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。

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**Z**5内分解多项式。

4．试求。

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：。

|  |  |
| --- | --- |
| 得分 |  |

**三、（20分）**给的正整数，

1. 利用简化剩余类的概念，证明欧拉定理：正整数与互素，则。
2. 环是域当且仅当是素数。

|  |  |
| --- | --- |
| 得分 |  |

**四、（25分）**设是群，分别是的幺元，为到的同态映射，证明：

(1) 且对任意，；

(2) 的像是的子群；

(3) 的核是的正规子群；

(4) 记，则构成群；

(5) 群到群的映射满足：，则为一一映射；

(6) 。

|  |  |
| --- | --- |
| 得分 |  |

**五、（25分）**设素数*p*>3，有限域上的椭圆曲线：，*a*, *b*且。对上非无穷远点的任意点，，令，则构成群，定义无穷远点为单位元，其加法如下：①当时，则为无穷远点；②其它情形，，，

其中 。

若在上定义椭圆曲线，点且

(1) 求的值;

(2) 求点和的坐标；

(3) 求在中的阶。