整　　除

知识、方法、技能

整除是整数的一个重要内容，这里仅介绍其中的几个方面：整数的整除性、最大公约数、最小公倍数、方幂问题.

Ⅰ. 整数的整除性

初等数论的基本研究对象是自然数集合及整数集合. 我们知道，整数集合中可以作加、减、乘法运算，并且这些运算满足一些规律（即加法和乘法的结合律和交换律，加法与乘法的分配律），但一般不能做除法，即，如a,b是整除，$b\neq 0$，则$\frac{a}{b}$不一定是整数. 由此引出初等数论中第一个基本概念：整数的整除性.

定义一：（带余除法）对于任一整数a和任一整数b，必有惟一的一对整数q，r使得$a=bq+r$，$0\le r<b$，并且整数q和r由上述条件惟一确定，则q称为b除a的不完全商，r称为b除a的余数.

若$r=0$，则称b整除a，或a被b整除，或称a是b的倍数，或称b是a的约数（又叫因子），记为$b\mid a$.否则，$b\nmid a$.

任何a的非$\pm a,\pm 1$的约数，叫做a的真约数.

0 是任何整数的倍数，1 是任何整数的约数.

任一非零的整数是其本身的约数，也是其本身的倍数.

由整除的定义，不难得出整除的如下性质：

（1）若$a\mid b,b\mid c,$则$a\mid c.$

（2）若$a\mid b_i,$则$a\mid\sum_{i=1}^{n}c_ib_i,$其中$c_i\in Z,i=1,2,\cdots,n.$

（3）若$a\mid c$，则$ab\mid cb.$反之，亦成立.

（4）若$a\mid b,$则$\mid a\mid\le\mid b\mid$.因此，若$a\mid b,$又$b\mid a,$则$a=\pm b$.

（5）a、b互质，若$a\mid c,b\mid c,$则$ab\mid c.$

（6）p为质数，若$p\mid a_1\cdot a_2\cdot\cdots\cdot a_n,$则$p$必能整除$a_1,a_2,\cdots,a_n$中的某一个.

特别地，若 p 为质数， $p \mid a^n$,则$p \mid a$.

（7）如在等式 $\sum_{i=1}^{n} a_i = \sum_{k=1}^{m} b_k$ 中除开某一项外，其余各项都是 c 的倍数，则这一项也是 c 的倍数.

（8）n 个连续整数中有且只有一个是 n 的倍数.

（9）任何 n 个连续整数之积一定是 n 的倍数.

本讲开始在整除的定义同时给出了约数的概念，又由上一讲的算术基本定理，我们就可以讨论整数的约数的个数了.

定理一：设大于 1 的整数 a 的标准分解式为 $a = {p_1}^{\alpha_1} \cdot p^{\alpha_2} \cdots {p_n}^{\alpha_n}$ ($p_1 < p_2 < \cdots < p_n$ 为质数，α_i 均为非负整数)，则 a 的约数的个数为

$$d(a) = \prod_{i=1}^{n} (\alpha_i + 1).$$

所有的约数和为：

$$\sigma(a) = \prod_{i=1}^{n} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

事实上，由算术基本定理的推论知 $d(a) = \prod_{i=1}^{n} (\alpha_i + 1)$，而各约数的和就是 $\prod_{i=1}^{n} (1 + p_i + \cdots + pa_{i_i})$ 展开后的各项之和，所以

$$\sigma(a) = \prod_{i=1}^{n} (1 + p_i + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^{n} \frac{p_1^{\alpha_i} - 1}{p_i - 1}$$

例如，25200=$2^4 \cdot 3^2 \cdot 5^2 \cdot 7$，所以

$$d(25200) = (4+1)(2+1)(2+1)(1+1) = 90,$$

$$\sigma(25200) = \frac{2^5 - 1}{2 - 1} \times \frac{3^3 - 1}{3 - 1} \times \frac{5^3 - 1}{5 - 1} \times \frac{7^2 - 1}{7 - 1} = 99944.$$

Ⅱ．最大公约数和最小公倍数

定义二：设 a 、b 是两个不全为 0 的整数.若整数 c 满足：$c \mid a, c \mid b$，则称 c 为 a, b 的公约数，a 与 b 的所有公约数中的最大者称为 a 与 b 的最大公约数，记为 (a, b).如果 (a, b)=1，

则称a与b互质或互素.

定义三：如果d是a、b的倍数，则称d是a、b的公倍数. a与b的公倍数中最小的正数称为a与b的最小公倍数，记为$[a,b]$.

最大公约数和最小公倍数的概念可以推广到有限多个整数的情形，并用$(a_1,a_2,\cdots,a_n)$表示$a_1,a_2,\cdots,a_n$的最大公约数，$[a_1,a_2,\cdots,a_n]$表示$a_1,a_2,\cdots,a_n$的最小公倍数.

若$(a_1,a_2,\cdots,a_n)=1$，则称$a_1,a_2,a_3,\cdots,a_n$互质，若$a_1,a_2,\cdots,a_n$中任何两个都互质，则称它们是两两互质的.注意，n个整数互质与n个整数两两互质是不同的概念，前者成立时后者不一定成立（例如，3，15，8互质，但不两两互质）；显然后者成立时，前者必成立.

因为任何正数都不是0的倍数，所以在讨论最小公倍数时，一般都假定这些整数不为0. 同时，由于a,b与$|a|,|b|$有相同的公约数，且$(a,b)=(|a|,|b|)$（有限多个亦成立），因此，我们总限于在自然数集合内来讨论数的最大公约数和最小公倍数.

显然，若a,b的标准分解式为$a=\prod_{i=1}^{n}p_i^{\alpha_i}, b=\prod_{i=1}^{n}p_i^{\beta_i}$（$p_i$为质数，$a_i,\beta_i$为非负整数），则

$$(a,b)=\prod_{i=1}^{n}p_i^{\min(\alpha_i,\beta_i)} \qquad ①$$

$$[a,b]=\prod_{i=1}^{n}p_i^{man(\alpha_i,\beta_i)} \qquad ②$$

例如　$3960=2^3\cdot3^2\cdot5\cdot11$，

$756=2^2\cdot3^3\cdot7$，

则　（3960，756）$=2^2\cdot3^2=36$，

[3960，756]$=2^3\cdot3^3\cdot5\cdot7\cdot11=83160$.

求最大公约数也可以用辗转相除法，其理论依据是：

定理二：设a、b、c是三个不全为0的整数，且有整数t使得$a=bt+c$，则a、b与b、c有相同的公约数，因而$(a,b)=(b,c)$，即$(a,b)=(b,a-bt)$.

因为，若d是a、b的任一公约数，则由$d\mid a,d\mid b$和$a=bt+c$知$d\mid c$,即d是b、c的公约数；反之，若d是b、c的任一公约数，d也是a、b的公约数.

辗转相除法：设a、$b\in N^*$,且$a>b$，

由带余除法有

$$\left.\begin{aligned}
&a=bq_1+r_1,0<r_1<b,\\
&b=r_1q_2+r_2,0<r_2<r_1,\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n,0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1},r_{n+1}=0.
\end{aligned}\right\}\qquad ③$$

因为每进行一次带余除法，余数至少减 1，即$b>r_1>\cdots>r_n>r_{n+1}$，而 b 为有限数，因此，必有一个最多不超过 b 的正整数 n 存在，使得$r_n\neq 0$，而$r_{n+1}=0$，故由定理二得：

$$r_n=(r_{n+1},r_n)=(r_n,r_{n-1})=\cdots=(r_2,r_1)=(r_1,b)=(a,b).$$

例如，（3960，756）=（756，180）=（180，36）=36.

具体算式如下：

5（q_1）	3960（a） 3780	756（b） 720	4（q_2）
5（q_3）	180（r_1） 180	36（r_2）	
	0（r_3）		

由定义和上述求法不难得出最大公约数和最小公倍数的如下性质：

（1）$m\in N$,则$(am,bm)=m(a,b)$.

（2）设c为a,b的公约数，则$(\frac{a}{c},\frac{b}{c})=\frac{(a,b)}{c}$.特别地，若$c=(a,b)$,则$(\frac{a}{c},\frac{b}{c})=1$.

（3）设$a_1,a_2,\cdots,a_n$是任意 n 个正整数，如果$(a_1,a_2)=c_2,(c_2,a_3)=c_3,\cdots,(c_{n-1},a_n)=c_n$，则$(a_1,a_2,\cdots,a_n)=c_n$.

因$c_n\mid a_n,c_n\mid c_{n-1}$,而$c_{n-1}\mid a_{n-1},c_{n-1}\mid c_{n-2}$,故$c_{n-1}\mid a_{n-1},c_n\mid c_{n-2}$，如此类推得出$c_n$能整除$a_n,a_{n-1},\cdots,a_1$,于是$c_n$是它们的一个公约数.又设$c$为$a_1,a_2,\cdots,a_n$的任一公约数，则$c\mid a_1,c\mid a_2$，因而$c\mid c_2$，同理可推出$c\mid c_3$，如此类推最后可得$c\mid c_n$．于是$c\leq|c|\leq c_n$，故$c_n$是最大公约数.

（4）若$(a,b)=c$，则一定有整数x和y，使得$ax+by=c$.

特别地，$(a,b)=1\Leftrightarrow$存在x,y使得$ax+by=1$.

这可由辗转相除法的③式逆推而得$c=r_n=ax+by$.

（5）若$(a,b)=1$,则$(ac,b)=(c,b)$.

（6）$a,b\in N^*$

①$[ak,bk]=k[a,b]\qquad(k\in N^*)$；

②m为a,b的任一公倍数，则$[a,b]\mid m$；

③$(a,b)[a,b]=ab$，特别地，若$(a,b)=1$,则$[a,b]=ab$.

①可由③直接得到，②可由最小公倍数定义得，③根据①、②式知，

$(a,b)[a,b]=$

$$\prod_{i=1}^{n}p_i^{\min(\alpha_i,\beta_i)}=\prod_{i=1}^{n}p_i^{\alpha_i+\beta_i}=ab.$$

（7）设$a_1,a_2,\cdots,a_n$是任意n个正整数.若$[a_1,a_2]=m_2,[m_2,a_3]=m_3,\cdots,[m_{n-1},a_n]=m_n$,则$[a_1,a_2,\cdots,a_n]=m_n$.

这是一个求多个整数的最小公倍数的方法.它可用证明③类似的方法来证明.