武汉大学计算机学院
2010-2011 学年度第一学期 2009 级
《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 80 分）。

1. 试用两种方法计算乘法逆元素 $329^{-1} \bmod 667$ 。

2. 求解同余式组

$$\begin{cases} 5x \equiv 4 (\bmod 11) \\ 87x \equiv 16 (\bmod 61) \end{cases}。$$

3. 求解同余式 $f(x) \equiv x^4 + 7x + 1 \equiv 0 (\bmod 27)$ 。

4. 求解同余式 $7x^7 \equiv 8 (\bmod 41)$ 。

5. 求群{0，1，2，3，4，5，6，7，8，9，10，11}（关于模 12 的加法）的所有子群。

6. 构造有限域 GF(9),并且给出其加法和乘法表。

7. 对于由 GF（2）上的不可约多项式 x^4+x+1 扩成的有限域 GF（2^4），设 α 是一个本原元，求 α^3 的最小多项式。

8．求解递推关系

$$\begin{cases} f(n) = 5f(n-1) - 8f(n-2) + 4f(n-3) \\ f(0) = 0, f(1) = 1, f(2) = 2 \end{cases}。$$

二．证明：形如 4k+1 的素数有无穷多个。（10 分）

三. 简述对有限域概念的理解。（10 分）