武汉大学计算机学院

2014-2015 学年度第一学期 2013 级弘毅班

《信息安全数学基础》期末考试试卷（A）

姓名：_____ 学号：_____ 专业：_____成绩：_____

（注：①考试时间为 120 分钟；②所有的题目的解答均写在答题纸上，需写清楚题目的序号。每张答题纸都要写上姓名和序号。）

一． 计算题（每小题 10 分，共 50 分）。

1.求整数 s 和 t，使得 sa+tb=(a,b)：

(1) a=127, b=833; (2) a=987,b=2668。

2.运用模重复平方法计算 $473^{17} \bmod 713$。

3.求解同余式 $x^2+x+7\equiv 0$（mod 27）。

4.判断同余式 $x^2\equiv 102 \pmod{259}$是否有解？有解时求出其所有解。

5. 设 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&1&6\end{pmatrix}$，$\tau=\begin{pmatrix}1&2&3&4&5&6\\4&5&2&3&6&1\end{pmatrix}$， 计算 $\sigma\tau$，$\tau\sigma$，σ^{-1}。

二． 证明题（每小题 10 分，共 20 分）

1. 设 $m\geq 3$，证明：模 m 的最小正简化剩余系的各数之和等于 $m\varphi(m)/2$。

2. 应用勒让德符号证明形如 8k+3 的素数有无穷多个。

三. 简述题（每小题 10 分，共 30 分）

1. 简述求模 47 的最小原根的方法以及由此求解如下高次剩余 $x^5\equiv 29 \pmod{47}$的步骤。

2.给出集合{0,1,2,3,4,5,6,7}上的加法和乘法运算表，使得该系统构成有限域。（以 x^3+x+1 为模）

3.简述群的定义。