2017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 | 一 | 二 | 三 | 四 | 总分 |
| 得分 |  |  |  |  |  |

**一、解答题（每小题5分，共计25分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 将置换之积分解成不相交的轮换.

2. 判断方程是否有解，并给出判断过程（无需求解）.

3. 是中的不可约多项式吗？作为中的多项式是否不可约？若可约，试将它分解为不可约因式的积.

~~4. 在交换整环中，3是不可约元素吗？是素元素吗？给出判断结果以及判断理由.~~

5. 是中的不可约多项式，试用该多项式构造一个有限域，并指出该有限域中元素的个数，以及该域的特征.

**二、计算题（共计30分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 计算. **（5分）**

2. 利用中国剩余定理求解同余方程组**（8分）**

3. 设上的椭圆曲线为，其上的点，.

(1) 计算；**（5分）**

(2) 计算；**（5分）**

(3) 计算，并指出点的阶. **（7分）**

**三、应用题（15分）**

|  |  |
| --- | --- |
| 得分 |  |

RSA是现今应用最广泛的公钥密码系统，其数学原理为数论中的欧拉定理. 在RSA密码系统中，记两个不同的素数分别为和，，公钥为，私钥为，其中公钥和私钥满足：，欧拉函数为；明文为，密文为.

加密过程为：；

解密过程为：

请根据所学的相关数学知识回答下面两个问题：

(1) 已知公钥为，密文10，试求明文.**（5分）**

(2) 证明RSA解密的正确性.**（10分）**

**四、证明题（共计30分）**

|  |  |
| --- | --- |
| 得分 |  |

1. 设，证明的充要条件是. **（8分）**

2. 设是环，为到的同态映射，证明

(1) 是的理想；**（5分）**

(2) 是的子环；**（5分）**

(3) ；**（6分）**

(4) 若为满同态，是的理想且，则.**（6分）**