一. 计算题（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 $x^2+x+7\equiv0$（mod 27）。

解 因为（4，27）=1，所以由同余式的性质可以得到

$4x^2+4x+28\equiv0$（mod 27），即 $4x^2+4x+1\equiv0$（mod 27），于是

$(2x+1)^2\equiv0$（mod 27），因此 $2x+1\equiv0$（mod 9）, 利用一次同余式的求解方法得 $x\equiv4$（mod 9）, 所以原同余式的解为

$x\equiv4$，13，22（mod 27）。

3 求同余式 $x^2\equiv13\pmod{101}$ 的解。

解 因为 101=4*25+1，所以同余式 $x^2\equiv13\pmod{101}$ 的解为

$x\equiv\pm35\bmod 101$。

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：

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

二. 证明题（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

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

而

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

所以

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

同理可证

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

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

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

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

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

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

$\mathrm{ord}(a \cdot b)=\mathrm{ord}(a) \cdot \mathrm{ord}(b)$。

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

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

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

$$m \cdot n \mid k。$$

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