2016 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	1	2	3	4	5
得分					

一、完成下面各题（每小题 4 分，5 小题，共计 20 分）

1. 试求 $17^{42} \pmod{55}$ 。

2．判断 5 是否是模 77 的二次剩余，给出判断过程。

3. 分别在有理数域、复数域和有限域 $\mathbf{Z}_5$ 内分解多项式 $x^2 - 3x + 6$ 。

4．试求 $ord_{17}(6)$ 。

5．试分别给出非交换的群、非交换的环、非整环的环的例子。

得分	

二、（10 分）求解方程：$x^2 \equiv 36(\mathrm{mod}\,77)$。

得分	

三、（20 分）给的正整数 n，

(1) 利用简化剩余类的概念，证明欧拉定理：正整数 a 与 n 互素，则 $a^{\varphi(n)} \equiv 1(\mathrm{mod}\,n)$。

(2) 环 $\mathbf{Z}_n$ 是域当且仅当 n 是素数。

得分	

四、(25 分) 设 G_1, G_2 是群，e_1, e_2 分别是 G_1, G_2 的幺元，$f: G_1 \to G_2$ 为 G_1 到 G_2 的同态映射，证明：

(1) $f(e_1) = e_2$ 且对任意 $g \in G_1$，$f(g)^{-1} = f(g^{-1})$；

(2) f 的像 $\mathrm{Im} f = \{f(g) \mid g \in G_1\}$ 是 G_2 的子群；

(3) f 的核 $\mathrm{Ker} f = \{g \in G_1 \mid f(g) = e_2\}$ 是 G_1 的正规子群；

(4) 记 N=$\mathrm{Ker} f$，则 $G_1 / N = \{gN \mid g \in G_1\}$ 构成群；

(5) 群 G_1 / N 到群 $\mathrm{Im} f$ 的映射 ϕ 满足：$\phi(gN) = f(g)$，则 ϕ 为一一映射；

(6) $G_1 / \mathrm{Ker} f \cong \mathrm{Im} f$ 。

得分	

五、(25 分)设素数 p>3，有限域 $\mathbb{Z}_p$ 上的椭圆曲线 E：$y^2 \equiv x^3 + ax + b \pmod{p}$，$a, b \in \mathbb{Z}_p$ 且 $4a^3 + 27b^2 \neq 0$。对 E 上非无穷远点的任意点 $P_1 = (x_1, y_1)$，$P_2 = (x_2, y_2)$，令 $P_3 = P_1 + P_2 = (x_3, y_3)$，则 $(E, +)$ 构成群，定义无穷远点为单位元，其加法如下：①当 $x_1 = x_2, y_1 + y_2 = 0$ 时，则 $P_3 = P_1 + P_2$ 为无穷远点；②其它情形，$x_3 = \lambda^2 - x_1 - x_2$，$y_3 = \lambda(x_1 - x_3) - y_1$，

其中 $\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, 若 x_1 \neq x_2 \\ \dfrac{3x_1^2 + a}{2y_1}, 若 x_1 = x_2 \end{cases}$。

若在 $\mathbb{Z}_{23}$ 上定义椭圆曲线 $E: y^2 = x^3 + 3x + 1$，点 $P = (5, y) \in E$ 且 $2y \leq 23$

(1) 求 y 的值;

(2) 求点 $3P$ 和 $5P$ 的坐标;

(3) 求 $5P$ 在 $(E, +)$ 中的阶。