**网络空间安全学院2019-2020学年第2学期 参考答卷**

信息安全数学基础 A卷 闭卷 考试时间：150分钟

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2020-5-16

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 总分 | 核对人 |
| 题分 | 20 | 20 | 35 | 25 | 100 |  |
| 得分 |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **证明题(本大题3小题，共20分)** |
|  |  |

1. 试证明：对于非零整数，若。（6分）

**证明：**

，那么，=1,，得到。

1. 设为奇素数，，整数是模的平方剩余，且，试证明是模的原根。（8分）

**证明：**因为是模的平方剩余，根据欧拉判别法则，所以

由此，但为素数，且，所以.

又，，所以,即为模的原根。

1. 设为素数，试证明：存在无限多个正整数，使得。（6分）

**证明：**（1）时结论显然成立。

（2）时，根据费马小定理，如下条件的可以使得。

满足以上同余式的有无穷多个。

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **计算题(本大题2小题，共20分)** |
|  |  |

1. 试计算，结果取最小非负剩余。（10分）

解：根据扩展欧拉定理

1. 计算勒让德符号。（10分）

解：=1

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解方程或方程组(本大题3小题，共35分)** |
|  |  |

1. 求方程的整数解。（10分）

解：因为(5,13)=1,所以可令.

1. 求解同余式组。(10分)

解：

1. 求解同余式。（15分）

解：26个解。

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解答题(本大题2小题，共25分)** |
|  |  |

1. 试判断同余式是否有解，如果有解求出其解数。（10分）

解：20个解。

1. 设是上的多项式，

（1）试证明是上的不可约多项式。（6分）

（2）试求 在上的极小多项式。（4分）

（3）设是的4元子域，试在上分解多项式。（5分）

解：（1）没有1，2，3次不可约因式。

（2）是的根，所以是在上的极小多项式，根据极小多项式的结构，也是的根，所以在上的极小多项式也是。

（3）先求出阶为3的元素。因为，所以，，因此={0，1，}

i.在上没有一次因式。因此，如果可约，只能是两个2次不可约多项式的乘积。

Ii.不妨设



其中，

对比系数得到，

所以，，因此，所以根据和对称性，可设

，，故=