第一章

（1） 5,4,1,5.

（2） $100=2^2*5^2$, $3288=2^3*3*137$.

（4） a,b 可以表示成多个素因子的乘积 $a=p_1p_2\cdots p_r$, $b=q_1q_2\cdots q_s$,又因为(a, b)=1，表明 a, b 没有公共(相同)素因子. 同样可以将 a^n, b^n 表示为多个素因子相乘 $a^n=(p_1p_2\cdots p_r)^n$, $b^n=(q_1q_2\cdots q_s)^n$ 明显 a^n, b^n 也没有公共(相同)素因子.

（5） 同样将 a, b 可以表示成多个素因子的乘积 $a=p_1p_2\cdots p_r$, $b=q_1q_2\cdots q_s$, $a^n=(p_1p_2\cdots p_r)^n$, $b^n=(q_1q_2\cdots q_s)^n$,因为 $a^n|b^n$ 所以对任意的 i 有, p_i 的 n 次方$|b^n$, 所以 b^n 中必然含有 a 的所有素因子, 所以 b 中必然含有 a 的所有素因子, 所以 a|b.

（6） 因为非零 a, b, c 互素,所以(a, b)=(a, c)=1,又因为 $a=p_1p_2\cdots p_r$, $b=q_1q_2\cdots q_s$, $ab=p_1p_2\cdots p_rq_1q_2\cdots q_s$, 又因为 a, b, c 互素, 所以 a, b, c 中没有公共(相同)素因子, 明显 ab 和 c 也没有公共(相同)素因子.所以(ab, c)= (a, b)(a, c).

（7） 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107, 109, 113, 127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199.

（12） 对两式进行变形有 21=0(mod m), 1001=0(mod m),可以看出要求满足的 m 即使求 21 和 1001 的公约数, 为 7 和 1.

（13） (70!)/(61!)= 62*63*—*70=(-9)*(-8)*—*(-1)=-9!=-362880=1(mod 71). 明显 61!与 71 互素, 所以两边同乘以 61!, 所以 70!=61!(mod 71).

（14） 当 n 为奇数时 $2^n=(-1)^n=-1=2(\text{mod } 3)$, 两边同时加上 1 有 $2^n+1=0(\text{mod } 3)$, 所以结论成立.

当 n 为偶数时 $2^n=(-1)^n=1(\text{mod } 3)$, 两边同时加上 1 有 $2^n+1=2(\text{mod } 3)$, 所以结论成立.

（15） 第一个问：因为(c,m)=d, m/d 为整数.假设 $ac=k_1m+r$, $bc=k_2m+r$,有 $ac=k_1d(m/d)+r$, $bc=k_2d(m/d)+r$ 所以 ac=bc(mod m/d),因为(c,m/d)=1,所以两边可以同除以一个 c, 所以结论成立.

第二个问题：因为 a=b(mod m), 所以 $a-b=k_i*m_i$，a-b 是任意 m_i 的倍数，所以 a-b 是 m_i 公倍数，所以$[m_i]|a-b$.(利用式子：最小公倍数=每个数的乘积/最大公约数, 是错误的, 该式子在两个数时才成立)

（16） 将整数每位数的值相加, 和能被 3 整除则整数能被 3 整除, 和能被 9 整除则整数能被 9 整除, (1)能被 3 整除, 不能被 9 整除，(2)都不能，(3)都不能，(4)都不能

第二章

（5） 证明：显然在群中单位元 e 满足方程 $x^2=x$，假设存在一个元素 a 满足方程 $x^2=x$，则有 $a^2=a$，两边同乘以 a^{-1} 有 a=e. 所以在群中只有单位元满足方程 $x^2=x$.

（6） 证明：因为群 G 中每个元素都满足方程 $x^2=e$，所以对群中任意元素 a,b 有 aa=e, bb=e, $(ab)^2=abab=e$. 对 abab=e，方程两边左乘以 a，右乘以 b 有 aababb=(aa)ba(bb)=ba=acb=ab，有 ab=ba，所以 G 是交换群.

（7） 证明：充分性：因为在群中对任意元素 a,b 有 $(ab)^2=a^2b^2$ 即 abab=aabb，方程两边左乘以 a 的逆元右乘以 b 的逆元，有 $a^{-1}abab^{-1}=a^{-1}aabbb^{-1}$，有 ab=ba，所以 G 是交换群.

必要性：因为群 G 是交换群，所以对任意元素 a,b 有 ab=ba，方程两边左乘以 a 右乘以 b 有 abab=aabb，有 $(ab)^2=a^2b^2$.

（8）证明：因为 xaxba=xbc，所以 $x^{-1}xaxbaa^{-1}b^{-1}=x^{-1}xbca^{-1}b^{-1}$，所以存在唯一解 $x=a^{-1}bca^{-1}b^{-1}$

使得方程成立。

（9） 证明：对群中任意元素 a,b 有 $ab(ab)^{-1}=e$，方程两边先左乘以 a 的逆元有 $b(ab)^{-1}=a^{-1}$，在左乘以 b 的逆元有 $(ab)^{-1}=b^{-1}a^{-1}$，所以结论成立.

（12） 证明：显然 mZ 是群 Z 的一个非空子集，验证封闭性，结合律，单位元，逆元，得出 mZ 是一个群，所以 mZ 是 Z 的子群.

（因为对 mZ 中任意元素 am, bm 有 am-bm=(a-b)m，因为 a-b∈Z，所以(a-b)m∈mZ，所以 mZ 是群 Z 的一个子群）.

（13） 证明：设群 G 的两个子群为 G_1, G_2，则对任意 $a,b\in G_1\cap G_2$ 有 $ab^{-1}\in G_1, ab^{-1}\in G_2$，所以 $ab^{-1}\in G_1\cap G_2$，所以 $G_1\cap G_2$ 也是 G 的子群.

（14） 证明：设 G 是一个群，对任意 a,b∈G，存在一个 G 到 H 的映射 f,并且 f(ab)=f(a)f(b). 对任意 f(a),f(b)∈H 有 f(a)f(b)=f(ab)∈H，所以 H 满足运算的封闭性. 对任意 f(a),f(b),f(c)有 (f(a)f(b))f(c)=f(ab)f(c)=f((ab)c)，f(a)(f(b)f(c))=f(a)f(bc)=f(a(bc))，又因为 (ab)c=a(bc)，所以 (f(a)f(b))f(c)=f(a)(f(b)f(c))，所以 H 满足结合律. 对任意 f(a)∈H，有 f(ae)=f(a)=f(a)f(e)，所以 f(e)是 H 的单位元，对任意的 f(a)∈H，有 $f(aa^{-1})=f(e)=f(a)f(a^{-1})$，所以 f(a)的逆元为 $f(a^{-1})$. 所以 H 是一个群.

（16） 证明：设 a 到 a^{-1} 的一一映射为 f.

充分性：对任意 G 中 a,b 有 $f(a)=a^{-1}$，$f(b)=b^{-1}$，$f(ab)=(ab)^{-1}$ 又因为 f 同构，所以 $f(ab)=f(a)f(b)=(ab)^{-1}=a^{-1}b^{-1}=(ba)^{-1}$，由 $(ab)^{-1}=(ba)^{-1}$ 有 ba=ab，所以 G 是交换群.

必要性由上反推可得.

第四章

（3） 明显单位元为 1，设 c+di 是 a+bi 的逆元，有(a+bi)(c+di)=1,有 c+di=(a-bi)/(a^2+b^2),所以 a+bi 的逆元为 (a-bi)/(a^2+b^2).

（4）略，利用环的定义证明

（5）a⊕1=a，故 1 为零元。令 a⊕b=ab=1，即 b 为 a 的负元。由于 a 与 b 均为整数，该式不总成立。即 a 不一定有负元，不构成环。

（6） 按书上要求分别判断是否满足加法交换群,乘法封闭,乘法结合律,分配律。

第一个：是环,没有单位元,是交换环

第二个：是环,有单位元 1,是交换环

第三个：是环,有单位元 1,是交换环

第四个：不是环(不是加法交换群)

（8）不构成。

（11）证明：对任意的 x,y ∈ S,有 ax=0,ay=0,有 ax-ay=a(x-y)=0,所以 x-y ∈ S,又 axy=(ax)y=a(xy)=0,所以 xy∈S,所以 S 是 R 的子环

（15）除去与 100 互素的数，其他剩余类为零因子。

（20） 证明：设有限整环是 S,要证明 S 是域,需证对全体非零元,都有逆元.设 S={a_1,a_2….a_n},有 1∈S,对任意非零 a_i 有 a_iS={a_ia_1, a_ia_2…. a_ia_n},因为乘法封闭有 a_iS=S 所以 1∈a_iS,所以存在 a_j 使得 a_ia_i=1,即 a_i 的逆元存在.所以结论成立

（22）用交换环的定义来证明；有零因子，不是整环

（23） 显然 S 是一个交换环,单位元为 1(具体过程略),且无零因子(设对任意 S_1=a_1+b_1i,S_2=a_2+b_2i,假设 S_1S_2=0,若 S_2 不等于 0,建立方程 a_1a_2-b_1b_2=0,a_1b_2+a_2b_1=0,变形为 $a_1a_2b_2$=$b_1b_2b_2$, $a_1a_2b_2$=-$a_2a_2b_1$,有因为 S_2 不等于 0,可知 a_2,b_2 不为 0,所以 b_1=0,推出 a_1=0,所以 S_1=0,同理当 S_1 不等于 0,S_2=0),所以 S 是一个整环.然而由 3 题有对于非零元 a+bi,逆元为(a-bi)/(a^2+b^2)不属于 S.所以 S 不是域

（28）证明：I 是环 R 的加法子群(具体过程略),对任意的 i∈R,j∈I,设 j=4r, r∈R, 有 ij=ji=4ir, ir∈R, 所以 ij=ji∈I,所以 I 是 R 的理想. I 不等于(4),因为(4)={4x+4n,x∈R,n∈Z},x 取 2,n 取 1 有 12∈(4),但是 12 不属于 I,所以不相等.

（30） 第一个：证明：整数环中既有单位元,又是交换环,所以(s)={xs,x∈Z},(t)={yt,y∈Z},又因为 xs+yt=xk_1d+yk_2d=(xk_1+yk_2)d,所以(s)+(t)∈(d),又因为 d=(s,t),所以存在整数 u,v 使得 d=us+vt,所以 rd=rus+rvt,所以(d)∈(s)+(t),所以(s)+(t) =(d).

第二个：(s)={xs,x∈Z},(t)={yt,y∈Z},那么(s)∩(t)表示既要是 s 的倍数又要是 t 的倍数,m 是 s,t 的最小公倍数,明显(s)∩(t)=(m).

（37） 对任意的 x∈R,有 xI_1∈I_1,I_1x∈I_1, xI_2∈I_2,I_2x∈I_2.有 x(I_1+I_2)=x(a+b)=xa+xb∈I_1+I_2, (I_1+I_2)x=(a+b)x=ax+bx∈I_1+I_2,所以 I_1+I_2 也是 R 的理想

第三章

（2） 第一个问题：设该有限群为 G，对任意阶大于 2 的元素 $a \in G$，有 $a^n=e$，n 为使得上式成立的最小正整数且 $n>2$. 明显在群中存在一个 a^{-1}，且 $a \neq a^{-1}$(若相等则 $a^2=e$，与 a 的阶大于 2 矛盾)，有$(a^{-1})^n=e$，所以 a^{-1} 的阶也大于 2. 综上对任意阶大于 2 的元素 a，存在 a^{-1} 的阶也大于 2. 所以结论成立.

第二个问题：因为在群 G 中只有 e 的阶为 1，在由上个结论有阶大于 2 的元素个数为偶数，由已知条件 G 的阶为偶数可知结论成立.

（5） 对 a 生成一个阶为 n 的循环群 G，a^m 生成的循环群的阶为 $n/(n,m)=n$. 又因为 $a^m \in G$ 所以 a^m 也生成 G.

（6） 设 G 的阶为 n，由已知可得 G' 为一个群，又由 G 与 G' 同态可知 f(e)为 G' 的单位元，$f(g) \in G'$，且对任意 $g^k \in G$，有 $f(g^k)=(f(g))^k$，所以 G' 中任意元素都可以由 f(g)生成表示成$(f(g))^k$，当 k=n 时有$(f(g))^n=f(g^n)=f(e)$，所以 G' 也是也是一个循环群.

（8） 13 阶：e 的阶为 1，其他元素阶为 13，生成元 g^1 到 g^{12}.

16 阶：e 的阶为 1，g^2 阶为 8，g^4 阶为 4，g^6 阶为 8，g^8 阶为 2,g^{10} 的阶为 8，g^{12} 的阶为 4，g^{14} 的阶为 8，其余的 g 到 g^{15} 的阶为 16 且是生成元.

（9） 先分别求出 15 阶和 20 阶的正因子为 3,5 和 2,4,5,10 所以 15 阶的生成元为 g^3, g^5, 20 阶的生成元为 g^2, g^4, g^5, g^{10}.

（10） 略

（11） 因为 p 是素数，所以阶为 p 的群为循环群(3.3 推论 3)，又因为任意同阶的有限循环群同构(3.2 定理 2)，所以结论成立.

（12）群中存在一个除单位元以外的元素 a 阶为 p^m 的因子。不妨设元素 a 的阶为 p^n（$1 \le n \le m$），由元素 a 可生成 p^n 阶循环子群，则子群中元素 $a^{p^{n-1}}$ 的阶为 p，由元素 $a^{p^{n-1}}$ 为生成元生成的循环子群的阶为 p，因此阶为 p^m 的群一定存在一个阶为 p 的子群。

（13） 由题意可知 $a^m=e$，$b^n=e$，m,n 为使得上式成立的最小正整数，又因为 ab=ba，所以$(ab)^{mn}=a^{mn}b^{mn}=e$，又因为(m,n)=1，假设存在 i 使得$(ab)^i=e$,有$(ab)^{mi}=e$,有 $b^{mi}=e$,有 mi|n,有 i|n,同理 i|m,所以 i|mn,所以 mn 是使得$(ab)^i=e$ 成立的最小整数，结论成立。

（15） 设 H_1, H_2 是群 G 的两个正规子群, $H= H_1 \cap H_2$，所以有对任意的 $a \in G$, $h_1 \in H_1$ 有 $ah_1a^{-1} \in H_1$，同样对任意的 $h_2 \in H_2$ 有 $ah_2a^{-1} \in H_2$，所以对任意的 $h \in H_1 \cap H_2$ 有，$aha^{-1} \in H_1 \cap H_2$，所以结论成立. (先要证明 H 是 G 的子群，略)

（16） 由题意设 eH, aH 是 H 的唯一两个左陪集，仿照 3.4 定理 2 可证. (另证：$G=H \cup aH$, $G=H \cup Ha$，又因为 $H \cap aH=$空, $H \cap Ha=$空，所以有 aH=Ha).

（17） 由题意有 HN=NH，则对任意的 $h_1n_1 \in HN$, $h_2n_2 \in HN$,存在 n_1'，$n_2' \in N$，使 $h_1n_1=n_1'h_1$，$h_2n_2=n_2'h_2$，则$(h_1n_1)(h_2n_2)^{-1}=(n_1'h_1)(n_2'h_2)^{-1}= n_1'(h_1 h_2^{-1})n_2'^{-1}$，对于 $n_1'(h_1 h_2^{-1}) \in NH$，存在 $n_1'' \in N$，使得 $n_1'(h_1 h_2^{-1})=(h_1 h_2^{-1})n_1''$，所以原式$= (h_1 h_2^{-1})n_1'' n_2'^{-1} \in HN$，结论成立。

第六章

（1）{9,1,11,3,13,5,15,7,17}　　{0,10,2,12,4,14,6,16,8}　　不能

（2）一定不是，比如 $(m-1)^2 \equiv 1 \pmod m$

（3） 证明：在是模 m 的简化剩余系中任取 c_i，可知$(c_i, m)=1$，可证$(m-c_i, m)=1$(反证法证明)，所以对任意 c_i 有 $m-c_i$ 也是模 m 的简化剩余系，c_i 和 $m-c_i$ 是成对出现的，所以结论成立

（4） 证明：因为 p，q 是两个素数，由欧拉定理有：$p^{q-1}=1 \pmod q$，$q^{p-1}=1 \pmod p$，即 $q \mid p^{q-1}-1$，$p \mid q^{p-1}-1$，设 $p^{q-1}-1=nq$，$q^{p-1}-1=mp$(m，n 是正整数)，两式相乘有 $(p^{q-1}-1)(q^{p-1}-1)=p^{q-1}q^{p-1}-q^{p-1}-p^{q-1}+1=nmpq$，由条件之 p，q≥2，所以 $p^{q-1}q^{p-1}$ 必有因子 pq，上式两边同时模 pq 有：$-q^{p-1}-p^{q-1}+1=0 \pmod{pq}$，所以 $p^{q-1}+q^{p-1}=1 \pmod{pq}$.

（5） 证明同 4 题

（6） 第一个：x=1,5(mod7),第四个：x=3,5,17,19mod(28),第八个:无解

（7） 第一个：x=3(mod 7)，第八个：x=31+35k(mod105)k=0,1,2,

第九个：x=836(mod999)

（8）x=200+551k(mod2755)k=0,1,2,3,4

（9）(5)x=77(mod 85)　(6)x=27(mod 60)　　（7）无解

（11）x=2101(mod2310)

（12）提示：$M_i^{\varphi(m_i)} \equiv 1 \pmod{m_i}$ ，而 $M_i M_i^{-1} \equiv 1 \pmod{m_i}$，由中国剩余定理得证。

（13）第一个 x=67(mod 140)，第二个 x=557(mod 1540)

（14）x=58(mod 60)=58+60k

（16）构造同余式组 $x=1 \pmod{a_1}$…….$x=k \pmod{a_k}$，根据中国剩余定理由已知条件只 x 有解.所以 x-1……x-k 满足题目要求的连续整数

（19）证明：充分性：同余式组 $x=b_1 \pmod{m_1}$，$x=b_2 \pmod{m_2}$，由条件$(m_1,m_2) \mid (b_1-b_2)$，有 $b_1-b_2=k_1m_1+k_2m_2$，所以 $b_1-k_1m_1=b_2+k_2m_2$，所以同余式组有解为 $x=b_1-k_1m_1=b_2+k_2m_2$，

必要性：同余式组有解即存在 k_1, k_2 使得 $b_1+k_1m_1=b_2+k_2m_2$，$b_1-b_2=k_2m_2-k_1m_1$，$(m_1,m_2) \mid k_2m_2-k_1m_1= b_1-b_2$

（20）第一个 x=0,6(mod7),第二个 x=184(mod243)

第 7 章

（1） 证明第一个：设 a,b 是模 p 的两个平方剩余，那么(ab/p)=(a/p)(b/p)=1，所以 ab 也是模 p 的平方剩余

证明第二个：设 a 是模 p 的平方剩余,$(1/p)=(aa^{-1}/p)=(a/p)(a^{-1}/p)=(a^{-1}/p)=1$，所以 a^{-1} 也是模 p 的平方剩余

证明第三个：设 a 是模 p 的平方剩余，b 是模 p 的平方非剩余，(ab/p)=(a/p)(b/p)=-1，所以 ab 是模 p 的平方非剩余

证明第四个：设 a,b 是模 p 的两个平方剩余，那么(ab/p)=(a/p)(b/p)=1，所以 ab 是模 p 的平方剩余

（2） 求模 13 的平方剩余和平方非剩余

$1^2=1(\text{mod } 13),2^2=4(\text{mod } 13),3^2=9(\text{mod } 13),4^2=3(\text{mod } 13),5^2=12(\text{mod } 13),6^2=10(\text{mod } 13)$

所以 1,4,9,3,12,10 是模 13 的平方剩余　2,5,6,7,8,11 是模 13 的平方非剩余

p=23 时，1,2,3,4,6,8,9,12,13,16,18 是模 23 的平方剩余，5,7,10,11,14,15,17,19,20,21,22 是模 23 的平方非剩余

p=37 时，1,3,4,7,9,10,11,12,16,21,25,26,27,28,30,33,34,36 是模 37 的平方剩余

2,5,6,8,13,14,15,17,18,19,20,22,23,24,29,31,32,35 是模 37 的平方非剩余

P=41 时，1,2,4,5,8,9,10,16,18,20,21,23,25,31,32,33,36,37,39,40 是模 41 的平方剩余

3,6,7,11,12,13,14,15,17,19,22,24,26,27,28,29,30,34,35,38 是模 41 的平方非剩余

（3） 2 是模的二次剩余等价于 p 被 8 除余 1 或 7，满足条件的有：7，17，23，31，41，47，71，73，79，89，97；-2 是模 p 的二次剩余等价于：-1 和 2 同为 p 的二次剩余，或同为二次非剩余。满足条件的有：3，11，17，19，41，43，59，67，73，83，89，97.

（6） 证明：充分性：由-a 是模 p 的平方剩余，所以存在 $b^2=-a(\text{mod } p)$，又因为 b 总可以表示成两个数的乘积 uv^{-1}，所以存在 u,v 使得$(u/v)^2=-a(\text{mod } p)$，所以结论成立。以上不不可逆所以必要性成立

（8） 同第一题第四个

（10） $(13/47)=(-1)^{6*13}(47/13)=(8/13)=(2/13)=-1$　第二个是 1

（11） 有解

（18）-1；1；1；-1

（19） 第一个：有解

第二个　无解

第八章

（1） $ord_{41}(10)$：因为 $10^2=18(\text{mod } 41)$, $10^3=16(\text{mod } 41)$, $10^4=37(\text{mod } 41)$, $10^5=1(\text{mod } 41)$所以 $ord_{41}(10)=5$

（2） 模 11 的原根：$\psi(11)=10=2*5,q_1=2,q_2=5$,所以 g 是模 11 的原根的充要条件是 $g^2\neq1(\text{mod } 11)$, $g^5\neq1(\text{mod } 11)$,逐一验证有 $2^2=4(\text{mod } 11),2^5=10(\text{mod } 11)$,所以 2 是模 11 的一个原根。模 11 的原根个数应为 $\psi(\psi(11))=4$ 个，为 $2^1(\text{mod } 11),2^3(\text{mod } 11),2^7(\text{mod } 11),2^9(\text{mod } 11)$即 2,8,7,6

（3） 明显 55 不能表示成 8.2 节定理 2 的形式。也可以如 2 题进行逐一验证。

（4） 有 $\psi(\psi(47))=22$ 个，$\psi(47)=46=2*23$，所以 g 是模 47 的原根的充要条件是 $g^2\neq1(\text{mod } 47)$, $g^{23}\neq1(\text{mod } 47)$, 逐一验证有 $2^2=4(\text{mod } 47),2^{23}=1 (\text{mod } 47);3^2=9(\text{mod } 47), 3^{23}=1(\text{mod } 47);4^2=16(\text{mod } 47),4^{23}=1 (\text{mod } 47); 5^2=25(\text{mod } 47),5^{23}=46 (\text{mod } 47)$,所以 5 是模 47 的一个原根，所以 5 的指数为与 46 互素的数为模 47 的其他原根。

（5） 同 4 题

（6）证明：$ord_m(a)=st$，所以 $a^{st}=1(\text{mod } m)$，st 是使得等式成立的最小整数。明显有$(a^s)^t=1(\text{mod } m)$,假设有 $i<t$ 使得$(a^s)^i=1(\text{mod } m)$成立，矛盾，所以结论成立

（7） 证明：由题有 $p=2*((p-1)/2)$,运用 8.2 定理 3 可得结论

（8） 同 4 题

（9） 由条件之由 a 生成的循环群的阶为 n-1，$a,a^2.....a^{n-1}$ 两两互不相等，所以 $a,a^2.....a^{n-1}$ 构成一个模 n 的简化剩余系，所以 n 为素数。可参照 122，123 页各性质