第一章 整数的可除性
2015年03月10日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

1.3 最大公因数与广义欧几里得除法

思考题

1. 最大公因数$(a,\ b)$ 的数学表述是什么?
2. 如何判断两个整数$a,\ b$ 是否互素?
3. 如何计算两个整数$a,\ b$ 的最大公因数(a,b) ?
4. 如何估计计算最大公因数(a,b) 的时间$O((a,b))$?
5. 最大公因数有哪些性质?

   若$(a_1,c)=1,\ (a_2,c)=1$,, 则$(a_1\cdot a_2,c)=1$?
6. 如何构造互素的整数(a,b) ?
7. 如何得到贝祖等式, 即找到整数$s,\ t$ 使得$s\cdot a+t\cdot b=(a,b)$? 所需时间为多少?
8. 如何求一个整系数的可逆的2 阶矩阵$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a\cdot d-b\cdot c=1$

1.3.1 最大公因数

本节考虑多个整数的公共因数, 特别是它们的最大公因数以及最大公因数的计算.

定义1.3.1 设 $a_1, \ldots, a_n$ 是n $(n \geq 2)$ 个整数. 若整数 d 是它们中每一个数的因数, 那么 d 就叫做 $a_1, \ldots, a_n$ 的一个**公因数**.

如果整数$a_1, \ldots, a_n$ 不全为零, 那么整数$a_1, \ldots, a_n$ 的所有公因数中最大的一个公因数叫做**最大公因数**, 记作 $(a_1, \ldots, a_n)$. 特别地, 当$(a_1, \ldots, a_n) = 1$时, 我们称$a_1, \ldots, a_n$ **互素**或**互质**.

实际上, $d = (a_1, \ldots, a_n)$的数学表达式可叙述为:

(1) $d \mid a_1, \ldots, d \mid a_n$.

(2) 若$e \mid a_1, \ldots, e \mid a_n$, 则 $e \mid d$. (注意此处 e 为最大整数的表述)

我们将在定理7 中给予说明.

例1.3.1 两个整数14 和21 的公因数为$\{\pm 1, \pm 7\}$, 它们的最大公因数$(14, 21) = 7$.

例1.3.2 两个整数-15 和21 的公因数为$\{\pm 1,\ \pm 3\}$, 它们的最大公因数$(-15, 21) = 3$.

例1.3.3 三个整数$14,\ -15$ 和21 的公因数为$\{\pm 1\}$, 它们的最大公因数$(14, -15, 21) = 1$. 或者说, 三个整数$14,\ -15$ 和21 是互素的.

例1.3.4 设$a,\ b$ 是两个整数, 则 $(b,\ a) = (a,\ b)$.

例1.3.5 设$a,\ b$ 是两个正整数. 如果 $b \mid a$, 则$(a,\ b) = b$.

例1.3.6 设p 是一个素数, a 为整数. 如果 $p \nmid a$, 则 p 与a 互素.

证 设 $(a, p) = d$. 则有$d \mid p$ 及$d \mid a$.

因为p 是素数, 所以由$d \mid p$, 我们有 $d = 1$ 或 $d = p$.

对于 $d = p$, 由$d \mid a$, 我们有$p \mid a$, 这与假设$p \nmid a$ 矛盾.

因此, $d = 1$. 即$(a, p) = 1$. 结论成立.

定理1.3.1 设$a_1, \ldots, a_n$是n个不全为零的整数, 则

(i) $a_1, \ldots, a_n$与$|a_1|, \ldots, |a_n|$的公因数相同;

(ii) $(a_1, \ldots, a_n) = (|a_1|, \ldots, |a_n|)$.

证 (i) 设$d \mid a_i,\ 1 \le i \le n$, 由§1.1 例2, 有

$$d \mid |a_i|, \quad 1 \le i \le n.$$

故$a_1, \ldots, a_n$的公因数也是$|a_1|, \ldots, |a_n|$的公因数.

反之, 设$d \mid |a_i|,\ 1 \le i \le n$, 同样有$d \mid a_i,\ 1 \le i \le n$.

故$|a_1|, \ldots, |a_n|$的公因数也是$a_1, \ldots, a_n$的公因数.

(ii) 由(i)立得(ii).

例1.3.7 设$a,\ b$是整数. 则 $(a,\ b) = (a,\ -b) = (-a,\ b) = (|a|,\ |b|)$.

例1.3.8 我们有

1) $(-14, 21) = (14, -21) = (-14, -21) = (14, 21) = 7$.

2) $(-15, 21) = (15, -21) = (-15, -21) = (15, 21) = 3$.

定理1.3.2 设b 是任一正整数, 则$(0, b) = b$.

证 因为非零整数都是0 的因数, 而整数b 的最大因数为b, 所以$(0, b) = b$.

例1.3.9 1) $(0, 21) = 21$. 2) $(-15, 0) = 15$. 3) $(0, b) = |b|$.

定理1.3.3 设 $a,\ b,\ c$ 是三个不全为零的整数. 如果

$$a = q \cdot b + c, \tag{1}$$

其中q 是整数, 则$(a, b) = (b, c)$.

证 设$d = (a, b),\ d' = (b, c)$, 则$d \mid a,\ d \mid b$. 由§1.1 定理3,

$$d \mid a + (-q)b = c,$$

因而, d 是$b,\ c$ 的公因数. 从而, $d \le d'$.

同理, d' 是$a,\ b$ 的公因数, $d' \le d$. 因此, $d = d'$. 于是, 定理3成立.

注 需特别关注条件(1)的表述.

例1.3.10 因为$1859 = 1 \cdot 1573 + 286$, 所以$(1859, 1573) = (1573, 286)$.

例1.3.11 因为$1573 = 5 \cdot 286 + 143$, 所以$(1573, 286) = (286, 143) = 143$.

如何求最大公因数

怎样才能具体计算出两个整数$a,\ b$的最大公因数?

直接应用最大公因数的定义, 就需要知道整数的因数分解式, 这在$a,\ b$不是很大数时是可行的, 见§1.5 定理4.

但当$a,\ b$是很大数时, 整数分解本身就是很困难的事.

为此, 我们先给出一种算法"广义欧几里得除法或辗转相除法", 然后运用它求$a,\ b$的最大公因数.

1.3.2 广义欧几里得除法

***广义欧几里得除法** 设 $a,\ b$ 是任意两个正整数.

记 $r_{-2}=a,\ r_{-1}=b$. 反复运用欧几里得除法, 我们有

$$
\begin{aligned}
r_{-2} &= q_0\cdot r_{-1} + r_0, && 0\le r_0 < r_{-1},\\
r_{-1} &= q_1\cdot r_0 + r_1, && 0\le r_1 < r_0,\\
r_0 &= q_2\cdot r_1 + r_2, && 0\le r_2 < r_1,\\
&\cdots\cdots && \\
r_{n-3} &= q_{n-1}\cdot r_{n-2} + r_{n-1}, && 0\le r_{n-1} < r_{n-2},\\
r_{n-2} &= q_n\cdot r_{n-1} + r_n, && 0\le r_n < r_{n-1},\\
r_{n-1} &= q_{n+1}\cdot r_n + r_{n+1}, && r_{n+1}=0.
\end{aligned}
\tag{2}
$$

经过有限步骤, 必然存在n 使得$r_{n+1}=0$, 这是因为

$$0=r_{n+1}<r_n<\ldots<r_1<r_0<r_{-1}=b,$$

且b是有限正整数.

性质1.3.1 设a, b 是任意两个正整数. 则对于广义欧几里得除法(2),及$r_n \neq 0$, 有

$$b \geq \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \tag{3}$$

进而, $n \leq 5\log b$.

证 运用数学归纳法,可证明

$$r_{n-j} \geq F_j = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{j} - \left(\frac{1-\sqrt{5}}{2}\right)^{j}\right) \quad 0 \leq j \leq n+1. \tag{4}$$

对于$j = 0$, 有$r_n \geq 1 > 0 = F_0$,结论(4)成立.

又对于$j = 1$, 有$r_{n-1} \geq r_n + 1 > 1 = F_1$,结论(4)成立.

假设$j \leq k < n+1$ 时, 结论(4)成立.

对于$j = k+1$, 有

$$r_{n-(k+1)} \geq r_{n-k} + r_{n-(k-1)} \geq F_k + F_{k-1} = F_{k+1}.$$

由数学归纳法原理,对于$0 \leq j \leq n+1$, 结论(4)成立. 故命题成立. 证毕

1.3.2 广义欧几里得除法

定理1.3.4 设$a,\ b$是任意两个正整数, 则 $(a,b)=r_{n-1}$,
其中r_n 是广义欧几里得除法(1)中最后一个非零余数. 并且, 当$a>b$ 时, 计算(a,b) 的时间为$O(\log a\log^2 b)$.

证 根据广义欧几里得除法(2), 定理1.3.3, 以及定理1.3.2, 我们有

$$
\begin{aligned}
r_{-2} &= q_0\cdot r_{-1} + r_0, && (a,b)=(r_{-2},r_{-1})=(r_{-1},r_0),\\
r_{-1} &= q_1\cdot r_0 + r_1, && (r_{-1},r_0)=(r_0,r_1),\\
r_0 &= q_2\cdot r_1 + r_2, && (r_0,r_1)=(r_1,r_2),\\
&\cdots\cdots && \\
r_{n-3} &= q_{n-1}\cdot r_{n-2} + r_{n-1}, && (r_{n-3},r_{n-2})=(r_{n-2},r_{n-1}),\\
r_{n-2} &= q_n\cdot r_{n-1} + r_n, && (r_{n-2},r_{n-1})=(r_{n-1},r_n),\\
r_{n-1} &= q_{n+1}\cdot r_n + r_{n+1}, && (r_{n-1},r_n)=(r_n,r_{n+1})=(r_n,0)=r_n.
\end{aligned}
$$

因此, 由性质1.3.1 , 计算(a,b) 的时间$((a,b))$为

$$O(\log r_{-2}\log r_{-1}+\cdots+\log r_{n-1}\log r_n)=O(n\log a\log b)=O(\log a\log^2 b)$$

定理1.3.4 成立. 证毕

计算最大公因数

因为求两个整数的最大公因数在信息安全的实践中起着重要的作用, 所以我们将求两个整数的最大公因数之过程详述如下:

首先, 根据定理1, 将求两个整数的最大公因数转化为求两个非负整数的最大公因数;

其次, 运用欧几里得除法, 并根据定理3, 我们可以将求两个正整数的最大公因数转化为求两个较小非负整数的最大公因数;

反复运用欧几里得除法, 即广义欧几里得除法来, 将求两个正整数的最大公因数转化为求0 和一个正整数的最大公因数;

最后, 根据定理2, 求出两个整数的最大公因数.

例1.3.12 设$a=-1859,\ b=1573$, 计算(a,b).

解 由定理1, $(-1859,1573)=(1859,1573)$. 运用广义欧几里得除法,

$$1859=1\cdot 1573+286,\quad 1573=5\cdot 286+143,\quad 286=2\cdot 143.$$

根据定理4, $(-1859,1573)=143$.

例1.3.14 设$a = 46480,\ b = 39423$, 计算(a, b).

解 利用广义欧几里得除法, 方法一: 最小非负余数.

$$
\begin{aligned}
46480 &= 1\cdot 39423 + 7057 \\
39423 &= 5\cdot 7057 + 4138 \\
7057 &= 1\cdot 4138 + 2919 \\
4138 &= 1\cdot 2919 + 1219 \\
2919 &= 2\cdot 1219 + 481
\end{aligned}
\qquad
\begin{aligned}
1219 &= 2\cdot 481 + 257 \\
481 &= 1\cdot 257 + 224 \\
257 &= 1\cdot 224 + 33 \\
224 &= 6\cdot 33 + 26 \\
33 &= 1\cdot 26 + 7
\end{aligned}
\qquad
\begin{aligned}
26 &= 3\cdot 7 + 5 \\
7 &= 1\cdot 5 + 2 \\
5 &= 2\cdot 2 + 1 \\
2 &= 2\cdot 1.
\end{aligned}
$$

方法二: 绝对值最小余数.

$$
\begin{aligned}
46480 &= 1\cdot 39423 + 7057 \\
39423 &= 6\cdot 7057 + (-2919) \\
7057 &= 2\cdot 2919 + 1219 \\
2919 &= 2\cdot 1219 + 481 \\
1219 &= 3\cdot 481 + (-224)
\end{aligned}
\qquad
\begin{aligned}
481 &= 2\cdot 224 + 33 \\
224 &= 7\cdot 33 + (-7) \\
33 &= 5\cdot 7 + (-2) \\
7 &= 3\cdot 2 + 1 \\
2 &= 2\cdot 1.
\end{aligned}
$$

所以, $(46480,\ 39423) = 1$.

1.3.3 Bézout 等式: $s \cdot a + t \cdot b = (a, b)$

从广义欧几里得除法的演示中, 我们观察到

$$\begin{aligned}
r_n &= (-q_n) \cdot r_{n-1} + r_{n-2}, \\
r_{n-1} &= (-q_{n-1}) \cdot r_{n-2} + r_{n-3}, \\
r_{n-2} &= (-q_{n-2}) \cdot r_{n-3} + r_{n-4}, \\
&\cdots\cdots \\
r_2 &= (-q_2) \cdot r_1 + r_0, \\
r_1 &= (-q_1) \cdot r_0 + r_{-1}, \\
r_0 &= (-q_0) \cdot r_{-1} + r_{-2}.
\end{aligned}$$

这样, 逐次消去$r_{n-1},\ r_{n-2},\ \ldots, r_2,\ r_1,\ r_0$, 可找到整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = (a, b).$$

定理1.3.5 (Bézout) 设$a,\ b$ 是任意两个正整数, 则存在整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = (a, b). \tag{5}$$

(5) 叫做Bézout (贝祖)等式.

例1.3.15 设$a=-1859,\ b=1573$, 求$s,\ t$, 使$s\cdot a+t\cdot b=(a,b)$.

解 由例12, 我们有

$$\begin{aligned} 143 &= (-5)\cdot 286 + 1573 \\ &= (-5)\cdot(1859-1\cdot 1573) + 1573 \\ &= 5\cdot(-1859) + 6\cdot 1573. \end{aligned}$$

因此, 整数$s=5,\ t=6$ 满足$s\cdot a+t\cdot b=(a,b)$.

例1.3.16 设$a=169,\ b=121$, 求整数$s,\ t$, 使得

$$s\cdot a+t\cdot b=(a,b).$$

解 由例1.3.13 , 我们有

$$\begin{aligned}
1 &= (-11)\cdot 2 + 23\\
&= (-11)\cdot((-1)\cdot 23+25) + 23\\
&= 12\cdot((-1)\cdot 25+48) + (-11)\cdot 25\\
&= (-23)\cdot((-2)\cdot 48+121) + 12\cdot 48\\
&= 58\cdot((-1)\cdot 121+169) + (-23)\cdot 121\\
&= 58\cdot 169 + (-81)\cdot 121.
\end{aligned}$$

因此, 整数$s=58,\ t=-81$ 满足$s\cdot a+t\cdot b=(a,b)$.

例1.3.17 设$a = 46480,\ b = 39423$, 求整数$s,\ t$, 使得$s \cdot a + t \cdot b = (a, b)$.

解 由例14, 我们有方法一: 最小非负余数.

$$
\begin{aligned}
1 &= (-2) \cdot 2 + 5 \\
&= (-2) \cdot (7 - 1 \cdot 5) + 5 \\
&= 3 \cdot (26 - 3 \cdot 7) + (-2) \cdot 7 \\
&= (-11) \cdot (33 - 1 \cdot 26) + 3 \cdot 26 \\
&= 14 \cdot (224 - 6 \cdot 33) + (-11) \cdot 33 \\
&= (-95) \cdot (257 - 1 \cdot 224) + 14 \cdot 224 \\
&= 109 \cdot (481 - 1 \cdot 257) + (-95) \cdot 257 \\
&= (-204) \cdot (1219 - 2 \cdot 481) + 109 \cdot 481 \\
&= 517 \cdot (2919 - 2 \cdot 1219) + (-204) \cdot 1219 \\
&= (-1238) \cdot (4138 - 1 \cdot 2919) + 517 \cdot 2919 \\
&= 1755 \cdot (7057 - 1 \cdot 4138) + (-1238) \cdot 4138 \\
&= (-2993) \cdot (39423 - 5 \cdot 7057) + 1755 \cdot 7057 \\
&= 16720 \cdot (46480 - 1 \cdot 39423) + (-2993) \cdot 39423 \\
&= (-19713) \cdot 39423 + 16720 \cdot 46480 \\
&= (46480 - 19713) \cdot 39423 + (16720 - 39423) \cdot 46480 \\
&= (-22703) \cdot 46480 + 26767 \cdot 39423.
\end{aligned}
$$

方法二: 绝对值最小余数.

$$
\begin{aligned}
1 &= (-3)\cdot 2 + 7 \\
&= (-3)\cdot(-33+5\cdot 7) + 7 \\
&= (-14)\cdot(-224+7\cdot 33) + 3\cdot 33 \\
&= (-95)\cdot(481-2\cdot 224) + 14\cdot 224 \\
&= 204\cdot(-1219+3\cdot 481) + (-95)\cdot 481 \\
&= 517\cdot(2919-2\cdot 1219) + (-204)\cdot 1219 \\
&= (-1238)\cdot(7057-2\cdot 2919) + 517\cdot 2919 \\
&= 2993\cdot(-39423+6\cdot 7057) + (-1238)\cdot 7057 \\
&= 16720\cdot(46480-1\cdot 39423) + (-2993)\cdot 39423 \\
&= 16720\cdot 46480 + (-19713)\cdot 39423 \\
&= (16720-39423)\cdot 46480 + (46480-19713)\cdot 39423 \\
&= (-22703)\cdot 46480 + 26767\cdot 39423.
\end{aligned}
$$

因此, 整数$s=-22703,\ t=26767$ 满足$s\cdot a+t\cdot b=(a,b)$.

求s,t使得$s\cdot a+t\cdot b=(a,b)$的矩阵表达式

将前面的关系式用矩阵表示, 有

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} \qquad \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-3} \\ r_{n-2} \end{pmatrix} \qquad \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix}$$

$$\begin{pmatrix} r_{n-3} \\ r_{n-2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-2} \end{pmatrix} \begin{pmatrix} r_{n-4} \\ r_{n-3} \end{pmatrix} \qquad \begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix}$$

因此,

$$\begin{pmatrix} r_j \\ r_{j+1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}}_{A_j} \begin{pmatrix} r_{-2} \\ r_{-1} \end{pmatrix}$$

令$A_{-2}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}s_{-2}&t_{-2}\\u_{-2}&v_{-2}\end{pmatrix}$, 及对于$j\geq 0$,

$$A_j=\begin{pmatrix}0&1\\1&-q_{j+1}\end{pmatrix}\begin{pmatrix}0&1\\1&-q_j\end{pmatrix}\cdots\begin{pmatrix}0&1\\1&-q_1\end{pmatrix}\begin{pmatrix}0&1\\1&-q_0\end{pmatrix}=\begin{pmatrix}s_j&t_j\\u_j&v_j\end{pmatrix}.$$

我们有 $\begin{pmatrix}r_j\\r_{j+1}\end{pmatrix}=A_j\begin{pmatrix}r_{-2}\\r_{-1}\end{pmatrix}, \qquad -2\leq j\leq n.$

定理1.3.6 在上述符号下, 我们有

$$\begin{cases} s_{-2}=1 \\ s_{-1}=0 \end{cases}, \quad \begin{cases} t_{-2}=0 \\ t_{-1}=1 \end{cases}, \quad \begin{cases} s_j=u_{j-1} \\ t_j=v_{j-1} \end{cases}, \quad -1\le j\le n,$$

以及

$$\begin{pmatrix} s_j \\ s_{j-1} \end{pmatrix}=\begin{pmatrix} -q_j & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} s_{j-1} \\ s_{j-2} \end{pmatrix} \quad \text{和} \quad \begin{pmatrix} t_j \\ t_{j-1} \end{pmatrix}=\begin{pmatrix} -q_j & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} t_{j-1} \\ t_{j-2} \end{pmatrix}.$$

证 由A_j 的定义, 有

$$\begin{pmatrix} s_j & t_j \\ u_j & v_j \end{pmatrix}=\begin{pmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{pmatrix}\begin{pmatrix} s_{j-1} & t_{j-1} \\ u_{j-1} & v_{j-1} \end{pmatrix}=\begin{pmatrix} u_{j-1} & v_{j-1} \\ (-q_{j+1})u_{j-1}+s_{j-1} & (-q_{j+1})v_{j-1}+t_{j-1} \end{pmatrix}$$

推得 $\begin{cases} s_j=u_{j-1} \\ t_j=v_{j-1} \end{cases}$ 和 $\begin{cases} u_j=(-q_{j+1})u_{j-1}+s_{j-1} \\ v_j=(-q_{j+1})v_{j-1}+t_{j-1} \end{cases}$

进而, $\begin{cases} s_j=(-q_j)s_{j-1}+s_{j-2} \\ t_j=(-q_j)t_{j-1}+t_{j-2} \end{cases}$ 和 $\begin{cases} u_j=(-q_{j+1})u_{j-1}+u_{j-2} \\ v_j=(-q_{j+1})v_{j-1}+v_{j-2} \end{cases}$

用矩阵表示即为所求. 证毕

$j=n$ 时, 就是如下的定理.

1.3.4 Bézout 等式之证明

定理1.3.7 设$a,\ b$ 是正整数, 则

$$s_n \cdot a + t_n \cdot b = (a, b) \tag{6}$$

对于$j = 0,\ 1,\ 2,\ \ldots,\ n$ 这里$s_j,\ t_j$ 归纳地定义为

$$s_{-2} = 1,\ s_{-1} = 0; \quad t_{-2} = 0,\ t_{-1} = 1,$$

$$\begin{cases} s_j = (-q_j)s_{j-1} + s_{j-2}, \\ \qquad\qquad\qquad\qquad j = 0, 1, ..., n-1, n \\ t_j = (-q_j)t_{j-1} + t_{j-2}, \end{cases} \tag{7}$$

其中$q_j = \left[\dfrac{r_{j-2}}{r_{j-1}}\right]$ 是(2) 式中的不完全商.

证 只需证明: 对于$j = -2,\ -1,\ 0,\ \ldots, n-1, n$

$$s_j \cdot a + t_j \cdot b = r_j, \tag{8}$$

其中$r_j = (-q_j)r_{j-1} + r_{j-2}$ 是(2) 式中的余数.
因为$(a, b) = r_n$, 所以

$$s_n \cdot a + t_n \cdot b = (a, b).$$

对j 作数学归纳法来证明(8) .
$j = -2$ 时,有$s_{-2} = 1,\ t_{-2} = 0$, 以及

$$s_{-2} \cdot a + t_{-2} \cdot b = a = r_{-2}.$$

结论对于$j = -2$ 成立.
$j = -1$ 时, 有$s_{-1} = 0,\ t_{-1} = 1$, 以及

$$s_{-1} \cdot a + t_{-1} \cdot b = b = r_{-1}.$$

结论对于$j = -1$ 成立.

假设结论对于$-2 \le j \le k-1 \le n-1$ 成立. 即

$$s_j \cdot a + t_j \cdot b = r_j.$$

对于$j = k$, 我们有

$$r_k = (-q_k) r_{k-1} + r_{k-2}.$$

利用归纳假设, 我们得到

$$\begin{aligned} r_k &= (-q_k)(s_{k-1}a + t_{k-1}b) + (s_{k-2}a + t_{k-2}b) \\ &= ((-q_k)s_{k-1} + s_{k-2})a + ((-q_k)t_{k-1} + t_{k-2})b \\ &= s_k \cdot a + t_k \cdot b. \end{aligned}$$

因此, 结论对于$j = k$ 成立. 根据数学归纳法原理, (8) 对所有的j 成立. 这就完成了证明.

具体计算$s,\ t$ 使得 $s\cdot a+t\cdot b=(a,b).$

首先, 令$r_{-2}=a,\ r_{-1}=b,$

$s_{-2}=1,\ s_{-1}=0,\quad t_{-2}=0,\ t_{-1}=1.$

(1) 如果$r_{-1}=0$, 则令$s=s_{-2},\quad t=t_{-2}$. 否则, 计算

$$q_0=\left[\frac{r_{-2}}{r_{-1}}\right],\quad r_0=(-q_0)r_{-1}+r_{-2}.$$

(2) 如果$r_0=0$, 则令$s=s_{-1},\quad t=t_{-1}$. 否则,

计算$s_0=(-q_0)s_{-1}+s_{-2},\quad t_0=(-q_0)t_{-1}+t_{-2},$

以及 $q_1=\left[\frac{r_{-1}}{r_0}\right],\quad r_1=(-q_1)r_0+r_{-1}.$

(3) 如果$r_1=0$, 则令$s=s_0,\quad t=t_0$. 否则,

计算$s_1=(-q_1)s_0+s_{-1},\quad t_1=(-q_1)t_0+t_{-1},$

以及 $q_2=\left[\frac{r_0}{r_1}\right],\quad r_2=(-q_2)r_1+r_0.\quad \ldots\ldots$

(j+2) 若$r_j = 0,\ (j \geq 2)$, 则令

$$s = s_{j-1}, \quad t = t_{j-1}.$$

否则, 计算

$$s_j = (-q_j)s_{j-1} + s_{j-2}, \quad t_j = (-q_j)t_{j-1} + t_{j-2},$$

以及

$$q_{j+1} = \left[\frac{r_{j-1}}{r_j}\right], \quad r_{j+1} = (-q_{j+1})r_j + r_{j-1}.$$

最后, 一定有$r_{n+1} = 0$. 这时, 令

$$s = s_n, \quad t = t_n.$$

总之, 我们可以找到整数$s,\ t$, 使得

$$sa + tb = r_n = (a, b).$$

列表计算$s,\ t$ 使得$s\cdot a+t\cdot b=(a,b)$.

上述过程可以列成如下表格:

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				a
-2	1	0		b
-1	0	1	q_0	r_0
0	s_0	t_0	q_1	r_1
1	s_1	t_1	q_2	r_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-2$	s_{n-2}	t_{n-2}	q_{n-1}	r_{n-1}
$n-1$	s_{n-1}	t_{n-1}	q_n	r_n
n	s_n	t_n	q_{n+1}	$r_{n+1}=0$

(9)

其中,
$$\begin{cases} s_j = (-q_j)s_{j-1}+s_{j-2}, & t_j = (-q_j)t_{j-1}+t_{j-2}, \\ q_{j+1} = \left[\dfrac{r_{j-1}}{r_j}\right], & r_{j+1} = (-q_{j+1})r_j+r_{j-1}. \end{cases}$$

上述过程简述为:

j	s_j	t_j	q_{j+1}	r_{j+1}
$j-2$	s_{j-2}	t_{j-2}	q_{j-1}	r_{j-1}
$j-1$	s_{j-1}	t_{j-1}	q_j	r_j
j	s_j	t_j	q_{j+1}	r_{j+1}

计算过程: $s_j \to t_j \to q_{j+1} \to r_{j+1}$.

其中,
$$\begin{cases} s_j = (-q_j)s_{j-1} + s_{j-2}, \\ t_j = (-q_j)t_{j-1} + t_{j-2}, \\ q_{j+1} = \left[\dfrac{r_{j-1}}{r_j}\right], \\ r_{j+1} = (-q_{j+1})r_j + r_{j-1}. \end{cases}$$

例1.3.18 设$a = 1859,\ b = 1573$. 计算整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = (a, b).$$

解 根据表格(5) 及公式(6), 我们有

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				1859
-2	1	0		1573
-1	0	1	1	286
0	1	-1	5	143
1	-5	6	2	0

因此, $s = -5,\ t = 6$ 使得

$$(-5) \cdot 1859 + 6 \cdot 1573 = 143.$$

例1.3.19 设$a = 737,\ b = 635$. 计算整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = (a, b).$$

解 根据表格(5) 及公式(6), 我们有:

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				737
-2	1	0		635
-1	0	1	1	102
0	1	-1	6	23

j	s_j	t_j	q_{j+1}	r_{j+1}
1	-6	7	4	10
2	25	-29	2	3
3	-56	65	3	1
4	193	-224	3	0

因此, $s = 193,\ t = -224$ 使得

$$193 \cdot 737 + (-224) \cdot 635 = 1.$$

例1.3.20 设$a = 46480,\ b = 39423$, 计算整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = (a, b).$$

解 根据表格(5) 及公式(6), 我们有

j	s_j	t_j	q_{j+1}	r_{j+1}	j	s_j	t_j	q_{j+1}	r_{j+1}
-3				46480	5	-67	79	1	224
-2	1	0		39423	6	95	-112	1	33
-1	0	1	1	7057	7	-162	191	6	26
0	1	-1	5	4138	8	1067	-1258	1	7
1	-5	6	1	2919	9	-1229	1449	3	5
2	6	-7	1	1219	10	4754	-5605	1	2
3	-11	13	2	481	11	-5983	7054	2	1
4	28	-33	2	257	12	16720	-19713	2	0

因此, $s = 16720,\ t = -19713$ 使得

$$16720 \cdot 46480 + (-19713) \cdot 39423 = 1.$$

定理1.3.7的逆命题不成立. 但我们有

定理1.3.8 整数$a,\ b$ 互素的充分必要条件是存在整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = 1.$$

证 根据定理1.3.7, 我们立即得到命题的必要性.

反过来, 设$d = (a, b)$, 则有$d \mid a,\ d \mid b$. 现在若存在整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = 1.$$

则我们有

$$d \mid s \cdot a + t \cdot b = 1.$$

因此, $d = 1$. 即整数$a,\ b$ 互素.

例1.3.21 设四个整数$a,\ b,\ c,\ d$满足关系式:

$$a \cdot d - b \cdot c = 1.$$

则$(a,b) = 1,\ (a,c) = 1,\ (d,b) = 1,\ (d,c) = 1.$

例1.3.21 与整系数2 阶可逆矩阵的构造相关:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \det A = a \cdot d - b \cdot c$$

1.3.5 最大公因数进一步的性质

定理1.3.9 设$a,\ b$ 是任意两个不全为零的整数, d 是正整数. 则d 是整数$a,\ b$ 的最大公因数的充要条件是: (数学表述)

(i) $d \mid a,\ d \mid b$;

(ii) 若$e \mid a,\ e \mid b$, 则$e \mid d$.

证 若d 是整数$a,\ b$ 的最大公因数, 则显然有(i) 成立;

再由定理5, 存在整数$s,\ t$ 使得

$$s \cdot a + t \cdot b = d.$$

因此, 当$e \mid a,\ e \mid b$ 时, 有

$$e \mid s \cdot a + t \cdot b = d.$$

故(ii) 成立.

反过来, 假设(i) 和(ii) 成立, 那么

(i) 说明d 是整数$a,\ b$ 的公因数;

(ii) 说明d 是整数$a,\ b$ 的公因数中的最大数, 因为$e \mid d$时, 有$|e| \leq d$.

因此, d 是整数$a,\ b$ 的最大公因数.

定理1.3.10 设$a,\ b$ 是任意两个不全为零的整数,

(i) 若m 是任一正整数, 则$(a\cdot m, b\cdot m) = (a,b)m.$

(ii) 若非零整数d 满足$d \mid a,\ d \mid b$, 则$(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{|d|}.$

特别地, $*\ (\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1.$ (互素整数的构造)

证 设$d = (a,b),\ d' = (a\cdot m, b\cdot m)$. 由广义欧几里得除法(定理1.3.7),

存在整数$s,\ t$ 使得 $s\cdot a + t\cdot b = d.$

两端同乘m, 得到 $s(a\cdot m) + t(b\cdot m) = d\cdot m.$ 因此$d' \mid d\cdot m.$

又显然有$d\cdot m \mid a\cdot m,\ d\cdot m \mid b\cdot m$. 根据定理7 (ii), 有$d\cdot m \mid d'.$

故$d' = d\cdot m$. 即(i) 成立.

再根据(i), 当$d \mid a,\ d \mid b$时, 有

$$(a,\ b) = (\frac{a}{|d|}\cdot|d|,\ \frac{b}{|d|}\cdot|d|) = (\frac{a}{|d|},\ \frac{b}{|d|})|d| = (\frac{a}{d},\ \frac{b}{d})|d|.$$

因此, $(\frac{a}{d},\ \frac{b}{d}) = \frac{(a,b)}{|d|}.$

特别地, 取$d = (a,\ b)$, 有$(\frac{a}{(a,b)},\ \frac{b}{(a,b)}) = 1.$ 故(ii) 成立.

例1.3.22 设$a = 11 \cdot 200306,\ b = 23 \cdot 200306$. 计算$(a,\ b)$.

解 因为$(11,\ 23) = (11,\ 23 - 11 \cdot 2) = (11, 1) = 1$, 所以

$$(a,\ b) = (11 \cdot 200306,\ 23 \cdot 200306) = 200306.$$

最大公因数的运算性质

定理1.3.11 设$a,\ b,\ c$是三个整数, 且$b \neq 0,\ c \neq 0$. 如果$(a, c) = 1$, 则

$$(a \cdot b, c) = (b, c).$$

证 令$d = (a \cdot b, c),\ d' = (b, c)$. 有$d' \mid b,\ d' \mid c$. 进而$d' \mid a \cdot b,\ d' \mid c$. 再根据定理1.3.9, 得到$d' \mid d$.

反过来, 因为$(a, c) = 1$, 根据广义欧几里得除法, 存在整数$s,\ t$ 使得

$$s \cdot a + t \cdot c = 1.$$

两端同乘b, 得到

$$s \cdot (a \cdot b) + (t \cdot b) \cdot c = b.$$

再由$d \mid a \cdot b,\ d \mid c$, 我们得到$d \mid s \cdot (a \cdot b) + (t \cdot b) \cdot c$, 即$d \mid b$.

同样根据定理1.3.9, 我们得到$d \mid d'$.

故$d = d'$. 定理成立. 证毕

最大公因数的运算性质

定理1.3.12 设$a_1,\ \ldots,\ a_n,\ c$ 为整数. 如果$(a_i, c) = 1,\ 1 \le i \le n$. 则

$$(a_1 \cdots a_n,\ c) = 1.$$

证 我们对n 作数学归纳法. $n = 2$ 时, 命题就是定理1.3.11.

也可直接证明. 设$(a_1, c) = 1,\ (a_2, c) = 1$, 则存在整数$s_1,\ t_1$ 和$s_2,\ t_2$ 使得 $\quad s_1 \cdot a_1 + t_1 \cdot c = 1, \qquad s_2 \cdot a_2 + t_2 \cdot c = 1.$

进而,$(s_1 s_2) \cdot (a_1 a_2) = (1 - t_1 \cdot c)(1 - t_2 \cdot c) = 1 - (t_1 + t_2 - t_1 t_2 c) \cdot c,$

或 $\quad (s_1 s_2) \cdot (a_1 a_2) + (t_1 + t_2 - t_1 t_2 c) \cdot c = 1$

因此, $(a_1 \cdot a_2,\ c) = 1.$

假设$n - 1$ 时, 命题成立. 即 $\quad (a_1 \cdots a_{n-1},\ c) = 1.$

对于n, 根据归纳假设, 有$(a_1 \cdots a_{n-1},\ c) = 1$. 再根据$(a_n, c) = 1$ 及定理1.3.11, 得到$(a_1 \cdots a_{n-1} a_n,\ c) = ((a_1 \cdots a_{n-1}) a_n,\ c) = 1.$

因此, 命题对所有的n 成立. 证毕

最大公因数在可逆变换下的不变性

最后, 我们给出最大公因数在可逆变换下的不变性.

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & r \\ s & t \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}, \qquad q \cdot t - r \cdot s = 1.$$

定理1.3.13 设$a,\ b$ 和$u,\ v$ 都是不全为零的整数. 如果

$$a = q \cdot u + r \cdot v, \quad b = s \cdot u + t \cdot v,$$

其中$q,\ r,\ s,\ t$ 是整数, 且$q \cdot t - r \cdot s = 1$, 则$(a, b) = (u, v)$.

证 设$d = (a, b),\ d' = (u, v)$, 则$d' \mid u,\ d' \mid v$. 由§1.1 定理1.1.3, 可得到

$$d' \mid q \cdot u + r \cdot v = a, \quad d' \mid s \cdot u + t \cdot v = b.$$

因而, $d' \mid d$.

又由假设可解得$u = t \cdot a + (-s) \cdot b,\ v = (-r) \cdot a + q \cdot b$. 同理可得到$d \mid d'$.

因此, $d = d'$. 定理成立. 证毕

1.3.6 多个整数的最大公因数及计算

对于n 个整数$a_1, \ldots, a_n$的最大公因数, 我们可以用递归的方法, 将求它们的最大公因数转化为一系列求两个整数的最大公因数. 具体过程如下:

定理1.3.14 设$a_1, a_2, \ldots, a_n$ 是n 个整数, 且$a_1 \neq 0$. 令

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \quad \ldots, \quad (d_{n-1}, a_n) = d_n.$$

则$(a_1, a_2, \ldots, a_n) = d_n$, 且存在整数$s_1, s_2, \ldots, s_n$ 使得

$$s_1 \cdot a_1 + s_2 \cdot a_2 + \cdots + s_n \cdot a_n = d_n$$

证 对n 作数学归纳法. $n = 2$ 时, 有$(a_1, a_2) = d_2$, 且存在整数s_1, s_2 使得$s_1 \cdot a_1 + s_2 \cdot a_2 = d_2$, 结论成立.

假设$n - 1$ 时, 结论成立. 即当$(a_1, a_2) = d_2$, $(d_2, a_3) = d_3$, $\ldots$, $(d_{n-2}, a_{n-1}) = d_{n-1}$ 时, 有$(a_1, a_2, \ldots, a_{n-1}) = d_{n-1}$, 且存在整数$s_1, s_2, \ldots, s_{n-1}$ 使得

$$s_1 \cdot a_1 + s_2 \cdot a_2 + \cdots + s_{n-1} \cdot a_{n-1} = d_{n-1}.$$

对于n ,令$e=(a_1,a_2,\ldots,a_n)$, 有

$$e \mid a_1,\ e \mid a_1,\ \ldots,\ e \mid a_{n-1},\ e \mid a_n.$$

根据归纳假设: $(a_1,a_2,\ldots,a_{n-1})=d_{n-1}$, 有$e \mid d_{n-1}$. 再由广义欧几里得除法, 存在整数$s,\ t$ 使得

$$s\cdot d_{n-1}+t\cdot a_n=d_n.$$

得到$e \mid d_n$ 和$e \le d_n$, 以及

$$(s\cdot s_1)\cdot a_1+(s\cdot s_2)\cdot a_2+\cdots+(s\cdot s_{n-1})\cdot a_{n-1}+t\cdot a_n=d_n.$$

另一方面, 由$(d_{n-1},a_n)=d_n$, 得到$d_n \mid d_{n-1}$ 以及$d_n \mid a_n$. 进而,

$$d_n \mid a_1,\ d_n \mid a_2,\ \ldots,\ d_n \mid a_{n-1},\ d_n \mid a_n$$

因此, $d_n \le e$. 故$e=d_n$, 结论成立. 证毕

例1.3.23 计算最大公因数$(120, 150, 210, 35)$.

解 因为

$$(120, 150) = (120, 30) = 30,$$
$$(30, 210) = 30,$$
$$(30, 35) = (30, 5) = 5,$$

所以最大公因数$(120, 150, 210, 35) = 5$.

定理1.3.15 设$a_1, \ldots, a_n$是任意n个不全为零的整数, d是正整数. 则d是整数$a_1, \ldots, a_n$的最大公因数的充要条件是: (数学定义)

i) $d \mid a_1, \ldots, d \mid a_n$;

ii) 若$e \mid a_1, \ldots, e \mid a_n$, 则$e \mid d$.

证 必要性. 若d是整数$a_1, \ldots, a_n$的最大公因数, 则显然有i) 成立. 再由定理1.3.14, 存在整数$s_1, \ldots, s_n$使得

$$s_1 \cdot a_1 + s_2 \cdot a_2 + \cdots + s_n \cdot a_n = d$$

因此, 当$e \mid a_1, \ldots, e \mid a_n$有 $e \mid s_1 \cdot a_1 + s_2 \cdot a_2 + \cdots + s_n \cdot a_n = d$. 故ii) 成立.

反过来, 假设i) 和ii) 成立, 那么

i) 说明d是整数$a_1, \ldots, a_n$的公因数;

ii) 说明d是整数$a_1, \ldots, a_n$的公因数中的最大数, 因为$e \mid d$时, 有$|e| \leq d$.

因此, d是整数$a_1, \ldots, a_n$的最大公因数. 证毕

形为2^a-1的整数及其最大公因数

引理1.3.1 设$a,\ b$是两个正整数. 则2^a-1被2^b-1除的最小正余数是2^r-1, 其中r是a模b的最小正余数.

证 当$a<b$时, $r=a$, 结论显然成立. 当$a\geq b$. 对$a,\ b$用欧几里得除法, 存在不完全商q及最小正余数r使得

$$a=q\cdot b+r,\quad 1\leq r\leq b,$$

进而,

$$2^a-1=2^r((2^b)^q-1)+2^r-1=(2^b-1)q_1+2^r-1,$$

其中$q_1=2^r((2^b)^{(q-1)}+\cdots+1)$为整数, 结论也成立.

引理1.3.2 设$a,\ b$是两个正整数. 则2^a-1和2^b-1的最大公因数是$2^{(a,b)}-1$.

证 运用广义欧几里得除法及引理1.3.1立即得到结论.

定理1.3.16 设$a,\ b$ 是两个正整数. 则正整数2^a-1 和2^b-1 互素的充要条件是a 和b 互素.

证 因为

$$(2^a-1, 2^b-1) = 2^{(a,b)}-1,$$

而$2^{(a,b)}-1=1$ 的充要条件是$(a,b)=1$. 因此, 定理成立. 证毕