南开大学网络空间安全学院本科生 2020-2021 学年第二学期

《信息安全数学基础》试卷（A 卷）

学号_____ 姓名_____

题号	一	二	三	总分
得分				

一、解答题（本题共 25 分，每小题 5 分）

得分	

1. 判断 6 是否为 17 的原根，并说明理由。

2. 判断 429 是否是模 563 的二次剩余，给出判断过程。

3. 将$\begin{pmatrix}1&2&3&4&5&6&7&8\\8&5&2&6&1&4&3&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\4&2&1&7&8&3&5&6\end{pmatrix}$分解成不相交的轮换。

4. x^3+2x^2+2x+1和x^3+x^2+2x+1在$\mathbb{Z}_3[x]$中是否可约？若存在可约多项式，则将其分解；若存在不可约多项式，则利用不可约多项式构造一个有限域并指出有限域中元素的个数和有限域的特征。

5. 请写出两个阶为4的循环群（标明集合和具体运算），并分别写出生成元。

二、计算与应用题（本题共 40 分）

得分	

1. 计算 $17^{42} \pmod{55}$，写出计算过程。（**5 分**）

2. RSA 加密体制中的主要参数如下：公钥为 (n,e)，其中 $n = p \times q$， p 和 q 为素数；私钥为 (d,p,q)，公钥 e 和私钥 d 满足：$de \equiv 1 (\bmod \varphi(n))$；明文为 m，密文为 c。加密过程为 $c = m^e \pmod{n}$，解密过程为 $m = c^d \pmod{n}$。请根据所学数学知识回答下面两个问题：

(1) 设公钥为 $(n,e) = (143,17)$，请计算私钥 d。（请写出计算过程）（**5 分**）

(2) 设三个用户对**同一**明文 m 进行加密，使用的公钥分别为 $(n_1,e) = (65,3)$，$(n_2,e) = (77,3)$，$(n_3,e) = (51,3)$，得到的密文分别是 $c_1 = 25$，$c_2 = 76$，$c_3 = 31$，试破解出明文 m。（不要使用分解 n 的方法）（**10 分**）

3. 椭圆曲线版本的 ElGamal 加密体制如下：

- 密钥生成算法：设 E_p 是有限域 $\mathbf{F}_p$ 上的椭圆曲线，G 是 E_p 中具有较大**素数**阶 n 的一个点。随机选取一个整数 d 使得 $2 \le d \le n-1$，计算 $P = dG$。私钥为 d，公钥为 (P, G, E_p, n)。
- 加密算法：将明文编码为椭圆曲线上一点 P_m，选取随机数 r：$1 \le r \le n-1$，计算 $(c_1, c_2) = (r \cdot G, P_m + r \cdot P)$。
- 解密算法：计算 $P_m = c_2 - d \cdot c_1$，将 P_m 解码得到明文。

请根据所学数学知识回答下列问题：

(1) 设选取的椭圆曲线为 $E_{11}(1,6)$，私钥为 $d = 2$，密文为 $(c_1, c_2) = ((8,3),(5,9))$，计算明文点 P_m。**（8 分）**

(2) 设选取的椭圆曲线为 $E_{11}(1,6)$，$G = (10,2)$，计算 n。**（12 分）**

三、证明题（本题共 35 分）

得分	

1. 设 k 为正整数，证明：

(1) 两个形如 $6k+5$ 的整数的积形如 $6k+1$。**（5 分）**

(2) 若方程 $\varphi(x)=k$ 只有唯一一个解 x_0，则 $36 \mid x_0$。（**提示：考虑 2,3 与 x_0 之间满足何种关系时方程会有两个解，例如 $\varphi(2x_0)=\varphi(x_0)$ 在何时成立**）**（10 分）**

2. 设 R 是一个交换环，H 是 R 的子环，I 是 R 的理想，$H+I=\{h+a \mid h\in H, a\in I\}$，证明：

(1) $H+I$ 是 R 的子环；**（5 分）**

(2) $H\bigcap I$ 是 H 的理想；**（5 分）**

(3) $H/H\bigcap I\cong (H+I)/I$ 。**（10 分）**