

《信息安全数学基础》试卷 (A 卷)

学号_____

姓名_____

题号	一	二	三	四	总分
得分					

一、解答题 (共计 25 分)

得分

1. 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 2 & 1 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix}$, 将 $\sigma^{-1}\tau$ 分解成不相交的轮换. (4 分)

解: $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 6 & 3 & 1 \end{pmatrix}$

$\sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 3 & 5 & 2 \end{pmatrix} = (1\ 6\ 2)(3\ 4)$

2. 判断 5 是否为 19 的原根, 并说明理由. (5 分)

解: $\varphi(19) = 18$, $5^{18} \equiv 1 \pmod{19}$

18 的非平凡因子有 2, 3, 6, 9

$\therefore 5^2 \equiv 6 \pmod{19}, 5^3 \equiv 11 \pmod{19}, 5^6 \equiv 7 \pmod{19}, 5^9 \equiv 1 \pmod{19}$

$\therefore 5$ 不是 19 的原根

3. 判断方程 $x^2 \equiv 105 \pmod{1009}$ 是否有解, 给出判断过程(无需求解) (5分)

解: $\left(\frac{105}{1009}\right) = (-1)^{\frac{105-1}{2} \cdot \frac{1009-1}{2}} \left(\frac{64}{105}\right) = \left(\frac{8^2}{105}\right) = 1$
 \therefore 有解.

4. 利用多项式 $x^3 + 2x + 1$ 构造一个有限域, 并写出有限域中元素的个数和有限域的特征 (答案不唯一, 写出一个合理答案即可). (5分)

解: $\frac{\mathbb{Z}_3[x]}{\langle x^3 + 2x + 1 \rangle}$
 元素个数 $= 3^3 = 27$
 特征为 3

5. 设 G 为无限阶循环群, 生成元为 a . 构造从 \mathbb{Z} 到 G 的映射 $f: \mathbb{Z} \rightarrow G$, 满足 $f(n) = a^n, n \in \mathbb{Z}$. 请说明 f 是满同态映射的理由, 并指出同态核 $\ker f$, 最后写出结合上述条件与同态基本定理得到的结论. (6分)

解: $\forall n_1, n_2 \in \mathbb{Z}, f(n_1 + n_2) = a^{n_1 + n_2} = a^{n_1} \cdot a^{n_2} = f(n_1) \cdot f(n_2)$
 对 $\forall b \in G, \exists m \in \mathbb{Z} \text{ s.t. } a^m = b$
 $\ker f = \{0\}$
 $\frac{\mathbb{Z}}{\langle 0 \rangle} \cong G$ (或 $\mathbb{Z} \cong G$)

二、计算题（共计 25 分）

得分

1. 计算 $2^{10000} \pmod{55}$. (5 分)

解: $\varphi(55) = 40$. $10000 = 250 \times 40$

$$2^{10000} \equiv (2^{40})^{250} \equiv 1^{250} \equiv 1 \pmod{55}$$

2. 设 \mathbb{Z}_{23} 上的椭圆曲线为 $E: y^2 = x^3 + 3x + 1$, $P = (5, 7)$ 是其上一点

(1) 求点 $2P$ 的坐标; (5 分)

(2) 求点 $3P$ 的坐标; (5 分)

(3) 求点 $5P$ 的阶. (10 分)

解: (1) $k \equiv \frac{3 \times 5^2 + 3}{2 \times 7} \equiv \frac{39}{7} \equiv \frac{39}{7} \times 70 \equiv -1 \pmod{23}$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 1 - 5 - 5 \equiv 14 \pmod{23} \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv -(5 - 14) - 7 \equiv 2 \pmod{23} \end{cases}$$

$$\therefore 2P = (14, 2)$$

(2) $3P = 2P + P$

$$k \equiv \frac{7 - 2}{5 - 14} \equiv -\frac{5}{9} \equiv -\frac{5}{9} \times 162 \equiv 2 \pmod{23}$$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 4 - 5 - 14 \equiv 8 \pmod{23} \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv 2(5 - 8) - 7 \equiv 10 \pmod{23} \end{cases}$$

$$\therefore 3P = (8, 10)$$

(3) $5P = 3P + 2P$

$$k \equiv \frac{10 - 2}{8 - 14} \equiv -\frac{4}{3} \equiv -\frac{4}{3} \times 24 \equiv 14 \pmod{23}$$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 14^2 - 14 - 8 \equiv 13 \pmod{23} \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv 14(14 - 13) - 2 \equiv 12 \pmod{23} \end{cases}$$

$$\therefore 5P = (13, 12)$$

$$10P = 5P + 5P$$

$$k \equiv \frac{3 \times 13^2 + 3}{2 \times 12} \equiv \frac{81}{4} \equiv \frac{81}{4} \times 24 \equiv 4 \pmod{23}$$

$$\begin{cases} x_3 \equiv k^2 - x_1 - x_2 \equiv 4^2 - 13 - 13 \equiv 13 \pmod{23} \\ y_3 \equiv k(x_1 - x_3) - y_1 \equiv 4(13 - 13) - 12 \equiv 11 \pmod{23} \end{cases}$$

$$\therefore 10P = (13, 11)$$

$$15P = 10P + 5P, k \equiv \frac{12 - 11}{13 - 13} = \infty$$

$$\therefore 5P \text{ 的阶为 } 3.$$

三、应用题（共 15 分）

得分	
----	--

Rabin 是一种公钥密码算法，主要参数如下：私钥为 (p, q) (p 和 q 为素数)，公钥为 $n = p \times q$ ，明文为 m ，密文为 c 。

加密过程为： $c = m^2 \pmod{n}$

解密过程为：求解方程 $x^2 = c \pmod{n}$

现已知 $p = 19, q = 23$ ，请根据所学的数学知识回答下面两个问题：

1. 设明文消息为 66，求对应的密文。（3 分）

2. 计算上一问中的密文所对应的 4 个可能的明文（12 分）

解： 1. $c \equiv 66^2 \equiv 423 \pmod{437}$

2. 解方程 $x^2 \equiv 423 \pmod{437}$

可转化为 $\begin{cases} x^2 \equiv 5 \pmod{19} \\ x^2 \equiv 9 \pmod{23} \end{cases} \Rightarrow \begin{cases} x \equiv \pm 9 \pmod{19} \\ x \equiv \pm 3 \pmod{23} \end{cases}$

$$\therefore \begin{cases} x \equiv 9 \pmod{19} \\ x \equiv 3 \pmod{23} \end{cases}$$

$$x \equiv 23 \times 5 \times 9 + 19 \times 17 \times 3 \equiv 256 \pmod{437}$$

$$\begin{cases} x \equiv 9 \pmod{19} \\ x \equiv -3 \pmod{23} \end{cases}$$

$$\therefore x \equiv 23 \times 5 \times 9 + 19 \times 17 \times (-3) \equiv 66 \pmod{437}$$

$$\begin{cases} x \equiv -9 \pmod{19} \\ x \equiv 3 \pmod{23} \end{cases}$$

$$\therefore x \equiv 23 \times 5 \times (-9) + 19 \times 17 \times 3 \equiv 371 \pmod{437}$$

$$\begin{cases} x \equiv -9 \pmod{19} \\ x \equiv -3 \pmod{23} \end{cases}$$

$$\therefore x \equiv 23 \times 5 \times (-9) + 19 \times 17 \times (-3) \equiv 181 \pmod{437}$$

\therefore 可能的明文是 66, 181, 256, 371 $\pmod{437}$

四、证明题（共计 35 分）

得分	
----	--

1. 设 n 是一个正整数，证明：

(1) $42 | (n^7 - n)$ (7 分)

(2) $\varphi(2n) = \begin{cases} \varphi(n) & n \text{ 为奇数} \\ 2\varphi(n) & n \text{ 为偶数} \end{cases}$ (7 分)

证明：(1) 根据费马小定理 $n^7 \equiv n \pmod{7}$, $n^3 \equiv n \pmod{3}$
 $n^2 \equiv n \pmod{2}$

$$\therefore n^7 = (n^2)^3 \cdot n = (n^3)^2 \cdot n$$

$$\therefore n^7 \equiv n^2 \cdot n \equiv n^3 \equiv n \pmod{3}$$

$$n^7 \equiv (n^2)^3 \cdot n \equiv n^3 \cdot n \equiv n^4 \equiv (n^2)^2 \equiv n^2 \equiv n \pmod{2}$$

$$\therefore n^7 \equiv n \pmod{42}. \text{ 即 } 42 | (n^7 - n)$$

(2) n 为奇数时, $(2, n) = 1 \therefore \varphi(2n) = \varphi(2) \cdot \varphi(n) = \varphi(n)$.

n 为偶数时, 设 $n = 2^s \cdot t$, t 为奇数.

$$\begin{aligned} \varphi(2n) &= \varphi(2^{s+1} \cdot t) = \varphi(2^{s+1}) \varphi(t) \\ &= 2^s \cdot \varphi(t) \\ &= 2 \cdot 2^{s-1} \varphi(t) \\ &= 2 \cdot \varphi(2^s) \varphi(t) \\ &= 2 \varphi(2^s \cdot t) \\ &= 2 \varphi(n) \end{aligned}$$

\therefore 得证.

2. 请证明以下命题:

(1) 域是整环; (7分)

(2) 有限交换整环是域; (7分)

(3) 不存在元素个数为 50 的整环; (7分)

证明: (1) 设 F 为域, 即证 F 中不存在零因子

假设 F 中存在零因子, 即存在 $a, b \in F$, $a \neq 0, b \neq 0$, 满足 $a \cdot b = 0$.

已知 F 为域, 那么 a, b 均为可逆元素, 于是有

$$a \cdot b \cdot b^{-1} = (a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1} = 0$$

$$a \cdot b \cdot b^{-1} = a \cdot (b \cdot b^{-1}) = a$$

$\Rightarrow a = 0$ 矛盾

同理可证 $b = 0$ 矛盾

\therefore 假设不成立, 即不存在零因子, \therefore 域是整环.

(2) 设 $(F, +, \cdot)$ 为有限整环, 其中元素为 $F = \{a_1, a_2, \dots, a_n\}$.

$$a_i \neq a_j \quad (i \neq j).$$

对 $\forall a \in F$, 构造集合 $a \cdot F = \{a \cdot a_1, \dots, a \cdot a_n\}$.

由于封闭性 $a \cdot a_i \in F \quad \therefore a \cdot F \subseteq F$

对于 $\forall a \cdot a_i, a \cdot a_j$, $a \cdot a_i \neq a \cdot a_j$ 否则 $a(a_i - a_j) = 0$ 矛盾

$\therefore a \cdot F$ 与 F 势相等 $\therefore a \cdot F = F$

那么一定存在 $a \cdot a_i \in a \cdot F$ 使 $a \cdot a_i = 1$.

即有: 任意非零元素一定存在逆元

\therefore 有限整环是域

(3) 假设存在元素了数为50的素环, 那么该素环不是有限素环.

则为有限域. 而有限域的元素了数为素数或素数方幂.

∴ 50不是素数, 也不是素数方幂

∴ 矛盾

∴ 假设不成立

∴ 不存在元素了数为50的素环.