**计算机科学与技术学院2014-2015学年第2学期 考试试卷**

信息安全数学基础 A卷 闭卷

姓名\_\_\_\_\_\_\_\_\_\_\_\_班级\_\_\_\_\_\_\_\_\_\_\_\_学号\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_考试日期 2015-5-27

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 题号 | 一 | 二 | 三 | 四 | 五 | 总分 | 核对人 |
| 题分 | 20 | 30 | 25 | 10 | 15 | 100 |  |
| 得分 |  |  |  |  |  |  |  |

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

1. 对于，证明：。（6分）
2. 对于非零整数，证明：集合中最小的正整数为。（7分）
3. 证明：对于标准分解式，若均有。（7分）

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **计算题(本大题3小题，共30分)** |
|  |  |

1. 计算，结果取最小非负剩余。（10分）

1. 计算，结果取最小非负剩余。（10分）
2. 计算勒让德符号。（10分）

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解同余方程或方程组(本大题2小题，共25分)** |
|  |  |

1. 求解同余式组.(10分)
2. 求解同余式（15分）.

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **解答题(本大题1小题，共10分)** |
|  |  |

1. 试判断421是否是模693的8次剩余。（10分）

|  |  |  |
| --- | --- | --- |
| 得分 | 评卷人 | 1. **有限域(本大题1小题，共15分)** |
|  |  |

1. 在有限域中

（1）试判断元素是否为域的本原元。（5分）

（2）试求域的8元子域（要求所有元素写成次数小于6的多项式的形式）。（5分）

（3）求在域中的乘法逆元。（5分）