

《信息安全数学基础》试卷（B 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 $x^2 \equiv 501(mod\ 1013)$ 是否有解，给出判断过程(无需求解). （5 分）

2. 判断 3 是否为 17 的原根，请说明理由. （5 分）

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

4. 构造 16 个元素的有限域. (5 分)

5. p 为素数, p 阶群是否为循环群, 为什么? 如果是循环群, 生成元有多少个? (5 分)

二、计算题（共计 25 分）

得分	
----	--

1. 求解方程: $x^2 \equiv 36 \pmod{77}$. (8 分)

2. 设 \mathbb{Z}_7 上的椭圆曲线为 $E: y^2 = x^3 - 2x - 3$, $P = (3, 5)$ 是其上一点

(1) 计算 $2P$; (5 分)

(2) 计算 $9P$; (7 分)

(3) 求点 P 的阶. (5 分)

三、应用题（共 15 分）

得分	
----	--

RSA 是现今应用最广泛的公钥密码系统，其数学原理为数论中的欧拉定理. 在 RSA 密码系统中，记两个不同的素数分别为 p 和 q ， $n = p \times q$ ，公钥为 (n, e) ，私钥为 (d, p, q) ，欧拉函数为 $\varphi(\cdot)$ ；明文为 m ，密文为 c .

加密过程为： $c = m^e \pmod n$ ；

解密过程为： $m = c^d \pmod n$

请根据所学的相关数学知识回答下面两个问题：

- (1) 已知公钥为 $(n, e) = (35, 5)$ ，明文 $m = 20$ ，试求密文 c .（5 分）
- (2) 证明 RSA 解密的正确性.（10 分）

四、证明题（共计 35 分）

得分	
----	--

1. 设 a 是偶数， b 是奇数，证明 $(a, b) = (a/2, b)$. （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) $\text{im}f$ 是 R_2 的子环; (6 分)

(2) $R_1/\ker f$ 与 $\text{im}f$ 同构; (7 分)

(3) 若 $R_1 = \mathbb{Z}[x]$, 理想 $\langle x+1 \rangle$ 是 R_1 的素理想而非极大理想; (6 分)

(4) 若 $R_1 = \mathbb{Z}[x]$, 商环 $R_1/\langle x^2+5 \rangle$ 不是欧几里得环 (提示: 找到此时的 R_2) (8 分)