2020年南开大学网络空间安全学院信息安全专业

《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（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，将σ^{-1}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)**

$\mathbb{Z}_5[x]/x^2-2$ $5^2=4$

$p=2$

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）**

$(\mathbb{Z}_6, +)$

p $p-1$

阶6， $\varphi(n)=2$

$1, -1$

二、计算题（共计25分）

得分	

1. 计算$7^{7^{7^{7^{7^{7^{7}}}}}}$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，$f: R_1 \to R_2$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）