第5章　初等数论

5.1　整除关系与素数

习题 5.1 及参考答案

1. 分别讨论下述集合上的整除关系具有何种性质.

(1) 整数集 **Z**.

(2) 自然数集 **N**.

(3) 正整数 n 的正因数集 D_n.

解　(1) 整数集 **Z** 上的整除关系具有自反性和传递性.

(2) 自然数集 **N** 上的整除关系具有自反性、反对称性和传递性.

(3) 正整数 n 的正因数集 D_n 上的整除关系与 n 的值有关. 当 $n\geqslant 2$ 时,该集合上的整除关系具有自反性、反对称性和传递性;当 $n=1$ 时,该集合上的整除关系具有自反性、对称性、反对称性和传递性.

2. 写出 35 的所有因数集合及所有正因数集合 D_{35}.

解　35 的所有因数集合为 $\{-35,-7,-5,-1,1,5,7,35\}$. $D_{35}=\{1,5,7,35\}$.

3. 证明:若关于 λ 的整系数方程 $a_n\lambda^n+a_{n-1}\lambda^{n-1}+\cdots+a_1\lambda+a_0=0(n\in\mathbf{Z}^+)$ 有有理数根 $\frac{r}{s}$,其中 $\gcd(r,s)=1$,则 $r|a_0$ 且 $s|a_n$.

证　根据题意,有

$$a_n\left(\frac{r}{s}\right)^n+a_{n-1}\left(\frac{r}{s}\right)^{n-1}+\cdots+a_1\left(\frac{r}{s}\right)+a_0=0$$

去掉分母,得

$$a_nr^n+a_{n-1}sr^{n-1}+\cdots+a_1s^{n-1}r+a_0s^n=0$$

于是 $a_0s^n=-a_nr^n-a_{n-1}sr^{n-1}-\cdots-a_1s^{n-1}r$,进而 $r|a_0s^n$. 类似地,有 $s|a_nr^n$. 由于 $\gcd(r,s)=1$,因而 $r|a_0$ 且 $s|a_n$.

4. 证明:若 a 为正奇数,则 $8|a^2-1$.

证　设 $a=2k+1$,则 $a^2-1=(a-1)(a+1)=4k(k+1)$. 由于 k 和 $k+1$ 中必有一个偶数,故有 $8|a^2-1$.

5. 令 $m=8$,分别求出下述 n 除以 m 的商和余数.

(1) $n=7$.

(2) $n=-7$.

(3) $n=58$.

(4) $n=-48$.

解　(1) $7=0\times 8+7$.

(2) $-7=(-1)\times 8+1$.

(3) $58=7\times8+2$.

(4) $-49=(-7)\times8+7$.

6. 分别计算以下各式.

(1) $2019 \bmod 19$.

(2) $-2019 \bmod 19$.

解 (1) 因为 $2019=106\times19+5$,所以 $2019 \bmod 19=5$.

(2) 因为 $-2019=(-107)\times19+14$,所以 $-2019 \bmod 19=14$.

7. 计算 12345 的八进制数.

解 因为 $12345=1543\times8+1$,$1543=192\times8+7$,$192=24\times8+0$,$24=3\times8+0$,$3=0\times8+3$,所以 $12345=(30071)_8$.

8. 分别计算以下各式.

(1) $\varphi(6)$.

(2) $\varphi(8)$.

(3) $\varphi(10)$.

解 (1) $\varphi(6)=2$.

(2) $\varphi(8)=4$.

(3) $\varphi(10)=8$.

9. 证明:存在无限多个素数且它们是可列的.

证 假设只有有限个素数,分别为 $p_1,p_2,\cdots,p_k$. 令 $n=p_1p_2\cdots p_k+1\in\mathbf{N}$. 根据素因数分解定理,必存在 $1\leqslant i\leqslant k$,使得 $p_i\mid n$,进而 $p_i\mid 1$,不可能. 结论得证.

因为自然数是可列的,由上面的结论可知,素数是可列的(但无法用列举法给出).

10. 对 2015 进行素因数分解.

解 容易知道,5 是 2015 的素因数,即 $2015=5\times403$. 若 403 是合数,则其必有一个小于或等于 $\sqrt{403}(<21)$的素因数,即 2,3,5,7,11,13,17,19. 易验证 13 是 403 的素因数,即 $403=13\times31$. 显然,31 是素数,故 2015 的素因数分解为

$$2015 = 5\times13\times31$$

11. 计算 $\gcd(2035,2019)$,并给出贝祖系数 s 和 t,使得 $\gcd(2035,2019)=2035s+2019t$.

解 因为 $2035=1\times2019+16$,$2019=126\times16+3$,$16=5\times3+1$,$3=3\times1+0$,所以 $\gcd(2015,2019)=1$. 由于 $1=16-5\times3$,$3=2019-126\times16$,$16=2035-1\times2019$,于是 $1=16-5\times(2019-126\times16)=631\times16-5\times2019=631\times(2035-1\times2019)-5\times2019=631\times2035-636\times2019$. 所以 $s=631$,$t=-636$.

12. 证明:对于任意不全为 0 的整数 m 和 n,若存在整数 s 和 t 使得 $\gcd(n,m)=ns+mt$,则 $\gcd(s,t)=1$.

证 设 $\gcd(m,n)=d$,$\gcd(s,t)=k$,则存在 $n',m',s',t'\in\mathbf{Z}$,使得 $m=dm'$,$n=dn'$,$s=ks'$,$t=kt'$,进而 $d=ns+mt=dk(n's'+m't')$,于是 $dk\mid d$,进而 $k=1$,即 $\gcd(s,t)=1$.

13. 证明:若 $\gcd(m,n_1)=1$ 且 $\gcd(m,n_2)=1$,则 $\gcd(m,n_1n_2)=1$.

证 因为 $\gcd(m,n_1)=1$,存在整数 s_1,t_1 使得 $s_1m+t_1n_1=1$. 类似地,因为 $\gcd(m,n_2)=1$,存在整数 s_2,t_2 使得 $s_2m+t_2n_2=1$. 于是,有 $(s_1m+t_1n_1)(s_2m+t_2n_2)=1$,进而

$$(s_1s_2m+s_1t_2n_2+s_2t_1n_1)m+t_1t_2\cdot n_1n_2=1$$

因此，$\gcd(m,n_1n_2)=1$.

14. 证明：在偏序集$(\mathbf{Z}^+,|)$中，任意两个元素均存在下确界，其中$|$是整除关系.

证 对于任意 $x,y\in\mathbf{Z}^+$，根据公因数的定义知，$\gcd(x,y)|x$ 且 $\gcd(x,y)|y$，所以 $\gcd(x,y)$是$\{x,y\}$的下界. 假定 z 是$\{x,y\}$的下界，则 $z|x$ 且 $z|y$，即 z 是 x 与 y 的公因数. 根据欧几里得算法知，存在整数 s 和 t 使得 $\gcd(x,y)=xs+yt$，于是 $z|\gcd(x,y)$，即 $\gcd(x,y)$是$\{x,y\}$的下确界.

5.2 模同余关系

习题 5.2 及参考答案

1. 下述结论是否成立？

(1) $2019\equiv1983(\mathrm{mod}\ 18)$.

(2) $36^2\equiv-1(\mathrm{mod}\ 15)$.

解 (1) 成立，因为 $2019-1983=38=2\times18$.

(2) 不成立，因为$36^2-(-1)=1297=86\times15+7$，不是 15 的倍数.

2. 设 p 是素数. 证明：对于任意整数 n，若 $n^2\equiv1(\mathrm{mod}\ p)$，则 $n\equiv1(\mathrm{mod}\ p)$或 $n\equiv-1(\mathrm{mod}\ p)$.

证 由已知 $n^2\equiv1(\mathrm{mod}\ p)$，有 $p|n^2-1$，即 $p|(n-1)(n+1)$. 因为 p 是素数，于是 $p|n-1$ 或 $p|n+1$，因而 $n\equiv1(\mathrm{mod}\ p)$或 $n\equiv-1(\mathrm{mod}\ p)$.

3. 设 m 是正整数，对于任意整数 x 和 y，判断下列结论是否成立，并给出理由.

(1) 若 $x^2\equiv y^2(\mathrm{mod}\ m)$，则 $x\equiv y(\mathrm{mod}\ m)$或 $x\equiv-y(\mathrm{mod}\ m)$.

(2) 若 $x^2\equiv y^2(\mathrm{mod}\ m^2)$，则 $x\equiv y(\mathrm{mod}\ m)$或 $x\equiv-y(\mathrm{mod}\ m)$.

解 (1) 不成立. 例如，$5^2\equiv3^2(\mathrm{mod}\ 16)$，但 $5\equiv3(\mathrm{mod}\ 16)$或 $5\equiv-3(\mathrm{mod}\ 16)$均不成立.

(2) 不成立. 例如，$17^2\equiv8^2(\mathrm{mod}\ 15^2)$，但 $17\equiv8(\mathrm{mod}\ 15)$或 $17\equiv-8(\mathrm{mod}\ 15)$均不成立.

4. 分别写出 $\mathbf{Z}_5=\{0,1,2,3,4\}$关于模 5 加法运算$+_5$和模 5 乘法运算$\cdot_5$的运算表.

解 $\mathbf{Z}_5$ 关于模 5 加法运算$+_5$和模 5 乘法运算$\cdot_5$的运算表分别如表 5-1 和表 5-2 所示.

表 5-1

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

表 5-2

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

5. 证明：若 $\gcd(m,n)=1$，则 $a\equiv b(\bmod m)$ 当且仅当 $an\equiv bn(\bmod m)$.

证 ($\Rightarrow$)因为 $a\equiv b(\bmod m)$，于是 $m\mid a-b$，进而 $m\mid(a-b)n$，所以 $an\equiv bn(\bmod m)$.

($\Leftarrow$)因为 $an\equiv bn(\bmod m)$，于是 $m\mid(a-b)n$. 因为 $\gcd(m,n)=1$，所以 $m\mid a-b$，即 $a\equiv b(\bmod m)$.

6. 计算下列幂模.

(1) $2^{2019} \bmod 7$.

(2) $7^{2019} \bmod 11$.

解 (1) 由于 $\gcd(2,7)=1$，根据费马小定理，有 $2^6\equiv 1(\bmod 7)$. 因为 $2019=6\times 336+3$，于是 $2^{2019}=2^{6\times 336+3}=(2^6)^{336}\times 2^3\equiv 1^{336}\times 2^3\equiv 1(\bmod 7)$，即 $2^{2019} \bmod 7=1$.

(2) 由于 $\gcd(7,11)=1$，根据费马小定理，有 $7^{10}\equiv 1(\bmod 11)$. 因为 $2019=10\times 201+9$，于是 $7^{2019}=7^{10\times 201+9}=(7^{10})^{201}\times 7^9\equiv 1^{201}\times 7^9\equiv 7^9(\bmod 11)$. 又因为

$$7^2 = 49 \equiv 5(\bmod 11)$$
$$7^4 = (7^2)^2 \equiv 5^2 \equiv 3(\bmod 11)$$
$$7^8 = (7^4)^2 \equiv 3^2 \equiv 9(\bmod 11)$$

因而，$7^9=7^8\times 7\equiv 9\times 7\equiv 8(\bmod 11)$，即 $7^{2019} \bmod 11=8$.

7. 证明：

(1) 15 是 7 模 26 的乘法逆元，并求解线性同余方程 $15x\equiv 1(\bmod 26)$.

(2) 937 是 13 模 2436 的乘法逆元，并求解线性同余方程 $13x\equiv 1(\bmod 2436)$.

解 (1) 由于 $15\times 7\equiv 1(\bmod 26)$，所以 15 是 7 模 26 的乘法逆元. 由已知 $15x\equiv 1(\bmod 26)$，得到 $15\times 7x\equiv 7(\bmod 26)$，进而 $x\equiv 7(\bmod 26)=7$.

(2) 由于 $937\times 13\equiv 1(\bmod 2436)$，所以 937 是 13 模 2436 的乘法逆元. 由已知 $13x\equiv 1(\bmod 2436)$，得到 $937\times 13x\equiv 937(\bmod 2436)$，进而 $x\equiv 937(\bmod 2436)=937$.

8. 求解下列线性同余方程.

(1) $8x\equiv 2(\bmod 6)$.

(2) $4x\equiv -1(\bmod 6)$.

(3) $3x\equiv 4(\bmod 7)$.

(4) $256x\equiv 158(\bmod 337)$.

解 (1) 由于 $\gcd(8,6)=2\mid 2$，所以 $8x\equiv 2(\bmod 6)$ 有两个解. 容易验证，$\mathbf{Z}_6=\{0,1,2,3,4,5\}$ 中的 1 和 4 是其解.

(2) 由于 $\gcd(4,6)=2\nmid -1$，所以 $4x\equiv -1(\bmod 6)$ 没有解.

(3) 由于 $\gcd(3,7)=1\mid 2$，所以 $3x\equiv 4(\bmod 7)$ 只有一个解. 容易验证，$\mathbf{Z}_7=\{0,1,2,3,4,5,6\}$ 中的 6 是其解.

(4)由于 $\gcd(256,337)=1\mid 158$，所以 $256x\equiv 158(\bmod 337)$ 只有一个解. 由欧几里得算法知

$$337 = 1\times 256+81$$
$$256 = 3\times 81+13$$
$$81 = 6\times 13+3$$
$$13 = 4\times 3+1$$
$$3 = 3\times 1+0$$

进而

$$\begin{aligned}1 &= 13-4\times 3\\ 3 &= 81-6\times 13\\ 13 &= 256-3\times 81\\ 81 &= 337-1\times 256\end{aligned}$$

于是,有

$$\begin{aligned}1 &= 13-4\times 3 = 13-4(81-6\times 13)\\ &= 25\times 13-4\times 81\\ &= 25\times(256-3\times 81)-4\times 81\\ &= 25\times 256-79\times 81\\ &= 25\times 256-79(337-1\times 256)\\ &= 104\times 256-79\times 337\end{aligned}$$

进而 $s=104$. 由于 $k=b/\gcd(a,m)=158/\gcd(256,337)=158$,故

$$x = ks \bmod 337 = 158\times 104 \bmod 337 = 256$$

9. 利用中国剩余定理求解下列线性同余方程组.

$$\begin{cases}x\equiv 1(\bmod 5)\\ x\equiv 5(\bmod 6)\\ x\equiv 4(\bmod 7)\\ x\equiv 10(\bmod 11)\end{cases}$$

解 令 $m_1=5,m_2=6,m_3=7,m_4=11$,于是 $m=m_1m_2m_3m_4=5\times 6\times 7\times 11=2310$,进而

$$M_1=\frac{m}{m_1}=462,\quad M_2=\frac{m}{m_2}=385,\quad M_3=\frac{m}{m_3}=330,\quad M_4=\frac{m}{m_4}=210$$

根据 $M_ix_i\equiv 1(\bmod m_i)$,$i=1,2,3,4$,分别求得 $x_1=3,x_2=1,x_3=1,x_4=1$. 由于 $a_1=1,a_2=5,a_3=4,a_4=10$,取

$$x = a_1M_1x_1+a_2M_2x_2+a_3M_3x_3+a_4M_4x_4 = 6731$$

则所给线性同余方程组的解为 $6731 \bmod 2310=2111$,所有解为 $x=2111+2310k,k\in\mathbf{Z}$.

10. 证明(**Wilson 定理**):设 $p>1$,则 p 是素数的充要条件是 $(p-1)!\equiv -1(\bmod p)$.

证 ($\Rightarrow$)当 $p=2,3$ 时,结论显然成立. 下面设 $p>3$ 并考虑集合 $S=\{2,3,\cdots,p-2\}$.

任取 $a\in S$,则 $\gcd(a,p)=1$,于是存在整数 x 和 y 使得 $ax+py=1$,进而 $ax\equiv 1(\bmod p)$. 令 $b\equiv x(\bmod p)$,由于 $a\in S$,于是 $b\neq 1,p-1$,因此 $b\in S$ 且 $ab\equiv 1(\bmod p)$.

下面证明 $a\neq b$. 若 $a=b$,则 $a^2\equiv 1(\bmod p)$,进而 $p\mid(a-1)(a+1)$. 因为 p 是素数,于是 $p\mid(a-1)$或 $p\mid(a+1)$,这都是不可能的.

由上面的讨论知,S 中的数可分成 $(p-3)/2$ 对,每对数 a 和 b 满足 $ab\equiv 1(\bmod p)$. 因此 $2\times 3\times\cdots\times(p-2)\equiv 1(\bmod p)$,进而 $(p-1)!\equiv -1(\bmod p)$.

($\Leftarrow$)若 $p=ab(1<a,b<p)$,由于 $1<a<p$,显然 $a\mid(p-1)!$. 根据 $(p-1)!\equiv -1(\bmod p)$,知 $p\mid(p-1)!+1$,由 $p=ab$ 可得出 $a\mid(p-1)!+1$,于是

$$a\mid((p-1)!+1)-(p-1)!$$

即 $a\mid 1$,不可能.

5.3 RSA 密码算法

习题 5.3 及参考答案

1. 说明：若已知 n 及 $\varphi(n)$，其中 n 是两个素数 p 和 q 的乘积，则容易求出 p 和 q.

解 由于 $n=pq$，$\varphi(n)=(p-1)(q-1)=pq-(p+q)+1$，于是 $p+q=n-\varphi(n)+1$，这时 p 和 q 是一元二次方程 $x^2-(n-\varphi(n)+1)x+n=0$ 的两个根，已知 n 及 $\varphi(n)$即可求出 p 和 q.

2. 用 00～25 分别表示 A～Z，每个字母用两位数字表示，在 RSA 密码算法中，取$(n,e)=(35,7)$.

(1) 把 STOP 加密.

(2) 把 32 14 32 解密.

解 (1) STOP 表示为 18 19 14 15. 由于 $7=(111)_2=2^2+2+1$，使用逐次平方法有

$$18^2\equiv 9(\mathrm{mod}\ 35),18^4\equiv 9^2(\mathrm{mod}\ 35)\equiv 11(\mathrm{mod}\ 35)$$

所以 $18^7=18^4\times 18^2\times 18\equiv 11\times 9\times 18(\mathrm{mod}\ 35)\equiv 32(\mathrm{mod}\ 35)$. 类似地，有 $19^7\equiv 19(\mathrm{mod}\ 35)$，$14^7\equiv 14(\mathrm{mod}\ 35)$，$15^7\equiv 15(\mathrm{mod}\ 35)$. 因此，使用 RSA 密码算法将 18 19 14 15(即 STOP)加密为 32 19 14 15.

(2) 显然，$7\times 7\equiv 1(\mathrm{mod}\ 24)$，于是 $d=7=(111)_2=2^2+2+1$，使用逐次平方法有 $32^7\equiv 18(\mathrm{mod}\ 35)$，$14^7\equiv 14(\mathrm{mod}\ 35)$. 使用 RSA 密码算法将 32 14 32 解密为 18 14 18，即 SOS.

自 测 题 5

一、填空题(每小题 3 分，共 15 分)

1. 整数集合 $\mathbf{Z}$ 关于整数的加法运算＋和乘法运算·都是(　　)运算.

2. 若整数 $m|1$，则 $m=$(　　).

3. $-19(\mathrm{mod}\ 7)=$(　　).

4. 设 p 和 q 是素数，则欧拉函数 $\varphi(pq)=$(　　).

5. 线性同余方程 $3x\equiv 5(\mathrm{mod}\ 8)$ 的解为 $x=$(　　).

二、单选题(每小题 3 分，共 15 分)

1. 对于正整数 n，用 $\varphi(n)$表示小于或等于 n 且与 n 互素的正整数个数，则 $\varphi(12)=$(　　).

A. 1　　B. 2　　C. 3　　D. 4

2. 集合 $A=\{2^n|n\in\mathbf{N}\}$上的整除关系$|$是(　　)关系.

A. 偏序　　B. 线性序　　C. 良序　　D. 等价

3. 下列各式中，(　　)为真.

A. $446\equiv 278(\mathrm{mod}\ 7)$　　B. $445\equiv 536(\mathrm{mod}\ 18)$

C. $383\equiv 126(\mathrm{mod}\ 15)$　　D. $2019\equiv 1882(\mathrm{mod}\ 17)$

4. 设 p 是素数，则 $\mathbf{Z}_p=\{0,1,2,\cdots,p-1\}$关于模 p 的乘法运算·$_p$(　　).

A. 每个元素都有逆元　　B. 每个元素都没有逆元

C. 每个非零元素都有逆元　　D. 每个非零元素都没有逆元

5. 线性同余方程 $9x\equiv 12 \pmod{21}$ 的所有解为(　　).

A. 5,12　　B. 6,13,20　　C. 7,13,20　　D. 13,20

三、判断题(每小题 3 分,共 15 分)

1. 对于整除关系 $|$,有 $0|0$.　　(　　)

2. 对任意整数 m 和 n,若 $m|n$ 且 $n|m$,则 $m=n$.　　(　　)

3. 对任意整数 m,n 和 k,若 $\gcd(m,n)=1$,$m|k$ 且 $n|k$,则 $mn|k$.　　(　　)

4. 整数集 $\mathbf{Z}$ 上的模 m 同余关系 $\equiv_m$ 是等价关系.　　(　　)

5. 线性同余方程 $4x\equiv 9 \pmod{14}$ 无解.　　(　　)

四、(10 分) 计算 $\gcd(540,168)$,并求出贝祖系数 s 和 t,使得 $\gcd(540,168)=540s+168t$.

五、(10 分) 有多少对正整数 (m,n) 的最小公倍数 $\operatorname{lcm}(m,n)=2^3\times 3^5$?

六、(10 分) 证明:

(1) 设 a,b 和 m 是整数,其中 $m>1$. 若 $a\equiv b \pmod{m}$,则 $a^2\equiv b^2 \pmod{m}$.

(2) 在任何 1～200 的 103 个不同整数中,必存在两个整数,其差恰为 5.

七、(10 分) 利用中国剩余定理求解下列线性同余方程组.

$$\begin{cases} x\equiv 1 \pmod{3} \\ x\equiv 2 \pmod{5} \\ x\equiv 3 \pmod{7} \end{cases}$$

八、(15 分) 对于 $x\in\mathbf{N}$,令 $\pi(x)$ 表示小于或等于 x 的素数个数. 设 $A=\{x\in\mathbf{N}\mid 2\leqslant x\leqslant 9\}$,定义 A 上的关系

$$\ll=\{(x,x)\mid x\in A\}\cup\{(x,y)\in A^2\mid \pi(x)<\pi(y)\}$$

(1) 验证 $(A,\ll)$ 是偏序集,并画出 $(A,\ll)$ 的哈斯图.

(2) 求出 $(A,\ll)$ 的所有极大元.

(3) 给出 A 的一个子集 B 的例子,使 B 存在最大元,但无最小元.

自测题 5 参考答案

一、1. 封闭(或代数)

2. ± 1

3. 2

4. $(p-1)(q-1)$

5. 7.

二、1. D　2. B　3. A　4. C　5. B

三、1. √　2. ×　3. √　4. √　5. √

四、**解**　根据带余除法有

$$\begin{aligned} 540 &= 3\times 168+36 \\ 168 &= 4\times 36+24 \\ 36 &= 1\times 24+12 \\ 24 &= 2\times 12+0 \end{aligned}$$

于是,$\gcd(540,168)=12$.

由上述等式可知

$$12 = 36 - 1 \times 24$$
$$24 = 168 - 4 \times 36$$
$$36 = 540 - 3 \times 168$$

因此，$\gcd(540,168) = 36 - 1 \times 24 = 36 - 1 \times (168 - 4 \times 36) = 5 \times 36 - 1 \times 168 = 5 \times (540 - 3 \times 168) - 1 \times 168 = 5 \times 540 - 16 \times 168$，进而 $s = 5$ 且 $t = -16$.

五、**解**　显然，根据公倍数的定义知 $m = 2^x 3^y$ 且 $n = 2^r 3^s$. 由已知 $\mathrm{lcm}(m,n) = 2^3 3^5$ 可得 $\max(x,r) = 3$ 且 $\max(y,s) = 5$，进而有 7 种可能的 (x,r)，分别为 $(0,3),(1,3),(2,3),(3,3),(3,2),(3,1),(3,0)$. 同理，有 11 种可能的 (y,s). 根据乘法原理，有 $7 \times 11 = 77$ 对满足条件的正整数 (m,n).

六、**证**　(1) 因为 $a \equiv b \pmod m$，所以 $m \mid (a-b)$. 而 $a^2 - b^2 = (a-b)(a+b)$，于是 $m \mid (a^2 - b^2)$，即 $a^2 \equiv b^2 \pmod m$.

(2) 令 h_i 是所取 103 个整数中的第 i 个，这时 $1 \leqslant h_i \leqslant 200$，$1 \leqslant i \leqslant 103$. 取 $g_i = h_i + 5$，则 $6 \leqslant g_i \leqslant 205$，$1 \leqslant i \leqslant 103$. 于是得到 206 个整数 $h_1, h_2, \cdots, h_{103}, g_1, g_2, \cdots, g_{103}$，它们的取值范围都为 1～205. 因此，必有两个整数相同，显然一个是 h_i，另一个是 g_j. 而 $g_j = h_j + 5$，所以 $h_i = h_j + 5$，这时 $h_i - h_j = 5$，结论得证.

七、**解**　令 $m_1 = 3, m_2 = 5, m_3 = 7$，于是 $m = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$，进而

$$M_1 = \frac{m}{m_1} = 35, \quad M_2 = \frac{m}{m_2} = 21, \quad M_3 = \frac{m}{m_3} = 15$$

根据 $M_i x_i \equiv 1 \pmod{m_i}$，$i = 1,2,3$，分别求得 $x_1 = 2, x_2 = 1, x_3 = 1$. 由于 $a_1 = 1, a_2 = 2, a_3 = 3$，取

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 = 52 \bmod 105$$

则所给线性同余方程组的解为 $52 \bmod 105 = 52$，所有解为 $x = 52 + 105k, k \in \mathbf{Z}$.

八、**解**　(1) 容易验证，$(A, \ll)$ 是偏序集且 $\mathrm{COV}(A) = \{(2,3),(2,4),(3,5),(3,6),(4,5),(4,6),(5,7),(5,8),(5,9),(6,7),(6,8),(6,9)\}$. 因而 $(A, \ll)$ 的哈斯图如图 5-1 所示.

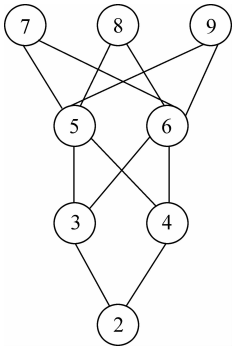

图　5-1

(2) 7,8,9.

(3) 取 $B = \{3,4,5\}$.

第6章　图　　论

6.1　图的基本概念

习题 6.1 及参考答案

1. 如图 6-1 所示，用 1，2，3，4，5，6 表示 6 个人，两个点之间的无向边表示对应的两个人认识，则图 6-1 所示的含义是什么？能得出任意 6 个人中有 3 个人相互认识或相互不认识的结论吗？

解　图 6-1 表示有 1，2，3，4，5，6 共 6 个人，其中 1 与 3 认识，1 与 4 认识，2 与 3 认识，2 与 5 认识，3 与 6 认识.

能得出任意 6 个人中有 3 个人相互认识或相互不认识的结论，其理由如下：

对于节点 1 来说，考虑其与节点 2，3，4，5，6 的关系，1 至少与其中 3 个人认识或不认识. 不妨假设 1 与其中 2，3，4 认识. 在 3，4，5 中，若有 2 个人相互认识，则存在 3 个人相互认识，例如 3 与 4 认识，则 1，3，4 相互认识；若 3，4，5 中没有任何 2 个人相互认识，则 3，4，5 相互不认识. 最后的结论如图 6-2 所示.

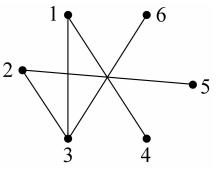

图　6-1

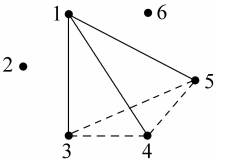

图　6-2

2. 在一次 10 周年同学会上，想统计所有人握手的次数之和，应该如何建立该问题的图模型？

解　将每个同学作为一个节点，如果两个人握过一次手，就在相应的两个节点之间画一条无向边，由此得到一个无向图.

一个人握手的次数就是这个节点与其他节点所连接的边的条数，进而可得出所有人握手的次数之和.

3. 在一次联欢舞会上，要得出跳了奇数次舞的人数的规律，应该如何建立图模型？特别地，一个人单独跳一次舞该如何处理呢？某两人多次跳舞又如何处理？

解　将联欢舞会上的每个人作为一个节点，若两个人跳过一次舞，则在相应的两个节点之间画一条无向边，由此得到一个无向图. 一个人跳舞的次数就是这个人对应的节点与其他节点所连接的边的条数，进而可得出跳了奇数次舞的人数.

一个人单独跳了一次舞，可以认为自己跟自己跳，这时在该节点处有一个环；也可以认为联欢舞会上单独跳舞不计入跳舞次数. 若两人多次跳舞，则在对应的节点之间出现平行边（多重边），其重数是这两人跳舞的次数.

4. 任意 $n(n\geqslant 2)$ 个人的组里必有两个人有相同个数的朋友，解答此问题的图模型该如何建立？

解 将该组里的每个人作为一个节点，若两个人是朋友，则在相应的两个节点之间连一条无向边，由此得到一个无向图.

5. (**3 户 3 井问题**)在一个地方有 3 户人家，并且有 3 口井供他们使用. 由于土质和气候的关系，有的井中的水常常干枯，因此各户人家要到有水的井去打水. 不久，这 3 户人家成了冤家，于是决定各自修一条路通往水井，打算使得他们在去水井的路上不会相遇. 建立解决此问题的图模型.

解 将 3 户人家分别作为 3 个节点，将 3 口井分别作为另外 3 个节点，若一户人家与一口井之间有一条路，则在相应的两个节点之间连一条无向边，这样就得到一个无向图.

6. (**过河问题**)某人挑一担菜并带一只狼和一只羊要从河的一岸到对岸去. 由于船太小，只能带狼、菜、羊中的一种过河. 由于明显的原因，当人不在场时，狼要吃羊，羊要吃菜. 通过建立图模型给出此问题的答案.

解 不妨认为过河的方向是从北岸到南岸，则在北岸可能出现的状态为 $2^4=16$ 种，其中安全状态有下面 10 种：(人，狼，羊，菜)，(人，狼，羊)，(人，狼，菜)，(人，羊，菜)，(人，羊)，(∅)，(菜)，(羊)，(狼)，(狼，菜)；不安全的状态有下面 6 种：(人)，(人，菜)，(人，狼)，(狼，羊，菜)，(狼，羊)，(羊，菜).

现将北岸的 10 种安全状态作为 10 个节点，而渡河的过程则是状态之间的转移，由此得到一个无向图，如图 6-3 所示.

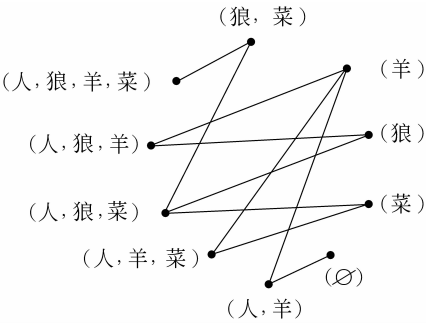

图 6-3

从图 6-3 可以得出两种安全的渡河方案：

第 1 种：(人，狼，羊，菜)→(狼，菜)→(人，狼，菜)→(狼)→(人，狼，羊)→(羊)→(人，羊)→(∅).

第 2 种：(人，狼，羊，菜)→(狼，菜)→(人，狼，菜)→(菜)→(人，羊，菜)→(羊)→(人，羊)→(∅).

7. (**分油问题**)有 3 个油桶 A,B,C，分别可装 8kg、5kg 和 3kg 油. 假设 A 桶已经装满了油，在没有其他度量工具的情况下，要将油平分，通过建立图模型给出此问题的答案.

解 用 (B,C) 表示 B，C 两个油桶的状态(即桶内装油的千克数)，由于 $B=0,1,2,3,4,5$ 且 $C=0,1,2,3$，于是所有状态共 $6\times 4=24$ 种.

现将这 24 种状态看作 24 个节点，当且仅当两种状态可以相互转换时，在两个节点之间连一条无向边，由此得到一个无向图，如图 6-4 所示.

从图 6-4 中可以看出，有两种将油平分的方案：

第 1 种：(0,0)→(0,3)→(3,0)→(3,3)→(5,1)→(0,1)→(1,0)→(1,3)→(4,0).

第 2 种：(0,0)→(5,0)→(2,3)→(2,0)→(0,2)→(5,2)→(4,3)→(4,0).

8. 证明：任何 n 阶完全图 K_n 的边数为 $n(n-1)/2$.

证 n 阶简单图的边数为 $C_n^2=n(n-1)/2$.