离散数学6 初等数论

离散数学6 初等数论
第19章 初等数论
- 素数
  - 整除、带余除法
  - 整除的性质
  - 素数、合数
  - 素数与合数的性质
  - 素因子分解——算术基本定理
  - 素数检测——Eratosthene筛法
- 最大公约数与最小公倍数
  - 互素
  - 辗转相除法——求最大公因子
- 同余
- 一次同余方程
  - 中国剩余定理
- 欧拉定理与费马小定理

应用
- 产生均匀伪随机数
  - 线性同余法
  - 乘同余法

第19章 初等数论

素数

整除、带余除法

设 a,b 是两个整数，且 $b\neq 0$. 如果存在整数 c 使 $a=bc$，则称 a 被 b 整除，或 b 整除 a，记作 $b\mid a$. 此时，又称 a 是 b 的倍数，b 是 a 的因子. 把 b 不整除 a 记作 $b\nmid a$.

例如，10 被 ±1，±2，±5 和 ±10 整除，10 有 8 个因子 ±1，±2，±5 和 ±10. 由于正负因子是成对出现的，通常只考虑正因子. 显然，任何正整数都有两个正因子：1 和它自己，称作它的平凡因子. 除平凡因子之外的因子称作真因子. 例如，2 和 5 是 10 的真因子.

设 a,b 是两个整数，且 $b\neq 0$，则存在惟一的整数 q 和 r，使得

$$a=qb+r,\qquad 0\leqslant r<|b|.$$

这个式子称作带余除法. 记余数 $r=a \bmod b$.

例如，$23=5\times 4+3$，$23 \bmod 4=3$；$-10=-4\times 3+2$，$-10 \bmod 3=2$；$15=5\times 3+0$，$15 \bmod 3=0$.

显然，$b\mid a$ 当且仅当 $a \bmod b=0$.

整除的性质

不难验证，整除有下述性质：

性质 19.1 如果 $a \mid b$ 且 $a \mid c$，则对任意的整数 x,y，有 $a \mid xb+yc$；

性质 19.2 如果 $a \mid b$ 且 $b \mid c$，则 $a \mid c$；

性质 19.3 设 $m \neq 0$，则 $a \mid b$ 当且仅当 $ma \mid mb$.

性质 19.4 如果 $a \mid b$ 且 $b \mid a$，则 $a = \pm b$.

性质 19.5 如果 $a \mid b$ 且 $b \neq 0$，则 $|a| \leqslant |b|$.

素数、合数

定义 19.1 如果正整数 a 大于 1 且只能被 1 和它自己整除，则称 a 是**素数**；如果 a 大于 1 且不是素数，则称 a 是**合数**. 素数也称做**质数**.

例如，5 和 13 是素数，4 和 15 是合数.

素数与合数的性质

素数和合数有下述性质：

性质 19.6 如果 $d>1$，p 是素数且 $d \mid p$，则 $d=p$.

性质 19.7 设 p 是素数且 $p \mid ab$，则必有 $p \mid a$ 或者 $p \mid b$.

更一般地，设 p 是一个素数且 $p \mid a_1 a_2 \cdots a_k$，则必存在 $1 \leqslant i \leqslant k$，使得 $p \mid a_i$.

注意：当 d 不是素数时，$d \mid ab$ 不一定能推出 $d \mid a$ 或 $d \mid b$. 如，$6 \mid 4 \times 9$，但 $6 \nmid 4$ 且 $6 \nmid 9$.

性质 19.8 $a>1$ 是合数当且仅当 $a=bc$，其中 $1<b<a$，$1<c<a$.

性质 19.9 合数必有素数因子，即设 a 是一个合数，则存在素数 p，使得 $p \mid a$.

根据性质 19.9，任何大于 1 的整数要么是素数、要么可以分解成素数的乘积. 这样的分解是惟一的，这就是下述算术基本定理，它表明素数是构成整数的“基本元素”.

素因子分解——算术基本定理

算术基本定理 任何大于 1 的整数 a 有素因子分解

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

其中，$p_1, p_2, \cdots, p_k$ 是不相同的素数，$r_1, r_2, \cdots, r_k$ 是正整数，并且在不计顺序的情况下，该表示是唯一的.

素数检测——Eratosthene筛法

有无穷多个素数. 记 $\pi(n)$ 为小于等于 n 的素数个数.

素数定理 $\lim\limits_{n \to +\infty} \dfrac{\pi(n)}{n/\ln n} = 1$

埃拉托斯特尼(Eratosthene)筛法——求任意给定正整数以内所有素数的方法.

最大公约数与最小公倍数

互素

a 与 b 的公因子（公约数）与公倍数，最大公因子（最大公约数）$\gcd(a,b)$ 与最小公倍数 $\operatorname{lcm}(a,b)$. 如果 $\gcd(a,b)=1$，则称 a 和 b **互素**.

定理 11.1 （1）若 $a \mid m, b \mid m$，则 $\operatorname{lcm}(a,b) \mid m$.

（2）若 $d \mid a, d \mid b$，则 $d \mid \gcd(a,b)$.

（3）设 $a=qb+r$，其中 a、b、q、r 都是整数，则 $\gcd(a,b)=\gcd(b,r)$.

（4）设 a 和 b 不全为 0，则存在整数 x 和 y，使得 $\gcd(a,b)=xa+yb$.

（5）a 和 b 互素的充分必要条件是存在整数 x 和 y 使得 $xa+yb=1$.

设 $a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，$b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$，其中 $p_1,p_2,\cdots,p_k$ 是不同的素数，$r_1,r_2,\cdots,r_k,s_1,s_2,\cdots,s_k$ 是非负整数，则

$$\gcd(a,b)=p_1^{\min(r_1,s_1)}p_2^{\min(r_2,s_2)}\cdots p_k^{\min(r_k,s_k)}$$
$$\operatorname{lcm}(a,b)=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}$$

辗转相除法——求最大公因子

设整数 a,b，且 $b\neq 0$. 做带余除法

$$a=q_1b+r_2,\quad 0\leqslant r_2<|b|.$$

若 $r_2>0$，再对 b 和 r_2 做带余除法，得

$$b=q_2r_2+r_3,\quad 0\leqslant r_3<r_2,$$

重复上述过程. 由于 $|b|>r_2>r_3>\cdots\geqslant 0$，必存在 k 使 $r_{k+1}=0$. 于是，有

$$\begin{aligned}
a&=q_1b+r_2, && 1\leqslant r_2<|b|,\\
b&=q_2r_2+r_3, && 1\leqslant r_3<r_2,\\
r_2&=q_3r_3+r_4, && 1\leqslant r_4<r_3,\\
&\vdots\\
r_{k-2}&=q_{k-1}r_{k-1}+r_k, && 1\leqslant r_k<r_{k-1},\\
r_{k-1}&=q_kr_k.
\end{aligned}$$

根据定理 19.6，有

$$\gcd(a,b)=\gcd(b,r_2)=\cdots=\gcd(r_{k-1},r_k)=r_k.$$

这就是辗转相除法，又叫做欧几里得(Euclid)算法.

同余

、

如果 $m \mid a-b$，则称 a 与 b **模 m 同余**，记作 $a\equiv b \pmod m$.

（1）同余关系是等价关系，即同余关系具有自反性、传递性和对称性.

（2）模算术运算 若 $a\equiv b\pmod m$，$c\equiv d\pmod m$，则

$$a\pm c\equiv b\pm d\pmod m,\quad ac\equiv bd\pmod m,\quad a^k\equiv b^k\pmod m$$

其中 k 是非负整数.

整数 a 在模 m 同余关系下的等价类称作 a 的**模 m 等价类**，记作 $[a]_m$，简记作 $[a]$. 整数集合 $\mathbf{Z}$ 在模 m 同余关系下的商集记作 $\mathbf{Z}_m$. 在 $\mathbf{Z}_m$ 上定义加法和乘法如下：

$$[a]+[b]=[a+b],\quad [a]\cdot[b]=[ab]$$

一次同余方程

4. 一次同余方程

定理 11.2 设 $m>0$，一次同余方程 $ax \equiv c \pmod{m}$ 有解的充分必要条件是 $\gcd(a,m) \mid c$.

设 x_0 是方程的一个解，则方程的解可写成 $x \equiv x_0 \pmod{m}$.

如果 $ab \equiv 1 \pmod{m}$，则称 b 是 a 的**模 m 逆**，记作 $\boldsymbol{a}^{-1} \pmod{\boldsymbol{m}}$ 或 $\boldsymbol{a}^{-1}$.

定理 11.3 (1) a 的模 m 逆存在的充分必要条件是 a 与 m 互素.

(2) 设 a 与 m 互素，则在模 m 下 a 的模 m 逆是唯一的，即 a 的任意两个模 m 逆都模 m 同余.

中国剩余定理

中国剩余定理(孙子定理) 设正整数 $m_1, m_2, \cdots, m_k$ 两两互素，则一次同余方程组

$$
\begin{gathered}
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\vdots \\
x \equiv a_k \pmod{m_k}
\end{gathered}
$$

有整数解，并且在模 $m=m_1 m_2 \cdots m_k$ 下解是唯一的，即任意两个解都是模 m 同余的.

令 $M_i = m/m_i$，设 M_i 的模 m_i 逆为 M_i^{-1}，$i=1,2,\cdots,k$，则同余方程组的解为

$$x \equiv a_1 M_1^{-1} M_1 + a_2 M_2^{-1} M_2 + \cdots + a_k M_k^{-1} M_k \pmod{m}$$

设 $m_1, m_2, \cdots, m_k$ 是 k 个大于 1 的两两互素的正整数，x 的模表示 $x=(x_1, x_2, \cdots, x_k)$，其中 $x_i = x \bmod m_i$，$i=1,2,\cdots,k$. 利用整数的模表示可以做 $m=m_1 m_2 \cdots m_k$ 以内的加、减、乘运算.

欧拉定理与费马小定理

5. 欧拉定理和费马小定理

欧拉函数 $\phi(n)$ 等于 $\{0,1,\cdots,n-1\}$ 中与 n 互素的个数. 当 n 为素数时，$\phi(n)=n-1$.

欧拉定理 设 a 与 n 互素，则 $a^{\phi(n)} \equiv 1 \pmod{n}$.

费马小定理 设 p 是素数，a 与 p 互素，则 $a^{p-1} \equiv 1 \pmod{p}$.

另一种形式，设 p 是素数，则对任意的整数 a，$a^p \equiv a \pmod{p}$.

① 为了区别于著名的费马大定理，通常将此定理冠名为费马小定理. 费马(Pirre de Fermat)是 17 世纪著名的数学家，他提出了许多未加证明的定理，其中最著名的当数费马大定理：对所有的正整数 a,b,c 和 n，当 $n>2$ 时，$a^n+b^n \neq c^n$. 费马大定理直到 1995 年才被英国数学家 Andrew Wiles 证明.

应用

产生均匀伪随机数

线性同余法

最常用的产生(0,1)上均匀分布伪随机数的方法是线性同余法. 选择4个非负整数:模数 m,乘数 a,常数 c 和种子数 x_0,其中 $2\leqslant a<m, 0\leqslant c<m, 0\leqslant x_0<m$,按照下述递推公式产生伪随机数序列:

$$x_n=(ax_{n-1}+c) \bmod m, \quad n=1,2,\cdots \tag{19.6}$$

为了得到(0,1)上均匀分布伪随机数,取

$$u_n=x_n/m, \qquad n=1,2,\cdots \tag{19.7}$$

种子数 x_0 在计算时随机给出,其他3个参数 m,a 和 c 是固定不变的,它们的取值决定了所产生的伪随机数的质量.

式(19.6)至多能产生 m 个不同的数,因此得到的序列一定会出现循环,即存在正整数 n_0 和 l,使得所有的 $n\geqslant n_0$ 都有 $x_{n+l}=x_n$. 使得上式成立的最小正整数 l 称作该序列的周期. 例如,取

乘同余法

取 $c=0$,公式(19.6)简化为

$$x_n=ax_{n-1} \bmod m, \quad n=1,2,\cdots. \tag{19.8}$$

称作乘同余法. 采用乘同余法时,显然不能取 $x_0=0$. 取 $m=2^{31}-1, a=7^5$ 的乘同余法是最常用的均匀伪随机数发生器,它的周期是 $2^{31}-2$. 取种子数 $x_0=1$,得到伪随机数如下: