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，将分解成不相交的轮换.**（5分）**

4. 利用多项式构造一个有限域，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）**

5. 请写出循环群的所有生成元，以及该循环群的所有非平凡循环子群.**（5分）**

**二、计算题（共计25分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 计算的十进制表示中的末位两位数字.**（5分）**

2. 已知椭圆曲线上一点，

(1) 求点的坐标；**（6分）**

(2) 求点的坐标；**（6分）**

(3) 求点的阶. **（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（和为素数），公钥为，明文为，密文为.

加密过程为：

解密过程为：求解方程

请根据所学的数学知识回答：已知，求出密文所对应的4个可能的明文.

**四、证明题（共计35分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 设是正整数，是欧拉函数，证明：. **（8分）**



2. 设是环，为到的满同态映射，证明



(1) 是的理想；**（6分）**



(2) ；**（7分）**

(3) 若，理想是的素理想而非极大理想；**（6分）**



(4) 若，商环不是唯一析因环（提示：找到此时的）**（8分）**