武汉大学计算机学院

2011-2012 学年度第一学期 2010 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．　计算题（每小题 10 分，共 70 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．求 13 的倍数，使得该数被 3，5，7，11 除的余数是 2。

3. 求同余式 $x^2 \equiv 52 \pmod{101}$ 的解。

4．假设椭圆曲线 $y^2 = x^3 + x + 6 \pmod{11}$ 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，$\lambda=\dfrac{y_2-y_1}{x_2-x_1}$，$(b)$ $x_1=x_2$，且 $Q \neq -P$ 时，$\lambda=\dfrac{3x_1^2+1}{2y_1}$

若 $P=(5,2)$，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 (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))。

7 求解递推关系

$$\begin{cases} a_n = 7a_{n-1} - 12a_{n-2} \\ a_0 = 2, a_1 = 7 \end{cases}$$

二. 证明题（10 分）

证明：群 G 是交换群的充要条件是对任意 a, b∈G, 有

$(a\ b)^3=a^3\ b^3$, $(a\ b)^5=a^5b^5$.（10 分）

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 $x^n \equiv a(\bmod m)$，$m = 2,4, p^\alpha$或$2p^\alpha$ 的一般方法。

（2）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，试给出该群的运算表。