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 $x^2\equiv 13 \pmod{101}$ 的解。

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

$x\equiv \pm 35 \bmod 101$。

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：

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

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

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

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

证明：由乘法逆元素的含义，有

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

即

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

而

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

所以

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

同理可证

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

因为 p,q 互素，且 N=pq，从而有

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

进一步，因为

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

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

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

从而结论成立。

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

ord(a · b)=ord(a) · 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 $a^{m\cdot n}=(a^m)^n=e$，从而由群中元素指数的性质得

$$k|\ m\cdot n;$$

其次由 ord(a · 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

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

根据指数阶的性质

$$\mathrm{ord}(a^k)=\mathrm{ord}(a)/(\mathrm{ord}(a),k)$$

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

$$m\cdot n|k。$$

由此得 k= m · n,即 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）

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

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	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

*	e	a	b	c
e	e	a	b	c

a	a	b	c	e
b	b	c	e	a
c	c	e	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

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

（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

*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c