武汉大学计算机学院
2009-2010 学年度第一学期 2008 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． 名词解释（每小题 4 分，共 20 分）。

1.最大公因数； 2. 平方非剩余；3.群； 4.指数； 5.群同态。

二． 计算题（每小题 10 分，共 60 分）。

1. 求最大公因数（987，2668），并且计算出最小的正整数 b,使得 987a+2668b=(987,2668)。

2. 运用模的重复平方算法计算 $2^{567} \bmod 61$。

3.求同余式 $x^2 \equiv 76 \pmod{103}$的解。

4. 求解同余式组

$$\begin{cases} x \equiv 2 \pmod 9 \\ 3x \equiv 4 \pmod 5 \\ 4x \equiv 3 \pmod 7 \end{cases}。$$

5. 设 S={e, a, b, c}为有限集合，<S, *>为群。在群同构的意义下<S, *>只有两种，试给出这两种运算表。

6. 求$(x^7+ x^6 +1)$关于模 $m(x)=x^8+x^4+x^3+x+1$ 的乘法逆元(即求使得等式 $a(x)(x^7+ x^6 +1)+q(x)m(x)=1$ 成立的多项式 a(x))。

三. 简述题（每小题 10 分，共 20 分）

（1） 请描述利用原根和指标求解高次同余式 $x^n \equiv a \pmod m$，$m = 2,4, p^\alpha$ 或 $2p^\alpha$ 的一般方法。

（2）请写出两种概率素性检测方法。