“信息安全数学基础”习题答案

第一章

1、证明：

(1) $\because a\mid b\Rightarrow b=ma(m\in Z),\quad c\mid d\Rightarrow d=nc(n\in Z),$
$\therefore bd=acmn(mn\in Z)$，即$ac\mid bd$。

(2) $\because a\mid b_1,a\mid b_2,\cdots,a\mid b_k,\therefore$根据整除的性质1－1(3)及递归法，可证得：
$a\mid(b_1c_1+b_1c_1+\cdots+b_kc_k)$，其中$c_1,c_2,\cdots c_k$为任意整数。

2、证明：

根据例题1-2(2)的证明结论知：
$\because(3,5)=1$，又$\because 3\mid a$且$5\mid a,\quad\therefore 15\mid a$，
又$\because(15,7)=1$，且$7\mid a,\quad\therefore 105\mid a$ 。

3、证明：

因为$n>p>n^{1/3}$，且 p 是 n 的最小素因数，若假设 n/p 不是素数，则有

$n/p=p_1\times p_2\times\cdots\times p_k$，（其中$k\geq 2,\ p_1,p_2,\cdots,p_k$为素数且均$\geq p$）
若 $k=2$，则$n/p=p_1\times p_2\geq p^2,\ \therefore n\geq p^3$, 即$p\leq n^{1/3}$, 与题设$n>p>n^{1/3}$矛盾，
所以假设不成立，即n/p为素数得证。

7、证明：

首先证明形如 6*k*-1 的正整数 *n* 必含有 6*k*-1 形式的素因子，这显然是成立的。因为如果其所有素因数均为 6*k*+1 形式，则$n=p_1\times p_2\times\cdots\times p_j,(p_i=6k_i+1,\ i=1,2,\cdots,j)$,从而得到 *n* 是形如 6*k*+1 形式的正整数，这与题设矛盾。

其次，假设形如 6*k*-1 的素数为有限个，依次为$q_1,q_2,\cdots q_s$，考虑整数 $n=6q_1q_2\cdots q_s-1$，则 *n* 是形如 6*k*-1 的正整数，所以 *n* 必有相同形式的素因数 *q*，使得使得 $q=q_j$ (1≤*j*≤*s*)。
由整数的基本性质(3)有：

$$q\mid(6q_1q_2\cdots q_s-n)=1,$$

这是不可能的。故假设错误，即存在无穷多个形如 4*k*-1 的素数得证。

11、解：

	n^2			n^3		
	最小非负余数	最小正余数	绝对值最小余数	最小非负余数	最小正余数	绝对值最小余数
3	0、1	1、3	0、1	0、1、2	1、2、3	-1、0、1
4	0、1	1、4	0、1	0、1、3	1、3、4	-1、0、1
8	0、1、4	1、4、8	1，0	0、1、3、5、7	1、3、5、7、8	3、1、-3、-1、0
10	0、1、4、5、6、9	1、4、5、6、9、10	-4、-1、0、1、4、5	0,1,2,3,4,5,6,7,8,9	1,2,3,4,5,6,7,8,10	-5,-4,-3,-2,-1,0,1,2,3,4

13、解：

(1)

$$259 = 222\times 1 + 37$$

$$222 = 37\times 6$$

$$\Rightarrow (222,259) = 37$$

$$37 = 259 - 222\times 1,\quad \therefore s = 1,\ t = -1$$

(2)

$$1395 = 713\times 1 + 682$$

$$713 = 682\times 1 + 31$$

$$682 = 31\times 22$$

$$\Rightarrow (1395,713) = 31$$

$$31 = 713 - 682\times 1 = 713 - (1395 - 713\times 1) = 2\times 713 + (-1)\times 1395,$$

$$\therefore s = -1,\ t = 2$$

16、解：

(1)

$$(112,56) = 56$$

$$[112,56] = \frac{112\times 56}{(112,56)} = 112$$

(2)

$$(67,335) = 67$$

$$[67,335] = \frac{67\times 335}{(67,335)} = 335$$

(3)

$$(1124,1368) = 4$$

$$[1124,1368] = \frac{1124\times 1368}{(1124,1368)} = 384408$$

19、解：

$\because (7,4)=1, c=0, \therefore 7\times(-1)+4\times 2=1$

$\therefore s=-1, t=2$

而不定方程的一切解为：$\begin{cases} x=-\dfrac{4k}{1}=-4k \\ y=\dfrac{7k}{1}=7k \end{cases}$ 其中，$k=0,\pm1,\pm2,\cdots$

又$\begin{cases} |x|\le 1000 \\ |y|\le 1000 \end{cases} \therefore k\le 142$

$\therefore$ 方程的全部解为$\begin{cases} x=-4k \\ y=7k \end{cases}$，其中 ，$k=0,\pm1,\cdots\pm142$

第二章

1、解：

(1) 错误。反例：a=7, b=3, m=8

(2) 错误。该命题当 m 为素数时才成立（$\because a^2+b^2 \equiv 0(\text{mod } m) \Leftrightarrow (a+b)(a-b)\equiv 0(\text{mod } m) \Leftrightarrow m|(a+b)(a-b)$，而只有 m 为素数时，才$\Leftrightarrow m|(a+b)$ 或 $m|(a-b)$）

(3) 错误。反例：a=1, b=4, m=3

(4) 正确。

证明：当 a, b 为偶数时，设 $a=2k, b=2k'$，则 $a^2=(2k)^2=4k^2$，$b^2=(2k')^2=4k'^2$，因为 $4k^2\equiv 4k'^2\equiv 0(\text{mod}4)$，所以 $a^2 \equiv b^2(\text{mod}4)$；

当 a, b 为奇数时，设 $a=2k+1, b=2k'+1$，则 $a^2=(2k+1)^2=4(k^2+k)+1$，$b^2=(2k'+1)^2=4(k'^2+k')+1$，因为 $4(k^2+k)+1\equiv 4(k'^2+k')+1\equiv 1(\text{mod}4)$，所以 $a^2 \equiv b^2(\text{mod}4)$。

4、解：

设未知数为 x，则根据弃九法，有：

$$((7+8+9+5+4)\bmod 9\times(9+8+3+5+1)\bmod 9)\bmod 9=(7+7+6+5+x+4+8+5+4)\bmod 9$$

解之得：x=2

5、解：

因为 $\text{ord}_7(3)=6$，即 $3^6\equiv 1(\text{mod } 7)$，所以

$3^{3025}\equiv((3^6)^{504}\times 3)\equiv 1\times 3\equiv 3(\text{mod}\,7)$，故此后第 3^{3025} 是星期日。

6、解：

因为 $\text{ord}_{100}(3)=20$, 即 $3^{20}\equiv 1(\text{mod } 100)$，所以

$3^{408}\equiv(3^{20})^{20}\times 3^8\equiv 1\times 3^8\equiv 61(\text{mod}100)$，故 3^{408} 写成十进制时的最后两位数是 61。

9、解：

(1) 模 11 的一组全为奇数的完全剩余系为：1，3，5，7，9，11，13，17，19，21

(2) 模 11 的一组全为偶数的完全剩余系为：0，2，4，6，8，10，12，14，16，18，20

(3) 设模 m 的完全剩余系为：$k_0m,\ k_1m+1,\ k_2m+2,\ \cdots,\ k_{m-1}m+(m+1),\ \ (k_i\in Z)$

由于 2|m，所以 $2\,|\,k_im+r_i\ (k_i\in Z,\ r_i=0,2,4,\cdots,m-2)$，

而 $2\nmid k_jm+r_j\ (k_j\in Z,\ r_j=1,3,5,\cdots,m-1)$，

因此，模 m 的完全剩余系中一半是偶数，一半是奇数。

12、

证明：因为{1，2，…，n}中，与 n 互素的个数为 $\varphi(n)$，将{1，2，…，nk}分成 k 个集合，每个集合由 n 个连续的整数构成。每个集合都是一组模 n 的完全剩余系，由例题 2-8 的结论：

模 m 的同一个剩余类中任意两个整数与 m 的最大公约数相同知，每个集合中与 n 互素的整数为 $\varphi(n)$ 个，故在不超过 nk 的正整数中，和 n 互素的整数的个数为 $k\varphi(n)$ 。

13、（该题有问题，可不做）

证明：

因为 $a+a^2+\cdots+a^{\varphi(m)}=\dfrac{a(a^{\varphi(m)}-1)}{a-1}$，所以原命题等价于证明 $\dfrac{a(a^{\varphi(m)}-1)}{a-1}\equiv 0(\bmod m)$，

又因为(*a, m*)=1？，由同余的性质 2-2(1)和(5)知，

$$\frac{a(a^{\varphi(m)}-1)}{a-1}\equiv 0(\bmod m)\Leftrightarrow a(a^{\varphi(m)}-1)\equiv 0(\bmod m)$$

又因为(*a,m*)=1，所以由欧拉定理有 $a^{\varphi(m)}=1(\bmod m)$，即 $a(a^{\varphi(m)}-1)\equiv 0(\bmod m)$ 成立。

所以，原命题 $a+a^2+\cdots+a^{\varphi(m)}\equiv 0(\bmod m)$ 成立。

15、证明：

(1) 由 Wilson 定理有：

n 是素数$\Leftrightarrow (n-1)!\equiv -1(\bmod n)\Leftrightarrow (n-1)!+1\equiv 0(\bmod n)\Leftrightarrow n\mid (n-1)!+1$

(2) 由 Wilson 定理有：

n 是素数 $\Leftrightarrow (n-1)!\equiv -1(\bmod n)\Leftrightarrow$

$(n-1)!\equiv n-1(\bmod n)\Leftrightarrow (n-2)!(n-1)\equiv n-1(\bmod n)$，

又因为 ((*n*-1), *n*) = (-1, *n*) = (1, *n*) = 1，所以由同余的性质 2-2(1)和(5)有：

$(n-2)!(n-1)\equiv n-1(\bmod n)\Leftrightarrow (n-2)!\equiv 1(\bmod n)\Leftrightarrow n\mid ((n-2)!-1)$

即 n 是素数的充要条件为 n|((*n*-2)!-1)。

(3) 由 Wilson 定理有：

n 是素数 $\Leftrightarrow (n-1)!\equiv -1(\bmod n)$

$$\begin{aligned}
&\Leftrightarrow (n-k)!(n-(k-1))(n-(k-2))\cdots(n-1)\equiv -1(\bmod n)\\
&\Leftrightarrow (n-k)!(-(k-1))(-(k-2))\cdots(-1)\equiv -1(\bmod n)\\
&\Leftrightarrow (n-k)!(k-1)!(-1)^{k-1}\equiv -1(\bmod n)\\
&\Leftrightarrow (n-k)!(k-1)!\equiv -(-1)^{k-1}(\bmod n)\\
&\Leftrightarrow n\mid \left((n-k)!(k-1)!+(-1)^{k-1}\right)
\end{aligned}$$

17、证明：

（方法一）首先，令 $p=4k+1(k\geq 0)$，则

$$(\frac{p-1}{2}!)^2 \equiv (2k!)^2 \equiv 2k\times(-(p-2k))\times(2k-1)\times(-(p-(2k-1))\cdots\times 1\times(-(p-1))$$

$$\equiv (-1)^{2k}\times 2k\times(2k+1)\times(2k-1)\times(2k+2)\cdots\times 1\times 4k \equiv (-1)^{2k}\times(4k)!\equiv(-1)^{2k}\times(p-1)!=-1(\mathrm{mod}\ p)$$

所以 $x^2\equiv$ -1 (mod p)的解为： $x\equiv\pm\frac{p-1}{2}!(\mathrm{mod}\ p)$ 。

又因为 p 为奇素数，所以 $\frac{p-1}{2}!$ 和 $-\frac{p-1}{2}!$ 模 p 不同余，

综上可证，同余式 $x^2\equiv$ -1 (mod p)有两个不同的解 $x\equiv\pm\frac{p-1}{2}!(\mathrm{mod}\ p)$ 。

（方法二）由第三章的知识有，因为 p 为 4k+1 形式的素数，所以 $\left(\frac{-1}{p}\right)=1$ ，即

同余式 $x^2\equiv$ -1 (mod p)有两个不同的解。再由方法一中的证明过程可得：

$x^2\equiv$ -1 (mod p)的两个不同的解为： $x\equiv\pm\frac{p-1}{2}!(\mathrm{mod}\ p)$ 。

18、解：

(1) 利用算法 2-1，有

$m_0=1,a_0=2,b_0=2,m_1=1,a_1=4,b_1=8,m_2=1,a_2=16,b_2=6,$

$m_3=,0a_3=12,b_3=6,m_4=1,a_4=22,b_4=10,m_5=1,a_5=57,b_5=21,$

$m_6=0,a_6=16,b_6=21,m_7=0,a_7=12,b_7=21,m_8=0,a_8=22,b_8=21,$

$m_9=1,a_9=57,b_9=38,$

故， $2^{567}\bmod 61=38$ 。

(2) 运用相同的算法，有 $41^{54321}\bmod 103=93$ 。

19、解：

(1)（方法一）

$$\varphi(325)=325\times(1-\frac{1}{5})\times(1-\frac{1}{13})=240\Rightarrow 7^{-1}\bmod 325=7^{240-1}\bmod 325=7^{239}\bmod 325$$

利用算法 2-1，解得 $7^{325}\bmod 325=93$

（方法二）

$325=46\times 7+3$

$7=2\times 3+1$

$3=3\times 1$

故$(7,325)=1=7-2\times 3=7-2\times(325-46\times 7)=93\times 7-2\times 325$

$\Rightarrow s=93,$ 即$7^{-1}\bmod 325=93$

(2) 61^{-1} mod 1024 = 789

(3) 79^{-1} mod 2623 = 2457

24、解：

(1) 取模 11 的最小非负完全剩余系：$0,\cdots,10$，直接计算可知，2 是同余式 $x^3-2x+7\equiv 0(\mathrm{mod}11)$ 的解，故该同余式的解为：$x\equiv 2(\mathrm{mod}11)$，解数为 1。

(2) 取模 7 的最小非负完全剩余系：0, ⋯, 6，直接计算可知， 0 和 2 是同余式 $x^5-2x^4+14\equiv 0(\mathrm{mod}7)$ 的解，故该同余式的解为：$x\equiv 0,2(\mathrm{mod}7)$，解数为 2。

(3) 该同余式的解为：$x\equiv 7,19(\mathrm{mod}24)$，解数为 2。

(3) 该同余式无解为

25、解：（过程略，见算法 2-7）

(1) 因为(5,11)=1|4，所以同余式$5x\equiv 4(\mathrm{mod}11)$有 1 个解，其解为：

$x\equiv 4\times 5^{-1}\equiv 3(\mathrm{mod}\ 11)$。

(2) 因为(3,9)=3|6，所以同余式$3x\equiv 6(\mathrm{mod}9)$有 3 个解，其解为：$x\equiv 2,5,8(\mathrm{mod}9)$。

(3) $87x\equiv 16(\mathrm{mod}61)\Leftrightarrow 26x\equiv 16(\mathrm{mod}61)$，所以原同余式有 1 个解，其解为：

$x\equiv 10(\mathrm{mod}61)$。

26、解：

设至少 x 周后，他可以在周三休息，

如果周三是他休息的第一天，则$7x+2\equiv 0(\mathrm{mod}13)$，解为 $x\equiv 9$ (mod13)。

如果周三是他休息的第二天，则$7x+1\equiv 0(\mathrm{mod}13)$，解为 $x\equiv 11$ (mod13)。

如果周三是他休息的第一天，则$7x\equiv 0(\mathrm{mod}13)$，解为 $x\equiv 13$ (mod13)。

综上，至少在 9 周之后，他可以在周三休息。

28、解：

(1) 原题设等价于：

$$\begin{cases}x\equiv 3(\mathrm{mod}11)\\ x\equiv 2(\mathrm{mod}72)\\ x\equiv 1(\mathrm{mod}13)\end{cases}$$

根据中国剩余定理，可知：

$m_1=11,m_2=72,m_3=13$

$M_1=72\times 13=936,M_2=11\times 13=143,M_3=11\times 72=792$

$M_1^{'}=936^{-1}\ \mathrm{mod}11=1,M_2^{'}=143^{-1}\ \mathrm{mod}\ 72=71,M_3^{'}=792^{-1}\ \mathrm{mod}13=12,$

$\therefore x\equiv 936\times 1\times 3+143\times 71\times 2+792\times 12\times 1\equiv 1730(\mathrm{mod}10296)$

$\Rightarrow x\equiv 1730(\mathrm{mod}10296)$

所以，该数为 1730。

(2) 原题设等价于：

$$\begin{cases} x \equiv 1(\mathrm{mod}\,2) \\ x \equiv 2(\mathrm{mod}\,5) \\ x \equiv 3(\mathrm{mod}\,7) \\ x \equiv 4(\mathrm{mod}\,9) \end{cases}$$

根据中国剩余定理，可知：

$m_1 = 2, m_2 = 5, m_3 = 7, m_4 = 9$

$M_1 = 5\times 7\times 9 = 315, M_2 = 2\times 7\times 9 = 126, M_3 = 2\times 5\times 9 = 90, M_4 = 2\times 5\times 7 = 70,$

$M_1^{'} = 315^{-1} \bmod 2 = 1, M_2^{'} = 126^{-1} \bmod 5 = 1, M_3^{'} = 90^{-1} \bmod 7 = 6, M_4^{'} = 70^{-1} \bmod 9 = 4,$

$\therefore x \equiv 315\times 1\times 1 + 126\times 1\times 2 + 90\times 6\times 3 + 70\times 4\times 4(\mathrm{mod}\,630)$

$\Rightarrow x \equiv 157(\mathrm{mod}\,630)$

所以，该数为 157。

31、解：

因为 $6x \equiv 4(\mathrm{mod}\,8)$ 有 2 个解，其解为： $x \equiv 2, 6(\mathrm{mod}\,8)$

所以原同余式组等价于：

$$\begin{cases} x \equiv 5(\mathrm{mod}\,7) \\ x \equiv 2, 6(\mathrm{mod}\,8) \end{cases}$$

根据中国剩余定理可求得：该同余时组有 2 个解，其解为 $x \equiv 26, 54(\mathrm{mod}\,56)$ 。

32、解：

原同余式组等价于：

$$\begin{cases} x \equiv 3(\mathrm{mod}\,11) \\ x \equiv 6(\mathrm{mod}\,9) \end{cases}$$

根据中国剩余定理可求得：该同余式组的解为 $x \equiv 69(\mathrm{mod}\,99)$ 。

33、解：

该命题等价于求解同余式组 $\begin{cases} x \equiv 2^{1000000}(\mathrm{mod}\,11) \\ x \equiv 2^{1000000}(\mathrm{mod}\,5) \end{cases}$

因为 $\mathrm{ord}_{11}(2)=10$，$\mathrm{ord}_5(2)=4$，所以

$$\begin{cases} x \equiv 2^{1000000}(\mathrm{mod}\,11) \\ x \equiv 2^{1000000}(\mathrm{mod}\,5) \end{cases} \Leftrightarrow \begin{cases} x \equiv (2^{10})^{100000} \equiv 1(\mathrm{mod}\,11) \\ x \equiv (2^4)^{250000} \equiv 1(\mathrm{mod}\,5) \end{cases}$$

根据中国剩余定理可求得：该同余式组的解为 $x \equiv 1(\mathrm{mod}\,55)$ 。

所以，$2^{1000000} \bmod 55 = 1$。

第三章

1、解：

(1)

j	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10	±11
$a=j^2 \bmod 23$	1	4	9	16	2	13	3	18	12	8	6

所以，23 的平方剩余为：1，2，3，4，6，8，9，12，13，16，18，

23 的平方非剩余为：5，7，10，11，14，15，17，19，20，21，22

(2)

j	±1	±5	±7	±11
$a=j^2 \bmod 24$	1	1	1	1

所以，24 的平方剩余为：1

24 的平方非剩余为：5，7，11，13，17，19，23

2、解：

(1) $x^2 \equiv 2(\bmod 3)$

$\because (\frac{2}{37}) = (-1)^{\frac{37^2-1}{8}} = -1, \therefore$ 同余式无解，解数为 0.

(2) $x^2 \equiv 3(\bmod 39) \Leftrightarrow \begin{cases} x^2 \equiv 3 \equiv 0(\bmod 3) \\ x^2 \equiv 3(\bmod 13) \end{cases}$

又 $\because (\frac{3}{13}) = (-1)^{\frac{3-1}{2}\times\frac{3-1}{2}}(-1) = 1$

所以，同余式有解，解数为 2。

(3) $x^2 \equiv 4(\bmod 45) \Leftrightarrow \begin{cases} x^2 \equiv 4(\bmod 3^2) & (1) \\ x^2 \equiv 4(\bmod 5) & (2) \end{cases}$

又 $\because (\frac{4}{3}) = 1, (\frac{4}{5}) = 1$，所以(1)(2)的解数分别为2，故原同余式的解数为4 。

(4) $x^2 \equiv 5(\bmod 48) \Leftrightarrow \begin{cases} x^2 \equiv 5(\bmod 3) & (1) \\ x^2 \equiv 5(\bmod 2^4) & (2) \end{cases}$

又 $\because (\frac{5}{3}) = (\frac{2}{3}) = -1, \therefore$ 同余式(1)无解，

所以原同余式也无解。

3、证明：

(1) 设模 p 的所有平方剩余的乘积对模 p 的剩余是 A，因为 p 是奇素数，

则由定理 3-2 有：

$$A \equiv 1^2 \cdot 2^2 \cdots \left(\frac{p-1}{2}\right)^2$$

$$\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) \cdot (-1)^{\frac{p-1}{2}}$$

$$\equiv 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot (-1)^{\frac{p-1}{2}}$$

$$\equiv (p-1)!(-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

又由 Wilson 定理有，$A \equiv (-1) \cdot (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\, p)$。

∴ 当 p 是奇素数时，模 p 的所有平方剩余的乘积对模 p 的剩余是 $(-1)^{\frac{p+1}{2}}$。

(2) 设模 p 的所有平方非剩余的乘积对模 p 的剩余是 B，则有：

$$A \times B \equiv (p\text{-}1)! \ (\mathrm{mod}\, p),$$

又由 Wilson 定理和(1)的证明结果有：

$$B \cdot (-1)^{\frac{p+1}{2}} \equiv -1 (\mathrm{mod}\, p)$$

$$\Leftrightarrow B \equiv (-1) \cdot (-1)^{\frac{p+1}{2}} \equiv (-1)^{\frac{p-1}{2}+2} \equiv (-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

∴ 当 p 是奇素数时，模 p 的所有平方非剩余的乘积对模 p 的剩余是 $(-1)^{\frac{p-1}{2}}$。

(3) 设模 p 的所有平方剩余的和对模 p 的剩余是 C，模 p 的所有平方非剩余的和对模 p 的剩余是 D，则由定理 3-2 有：

$$C = 1^2 + 2^2 + \cdots + \left(\frac{p-1}{2}\right)^2 = \frac{(p^2-1) \cdot p}{24} (\mathrm{mod}\, p)$$，其中 $\frac{(p^2-1) \cdot p}{24}$ 为整数，

因为 p 是奇素数，且 p>3，而 $24 = 2^3 \times 3$，所以 $(p, 24)=1$，即 $24 \mid (p^2\text{-}1)$。

所以，$C \equiv 0 (\mathrm{mod}\, p)$，即模 p 的所有平方剩余的和对模 p 的剩余是 0。

又因为 $D \equiv (1+2+\cdots+p-1) - C \equiv \frac{(p-1) \cdot p}{2} - 0 \equiv \frac{(p-1) \cdot p}{2} (\mathrm{mod}\, p)$，

而 p 为大于 3 的奇素数，即 $2 \mid (p\text{-}1)$，所以 $D \equiv 0 (\mathrm{mod}\, p)$，即

模 p 的所有平方非剩余的和对模 p 的剩余是 0。

4、解：

(1) $$\left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right) \times \left(\frac{3}{17}\right) = 1 \times (-1)^{\frac{3-1}{2} \times \frac{17-1}{2}} \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

(2) $$\left(\frac{23}{37}\right) = (-1)^{\frac{23-1}{2} \times \frac{31-1}{2}} \left(\frac{31}{23}\right) = -\left(\frac{8}{23}\right) = -\left(\frac{2}{23}\right) \times \left(\frac{2}{23}\right) \times \left(\frac{2}{23}\right) = -1$$

(3) $\left(\frac{24}{23}\right)=\left(\frac{1}{23}\right)=1$

(4) $\left(\frac{21}{29}\right)=(-1)^{\frac{21-1}{2}\times\frac{29-1}{2}}\left(\frac{29}{21}\right)=\left(\frac{8}{21}\right)=\left(\frac{2}{21}\right)\times\left(\frac{2}{21}\right)\times\left(\frac{2}{21}\right)=-1$

5、证明：

假设形如 8*k*+5 的素数只有有限多个，设这些素数为 $p_1,p_2,\cdots p_k$，考虑整数

$$N=\left(p_1p_2\cdots p_k\right)^2+4,$$

因为 $p_1p_2\cdots p_k$ 为奇数，所以，$N=(2k+1)^2+4=4\left(k^2+k\right)+5=4k\left(k+1\right)+5$，

又因为 *k* 中 *k*+1 一定有一个为偶数，故 $N=4\times2k^{'}+5=8k^{'}+5$。

因为 $N>p_i,i=1,2,\cdots,k$，所以，*N* 为形如 8*k*+5 的合数，其任意素因数 *p* 均为奇素数，且

$\left(p_i,p\right)=1,\ (i=1,2,\cdots,k)$（假设 $p=p_i$，则 $p|(N-(p_1p_2\ldots p_k)^2=4$，这是不可能的。）

$\therefore\ \left(\frac{-4}{p}\right)=\left(\frac{4}{p}\right)\left(\frac{-1}{p}\right)=\left(\frac{-1}{p}\right)=\left(\frac{-4+N}{p}\right)=\left(\frac{(p_1p_2\cdots p_k)^2}{p}\right)=1=(-1)^{\frac{p-1}{2}}$，

由该式可知，*p* 是 4*k*+1 形式的素数，即 *p* 只可能为 8*k*+1 和 8*k*+5 形式的素数。
若 N 的素因数均为 8*k*+1 形式，则 *N* 为 8*k*+1 形式，所以 *N* 的素因数中至少包含一个 8*k*+5 形式的奇素因数 *p*，即存在整数 $j\ \ (1\le j\le k)$，使得 $p=p_j$，这与 $\left(p,p_i\right)=1,(i=1,2,\cdots,k)$ 矛盾。故，假设不成立，即形如 8*k*+5 的素数有无限多个得证。

6、解：

(1) $\left(\frac{23}{75}\right)=\left(\frac{23}{5}\right)^2\left(\frac{23}{3}\right)=\left(\frac{2}{3}\right)=-1$

(2) $\left(\frac{77}{45}\right)=\left(\frac{32}{5}\right)\left(\frac{32}{3}\right)^2=\left(\frac{2}{5}\right)=-1$

(3) $\left(\frac{25}{33}\right)=\left(\frac{5}{33}\right)^2=1$

(4) $\left(\frac{21}{25}\right)=\left(\frac{21}{5}\right)^2=1$

12、解：

(1)$\because \left(\frac{176}{401}\right)=\left(\frac{2^4}{401}\right)\left(\frac{11}{401}\right)=(-1)^{\frac{401-1}{2}\cdot\frac{11-1}{2}}\cdot\left(\frac{5}{11}\right)=(-1)^{\frac{11-1}{2}\cdot\frac{5-1}{2}}\cdot\left(\frac{1}{5}\right)=1$，所以同余式有解。

又$\because p=401\equiv 1(\bmod 4)$，运用情形2： $p-1=2^4\times 25$，$t=4,s=25$

任意选择模 401 的平方非剩余，n=3,$\left(\frac{3}{401}\right)=-1$，

计算$\left(176^{25}\right)^4 \bmod 401=400,$所以，$j_0=1,a_1=a\times n^2=176\times 9$

计算$\left(a_1^{25}\right)^2 \bmod 401=400,$所以，$j_1=1,a_2=a_1\times n^4=1584\times 81$

计算$a_2^{25} \bmod 401=1,$所以，$j_2=0$

因此，原同余式的解为$x\equiv\pm 176^{\frac{25+1}{2}}\times 3^{25\times(1+2)}(\bmod p)\equiv\pm 101(\bmod 401)$

(2) $\because \left(\frac{176}{103}\right)=\left(\frac{2^4}{103}\right)\left(\frac{11}{103}\right)=(-1)^{\frac{103-1}{2}\cdot\frac{11-1}{2}}\cdot\left(\frac{4}{11}\right)=(-1)\cdot 1=-1$，所以同余式有解。

14、解：（该同余式的求解也可以参见定理 2-14，即先求$x^2\equiv 41(\bmod 2)$的解 ）

$\because 41\equiv 1(\bmod 8),\therefore$同余式有4个解。

$x^2\equiv 41(\bmod 8)$的解为：$x=\pm(1+4t_3),t_3=0,1,\cdots$

由$(1+4t_3)^2\equiv 41(\bmod 16)$得 $t_3\equiv 1(\bmod 2)$

故$x^2\equiv 41(\bmod 16)$的解为：$x=\pm(1+4(1+2t_4))=\pm(5+8t_4),t_4=0,1,\cdots$

由$(5+8t_4)^2\equiv 41(\bmod 32)$得 $t_4\equiv 1(\bmod 2)$

故$x^2\equiv 41(\bmod 32)$的解为：$x=\pm(13+16t_5),t_5=0,1,\cdots$

由$(13+16t_5)^2\equiv 41(\bmod 64)$得 $t_5\equiv 0(\bmod 2)$

故$x^2\equiv 41(\bmod 64)$的解为：$x=\pm(13+32t_6),t_6=0,1,\cdots$

即，同余式$x^2\equiv 41(\bmod 64)$的解为：$x\equiv 13,19,45,51(\bmod 64)$

第四章

2、解：

(1) $\varphi(18)=6$，其正因数为 1, 2, 3, 6，

$5^1 \equiv 5(\mathrm{mod}\,18), 5^2 \equiv 7(\mathrm{mod}\,18), 5^3 \equiv -1(\mathrm{mod}\,18), 5^6 \equiv 1(\mathrm{mod}\,18)$ $\therefore \mathrm{ord}_{18}(5)=6$。

(2) $\varphi(79)=78$，其正因数为 1, 2, 3, 6, 13, 26, 39, 78

$\because 4^1 \equiv 4(\mathrm{mod}\,79),\ 4^2 \equiv 16(\mathrm{mod}\,79),\ 4^3 \equiv 64(\mathrm{mod}\,79),\ 4^6 \equiv -12(\mathrm{mod}\,79),$

$4^{13} \equiv 23(\mathrm{mod}\,79),\ 4^{26} \equiv 55(\mathrm{mod}\,79),\ 4^{39} \equiv 1(\mathrm{mod}\,79)$，

$\therefore \mathrm{ord}_4(4)=39$。

(3) $\because (9,11)=1,\ \therefore \mathrm{ord}_{99}(91)=\left[\mathrm{ord}_{11}(91), \mathrm{ord}_9(91)\right]$,

又 $\because \mathrm{ord}_9(91)=\mathrm{ord}_9(1)=1,\ \mathrm{ord}_{11}(91)=\mathrm{ord}_{11}(3)$，

而 $\varphi(11)=10$，其正因数为 1，2，5，10

计算：$3^1 \equiv 3(\mathrm{mod}\,11), 3^2 \equiv 9(\mathrm{mod}\,11), 3^5 \equiv 1(\mathrm{mod}\,11),$ 所以 $\mathrm{ord}_{11}(3)=5$

$\therefore ord_{99}(91)=[1,5]=5$

(4) $\because (3,73)=1, \therefore \mathrm{ord}_{219}(7)=\left[\mathrm{ord}_3(7), \mathrm{ord}_{73}(7)\right]$

又 $\because ord_3(7)=ord_3(1)=1$，而

$\varphi(73)=72$，其正因数为 1，2，3，4，6，8，9，12，18，24，36，72，经计算得：$\mathrm{ord}_{73}(7)=24$

$\therefore \mathrm{ord}_{219}(7)=[1,24]=24$。

5、解：

$\varphi(101)=100=2^2\times 5^2$，$\therefore 100$ 的素因数为 2 和 5.

$100/2=50;\ 100/5=20$，验证：$2^{20} \equiv -95(\mathrm{mod}\,101);\ 2^{50} \equiv 100(\mathrm{mod}\,101)$

所以，2 是模 101 的原根。

6、解：

$\because$ 2 是模 101 的一个原根，又 $\because$ $2^{100} \equiv 8074 \neq 1(\mathrm{mod}\ 101^2)$，

$\therefore$ 根据定理 4-2 有：2 或 2+101=103 都是模 101^2 的原根。

7、解：

由定理 4-2 和上题可知，103 和 $2+101^2=10203$ 都是模 2×101^2 的原根。

8、解：

$\because \varphi(43)=42=2\times3\times7,\quad 42/2=21,\ 42/3=14,\ 42/7=6$

验证：$2^6 \bmod 43=21,\ 2^{14} \bmod 43=1,\ 3^6 \bmod 43=-2,\ 3^{14} \bmod 43=36,\ 3^{21} \bmod 43=42,$

故，3 是模 43 的最小原根。计算：

$3^1 \bmod 43=3, 3^2 \bmod 43=9, 3^3 \bmod 43=27, 3^4 \bmod 43=38, 3^5 \bmod 43=28,$
$3^6 \bmod 43=41, 3^7 \bmod 43=37, 3^8 \bmod 43=25, 3^9 \bmod 43=32, 3^{10} \bmod 43=10,$
$3^{11} \bmod 43=30, 3^{12} \bmod 43=4, 3^{13} \bmod 43=12, 3^{14} \bmod 43=36, 3^{15} \bmod 43=22,$
$3^{16} \bmod 43=23, 3^{17} \bmod 43=26, 3^{18} \bmod 43=35, 3^{19} \bmod 43=19, 3^{20} \bmod 43=14,$
$3^{21} \bmod 43=42, 3^{22} \bmod 43=40, 3^{23} \bmod 43=34, 3^{24} \bmod 43=16, 3^{25} \bmod 43=5,$
$3^{26} \bmod 43=15, 3^{27} \bmod 43=21, 3^{28} \bmod 43=6, 3^{29} \bmod 43=18, 3^{30} \bmod 43=11,$
$3^{31} \bmod 43=33, 3^{32} \bmod 43=13, 3^{33} \bmod 43=39, 3^{34} \bmod 43=31, 3^{35} \bmod 43=7,$
$3^{36} \bmod 43=21, 3^{37} \bmod 43=20, 3^{38} \bmod 43=17, 3^{39} \bmod 43=8, 3^{40} \bmod 43=24,$
$3^{41} \bmod 43=29, 3^{42} \bmod 43=10,$

所以，以 3 为底的模 43 的指标为：

	0	1	2	3	4	5	6	7	8	9
0		42	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

查表可知，$3^{29}\equiv 18(\bmod 43)$，即有$x^{12}\equiv 18\equiv 3^{29}(\bmod 43)$

令$x=3^y(\bmod 43)\Leftrightarrow 3^{12y}\equiv 3^{29}(\bmod 43)$，由性质$4-2$知，$12y\equiv 29(\bmod 42)$
$\because (12,42)=6\nmid 29,\quad \therefore$此同余式无解。

9、解：（过程略）

(1) 查表可知，$\text{ind}_6 7=39$，$\because (22,\varphi(41))=2,$不能整除39，所以，同余式无解。

(4) 解：原方程等价于 $x^{30}\equiv 37\times5^{-1}\equiv 37\times33\equiv 32(\bmod 41)$，

通过查表得知，$\text{ind}_6 32=10$，即$6^{10}\equiv 32(\bmod 41), \therefore x^{30}\equiv 6^{10}\equiv 32(\bmod 41)$

令$x=6^y \bmod 41\Leftrightarrow 6^{30y}\equiv 6^{10}(\bmod 41)\Rightarrow 30y\equiv 10(\bmod 40)$，

因为(30,40)=10|10，所以该同余式有 10 个解，其解为：

$y\equiv 3,7,11,15,19,23,27,31,35,39(\bmod 40),$

通过查表得原同余式的解为：$x\equiv 11,29,28,3,34,30,12,13,38,7(\bmod 41)$

第五章

1、解：×表示不构成代数系统，√表示构成代数系统。

(1) ×

(2) √

(3) √

(4) ×

(5) ×

(6) √

(7) 加法×，乘法√

(8) √

(9) √

(10) 加法×，乘法√

2、解：

	交换律	结合律	分配律	单位元	零元	逆元
2	√	√		N 阶 0 矩阵	无	N 阶负阵
	×	√		N 阶单位阵	N 阶 0 阵	除 0 阵外逆元为其逆矩阵
3	√	√		1	无	1 的逆元为 1，其他元素无逆
6	×	√		无	$\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix}$	无
7	√	√		1	无	1 的逆元为 1，其他元素无逆
8	√	√		0	无	0 的逆元为 0，其他元素 i 的逆元为 n-i
9	√	√		全集	空集	全集的逆元为本身，其他元素无逆元
	√	√		空集	全集	空集的逆元为本身，其他元素无逆元
10	√	√		1	0	1 的逆元为 1

6、解：

(2) 加法乘法均构成群

(3) 幺半群

(6) 半群

(7) 乘法构成幺半群

(8) 群
(9) 并集和交集均构成幺半群
(10) 乘法构成群

7、解：是幺半群。

11、证明：

首先，设k_1为$a*b$的阶，k_2为$(b*a)$的阶，即$(a*b)^{k_1}=e,\ (b*a)^{k_2}=e,$，

$\therefore a^{-1}*(a*b)^{k_1}*b^{-1}=(b*a)^{k_1-1}=a^{-1}*b^{-1}$，$\therefore (b*a)^{k_1}=a^{-1}*b^{-1}*b*a=e$

即：$(b*a)^{k_1}=e$，所以，$k_2\mid k_1$，

同理，$k_1\mid k_2$

所以，$k_1=k_2$，得证。

12、证明：
首先，若群为交换群，则，根据定理 5-7，直接得证。
其次，$(x*y)^2=x^2*y^2\Rightarrow x*(y*x)*y=x*(x*y)*y$，根据群的消去律，$y*x=x*y$，命题得证。

15、 证明：

首先，*H* 是 *G* 的子群，那么 *H* 至少含有一个元素 *e*，则$xex^{-1}=e\in xHx^{-1}$，即xHx^{-1}是 G 的非空子集。

其次，$\forall xh_1x^{-1},xh_2x^{-1}\in xHx^{-1},$ 其中$h_1,h_2\in H$，因为$(xh_2x^{-1})^{-1}=(xh_2^{-1}x^{-1})$，

而$(xh_1x^{-1})(xh_2{}^{-1}x^{-1})=xh_1x^{-1}xh_2x^{-1}=xh_1h_2{}^{-1}x^{-1}$，其中由 *H* 是 *G* 的子群得$h_1h_2^{-1}\in H$，

所以$xh_1h_2{}^{-1}x^{-1}\in xHx^{-1}$。根据子群的判断定理二证得：$xHx^{-1}$构成 *G* 的子群。

16、证明：首先，因为$\exists e\in S,$使得$eSe^{-1}=S$，所以 *N*(*s*)为非空集合，

其次，$\forall x_1,x_2\in N(s),$有$x_1Sx_1^{-1}=S,x_2Sx_2^{-1}=S,$

则$x_1x_2S(x_1x_2)^{-1}=x_1x_2Sx_2{}^{-1}x_1{}^{-1}=x_1Sx_1^{-1}=S$，即$x_1x_2\in N(s),$

又因为$\forall x\in N(s),$有$xSx^{-1}=S$，则$x^{-1}Sx=x^{-1}(xSx^{-1})x=x^{-1}xSx^{-1}x=S$，即$x^{-1}\in N(s),$

所以，根据子群的判定定理一证得：*N*(*S*)构成 *G* 的子群。

20、证明：

$f:A\to|A|, f(A)=|A|$,设$\forall A,B\in G$,则$f(A\times B)=|A\times B|=|A|\times|B|=f(A)\cdot f(B)$,

命题得证。

21、证明：

$\forall a,b\in G, a=2^{m_1}3^{n_1}, b=2^{m_2}3^{n_2}$，则$a\times b=2^{m_1}3^{n_1}\times 2^{m_2}3^{n_2}=2^{m_1+m_2}3^{n_1+n_2}$，

则$f(a\times b)=2^{m_1+m_2}=2^{m_1}\times 2^{m_2}=f(a)\times f(b)$，得证。

23、证明：

设$\bullet,*$分别是G_1,G_2上的运算,因为$\varphi:G_1\to G_2$是同构映射，所以

$\forall a,b\in G_1, \varphi(a\bullet b)=\varphi(a)*\varphi(b)$，设$\varphi(a)=a', \varphi(b)=b'\in G_2$，则由$\varphi:G_1\to G_2$为双射

得：$\varphi^{-1}(a')=a, \varphi^{-1}(b')=b$，

故：$\varphi^{-1}(a'*b')=\varphi^{-1}(\varphi(a)*\varphi(b))=\varphi^{-1}(\varphi(a\bullet b))=a\bullet b=\varphi^{-1}(a')\bullet\varphi^{-1}(b')$，即：

又φ为双射，所以φ^{-1}也是双射，得证。

25、解：

(1) 共有 φ(15) = 8 个生成元，分别为，$a^1,a^2,a^4,a^7,a^8,a^{11},a^{13},a^{14}$

(2) 15 的正因子为，1，3，5，15，所以：

$\because|a^{d_1}|=\dfrac{|a|}{(|a|,d_1)}=\dfrac{15}{(15,d_1)}=1$，即$d_1=15,$

$\therefore 1$阶子群为：$<a^{15}>=<e>=\{e\}$

$\because|a^{d_3}|=\dfrac{|a|}{(|a|,d_5)}=\dfrac{15}{(15,d_3)}=3$，即$d_3=5,10,$

$\therefore 3$阶子群为：$<a^5>=<a^{10}>=\{e,a^5,a^{10}\}$

$\because|a^{d_5}|=\dfrac{|a|}{(|a|,d_5)}=\dfrac{15}{(15,d_5)}=5$，即$d_5=3,6,9,12$，

$\therefore 5$阶子群为：$<a^3>=<a^6>=<a^9>=<a^{12}>=\{e,a^3,a^6,a^9,a^{12}\}$

15阶子群为：$<a>=<a^2>=<a^4>=<a^7>=<a^8>=<a^{11}>=<a^{13}>=<a^{14}>=\{e,a^1,a^2,\cdots,a^{14}\}$

28、解：（该题是按照先进行前一个置换，再进行后一个置换的顺序计算的）

$$\sigma\tau=\begin{pmatrix}1&2&3&4&5\\3&4&2&5&1\end{pmatrix}=(1\quad 3\quad 2\quad 4\quad 5)$$

$$\tau\sigma=\begin{pmatrix}1&2&3&4&5\\5&4&2&1&3\end{pmatrix}=(1\quad 5\quad 3\quad 2\quad 4)$$

$$\sigma^{-1}=\begin{pmatrix}1&2&3&4&5\\2&1&5&3&4\end{pmatrix}=(1\quad 2)(\quad 3\quad 5\quad 4)$$

$$\tau^{-1}=\begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix}=(1\quad 3\quad 2\quad 4\quad)$$

$$\sigma^{-1}\tau=\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}=(1\quad 3\quad 5\quad 2\quad 4)\text{（5）}$$

$$\tau^{-1}\sigma=\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix}=(1\quad 4\quad 2\quad 5\quad 3)$$

$$\sigma^{-1}\tau\sigma=\begin{pmatrix}1&2&3&4&5\\4&5&3&2&1\end{pmatrix}=(1\quad 4\quad 2\quad 5\quad)\text{（3）}$$

29、解：（该题是按照先进行前一个置换，再进行后一个置换的顺序计算的）

$\alpha^{-1}=\alpha$，$\beta^{-1}=\beta$

(1) $x=\alpha^{-1}\beta=\begin{pmatrix}a&b&c&d&e\\d&e&a&b&c\end{pmatrix}$

(2) $x=\beta^{-1}\alpha=\begin{pmatrix}a&b&c&d&e\\c&d&e&a&b\end{pmatrix}$

补充题：写出$\langle Z_{13}^{*},\otimes\rangle$的所有生成元和子群。

解：$\because \varphi(13)=12=2^2\times 3,\ \therefore 12$的素因数为2和3，

$12/2=6,\ 12/3=4$，验证：$2^6\equiv -1(\mathrm{mod}13);\ 2^4\equiv 3(\mathrm{mod}13)$

$\therefore$2是模13的原根，即是$\langle Z_{13}^{*},\otimes\rangle$一个生成元。

又$\because \langle Z_{13}^{*},\otimes\rangle$是12阶循环群，$\varphi(12)=4$，

$\therefore \langle Z_{13}^{*},\otimes\rangle$共有4个生成元，分别为：2, 2^5mod13=6, 2^7mod13=11, 2^{11}mod13=7。

$\because \langle Z_{13}^{*},\otimes\rangle$是12阶循环群，12的正因子有1, 2, 3, 4, 6, 12，

$\therefore \langle Z_{13}^{*},\otimes\rangle$的子群有6个，分别是：

$\because |2^{d_1}| = \frac{|2|}{(|2|, d_1)} = \frac{12}{(12, d_1)} = 1$，即$d_1 = 12,$

$\therefore$ 1阶子群为：$< 2^{12} \bmod 13 = 1 >= \{1\}$

$\because |2^{d_3}| = \frac{|2|}{(|2|, d_2)} = \frac{12}{(12, d_2)} = 2$，即$d_2 = 6,$

$\therefore$ 2阶子群为：$< 2^6 >= \{1, 2^6\}$

$\because |2^{d_3}| = \frac{|2|}{(|2|, d_3)} = \frac{12}{(12, d_3)} = 3$，即$d_3 = 4, 8$，

$\therefore$ 3阶子群为：$< 2^4 >=< 2^8 >= \{1, 2^4, 2^8\}$

$\because |2^{d_4}| = \frac{|2|}{(|2|, d_4)} = \frac{12}{(12, d_4)} = 4$，即$d_4 = 3, 9$，

$\therefore$ 4阶子群为：$< 2^3 >=< 2^9 >= \{1, 2^3, 2^6, 2^9\}$

$\because |2^{d_6}| = \frac{|2|}{(|2|, d_6)} = \frac{12}{(12, d_6)} = 6$，即$d_6 = 2, 10$，

$\therefore$ 6阶子群为：$< 2^2 >=< 2^{10} >= \{1, 2^2, 2^4, 2^6, 2^8, 2^{10}\}$

12阶子群为：$< a >=< a^5 >=< a^7 >=< a^{11} >= \{1, 2, 3, \cdots, 12\}$

第六章

1、证明：
首先，不难验证，集合对于加法构成群。

又对 $\forall a_1,b_1,a_2,b_2, a_1+b_1i+(a_2+b_2i)=(a_1+a_2)+(b_1+b_2)i=a_2+b_2i+(a_1+b_1i)$

故，构成交换群。
其次，对于乘法，可验证其满足封闭性和结合性，可以构成半群。
根据环的定义，可构成环。

3、解:

$\because 2\otimes 6=0(\mathrm{mod}12),3\otimes 4=0(\mathrm{mod}12),3\otimes 8=0(\mathrm{mod}12),4\otimes 9=0(\mathrm{mod}12),6\otimes 10=0(\mathrm{mod}12),$

$\therefore$ 零因子为 2，3，4，6，8，9，10

6、证明：
(1)

$\forall a,b\in S_1\cap S_2\Rightarrow a,b\in S_1,a,b\in S_2$

$\Rightarrow a-b,ab\in S_1,a-b,ab\in S_2$(因为$S_1$、$S_2$是环)

$\Rightarrow a-b,ab\in S_1\cap S_2$，得证

(2) 不一定。

10、证明：（略）

11、证明：

根据例题 6-12，可验证，$\left\langle Q(\sqrt{5}),+,\bullet\right\rangle$ 是整环。

对于 $Q(\sqrt{5})$ 中任意元素 $a+b\sqrt{5}$，a,b 不全为零，存在 $c=\frac{a}{a^2-5b^2}-\frac{b}{a^2-5b^2}\sqrt{5}\in Q(\sqrt{5})$，

使得，$c(a+b\sqrt{5})=(a+b\sqrt{5})c=1$，即，c 是 $a+b\sqrt{5}$ 的逆元，故 $\left\langle Q(\sqrt{5}),+,\bullet\right\rangle$ 是域。

13、证明：

$\because$ F 是域，由域的定义知，$\forall a,b\in F, b\neq 0$，有 $ab^{-1}\in F$，即 $\frac{a}{b}\in F$，

$\therefore$ $A(F)\subseteq F$。

又由分式域的定义知，$F\subseteq A(F)$。

$\therefore$ $A(F)=F$，即域 F 的分式域为 F 自身。

第七章

2、解：

因为 32-1=31 为素数，所以由定理 7-24 知 GF(2)上的 5 次不可约多项式均为 5 次本原多项式，其不可约多项式的根也均为本原元。且因 $\varphi(31)=30$，所以 $GF(32)$中，除了 0 和 1 以外的其他元素均为本原元。

进而由不可约多项式 x^5+x^2+1 构造的 GF(32)中的本原元即为 $\alpha=\overline{x}$，其最小多项式即为 x^5+x^2+1。

3、解：

因为 7 为素数，所以 GF(7)=$\langle Z_7,\oplus,\otimes\rangle$，其加法记为模 7 加法，乘法即为模 7 乘法。

加法表：

mod7 加法	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

乘法表：

mod7 乘法	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

4、解：

因为 $9=3^2$，所以构造 $\mathrm{GF}(9)=\mathrm{GF}(3^2)=\left\{\overline{a_0+a_1x}\mid a_0,a_1\in Z_3\right\}$，

取不可约多项式 $g(x)=x^2+1$ 构造该有限域，则其加法表和乘法表如下：

加法表：

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x	2x+1	2x+2
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0

x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x	0	0	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x+1	1	1	0	x+1	x+2	x
2x+2	2x+2	2x	2x+2	2	2	1	x+2	x	x+1

乘法表：

	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	2x	2	x+2	1	x+2

8、解：（过程略）

$$\overline{x^7+x^4+x^2+x+1}\cdot\overline{x^6+x^5+x^3+x+1}$$

$$=(x^7+x^4+x^2+x+1)(x^6+x^5+x^3+x+1)\bmod(x^8+x^4+x^3+x+1)$$

$$=(x^{13}+x^{12}+x^9+x^5+1)\bmod(x^8+x^4+x^3+x+1)$$

$$=\left(x^5(x^8+x^4+x^3+x+1)+x^{12}-x^8-x^6+1\right)\bmod(x^8+x^4+x^3+x+1)$$

$$=\left(x^5(x^8+x^4+x^3+x+1)+x^4(x^8+x^4+x^3+x+1)-2x^8-x^7-x^6-x^5+x^4+1\right)\bmod(x^8+x^4+x^3+x+1)$$

$$=x^7+x^6+x^5+x^4+1$$

9、解：

$$s(x)\overline{x^7+x^4+x^3+1}+t(x)\overline{x^8+x^4+x^3+x+1}=1$$

$$\because r_{-1}=x^8+x^4+x^3+x+1,t_0=x^7+x^4+x^3+1,$$

$$r_1=r_{-1}-xr_0=x^5+x^3+1,t_1=1-0\bullet x=1,s_1=0-x=-x$$

$$r_2=r_0-(x^2+1)r_1=x^4+x^2,t_2=0-(x^2+1),s_2=1-x(x^2+1)=x^3+x+1$$

$$r_3=r_1-xr_2=1,t_3=1-x(x^2+1)=x^3+x+1,s_3=x-x^4-x^2-x=x^4+x^2$$

$$r_4=0$$

$$\therefore\overline{x^7+x^4+x^3+1}^{-1}=\overline{x^4+x^2}$$

10、解：

$$\mathrm{GF}(16)=\mathrm{GF}(2^4)=\mathrm{GF}(2)[x]/(x^4+x+1)=\{a_0+a_1x+a_2x^2+a_3x^3\mid a_i\in Z_2,i=0,1,2,3\}$$

因为$16-1=15$的正因子为$1,3,5,15$，分别验证得, 只有$\bar{x}^{15}=\bar{1}$成立，

所以$\bar{x}$的阶为15，即$\bar{x}$为本原元，多项式x^4+x+1为本原多项式。

$$\overline{x}^{0}=1,\overline{x}^{1}=\overline{x},\overline{x}^{2}=\overline{x^2},\overline{x}^{3}=\overline{x^3},\overline{x}^{4}=\overline{x+1},\overline{x}^{5}=\overline{x^2+x},\overline{x}^{6}=\overline{x^3+x^2},$$
$$\overline{x}^{7}=\overline{x^3+x+1},\overline{x}^{8}=\overline{x^2+1},\overline{x}^{9}=\overline{x^3+x},\overline{x}^{10}=\overline{x^2+x+1},\overline{x}^{11}=\overline{x^3+x^2+x},$$
$$\overline{x}^{12}=\overline{x^3+x^2+x+1},\overline{x}^{13}=\overline{x^3+x^2+1},\overline{x}^{14}=\overline{x^2+1}=1$$

对数表和反对数表即可构造，略。