第5章　初等数论

初等数论又称为算术，它起源于古希腊. 被数学家高斯誉为“数学皇冠”的数论是一门研究整数特别是正整数性质的学科，它有近四千年的古老历史，却始终充满活力. 中国在数论研究方面也取得了辉煌的成就，例如中国剩余定理和陈氏定理等.

初等数论在算法学、密码学等计算机领域有着非常重要的应用，国外离散数学教材几乎都会有这部分内容，其讨论范围为离散的整数集 $\mathbf{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$.

通过对本章的学习，可较深入地体会集合、映射（即函数）、运算和关系在具体学科研究中所扮演的角色.

5.1　整除关系与素数

5.1.1　整除关系与带余除法

【定义 5-1】 整数集 $\mathbf{Z}$ 上的**整除关系**(divisibility relation)$|$定义为，对于任意 $m,n\in\mathbf{Z}$，$m|n$ 当且仅当存在 $q\in\mathbf{Z}$，使得 $n=qm$. 这时称 m 是 n 的**因数**(divisor/factor)或 n 是 m 的**倍数**(multiple).

根据定义 5-1 知，6 和 -6 的因数有 $1,-1,2,-2,3,-3,6,-6$，特别地有 $2|6$，$-2|6$，$2|-6$，$-2|-6$. 任意整数都是 0 的因数，即对于任意 $n\in\mathbf{Z}$，有 $n|0$，包括 $0|0$.

对于任意正整数 n，用 D_n 表示 n 的所有正因数组成的集合，于是 $D_{12}=\{1,2,3,4,6,12\}$.

对于任意整数 x,y,z,m 和 n，$\mathbf{Z}$ 上的整除关系具有如下性质：

(1) 对于任意 $x\in\mathbf{Z}$，有 $x|x$（自反性）.

(2) 若 $x|y$ 且 $y|x$，则 $x=y$ 或 $x=-y$.

(3) 若 $x|y$ 且 $y|z$，则 $x|z$（传递性）.

(4) 若 $x|y$ 且 $x|z$，则 $x|(my+nz)$.

可以证明下面的定理.

【定理 5-1】（带余除法） 对于整数 m 和 n，若 $m\neq 0$，存在唯一一对整数 q 和 r，使得

$$n=qm+r,\quad 0\leqslant r<|m|$$

其中，q 称为 n 除以 m 的**商**(quotient)，r 称为 n 除以 m 的**余数**(remainder).

证

(1) 存在性. 令 $A=\{n-km\mid k\in\mathbf{Z}\text{ 且 }n-km\geqslant 0\}$. 显然，$A\neq\varnothing$. 于是 A 中存在最小元素 r，这时设 $k=q$，即 $r=n-qm$，因而 $n=qm+r$，$r\geqslant 0$.

下面证明 $r<|m|$. 若 $r\geqslant|m|$，则 $n-qm-|m|\geqslant 0$. 由于 $n-qm-|m|\in A$，而 $n-qm-|m|<n-qm$，矛盾. 于是存在整数 q 和 r 使得 $n=qm+r$，$0\leqslant r<|m|$.

(2) 唯一性. 假设还存在一对整数 q' 和 r'，使得 $n=q'm+r'$，$0\leqslant r'<|m|$. 这时，$q'm+r'=qm+r$，于是 $(q'-q)m=r-r'$，进而 $m|r-r'$，因而 $r-r'=0$，即 $r'=r$，进而 $q'=q$，唯一性得证.

使用带余除法，有 $2019=252\times 8+3$，$2019=(-252)\times(-8)+3$.

显然，当 $m\neq 0$ 时，整除是余数为 0 时的带余除法.

设 b 为大于 1 的整数，则 b 进制数

$$(u_r u_{r-1}\cdots u_1 u_0)_b = u_r b^r + u_{r-1}b^{r-1} + \cdots + u_1 b + u_0$$

利用带余除法，可以将十进制数与其他进制的数进行转换. 例如十进制数 247 转换成八进制的方法如下：$247=30\times 8+7$，$30=3\times 8+6$，于是

$$247 = 30\times 8+7 = (3\times 8+6)\times 8+7 = 3\times 8^2+6\times 8+7$$

因此，$247=(367)_8$.

同理，$327 = 2^8+2^6+2^2+2^1+1=(101000111)_2$.

与带余除法密切相关的是模运算.

【定义 5-2】 对于正整数 m，定义 x **模 m 运算**(modulo m operation) $x \bmod m$ 是整数 x 除以 m 的余数.

根据带余除法知，$x \bmod m$ 是使 $x=qm+r$，$0\leqslant r<m$ 成立的整数 r. 这里，f 是 $\mathbf{Z}$ 上的模 m 运算，是一元运算.

下面给出模运算的 3 个最简单的应用.

将 26 个英文字母 a，b，c，…，z 分别对应于整数 0，1，2，…，25，为了保密，可以将每一个字母往后推移 3 位，若接收到的密文为 l oryh brx，则明文为 i love you. 这时的加密变换为 $c=(p+3)\bmod 26$，解密变换为 $p=(c-3)\bmod 26$，其中 p 是明文对应的整数，c 是密文对应的整数，3 是密钥. 这种密码称为**凯撒密码**(Caesar cipher)，早在公元前世纪罗马皇帝凯撒就使用该方法传递作战命令.

将大量记录存放在 m 个不同的链表，可以将每个记录的识别码 n 进行模 m 运算，运算结果为该记录所在的链表，即 $h(n)=n \bmod m$. 通常将 h 称为**散列函数**或**哈希函数**(hash function).

利用模运算产生(0,1)上服从均匀分布的**伪随机数**(pseudorandom number). 选取 4 个非负整数：模数 m，乘数 a，常数 c 和种子数 x_0，其中 $2\leqslant a<m$，$0\leqslant c<m$，$0\leqslant x_0<m$，按下式得到序列 $x_1, x_2, x_3, \cdots$：

$$x_n = (ax_{n-1}+c)\bmod m$$

令 $u_n=\dfrac{x_n}{m}$ $(n=1,2,3,\cdots)$，得到(0,1)上服从均匀分布的伪随机数.

5.1.2 素数与素因数分解

【定义 5-3】 对于大于 1 的正整数 p，若 $D_p=\{1, p\}$，即 p 的正因数只有 1 和 p，则称 p 为**素数**(prime)，否则称 p 为**合数**(composite number).

素数又称为质数. 1 既不是素数又不是合数. 最前面的几个素数依次为 2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53. 根据埃拉托色尼筛选法(the sieve of Eratosthene)，容易得知，在正整数序列中，越往后素数越少，但可以证明存在无限多个素

数，进而所有素数构成的集合是一个可列集.

检查一个大于 1 的正整数是否为素数称为素数测试. 素数测试不仅具有重要的理论意义，而且在计算机密码学中具有十分重要的应用价值.

【例 5-1】 证明：若 $a>1$，a^n-1 是素数，则 $a=2$ 且 n 是素数.

证 显然 n 为正整数.

若 $a>2$，则由 $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+1)$ 可知，a^n-1 是合数，因而 $a=2$.

当 n 为合数时，即 $n=ab$，$1<a<n$，$1<b<n$，有 $1<2^a-1<2^n-1$ 且 $2^n-1=(2^a)^b-1$. 容易验证 $x^m-y^m=(x-y)(x^{m-1}+x^{m-2}y+\cdots+y^{m-1})$，进而 $2^a-1\mid 2^n-1$，于是 2^n-1 是合数，因此 n 是素数.

1. 梅森素数

当 n 为素数时，$2^2-1=3$，$2^3-1=7$，$2^5-1=31$，$2^7-1=127$ 都是素数，$2^{11}-1=2047=23\times 89$ 是合数. 对于素数 p，2^p-1 称为梅森(Mersenne)素数. 到 2018 年 12 月为止，美国程序员 Patrick Laroche 利用 GIMPS(Greatest Internet Prime Mersenne Search)项目找到了第 51 个梅森素数 $2^{82\,589\,933}-1$，并获得该项目的 3000 美元奖励，这个数有 24 862 048 位. 你也可以加入梅森素数寻找的行列中(www. mersenne. org/prime. htm)，利用超算能力全球第一和第二的中国“神威·太湖之光”和“天河二号”超级计算机，也许你会在 15min 内成为名人.

2. 孪生素数

若两个素数之差为 2，这两个素数就称为**孪生素数**(twin prime)，例如 3 和 5、5 和 7、11 和 13、17 和 19、29 和 31 等.

是否存在无限对孪生素数是至今未解决的公开问题. 2013 年 5 月，美籍华人张益唐(Yitang Zhang)经过多年努力，在不依赖未经证明的推论的前提下，率先证明了一个“弱孪生素数猜想”，即“存在无限对其差小于 7000 万的素数”. 2014 年 2 月，他将素数对之差缩小到了 246.

3. 哥德巴赫猜想

哥德巴赫(C. Goldbach，1690—1764)在 1742 年提出“大于 4 的偶数是两个奇素数之和(俗称“1+1”)”的猜想. 现已经对直到 10^{14} 的所有的大于 4 的偶数都验证了该结论是正确的. 1966 年，我国数学家陈景润证明了“一个充分大的偶数是一个奇素数与不超过两个奇素数的乘积之和(俗称“1+2”)”，被称为陈氏定理，这是目前为止最好的结果.

若一个素数 p 是 a 的因数，则称 p 是 a 的素因数. 由于合数必存在素因数，于是有下述**素因数分解定理**(prime number decomposition theorem).

【定理 5-2】(素因数分解定理) 任何大于 1 的整数 n 均可分解成素数乘积，即

$$n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$$

其中 $p_1,p_2,\cdots,p_k$ 是不同的素数，$r_1,r_2,\cdots,r_k$ 是正整数.

证 对 n 使用数学归纳法. 当 $n=2$ 时显然成立. 假设大于 2、小于 k 的整数均可分解成素数的乘积. 当 $n=k$ 时，若 k 为素数，结论显然成立；若 k 为合数，则 $n=ab$，$1<a<n$，$1<b<n$. 根据归纳假设，a 和 b 均可分解成素数的乘积，进而 n 可分解成素数的乘积，有

$$8=2^3$$

$$12 = 2^2 \cdot 3$$
$$13 = 13^1 = 13$$
$$14 = 2^1 7^1 = 2 \cdot 7$$
$$21\ 560 = 2^3 \times 5 \times 7^2 \times 11$$

上述定理表明，从理论上讲，任何大于 1 的整数均可进行素因数分解，但一个较大的正整数的素因数分解问题是一个 NP 难问题. 当 $n=142\ 022$ 时，

$$F_n = 2^{2^n} + 1$$

的一个素因数到目前为止尚未找到. 同样，$10^{100} + 37$ 也未找到其一个素因数. 从理论上讲，1994 年 Shor 给出的量子算法在量子计算机上能有效解决该问题.

借助于素因数分解定理，可以证明以下结论.

【例 5-2】 证明：若 n 是合数，则 n 必有一个小于或等于 $\sqrt{n}$ 的素因数.

证 已知 n 是合数，于是存在 a 和 b 使得 $n = ab, 1 < a < n, 1 < b < n$. 于是 a 和 b 中必有一个小于或等于 $\sqrt{n}$. 这个因数或为素数，或根据素因数分解定理有素因数，这时总能找到一个小于或等于 $\sqrt{n}$ 的素因数.

因此，要检查 n 是否为素数，只需要检查 n 是否有一个小于或等于 $\sqrt{n}$ 且大于 1 的素因数即可. 根据此结论，可以编写一个程序以检验给定的正整数是否为素数. 同时，还可以对正整数进行素因数分解.

【例 5-3】 对 2019 进行素因数分解.

解 显然，若 2019 是合数，则其必有一个小于或等于 $\sqrt{2019} < 45$ 的素因数. 容易知道，3 是 2019 的素因数，即 $2019 = 3 \times 673$. 类似地，若 673 是合数，则其必有一个小于或等于 $\sqrt{673} < 26$ 的素因数：2，3，5，7，11，13，17，19，23. 由于 2，3，5，7，11，13，17，19，23 都不是 673 的素因数，因此 673 是素数. 故 2019 的素因数分解为

$$2019 = 3 \times 673$$

5.1.3 最大公因数

1. 最大公因数的定义和计算

【定义 5-4】 对于任意整数 m, n，若 $d \mid m$ 且 $d \mid n$，则称 d 为 m 和 n 的**公因数**(common divisor). 整数 m 和 n 的最大的公因数称为 m 和 n 的**最大公因数**(greatest common divisor)，用 $\gcd(m,n)$ 或 (m, n) 表示.

例如，由于 $-2 \mid 4$ 且 $-2 \mid -6$，所以 -2 是 4 和 -6 的公因数. 容易知道，4 和 -6 的所有公因数为 -1，-2，1 和 2，其最大公因数为 2，即 $\gcd(4, -6) = 2$.

整数 m 和 n 的最大公因数也可记为 (m, n)，即 $\gcd(m,n) = (m,n)$. 由于任何整数都是 0 的因数，因此 $\gcd(0, 0)$ 不存在. 若 $\gcd(m,n)$ 存在，则 $\gcd(m,n)$ 必为正整数.

显然，$\gcd(m, n) = \gcd(n, m) = \gcd(|m|, |n|)$ 且当 $m \neq 0$ 时 $\gcd(m, 0) = |m|$. 因此，在很多的时候，讨论的是两个正整数的最大公因数.

若 $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \in \mathbf{Z}^+$，$n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} \in \mathbf{Z}^+$（$p_1, p_2, \cdots, p_k$ 是不同的素数，$r_1, r_2, \cdots, r_k$ 和 $s_1, s_2, \cdots, s_k$ 是非负整数），则

$$\gcd(m,n) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_k^{\min(r_k, s_k)}$$

下面介绍求两个正整数 m 和 n 的最大公因数 $\gcd(m, n)$的有效算法——辗转相除法，又称为**欧几里得算法**(Euclid algorithm)，是在公元前 300 年欧几里得在其《几何原本》中给出的，这可以算是离散数学最早的算法研究成果.

先证明下面的定理.

【定理 5-3】 对于任意不全为 0 的整数 n，m 和 r，若存在整数 q 使得 $n = qm + r$，则 $\gcd(n, m) = \gcd(m, r)$.

证 显然，$d|n$ 且 $d|m$ 当且仅当 $d|m$ 且 $d|r$. 于是 n 和 m 与 m 和 r 有完全相同的公因数，进而 $\gcd(n, m) = \gcd(m, r)$.

对于正整数 n 和 m，多次使用带余除法，有

$$\begin{aligned} n &= q_1 m + r_1, 0 < r_1 < m \\ m &= q_2 r_1 + r_2, 0 < r_2 < r_1 \\ &\vdots \\ r_{k-2} &= q_{k-1} r_{k-1} + r_k, 0 < r_k < r_{k-1} \\ r_{k-1} &= q_k r_k \end{aligned}$$

由于 $r_k < \cdots < r_2 < r_1 < n$，这种 k 是存在的，于是 $\gcd(n, m) = \gcd(m, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k$.

因为

$$\begin{aligned} r_k &= r_{k-2} - q_{k-1} r_{k-1} \\ &\vdots \\ r_2 &= m - q_2 r_1 \\ r_1 &= n - q_1 m \end{aligned}$$

于是存在整数 s 和 t 使得

$$\gcd(n,m) = ns + mt$$

从欧几里得算法可得以下定理.

【定理 5-4】 对于任意不全为 0 的整数 n 和 m，根据欧几里得算法可得 $\gcd(n, m)$，且 $\gcd(n, m)$是 n 和 m 的整系数线性组合，即存在整数 s 和 t 使得 $\gcd(n,m)=ns+mt$.

上式中的 s 和 t 称为贝祖系数(Bézout coefficient). 它不是唯一的：若 $\gcd(n,m)=ns+mt$，则对于任意 $k\in\mathbf{Z}$，$\gcd(n,m)=n(s+km)+m(t-kn)$.

【例 5-4】 利用欧几里得算法计算 $\gcd(119, 35)$，并求出整数 s 和 t 使得 $\gcd(119, 35)=119s+35t$.

解 因为 $119 = 3 \times 35 + 14$，$35 = 2 \times 14 + 7$，$14 = 2 \times 7$，所以 $\gcd(119, 35) = 7$. 由于 $7 = 35 - 2 \times 14$，$14 = 119 - 3 \times 35$，于是 $7 = 35 - 2 \times (119 - 3 \times 35) = 119 \times (-2) + 35 \times 7$.

2. 互素关系

【定义 5-5】 设 $m, n \in \mathbf{Z}$，若 $\gcd(n, m) = 1$，则称 m 和 n **互素**(relatively prime 或 coprime).

整数集 $\mathbf{Z}$ 上互素关系具有对称性. 对于任意素数 p 和任意整数 n，显然 $\gcd(p, n) = 1$ 或 p，于是 p 与 n 互素或 $p|n$.

根据定理 5-4，可得以下定理.

【定理 5-5】 对于任意整数 m 和 n，$\gcd(n, m) = 1$ 的充要条件是存在整数 s 和 t 使得 $ns + mt = 1$.

由此可得以下定理.

【定理 5-6】 对于整数 m，n 和 k，下述结论成立.

(1) 若 $m|k$，$n|k$，且 $\gcd(m, n) = 1$，则 $mn|k$.

(2) 若 $m|nk$ 且 $\gcd(m, n) = 1$，则 $m|k$.

证 由于 $\gcd(m, n) = 1$，存在整数 s 和 t 使得 $ns+mt=1$，进而 $nks+mkt=k$.

(1) 若 $m|k$，$n|k$，则 $mn|kn$，$mn|km$，于是 $mn|kns$，$mn|kmt$，因此 $mn|nks+mkt$，即 $mn|k$.

(2) 若 $m|nk$，则 $m|nks+mkt$，这时 $m|k$.

【推论】 设 p 为素数且 $p|mn$，则 $p|m$ 或 $p|n$.

证 若 $p|m$，则 $\gcd(p, m) = 1$. 由定理 5-6 知，$p|n$.

下面定义正整数集 $\mathbf{Z}^+$ 上的重要函数——欧拉函数.

【定义 5-6】 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，称 $\varphi(n)$ 为**欧拉函数**(Euler function).

例如 $\varphi(1) = 1$，$\varphi(2) = 1$，$\varphi(3) = 2$，$\varphi(4) = 2$，$\varphi(5) = 4$，$\varphi(6) = 2$. 当 p 为素数时，$\varphi(p) = p - 1$.

设 n 是大于 1 的正整数 n，其素数分解为 $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是不同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，利用容斥原理可以证明以下定理.

【定理 5-7】 对于大于 1 的正整数 n，若 $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，其中 $p_1, p_2, \cdots, p_k$ 是不同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，则

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

特别地，若 p 和 q 是不同的素数，则 $\varphi(pq)=(p-1)(q-1)$.

证 设全集 $U = \{1,2,\cdots,n\}$，用 A_i 表示能被 p_i 整除的 U 中元素组成的集合，则

$$|A_i| = \frac{n}{p_i}, \quad i = 1,2,\cdots,k$$

$$|A_i \cap A_j| = \frac{n}{p_i p_j}, \quad i,j = 1,2,\cdots,k, i \neq j$$

$$\vdots$$

$$|A_1 \cap A_2 \cap \cdots \cap A_n| = \frac{n}{p_1 p_2 \cdots p_k}$$

因为 $|U| = n$ 且

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n}|A_i| - \sum_{1\leqslant i<j\leqslant n}|A_i \cap A_j| +$$

$$\sum_{1\leqslant i<j<k\leqslant n}|A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1}|A_1 \cap A_2 \cap \cdots \cap A_n|$$

所以

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup A_2 \cup \ldots \cup A_n}|$$

$$= |U| - \sum_{i=1}^{n}|A_i| + \sum_{1\leqslant i<j\leqslant n}|A_i \cap A_j| -$$

$$\sum_{1\leqslant i<j<k\leqslant n}|A_i\cap A_j\cap A_k|+\cdots+$$
$$(-1)^n|A_1\cap A_2\cap\cdots\cap A_n|$$
$$=n-\left(\frac{n}{p_1}+\frac{n}{p_2}+\cdots+\frac{n}{p_k}\right)+\left(\frac{n}{p_1p_2}+\frac{n}{p_1p_3}+\cdots+\frac{n}{p_{k-1}p_k}\right)+\cdots+$$
$$(-1)^n\frac{n}{p_1p_2\cdots p_k}$$
$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

若 p 和 q 是不同的素数，则 $\varphi(pq)=pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)=(p-1)(q-1)$.

5.1.4 最小公倍数

【定义 5-7】 对于任意整数 m,n，若 $m|d$ 且 $n|d$，则称 d 为 m 和 n 的**公倍数**(common multiple). 所有整数 m 和 n 的公倍数中，最小的非负整数称为 m 和 n 的**最小公倍数**(least common multiple)，记为 $\mathrm{lcm}(m,n)$或$[m,\ n]$.

例如，由于 $4|-12$ 且 $-6|-12$，所以 -12 是 4 和 -6 的公倍数. 4 和 -6 的公倍数很多，例如 $-12,-24,12,24,36$ 等，其最小非负公倍数为 12，即 $\mathrm{lcm}(4,\ -6)=12$.

显然，对于任意整数 $n\geqslant 0$，有 $\mathrm{lcm}(0,\ n)=0$，特别地 $\mathrm{lcm}(0,\ 0)=0$.

由于 $\mathrm{lcm}(m,\ n)=\mathrm{lcm}(n,\ m)=\mathrm{lcm}(|m|,\ |n|)$，因此在很多的时候，讨论的是两个正整数的最小公倍数.

若 $m=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}\in\mathbf{Z}^+$，$n=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}\in\mathbf{Z}^+$（$p_1,p_2,\cdots,p_k$ 是不同的素数，$r_1,r_2,\cdots,r_k$ 和 $s_1,s_2,\cdots,s_k$ 是非负整数），则

$$\mathrm{lcm}(m,n)=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}$$

【例 5-5】 设 $\mathbf{Z}^+$ 是正整数集合，证明偏序集$(\mathbf{Z}^+,|)$中任意两个元素均存在上确界以及下确界，其中 $|$ 是整除关系.

证 (1) 先证明 $\mathrm{lcm}(x,\ y)$是$\{x,y\}$的上确界. 对于任意 $x,y\in\mathbf{Z}^+$，根据公倍数的定义知，$x|\mathrm{lcm}(x,\ y)$且 $y|\mathrm{lcm}(x,\ y)$，所以 $\mathrm{lcm}(x,\ y)$是$\{x,y\}$的上界. 假定 z 是$\{x,y\}$的上界，则 $x|z$ 且 $y|z$，即 z 是 x 与 y 的公倍数. 根据带余除法知，存在整数 q 和 r 使得 $z=q\cdot\mathrm{lcm}(x,\ y)+r$，$0\leqslant r<\mathrm{lcm}(x,\ y)$. 由公倍数的定义知 $x|r$ 且 $y|r$，即 r 是 x 和 y 的非负公倍数. 由 $\mathrm{lcm}(x,\ y)$的定义知 $r=0$，即 $\mathrm{lcm}(x,\ y)$是$\{x,y\}$的上确界.

(2) 类似地可证明 x 与 y 的最大公约数 $\gcd(x,\ y)$是$\{x,y\}$的下确界(留作练习).

习题 5.1

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 $\mathbf{Z}$.

(2) 自然数集 $\mathbf{N}$.

(3) 正整数 n 的正因数集 D_n.

2. 写出 35 的所有因数集合及所有正因数集合 D_{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 $s|a_n$.

4. 证明：若 a 为正奇数，则 $8|a^2-1$.

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) $n=-48$.

6. 分别计算以下各式.

(1) $2019 \bmod 19$.

(2) $-2019 \bmod 19$.

7. 计算 12345 的八进制数.

8. 分别计算以下各式.

(1) $\varphi(6)$.

(2) $\varphi(8)$.

(3) $\varphi(10)$.

9. 证明：存在无限多个素数且它们是可列的.

10. 对 2015 进行素因数分解.

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

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 $\gcd(s, t)=1$. 试证明之.

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

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.

5.2 模同余关系

5.2.1 模同余关系

伟大的数学家高斯在 18 世纪末给出了整数集 $\mathbf{Z}$ 上的模 m 同余关系$\equiv_m$，其中 m 是正整数，其在计算机密码学中有重要应用.

【定义 5-8】 设 m 是正整数，定义整数集 $\mathbf{Z}$ 上的**模 m 同余关系**(modulo m congruence relation)$\equiv_m$ 如下：

$$(x,y)\in\equiv_m \text{ 当且仅当 } m\mid(x-y)$$

之所以称$\equiv_m$为模 m 同余关系，是因为 $m|(x-y)$当且仅当 x 除以 m 的余数与 y 除以 m 的余数相同，也就是说 $x\equiv_m y$ 当且仅当 $x \bmod m=y \bmod m$，由此可以看出模 m 同余关系与模 m 运算的区别和联系.

注意：$x\equiv_m y$ 在数论中常记为 $x\equiv y(\bmod m)$，实际上是 $x \bmod m=y \bmod m$，但不要与 $x=y \bmod m$ 混淆.

显然，有下述定理.

【定理 5-8】 模 m 同余关系是整数集 $\mathbf{Z}$ 上的等价关系，即具有

(1) **自反性**. 对任意 $x \in \mathbf{Z}$,有 $x \equiv x(\bmod m)$.

(2) **对称性**. 对任意 $x, y \in \mathbf{Z}$,若 $x \equiv y(\bmod m)$,则 $y \equiv x(\bmod m)$.

(3) **传递性**. 对任意 $x, y, z \in \mathbf{Z}$,若 $x \equiv y(\bmod m)$且 $y \equiv z(\bmod m)$,则 $x \equiv z(\bmod m)$.

证 (1) 对任意 $x \in \mathbf{Z}$,由于 $m|(x-x)$,所以有 $(x,x) \in \equiv_m$,于是 $\equiv_m$ 具有自反性.

(2) 对任意 $x,y \in \mathbf{Z}$,若 $(x,y) \in \equiv_m$,则 $m|(x-y)$,显然有 $m|-(x-y)$,即 $m|(y-x)$,于是有 $(y,x) \in \equiv_m$,因此,$\equiv_m$ 具有对称性.

(3) 对任意 $x,y,z \in \mathbf{Z}$,若 $(x,y) \in \equiv_m$ 且 $(y,z) \in \equiv_m$,则 $m|(x-y)$且 $m|(y-z)$,从而 $m|(x-y)+(y-z)$,即 $m|(x-z)$,所以 $(x,z) \in \equiv_m$,因此,$\equiv_m$ 具有传递性.

根据等价关系定义知,$\equiv_m$ 是 $\mathbf{Z}$ 上的等价关系.

由于模 m 同余关系 $\equiv_m$ 是 $\mathbf{Z}$ 上的等价关系,把其等价类称为**模 m 同余类**,其商集 $\mathbf{Z}/\equiv_m = \{[0], [1], \cdots, [m-1]\}$. 可以定义商集 $\mathbf{Z}/\equiv_m$ 上的加法运算和乘法运算. 为了方便,仅考虑模 m 剩余类 $\mathbf{Z}_m = \{0, 1, 2, \cdots, m-1\}$ 上的模 m 算术运算:模 m 加法运算 $+_m$ 和模 m 乘法运算 $\cdot_m$. 在不引起混淆的情况下,可将这两个运算简称为 $\mathbf{Z}_m$ 上的加法运算"+"和乘法运算"·".

对于任意 $x, y \in \mathbf{Z}$,有

$$x +_m y = (x + y) \bmod m$$

$$x \cdot_m y = (xy) \bmod m$$

例如,若 $m = 3, 3+_3(-5)=(-2) \bmod 3=1, 3 \cdot_3(-5)=(-15) \bmod 3=0$.

容易知道,模 m 加法运算 $+_m$ 和模 m 乘法运算 $\cdot_m$ 是 $\mathbf{Z}_m = \{0, 1, 2, \cdots, m-1\}$ 上的封闭运算.

【例 5-6】 分别写出 $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ 关于模 6 加法运算 $+_6$ 和模 6 乘法运算 $\cdot_6$ 的运算表.

解 $\mathbf{Z}_6$ 关于模 6 加法运算 $+_6$ 和模 6 乘法运算 $\cdot_6$ 的运算表分别如表 5-1 和表 5-2 所示.

表 5-1

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

表 5-2

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	4	1

模 m 同余关系还具有下述性质.

【定理 5-9】 设 m 是正整数,则

(1) 若 $a \equiv b(\bmod m)$且 $c \equiv d(\bmod m)$,则 $a + c \equiv b + d(\bmod m)$.

(2) 若 $a \equiv b(\bmod m)$且 $c \equiv d(\bmod m)$,则 $ac \equiv bd(\bmod m)$. 特别地,

- 对于正整数 n,若 $a \equiv b(\bmod m)$,则 $a^n \equiv b^n (\bmod m)$;
- 对于任意整数 c,若 $a \equiv b(\bmod m)$,则 $ac \equiv bc (\bmod m)$.

证 由于 $a \equiv b(\bmod m)$且 $c \equiv d(\bmod m)$,所以 $m|(a-b)$且 $m|(c-d)$. 于是,存在

整数 k 和 l 使得 $a-b=km$ 且 $c-d=lm$. 这时，

(1) $(a+c)-(b+d)=(k+l)m$，进而 $a+c\equiv b+d(\bmod m)$.

(2) $ac=(b+km)(d+lm)=bd+(bl+dk+klm)m$，进而 $ac\equiv bd(\bmod m)$.

【例 5-7】 求 3^{2019} 的个位数.

解 显然，3^{2019} 的个位数为 $3^{2019} \bmod 10$. 由于 $3^4\equiv 1(\bmod 10)$，而 $2019=4\times 405+3$，根据定理 5-10(2)，有 $3^{4\times 405}\equiv 1^{405}(\bmod 10)=1 \bmod 10$，$3^{4\times 405+3}\equiv 1\times 3^3(\bmod 10)=7 \bmod 10$，即 $3^{2019} \bmod 10=7$. 故 3^{2019} 的个位数为 7.

在用数论知识研究密码学时，经常进行幂模(power modulo)运算 $a^k \bmod m$. 利用模同余关系的性质，可以得到一些幂模运算结果，如例 5-7. 其次是考虑利用欧拉定理或费马小定理做幂模运算.

下面证明欧拉定理(Euler's theorem).

【定理 5-10】(欧拉定理) 若整数 a 与正整数 m 互素，即 $\gcd(a, m)=1$，则 $a^{\varphi(m)}\equiv 1(\bmod m)$，其中 $\varphi(m)$ 为欧拉函数.

证 令 S 是小于或等于 m 且与 m 互素的正整数组成的集合，于是 $|S|=\varphi(m)$，不妨记 $S=\{r_1, r_2, \cdots, r_{\varphi(m)}\}$. 由于 $\gcd(a, m)=1$，下面证明 $S=\{ar_1(\bmod m), ar_2(\bmod m), \cdots, ar_{\varphi(m)}(\bmod m)\}$.

一方面，由于 $\gcd(a, m)=1$ 且 $\gcd(r_i, m)=1$，于是 $\gcd(ar_i, m)=1(i=1,2,\cdots,\varphi(m))$，进而 $\{ar_1(\bmod m), ar_2(\bmod m), \cdots, ar_{\varphi(m)}(\bmod m)\}\subseteq S$.

另一方面，$ar_i(\bmod m)\neq ar_j(\bmod m)(i\neq j)$. 若 $ar_i(\bmod m)=ar_j(\bmod m)$，则 $m\mid ar_i-ar_j$，即 $m\mid a(r_i-r_j)$. 因为 $\gcd(a, m)=1$，因而 $m\mid r_i-r_j$，进而 $r_i=r_j$，不可能.

因此，有 $S=\{ar_1(\bmod m), ar_2(\bmod m), \cdots, ar_{\varphi(m)}(\bmod m)\}$. 由此可得，$ar_1(\bmod m)\cdot ar_2(\bmod m)\cdot\cdots\cdot ar_{\varphi(m)}(\bmod m)=r_1\cdot r_2\cdot\cdots\cdot r_{\varphi(m)}$，即

$$ar_1\cdot ar_2\cdot\cdots\cdot ar_{\varphi(m)}\equiv r_1\cdot r_2\cdot\cdots\cdot r_{\varphi(m)}(\bmod m)$$

$$a^{\varphi(m)}r_1\cdot r_2\cdot\cdots\cdot r_{\varphi(m)}\equiv r_1\cdot r_2\cdot\cdots\cdot r_{\varphi(m)}(\bmod m)$$

由于 $\gcd(r_i, m)=1(i=1,2,\cdots,\varphi(m))$，故 $a^{\varphi(m)}\equiv 1(\bmod m)$.

若 p 为素数，则 $\varphi(p)=p-1$. 于是，由欧拉定理可得费马小定理(Fermat's little theorem).

【定理 5-11】(**费马小定理**) 设 p 为素数且整数 a 与 p 互素，即 $\gcd(a, p)=1$，则 $a^{p-1}\equiv 1(\bmod p)$，即 $a^p\equiv a(\bmod p)$.

说明：

(1) 费马小定理的逆不成立，也就是说存在合数 n，即使 a 与 n 互素，$a^{n-1}\equiv 1(\bmod n)$ 仍成立，例如 $341=11\times 31$，而 $2^{341-1}\equiv 1(\bmod 341)$，但这样的 n[称为卡迈克尔(Carmichael)数]非常少.

(2) **费马大定理**(Fermat last theorem)如下：对任意正整数 a, b, c 和 n，当 $n>2$ 时，有 $a^n+b^n\neq c^n$[1995 年被英国数学家安德鲁·怀尔斯(Andrew Wiles)证明].

【例 5-8】 根据费马小定理分别计算 $5^{2019} \bmod 7$.

解 由于 $\varphi(7)=6$，根据费马小定理，有 $5^6\equiv 1(\bmod 7)$. 而 $2019=336\times 6+3$，所以 $5^{2019}=5^{336\times 6+3}=(5^6)^{336}\times 5^3\equiv 1\times 5^3(\bmod 7)=125 \bmod 7=6$.

最后介绍当 a，k 及 m 较大时计算 $a^k(\bmod m)$ 的较一般方法：**逐次平方法**(successive