

《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. 判断方程  $x^2 \equiv 111 \pmod{991}$  是否有解, 给出判断过程(无需求解). (5 分)

2. 判断 2 是否为 19 的原根, 请说明理由. (5 分)

3. 设  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 2 & 7 & 1 & 3 & 6 \end{pmatrix}$ , 将  $\tau^{-1}\sigma$  分解成不相交的轮换. (5 分)

4. 利用多项式 $x^2 - 2$ 构造一个有限域, 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)

5. 请写出循环群 $(\mathbb{Z}_6, +)$ 的所有生成元, 以及该循环群的所有非平凡循环子群. (5 分)

## 二、计算题（共计 25 分）

得分	
----	--

1. 计算 $777^{777}$ 的十进制表示中的末位两位数字. (5 分)

2. 已知椭圆曲线 $E_{17}(1,1): y^2 = x^3 + x + 1$ 上一点 $P = (6,6)$ ,

(1) 求点 $2P$ 的坐标; (6 分)

(2) 求点 $3P$ 的坐标; (6 分)

(3) 求点 $3P$ 的阶. (8 分)

### 三、应用题（共 15 分）

得分	
----	--

Rabin 算法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 $x^2 = c \pmod{n}$

请根据所学的数学知识回答：已知 $p = 19, q = 23$ ，求出密文 $c = 233$ 所对应的 4 个可能的明文。

#### 四、证明题（共计 35 分）

得分	
----	--

1. 设 $m, k$ 是正整数,  $\varphi(\cdot)$ 是欧拉函数, 证明:  $\varphi(m^k) = m^{k-1}\varphi(m)$ . (8 分)

2. 设 $R_1, R_2$ 是环,  $f: R_1 \rightarrow R_2$ 为 $R_1$ 到 $R_2$ 的满同态映射, 证明

(1)  $\ker f$ 是 $R_1$ 的理想; (6分)

(2)  $R_1/\ker f \cong R_2$ ; (7分)

(3) 若 $R_1 = \mathbb{Z}[x]$ , 理想 $\langle x \rangle$ 是 $R_1$ 的素理想而非极大理想; (6分)

(4) 若 $R_1 = \mathbb{Z}[x]$ , 商环 $R_1/\langle x^2 + 3 \rangle$ 不是唯一析因环 (提示: 找到此时的 $R_2$ ) (8分)