武汉大学计算机学院 2010-2011 学年第一学期

“信息安全数学基础”试卷(B 卷)

班级_____学号_____ 姓名_____

一. 计算题（每小题 10 分，共 80 分）。

1. 计算勒让德符号$\left(\frac{23}{31}\right)$, $\left(\frac{21}{29}\right)$, $\left(\frac{37}{101}\right)$。

2. 判断同余式 $x^2 \equiv 37 \pmod{101}$是否有解？有解时求出其所有解。

3. 求解同余式 $x^2+x+7 \equiv 0 \pmod{27}$。

4. 求模 47 的所有原根，并且建立它的关于最小正原根的指标表，由此求解如下高次剩余 $x^5 \equiv 29 \pmod{47}$。

5. 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。

6. 求 $F_{2^4} = F_2[x]/(x^4 + x^3 + 1)$ 的所有不可约多项式。

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 的最小多项式

8. 求解递推关系

$$\begin{cases} f(n) = f(n-1) + 9f(n-2) - 9f(n-3) \\ f(0) = 0, f(1) = 1, f(2) = 2 \end{cases}$$。

二. 证明：形如 8k-1 的素数有无穷多个。（10 分）

三. 简述有限域的构造方式。（10 分）