武汉大学计算机学院 2008-2009 学年第一学期

“信息安全数学基础”试卷(A 卷)

班级_____学号_____ 姓名_____

一． 名词解释（每小题 4 分，共 20 分）。

1.素数； 2.最小非负完全剩余系；3.平方剩余； 4.无限简单连分数；5.环同态。

二． 计算题（每小题 10 分，共 60 分）。

1. 求乘法逆元素（1）$11^{-1} \bmod 37$；（2）$113^{-1} \bmod 401$。

2. 求解同余式 $x^3+7x+2\equiv 0 \pmod{16}$。

3.判断同余式 $x^2\equiv 30 \pmod{113}$是否有解？有解时求出其所有解。

4. 求模 37 的最小原根，并且求解如下高次剩余

$x^4\equiv 34 \pmod{37}$。

5. 求 $Z/15Z$ 的所有子群。

6. 求 $F_{2^4}=F_2[x]/(x^4+x^3+1)$ 中的生成元 $g(x)$，并且计算出所有的生成元。

三. 证明题（每小题 10 分，共 20 分）

（1） 若 n 为 Blum 整数，则每个模 n 的平方剩余恰有 4 个平方根（即 4 个解），且其中有一个也是模 n 的一个平方剩余，称为原平方根。例如，139 的模 437 的原平方根为 24，另外三个平方根为 185，252，413。试证明上述结论。

（2）假设在椭圆曲线 $E: y^2 \equiv x^3+x+6 \pmod{11}$上， $\alpha=(2,7)$ 为生成元，试证明： $4\alpha=(10,2)$ 。