武汉大学计算机学院

2012-2013 学年度第一学期 2011 级

《信息安全数学基础》期末考试试卷(B 卷)

班级____________学号___________ 姓名___________

一． 计算题（每小题 10 分，共 60 分）。

1. 求模 6 剩余类加法群 $\langle Z_6,+\rangle$ 到模 7 剩余类乘法群 $\langle Z_7-\{0\},\times\rangle$ 的所有同构映射。

2. 分别用模 4 和模 5 的完全剩余系和简化剩余系来表示模 20 的完全剩余系和简化剩余系。

3.求解同余式 $x^2+x+7\equiv0 \pmod{27}$。

4.判断同余式 $x^2\equiv102 \pmod{259}$ 是否有解？有解时求出其所有解。

5. 求模 31 的所有原根，并且求解如下高次剩余

$x^6\equiv2 \pmod{31}$。

6. 求解同余式组

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

二. 证明题（共一题，20 分）

应用勒让德符号证明形如 8k+3 的素数有无穷多个。

三 解答题（共一题，20 分）

在 RSA 系统中，存在一种 $p-1$ 因子分解法，使得我们可以轻易地分解

因子n。若$n=pq$，且$p-1$的所有素因数均很小，即$p-1=\prod_{i=1}^{t} p_i^{a_i}$，其中，$p_i$为第$i$个素数，$a_i \geq 1$为整数，且所有$p_i < A$，$A$为已知的小正整数。试用这种方法分解整数$n=118829$。（提示：选取$A$为 14，$a=1$）（20 分）