带余整除法

定理 1. 设 a,b 为给定的整数， $a\neq 0$,则一定存在唯一的一对整数 q 与 r，满足 $b=qa+r$， $0\le r<|a|$。特别地 $a|b$ 的充要条件是 r=0.

证明：需证明存在性与唯一性问题。

定理 2. 设 $r\ge 2$ 是给定的正整数，则任一正整数 n 必可唯一表为：$n=a_k\cdot r^k+a_{k-1}\cdot r^{k-1}+\cdots+a_1\cdot r+a_0$，其中整数 $k\ge 0$，$0\le a_i\le r-1$ （$0\le i\le k$）。

（即正整数 n 的 r 进制表示）

例 1： $r=2$

$$3_{10}=1\times 2^1+1=11_2$$

$$9_{10}=1\times 2^3+0\times 2^2+0\times 2^1+1=1001_2$$

$r=8$

$$3677_{10}=7\times 8^3+1\times 8^2+3\times 8^1+5=7135_8$$

最大公约数与最小公倍数.

1. 最大公约数：设 $a_1,a_2,\cdots,a_k$ 为 k 个整数，且 $d|a_i,(i=1,\cdots,k)$，则称 d 为 $a_1,a_2,\cdots,a_k$ 公约数，其中最大的公约数记为（$a_1,a_2,\cdots,a_k$）。

例： $a_1=12$， $a_2=18$. 则 $d=\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6$, $(a_1,a_2)=(12,18)=6$

注：一般情况下仅考虑正整数的情况。

2. 互素：若（$a_1,a_2,\cdots,a_k$）=1，则称 $a_1,a_2,\cdots,a_k$ 为互素的。

3. 最小公倍数：设 $a_1,a_2,\cdots,a_k$ 为 k 个整数，若 $a_i|m$，$(i=1,\cdots,k)$ ，则 m 称为 $a_i(i=1,\cdots,k)$ 的公倍数。其中最小的公倍数记为 $[a_1,a_2,\cdots,a_k]$。

例：[12, 18]=36

4. 最大公约数的求解方法：

I. 先将待求正整数分解成素因数之积，然后取出它们所公有的素因数。（相同的素因数照公有的个数取）相乘。

例 1： $36=2\times 2\times 3\times 3=2^2\times 3^2$

$24=2\times 2\times 2\times 3=2^3\times 3^1$

则 $(36,24)=2^2\times 3=12$

例 2： $48=2^4\times3$， $60=2^2\times3\times5$， $72=2^3\times3^2$，则 $(48,60,72)=2^2\times3=12$.

II. 辗转相除法（Euclid 法）求(a, b). (a>b)

1)

$$a=b\cdot q_1+r_1,0\le r_1<b$$
$$b=r_1\cdot q_2+r_2$$
$$r_1=r_2\cdot q_3+r_3$$
$$\cdots\cdots$$
$$r_{n-3}=r_{n-2}\cdot q_{n-1}+r_{n-1}$$
$$r_{n-2}=r_{n-1}\cdot q_n+r_n$$
$$r_{n-1}=r_n\cdot q_{n+1}+r_{n+1}$$
$$r_n=r_{n+1}\cdot q_{n+2}+0$$

则 r_{n+1} 即为所求。

原理： $(a,b)=(b,r_1)=(r_1,r_2)=\cdots$

推论：设 d=(a, b), (a>b), 则存在整数 k_1, k_2, 使得 $k_1a+k_2b=d$

特别地当 d=1 时有： $k_1a+k_2b=1$

证明：由上述公式得到：

$$\begin{aligned}
d&=r_{n+1}=r_{n-1}-q_{n+1}\cdot r_n=k_{11}\cdot r_{n-1}+k_{12}\cdot r_n\\
&\quad(k_{11}=1,k_{12}=-q_{n+1},\text{以下类似})\\
&=k_{11}\cdot r_{n-1}+k_{12}\cdot(r_{n-2}-q_n\cdot r_{n-1})\\
&=k_{21}\cdot r_{n-2}+k_{22}\cdot r_{n-1}\\
&=k_{21}\cdot r_{n-2}+k_{22}\cdot(r_{n-3}-q_{n-1}\cdot r_{n-2})\\
&=k_{31}\cdot r_{n-3}+k_{32}\cdot r_{n-2}\\
&=\cdots\cdots=k_{(n-1)1}\cdot r_1+k_{(n-1)2}\cdot r_2\\
&=k_{(n-1)1}\cdot r_1+k_{(n-1)2}\cdot(b-q_2\cdot r_1)\\
&=k_{(n-1)2}\cdot b+(k_{(n-1)1}-k_{(n-1)2}\cdot q_2)\cdot r_1\\
&=k_{(n-1)2}\cdot b+(k_{(n-1)1}-k_{(n-1)2}\cdot q_2)\cdot(a-q_1\cdot b)\\
&[\text{令}k_1=(k_{(n-1)1}-k_{(n-1)2}\cdot q_2),\\
&\quad k_2=k_{(n-1)2}+(k_{(n-1)1}-k_{(n-1)2}\cdot q_2)\cdot q_1)]\\
&=k_1\cdot a+k_2\cdot b
\end{aligned}$$

2）至于 $(a_1,a_2,\cdots a_n)$，先求 $d_1=(a_1,a_2)$，再求 $d_2=(d_1,a_3)=(a_1,a_2,a_3)=\cdots$

例 1： $d=(6731,\ 2809)$

则 6731 = 2809 * 2 + 1113
2809 = 1113 * 2 + 583
1113 = 583 * 1 + 530
583 = 530 * 1 + 53
530 = 53 * 10 + 0　　故 d = 53

例 2： d = (735000, 421160, 238948)
d1 = (735000, 238948) = 4

d = (d1, 421160) = 4　　(4 | 421160)

5. 最小公倍数的求解方法. $[a_1,a_2,\cdots,a_n]$

I.　先将待求的$a_1,a_2,\cdots,a_n$分解成素因数之积，相同的素因数写成$p_i^{\alpha_i}$形式。

设$a_1,a_2,\cdots,a_n$所有出现的素因数为$p_1,\cdots,p_s$，则$[a_1,a_2,\cdots,a_n]=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$，其中$\beta_s$取形如$p_s^{\alpha_s}$中最大的$\alpha_s$.

例：$108=2^2\times3^3$ ， $28=2^2\times7$， $42=2\times3\times7$

则$\left[108,\quad 28,\quad 42\right]=2^2\times3^3\times7^1=756$

II.　先求$d=(a_1,a_2)$，则$[a_1,a_2]=\dfrac{a_1\times a_2}{d}$

III.　求$[a_1,a_2,\cdots,a_n]$，先求$[a_1,a_2]=m_1$，再求$[m_1,a_3]$，以此类推。

例 1：(108, 28)=4, 则$\left[108,\quad 28\right]=\dfrac{108\times28}{4}=2^2\times3^3\times7=m_1$， $(m_1,42)=2\times3\times7$， 则

$[m_1,42]=\dfrac{2\times3\times7\times2^2\times3^3\times7}{2\times3\times7}=2^2\times3^3\times7$

6. 性质：

① $d=(a_1,\cdots,a_n)$, 则$\left(\dfrac{a_1}{d},\cdots,\dfrac{a_n}{d}\right)=1$.

证明: 令$m=\left(\dfrac{a_1}{d},\cdots\cdots,\dfrac{a_n}{d}\right)$, 若$m>1$, 则由$m\mid\dfrac{a_i}{d}, i=1,\cdots,n$得到: $dm\mid a_i$

故dm为$a_1,\cdots,a_n$的一个公因子, 且$dm>d$, 这与 d 为最大公因子矛盾.

② $m(b_1,\cdots,b_n)=(mb_1,\cdots,mb_n)$　$m>0$.

证明: 设$d1=(b_1,\cdots,b_n)$, $d2=(mb_1,\cdots mb_n)$

I. 由$d1\mid b_i, i=1,\cdots,n$得: $md1\mid mb_i$, 故md1为mb_i (i=1, …, n)的公因子, 则由d2的定义知:md1≤d2

II. 由$d2\mid mb_i$， i=1, …, n, 及$m\mid d2$得: $\dfrac{d2}{m}\mid b_i$, 又由 d1 的定义知: $\dfrac{d2}{m}\le d1$,

即: d2≤md1

综上：md1=d2

③ $(a_1,a_2,\cdots,a_n)=((a_1,a_2),a_3,\cdots,a_n)$

$(a_1,\cdots,a_{k+r})=((a_1,\cdots,a_k),(a_{k+1},\cdots,a_{k+r}))$

④ 设(m, a)=1, 则(m, ab) = (m, b)

证明:由(m , b)=(m , b*1)= (m , b*(m , a))= (m , (mb , ab))= ((m , mb) , ab)

=(m , ab)

⑤ 设(m, a)=1,若 m | ab, 则 m | b

只需要证明 m 是 m 与 b 的最大公因子即可.

m=(m, ab)=(m,b) (根据性质④)

⑥ $m[a_1,\cdots,a_n]=[ma_1,\cdots,ma_n]$

$a_1a_2=[a_1,a_2]$.（a_1, a_2）

证明:先证 $m[a_1,\cdots,a_n]=[ma_1,\cdots,ma_n]$.

设 $d1=[a_1,\cdots,a_n]$, $d2=[ma_1,\cdots ma_n]$

I. 由 $a_i \mid d1$, i=1, …, n 得: $ma_i \mid md1$, 即 md1 为 $ma_1,\cdots,ma_n$ 的一个公倍数,

则由 d2 的定义知: d2≤md1

II. 由 $ma_i \mid d2$, i=1, …, n 得: $a_i \mid \frac{d2}{m}$, 即 $\frac{d2}{m}$ 为 $a_1,\cdots,a_n$ 的一个公倍数,

则由 d1 的定义知: $\frac{d2}{m} \geq d1$, 即 $d2 \geq md1$

综上：md1=d2

再证:$a_1a_2=[a_1,a_2]$.（a_1, a_2）

记 $d=(a_1, a_2)$, 则由 $(\frac{a_1}{d}, \frac{a_2}{d})=1$ 得:$[\frac{a_1}{d}, \frac{a_2}{d}]=\frac{a_1}{d}\cdot\frac{a_2}{d}$

从而得:$a_1\cdot a_2=[\frac{a_1}{d}, \frac{a_2}{d}]\cdot d\cdot d=[a_1, a_2]\cdot d$

⑦ 若 $a \mid a_1a_2\cdots a_n$, 且 $(a,a_i)=1$, $i=1,\cdots,n-1$, 则 $a \mid a_n$ 。

证明: 只需要证明 a 是 a 与 a_n 的最大公因子即可.

由 $(a, a_1)=1$ 得: $(a, a_n)=(a, a_1a_n)=\cdots=(a, a_1a_2\cdots a_n)$(此处反复运用性质 4)

又由 $a \mid a_1a_2\cdots a_n$ 得: $(a, a_1a_2\cdots a_n)=$ a

所以 $(a, a_n)=$ a 从而 $a \mid a_n$

⑧ 若 $(a, b_i)=1,\quad i=1,\cdots,n$，则 $(a, b_1b_2\cdots b_n)=1$。

证明:因为 $(m, b_1)=(m, b_1b_2)=\cdots=(m, b_1b_2\cdots b_n)$(此处反复运用性质 4)

⑨ 若 p 为素数，且 $p\mid a_1a_2\cdots a_n$，则至少存在一个 a_k，使得 $p\mid a_k$。

反证法:假设对所有的 a_i,i=1,…,n 上述结论均不成立,则由 p 为素数得:

(p, a_i)=1, i=1,…,n,从而 $(p, a_1a_2\cdots a_n)=1$,(由性质 8 得到)

从而与 $p\mid a_1a_2\cdots a_n$ 矛盾.