16^2 - 3 - 3 = 250 \equiv 8 \pmod{11}$$

$$y_3 = 16(3 - 250) - 1 = -3953 \equiv 7 \pmod{11}$$

求 $3p = 2p + p.$

$$\lambda = \frac{7 - 1}{8 - 3} = \frac{6}{5} = 6 \times 5^{-1} = 6 \times 9 = 54 \equiv 10 \pmod{11}.$$

$$\therefore x_4 = 10^2 - 3 - 8 \equiv 89 \equiv 1 \pmod{11}$$

$$y_4 = 10(3 - 1) - 1 \equiv 8 \pmod{11}$$

$$\therefore 3p = (1, 8)$$



二:

G 为一个群, $a, b \in G$, $ab = ba$ 由群封闭性 $ab \in G$,

设 ab 的阶为 k , $(ab)^k = e$.

根据题干, $a^m = b^n = e$. 因此 $(a^m)^n (b^n)^m = e$.

由群元阶的性质:

$$k \mid mn.$$

而 $(ab)^k = a^k b^k = e$. 所以 b^k 也是 a^k 的逆元.

设 a 逆元 a^{-1} 于是 $(aa^{-1})^k = e = a^k a^{-k}$

所以 $(a^{-1})^k = a^{-k}$ 也是 a^k 逆元. 根据群逆元唯一性.

$$b^k = a^{-k}.$$

所以 $(b^n)^k = b^{kn} = (a^{-k})^n$ 注意到 $b^n = e$.

所以 $a^{-kn} = e$.

所以 $m \mid (-kn) \Leftrightarrow m \mid kn$ 又根据题干 $(m, n) = 1$

所以 $(m, kn) = (m, k) = m \Rightarrow m \mid k$.

同理, a^k 也是 b^k 的逆元. 于是

$$a^k = b^{-k} \quad \text{由 } a^m = e \Rightarrow a^{km} = b^{-km} = e.$$

所以 $n \mid km$ $(n, km) = n$ 又 $(m, n) = 1$

$$(n, km) = (n, k) = n \Rightarrow n \mid k.$$

由于 $m \mid k$, $n \mid k$ 所以 $[m, n] \mid k$. 而 $(m, n) = 1$

因此 $[m, n] = mn$. 所以 $mn \mid k$.

又之前有 $k \mid mn$, $mn \mid k$

$\therefore k = mn$. 综上, ab 阶 $k = mn$.



三 = 1.

加法表:

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12

乘法表:

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2

2.

1) 密文 $C = M^e \bmod n$

$$\therefore C = 83^{101} \bmod 133$$

根据模重复平方法计算,

101 的二进制表示为 1100101

$$n_0 = 1$$

$$a_0 = a \equiv 83$$

$$b_1 = 83^2 \equiv 106 \pmod{133}$$

$$n_1 = 0$$

$$a_1 = 83$$

$$b_2 = b_1^2 \equiv 64$$

$$n_2 = 1$$

$$a_2 = 125$$

$$b_3 = 106$$

$$n_3 = 0$$

$$a_3 = 125$$

$$b_4 = 64$$

$$n_4 = 0$$

$$a_4 = 125$$

$$b_5 = 106$$

$$n_5 = 1$$

$$a_5 = 83$$

$$b_6 = 64$$

$$n_6 = 1$$

$$a_6 = 125$$

$$b_7 = 106$$

$$\text{因此 } 83^{101} \bmod 133 = 125$$

$$\text{密文 } C = 125$$



扫描全能王 创建

(2).

$$M = c^d \cdot \text{mod } n$$

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$n = 133 \quad e = 101$$

$$133 = 7 \times 19$$

$$\varphi(133) = \varphi(7) \varphi(19) = 108 \text{ 即计算 } 101d \equiv 1 \pmod{108}$$

利用广义欧几里得除法

$$101 = 0 \times 108 + 101$$

$$s[-2] = 1 \quad t[-2] = 0$$

$$108 = 1 \times 101 + 7$$

$$s[-1] = 0 \quad t[-1] = 1$$

$$101 = 14 \times 7 + 3$$

$$s[0] = 1 \quad t[0] = 0$$

$$7 = 2 \times 3 + 1$$

$$s[1] = -1 \quad t[1] = 1$$

$$3 = 3 \times 1 + 0$$

$$s[2] = (-14) \times (-1) + 1 = 15 \quad t[2] = (-14) \times 1 = -14$$

$$s[3] = (-2) \times 15 + 1 = -31 \quad t[3] = 29$$

因此 $(-31) \times 101 + 29 \times 108 = 1$

$$-31 \equiv 77 \pmod{108}$$

$$\therefore d = 77 \quad \text{原解密式即}$$

$$131^{77} \pmod{133}$$

运用模重复平方方法

$$n = 77 = (1001101)_2$$

$$n_0 = 1$$

$$a_0 = 131$$

$$b_1 = 4 \pmod{133}$$

$$n_1 = 0$$

$$a_1 = 131$$

$$b_2 = 16$$

$$n_2 = 1$$

$$a_2 = a_1 b_2 = 101 \quad b_3 = 16^2 \equiv 123$$

$$n_3 = 1$$

$$a_3 = 54$$

$$b_4 = 123^2 \equiv 100$$

$$n_4 = 0$$

$$a_4 = 54$$

$$b_5 = 100^2 \equiv 25$$

$$n_5 = 0$$

$$a_5 = 54$$

$$b_6 = 25^2 \equiv 93$$

$$n_6 = 1$$

$$a_6 = a_5 b_6 \equiv 101$$

因此 $M = 131^{77} \pmod{133} = 101$

明文 $M = 101$



扫描全能王 创建