### 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 卷)答案

- 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。

解: 因为833=127\*6+71, 127=71\*1+56, 71=56+15,

56=15\*3+11, 15=11+4, 11=4\*3-1;

所以 1=4\*3-11=15\*3-11\*4=15\*15-56\*4=15\*71-56\*19=

71\*34-127\*19=833\*34-127\*223,

即 t=34, s=-223.

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

解 因为(4,27)=1,所以由同余式的性质可以得到

 $4x^2+4x+28 \equiv 0 \pmod{27}$ , 即  $4x^2+4x+1 \equiv 0 \pmod{27}$ , 于是

 $(2x+1)^2 \equiv 0 \pmod{27}$ , 因此  $2x+1 \equiv 0 \pmod{9}$ , 利用一次同余式的

求解方法得  $x \equiv 4 \pmod{9}$ ,所以原同余式的解为

 $x \equiv 4, 13, 22 \pmod{27}$ .

3 求同余式 x<sup>2</sup> ≡ 13 (mod 101) 的解。

解 因为 101=4\*25+1,所以同余式  $x^2 \equiv 13 \pmod{101}$  的解为  $x \equiv \pm 35 \pmod{101}$ 。

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。

解: 首先证明 g(x) = x 是一个生成元,(k, 15) = 1,则  $g(x)^k$  为所有的生

成元。

 $K=1, 2, 4, 7, 8, 11, 13, 14, g(x)^k$ 分别为:

满绩小铺: 1433397577, 搜集整理不易, 自用就好, 谢谢!

$$x, x^2, x^3 + 1, x^2 + x + 1, x^3 + x^2 + x, x^3 + x^2 + 1, x^2 + x, x^3 + x^2$$

5. 构造有限域 GF(16)= $\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}$ 的加法和乘法表。(选择的求模多项式为 $m(x)=x^4+x+1$ )

解: 加法表为

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	6	5	4		2	1	0	15	14	13	12	11	10	9	8
	9	10				14		0	1	2	3	4	5	6	7
	8			•							2	5	4	7	6
	11						7					6	7	4	5
													6		4
															3
															2
															1
15				11	10	9	8	7	6	5	4	3	2	1	0
	0 1 2 3 4 5 6 7 8 9 10 11 12 13	0 1   1 0   2 3   3 2   4 5   5 4   6 7   7 6   8 9   9 8   10 11   11 10   12 13   13 12   14 15	0 1 2   1 0 3   2 3 0   3 2 1   4 5 6   5 4 7   6 7 4   7 6 5   8 9 10   9 8 11   10 11 8   11 10 9   12 13 14   13 12 15   14 15 12	0 1 2 3   1 0 3 2   2 3 0 1   3 2 1 0   4 5 6 7   5 4 7 6   6 7 4 5   7 6 5 4   8 9 10 11   9 8 11 10   10 11 8 9   11 10 9 8   12 13 14 15   13 12 15 14   14 15 12 13	0 1 2 3 4   1 0 3 2 5   2 3 0 1 6   3 2 1 0 7   4 5 6 7 0   5 4 7 6 1   6 7 4 5 2   7 6 5 4 3   8 9 10 11 12   9 8 11 10 13   10 11 8 9 14   11 10 9 8 15   12 13 14 15 8   13 12 15 14 9   14 15 12 13 10	0 1 2 3 4 5   1 0 3 2 5 4   2 3 0 1 6 7   3 2 1 0 7 6   4 5 6 7 0 1   5 4 7 6 1 0   6 7 4 5 2 3   7 6 5 4 3 2   8 9 10 11 12 13   9 8 11 10 13 12   10 11 8 9 14 15   11 10 9 8 15 14   12 13 14 15 8 9   13 12 15 14 9 8   14 15 12 13 10 11	0 1 2 3 4 5 6   1 0 3 2 5 4 7   2 3 0 1 6 7 4   3 2 1 0 7 6 5   4 5 6 7 0 1 2   5 4 7 6 1 0 3   6 7 4 5 2 3 0   7 6 5 4 3 2 1   8 9 10 11 12 13 14   9 8 11 10 13 12 15   10 11 8 9 14 15 12   11 10 9 8 15 14 13   12 13 14 15 8 9 10   13 12 15 14 9 8 11   14 15 12 <td< td=""><td>0 1 2 3 4 5 6 7   1 0 3 2 5 4 7 6   2 3 0 1 6 7 4 5   3 2 1 0 7 6 5 4   4 5 6 7 0 1 2 3   5 4 7 6 1 0 3 2   6 7 4 5 2 3 0 1   7 6 5 4 3 2 1 0   8 9 10 11 12 13 14 15   9 8 11 10 13 12 15 14   10 11 8 9 14 15 12 13   11 10 9 8 15 14 13 12   12 13 14 15 8 9 10 11</td><td>0 1 2 3 4 5 6 7 8   1 0 3 2 5 4 7 6 9   2 3 0 1 6 7 4 5 10   3 2 1 0 7 6 5 4 11   4 5 6 7 0 1 2 3 12   5 4 7 6 1 0 3 2 13   6 7 4 5 2 3 0 1 14   7 6 5 4 3 2 1 0 15   8 9 10 11 12 13 14 15 0   9 8 11 10 13 12 15 14 1   10 11 8 9 14 15 12 13 2   11 10 9 8 15 14</td><td>0 1 2 3 4 5 6 7 8 9   1 0 3 2 5 4 7 6 9 8   2 3 0 1 6 7 4 5 10 11   3 2 1 0 7 6 5 4 11 10   4 5 6 7 0 1 2 3 12 13   5 4 7 6 1 0 3 2 13 12   6 7 4 5 2 3 0 1 14 15   7 6 5 4 3 2 1 0 15 14   8 9 10 11 12 13 14 15 0 1   9 8 11 10 13 12 15 14 1 0   10 11 8 9 14 15</td><td>0 1 2 3 4 5 6 7 8 9 10   1 0 3 2 5 4 7 6 9 8 11   2 3 0 1 6 7 4 5 10 11 8   3 2 1 0 7 6 5 4 11 10 9   4 5 6 7 0 1 2 3 12 13 14   5 4 7 6 1 0 3 2 13 12 15   6 7 4 5 2 3 0 1 14 15 12   7 6 5 4 3 2 1 0 15 14 13   8 9 10 11 12 13 14 15 0 1 2   9 8 11 10 13 12 15 14</td><td>0 1 2 3 4 5 6 7 8 9 10 11   1 0 3 2 5 4 7 6 9 8 11 10   2 3 0 1 6 7 4 5 10 11 8 9   3 2 1 0 7 6 5 4 11 10 9 8   4 5 6 7 0 1 2 3 12 13 14 15   5 4 7 6 1 0 3 2 13 12 15 14   6 7 4 5 2 3 0 1 14 15 12 13   7 6 5 4 3 2 1 0 15 14 13 12   8 9 10 11 12 3 1 1 1 3 2 1</td><td>0 1 2 3 4 5 6 7 8 9 10 11 12   1 0 3 2 5 4 7 6 9 8 11 10 13   2 3 0 1 6 7 4 5 10 11 8 9 14   3 2 1 0 7 6 5 4 11 10 9 8 15   4 5 6 7 0 1 2 3 12 13 14 15 8   5 4 7 6 1 0 3 2 13 12 15 14 9   6 7 4 5 2 3 0 1 14 15 12 13 10   7 6 5 4 3 2 1 0 15 14 13 12 11   8 9 10 11</td><td>0 1 2 3 4 5 6 7 8 9 10 11 12 13   1 0 3 2 5 4 7 6 9 8 11 10 13 12   2 3 0 1 6 7 4 5 10 11 8 9 14 15   3 2 1 0 7 6 5 4 11 10 9 8 15 14   4 5 6 7 0 1 2 3 12 13 14 15 8 9   5 4 7 6 1 0 3 2 13 12 15 14 9 8   6 7 4 5 2 3 0 1 14 15 12 13 10 11   7 6 5 4 3 2 1 0 15 14 13</td><td>0 1 2 3 4 5 6 7 8 9 10 11 12 13 14   1 0 3 2 5 4 7 6 9 8 11 10 13 12 15   2 3 0 1 6 7 4 5 10 11 8 9 14 15 12   3 2 1 0 7 6 5 4 11 10 9 8 15 14 13   4 5 6 7 0 1 2 3 12 13 14 15 8 9 10   5 4 7 6 1 0 3 2 13 12 15 14 9 8 11   6 7 4 5 2 3 0 1 14 15 12 13 10 11 8   7 6 5 4</td></td<>	0 1 2 3 4 5 6 7   1 0 3 2 5 4 7 6   2 3 0 1 6 7 4 5   3 2 1 0 7 6 5 4   4 5 6 7 0 1 2 3   5 4 7 6 1 0 3 2   6 7 4 5 2 3 0 1   7 6 5 4 3 2 1 0   8 9 10 11 12 13 14 15   9 8 11 10 13 12 15 14   10 11 8 9 14 15 12 13   11 10 9 8 15 14 13 12   12 13 14 15 8 9 10 11	0 1 2 3 4 5 6 7 8   1 0 3 2 5 4 7 6 9   2 3 0 1 6 7 4 5 10   3 2 1 0 7 6 5 4 11   4 5 6 7 0 1 2 3 12   5 4 7 6 1 0 3 2 13   6 7 4 5 2 3 0 1 14   7 6 5 4 3 2 1 0 15   8 9 10 11 12 13 14 15 0   9 8 11 10 13 12 15 14 1   10 11 8 9 14 15 12 13 2   11 10 9 8 15 14	0 1 2 3 4 5 6 7 8 9   1 0 3 2 5 4 7 6 9 8   2 3 0 1 6 7 4 5 10 11   3 2 1 0 7 6 5 4 11 10   4 5 6 7 0 1 2 3 12 13   5 4 7 6 1 0 3 2 13 12   6 7 4 5 2 3 0 1 14 15   7 6 5 4 3 2 1 0 15 14   8 9 10 11 12 13 14 15 0 1   9 8 11 10 13 12 15 14 1 0   10 11 8 9 14 15	0 1 2 3 4 5 6 7 8 9 10   1 0 3 2 5 4 7 6 9 8 11   2 3 0 1 6 7 4 5 10 11 8   3 2 1 0 7 6 5 4 11 10 9   4 5 6 7 0 1 2 3 12 13 14   5 4 7 6 1 0 3 2 13 12 15   6 7 4 5 2 3 0 1 14 15 12   7 6 5 4 3 2 1 0 15 14 13   8 9 10 11 12 13 14 15 0 1 2   9 8 11 10 13 12 15 14	0 1 2 3 4 5 6 7 8 9 10 11   1 0 3 2 5 4 7 6 9 8 11 10   2 3 0 1 6 7 4 5 10 11 8 9   3 2 1 0 7 6 5 4 11 10 9 8   4 5 6 7 0 1 2 3 12 13 14 15   5 4 7 6 1 0 3 2 13 12 15 14   6 7 4 5 2 3 0 1 14 15 12 13   7 6 5 4 3 2 1 0 15 14 13 12   8 9 10 11 12 3 1 1 1 3 2 1	0 1 2 3 4 5 6 7 8 9 10 11 12   1 0 3 2 5 4 7 6 9 8 11 10 13   2 3 0 1 6 7 4 5 10 11 8 9 14   3 2 1 0 7 6 5 4 11 10 9 8 15   4 5 6 7 0 1 2 3 12 13 14 15 8   5 4 7 6 1 0 3 2 13 12 15 14 9   6 7 4 5 2 3 0 1 14 15 12 13 10   7 6 5 4 3 2 1 0 15 14 13 12 11   8 9 10 11	0 1 2 3 4 5 6 7 8 9 10 11 12 13   1 0 3 2 5 4 7 6 9 8 11 10 13 12   2 3 0 1 6 7 4 5 10 11 8 9 14 15   3 2 1 0 7 6 5 4 11 10 9 8 15 14   4 5 6 7 0 1 2 3 12 13 14 15 8 9   5 4 7 6 1 0 3 2 13 12 15 14 9 8   6 7 4 5 2 3 0 1 14 15 12 13 10 11   7 6 5 4 3 2 1 0 15 14 13	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14   1 0 3 2 5 4 7 6 9 8 11 10 13 12 15   2 3 0 1 6 7 4 5 10 11 8 9 14 15 12   3 2 1 0 7 6 5 4 11 10 9 8 15 14 13   4 5 6 7 0 1 2 3 12 13 14 15 8 9 10   5 4 7 6 1 0 3 2 13 12 15 14 9 8 11   6 7 4 5 2 3 0 1 14 15 12 13 10 11 8   7 6 5 4

# 乘法表为

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	0	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2

- 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

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

证明:由乘法逆元素的含义,有

$$q \cdot q^{-1} mod p = 1 + kp$$

即

$$p|(q \cdot q^{-1} \bmod p - 1)$$

而

$$p|(p \cdot p^{-1} modq)$$

所以

$$p|(q \cdot q^{-1} mod p + p \cdot p^{-1} mod q - 1)$$

同理可证

$$q|(q \cdot q^{-1} \mod p + p \cdot p^{-1} \mod q - 1)$$

因为p,q互素,且N=pq,从而有

$$N|(q \cdot q^{-1} \bmod p + p \cdot p^{-1} \bmod q - 1)$$

进一步,因为

$$0 < q \cdot q^{-1} \mod p \le q \cdot p = N$$

$$0$$

$$0 < q \cdot \mathbf{q}^{-1} \bmod \mathbf{p} + \mathbf{p} \cdot \mathbf{p}^{-1} \bmod \mathbf{q} - 1 \leq 2 \mathbf{N} - 1$$

从而结论成立。

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

$$ord(a \cdot b) = ord(a) \cdot ord(b)$$

证明: 假设 ord(a)=m, ord(b)=n, ord(a·b)=k, 则(m,n)=1。

首先由 ord(a)=m, ord(b)=n 可得 a <sup>m·n</sup>=(a<sup>m</sup>)<sup>n</sup>=e,从而由群中元素指数的 性质得

$$k \mid m \cdot n;$$

其次由  $ord(a \cdot b)=k$  可得 $(a \cdot b)^k=e$ ,因为 G 是有限交换群,所以得到  $a^k=b^{-k}$ ,从而

$$ord(a^k) = ord(b^{-k}) = ord(b^k) \circ$$

根据指数阶的性质

$$ord(a^k) = ord(a)/(ord(a),k)$$

满绩小铺: 1433397577, 搜集整理不易, 自用就好, 谢谢!

得

#### m(n,k)=n(m,k)

由于(m,n)=1,所以 m|(m,k),从而 m|k;同理可得 n|k, 由(m,n)=1 得 m·n|k。

由此得  $k= m \cdot n$ ,即  $ord(a \cdot b)=ord(a) \cdot ord(b)$ 。

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)

答: (1) 如果集合元素个数为1,即G={e},e\*e=e;

- (2) 如果集合元素个数为 2, 即 G={e, a}, e\*e=e= a\*a, e\*a= a\*e=a;
- (3) 如果集合元素个数为 3, 即 G={e, a, b},则运算表为

*	е	a	b
е	е	a	b
a	a	b	е
b	b	е	a

(4)如果该集合的元素个数为 4,而该代数系统能够成为一个群,所以元素 a,b,c 的阶为 2 或者 4,如果存在元素的阶为 4,不妨设 |a|=4,则该运算表为

*	е	a	b	С
е	е	a	b	С

满绩小铺 QQ: 1433397577, 搜集整理不易, 自用就好, 请勿倒卖, 谢谢!

a	a	b	С	е
b	b	С	е	a
С	С	е	a	b

如果不存在元素的阶为 4, 则 a, b, c 的阶都为 2, 于是, ab=ba=c, bc=cb=a, ac=b=ca, 则该运算表为

*	е	a	b	С
е	е	a	b	С
a	a	е	c	b
b	b	c	е	a
С	С	b	a	е

(5) 如果集合元素个数为 5, 即  $G=\{e, a, b, c, d\}$ , 则存在 5 阶元, 不妨设  $a^2=b$ ,  $a^3=c$ ,  $a^4=d$ , 则运算表为

*	е	a	b	С	d
е	e	a	b	С	d
a	a	b	С	d	е
b	b	С	d	е	a
c	С	d	е	a	b
d	d	е	a	b	С

满绩小铺: 1433397577, 搜集整理不易, 自用就好, 谢谢!