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（A）

一． 计算题（每小题 10 分，共 60 分）。

1. 计算勒让得符号$\left(\frac{2}{3}\right),\left(\frac{2}{17}\right),\left(\frac{3}{17}\right)$。

2. 求解同余式组

$$\begin{cases} x \equiv 2(\mathrm{mod}\,9) \\ 3x \equiv 4(\mathrm{mod}\,5) \\ 4x \equiv 3(\mathrm{mod}\,7) \end{cases}。$$

3. 求解同余式

$$f(x) \equiv x^4 + 7x + 4 \equiv 0(\mathrm{mod}\,27)。$$

4. 假设椭圆曲线$y^2 = x^3 + x + 6(\mathrm{mod}11)$上的两点$P=(x_1,y_1),Q=(x_2,y_2)$之和为$P_3=(x_3,y_3)=P+Q\neq O$的计算公式为

$$x_3 = \lambda^2 - x_1 - x_2，\quad y_3 = (x_1 - x_3)\lambda - y_1$$

其中(a) $x_1 \neq x_2$时，$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$，$(b)$ $x_1 = x_2$，且$Q \neq -P$时，$\lambda = \frac{3x_1^2 + 1}{2y_1}$

若$P=(8,3)$，试求 3P。

5. 构造有限域 GF(8)={0，1，2，3，4，5，6，7}的加法和乘法表。

6. 求模 11 的一组最小正完全剩余系$r_1, r_2, \cdots, r_{11}$，满足

$$r_i \equiv -1(\mathrm{mod}\,2), r_i \equiv 1(\mathrm{mod}\,3)，$$

$$r_i \equiv 1(\mathrm{mod}\,5), r_i \equiv 0(\mathrm{mod}\,7), 1 \le i \le 11。$$

二. 证明题（每小题 10 分，共 20 分）

（1）证明：如果 p 是素数，并且 $p \equiv 3(\mathrm{mod}\,4)$，那么

$$\frac{p-1}{2}! \equiv \pm 1 \qquad (\mathrm{mod}\,p)。$$

（2）若群 G 的每一个元都适合方程 $x^2 = e$, 那么 G 是交换群。

三. 简述题（20 分）

如果四个不同的元素{e, a, b, c}构成的集合和该集合上的二元运算能够成为一个群，试给出该群不同构的两种运算表。