2019 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. 设$\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&3&5&2&1&4\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5&6\\4&6&2&5&1&3\end{pmatrix}$，将$\sigma^{-1}\tau$分解成不相交的轮换. （**4 分**）

2. 判断 5 是否为 19 的原根，并说明理由.（**5 分**）

3. 判断方程$x^2 \equiv 105(mod\ 1009)$是否有解，给出判断过程(无需求解)（**5 分**）

4. 利用多项式x^3+2x+1构造一个有限域，并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. 设G为无限阶循环群，生成元为a. 构造从$\mathbb{Z}$到G的映射$f:\mathbb{Z}\to G$，满足$f(n)=a^n, n\in\mathbb{Z}$. 请说明f是满同态映射的理由，并指出同态核$\ker f$，最后写出结合上述条件与同态基本定理得到的结论.（**6 分**）

二、计算题（共计 25 分）

得分	

1. 计算$2^{10000}(mod\ 55)$.（**5 分**）

$2^n \equiv 1 \pmod{55}$

2. 设$\mathbb{Z}_{23}$上的椭圆曲线为E: $y^2 = x^3 + 3x + 1$， $P = (5,7)$是其上一点

(1) 求点$2P$的坐标；（**5 分**）

(2) 求点$3P$的坐标；（**5 分**）

(3) 求点$5P$的阶. （**10 分**）

(1) $k = 22$ $x_3 = k^2 - x_1 - x_2 = 14$

$y_3 = k(x_1 - x_3) - y_1 = 25$

(2)

三、应用题（共 15 分）

得分	

Rabin 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：$c = m^2 (mod\ \ n)$

解密过程为：求解方程$x^2 = c(mod\ \ n)$

现已知$p = 19, q = 23$，请根据所学的数学知识回答下面两个问题：

1. 设明文消息为 66，求对应的密文.（**3 分**）
2. 计算上一问中的密文所对应的 4 个可能的明文（**12 分**）

1. $c \equiv 66^2 \pmod{19 \times 23} = 423 \pmod{437}$

2. $x^2 \equiv 423 \pmod{437}$

$$\begin{cases} x^2 \equiv 423 \pmod{19} \\ x^2 \equiv 423 \pmod{23} \end{cases}$$

$x^2 \equiv 5 \pmod{19}$

$x^2 \equiv 9 \pmod{23}$

$x^2 \equiv 81$

$x \equiv \pm 9$

$x \neq$

四、证明题（共计 35 分）

得分	

1. 设n是一个正整数，证明：

(1) $42|(n^7-n)$ （7 分）

(2) $\varphi(2n)=\begin{cases}\varphi(n) & n\text{为奇数}\\ 2\varphi(n) & n\text{为偶数}\end{cases}$ （7 分）

(1) $42|(n^7-n)$

$42|n(n^6-1)$

$6\times7\mid(n^3+1)(n^3-1)n$

$(n+1)<n^2$

(2) $\varphi(2n)=\varphi(2)\varphi(n)$ 奇数可求

$=\varphi(n)$

$\varphi(2n)=2n\times\cdots\frac{1}{2}$

2. 请证明以下命题：

(1) 域是整环；（**7 分**）

(2) 有限交换整环是域；（**7 分**）

(3) 不存在元素个数为 50 的整环；（**7 分**）