2017 年南开大学计算机与控制工程学院信息安全专业

《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（每小题 5 分，共计 25 分）

得分	

1. 将置换之积

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

2. 判断方程$x^2 \equiv -6(mod\ 91)$是否有解，并给出判断过程（无需求解）.

3. x^3+2x+3是$\mathbb{Q}[x]$中的不可约多项式吗？作为$\mathbb{Z}_5[x]$中的多项式是否不可约？若可约，试将它分解为不可约因式的积.

~~4. 在交换整环$\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$中，3 是不可约元素吗？是素元素吗？给出判断结果以及判断理由.~~

5. $x^8+x^4+x^3+x+1$是$\mathbb{Z}_2[x]$中的不可约多项式，试用该多项式构造一个有限域，并指出该有限域中元素的个数，以及该域的特征.

二、计算题（共计 30 分）

得分	

1. 计算$2^{80}(mod77)$. **（5 分）**

2. 利用中国剩余定理求解同余方程组**（8 分）**

$$\begin{cases} x \equiv 3(mod4) \\ 3x \equiv 1(mod5) \\ 13x \equiv 14(mod19) \end{cases}$$

3. 设$\mathbb{Z}_{17}$上的椭圆曲线为$E: y^2 = x^3 + 2x + 3$，其上的点$P = (2, 7)$，$Q = (11, 8)$.

(1) 计算$P + Q$；**（5 分）**

(2) 计算$2P$；**（5 分）**

(3) 计算$11P$，并指出点P的阶. **（7 分）**

三、应用题（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)，其中公钥e和私钥d满足：$de \equiv 1(mod\varphi(n))$，欧拉函数为$\varphi(\cdot)$；明文为$m$，密文为$c$.

加密过程为：$c = m^e(mod\ n)$；

解密过程为：$m = c^d(mod\ n)$

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$(n, e) = (35, 5)$，密文c =10，试求明文m.（**5 分**）

(2) 证明 RSA 解密的正确性.（**10 分**）

四、证明题（共计 30 分）

得分	

1. 设$n \in \mathbb{N}$，证明$\varphi(n) = \frac{n}{2}$的充要条件是$n = 2^k, k \in \mathbb{N}$. **（8 分）**

2. 设R_1, R_2是环，$f: R_1 \to R_2$为R_1到R_2的同态映射，证明

(1) $\ker f$是R_1的理想；**（5 分）**

(2) $\mathrm{im} f$是R_2的子环；**（5 分）**

(3) $R_1/\ker f \cong \mathrm{im} f$；**（6 分）**

(4) 若f为满同态，I是R_1的理想且$\ker f \subseteq I$，则$R_1/I \cong R_2/f(I)$.**（6 分）**