武汉大学计算机学院

2014-2015 学年度第二学期 2013 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（1-4 每小题 10 分，第 5 小题 20 分，共 60 分）。

1. 求整数 s 和 t，1<t<127, 使得 sa+tb=(a,b), 其中 a=127, b=833。

2. 求解同余式 $x^2+x+7\equiv 0 \pmod{27}$。

3. 求同余式 $x^2\equiv 13 \pmod{101}$ 的解。

4. 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。

5. 构造有限域 GF(16)={0，1，2，3，4，5，6，7,8,9,10,11,12,13,14,15}（选择的求模多项式为 $m(x)=x^4+x+1$）的加法和乘法表，其中乘法表只要求完成下表的内容。

*	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1															
2															

3														

二. 证明题（每小题 10 分，共 20 分）

（1）已知 N=pq，p, q 是两个素数，证明如下等式

$$q \cdot q^{-1} \bmod p + p \cdot p^{-1} \bmod q = N + 1$$

（2）设 G 是有限交换群，对任意 a,b ∈ G，若（ord(a),ord(b)）=1，则 ord(a · b)=ord(a) · ord(b)。

三. 简述题（20 分）

如果一个集合的元素个数不超过 5 个，该集合在某种运算下构成一个群，试在同构意义下给出该集合可能的运算表。（提示：集合元素个数可以为 1, 2, 3, 4, 5；同构意义下的运算表属于同一种运算表）