信息安全数学基础

第一章 整除

熊虎
电子科技大学

第一章 整数

1.2 整数中的算法

辗转相除法（欧几里得算法）

该算法是用来求解给定整数 a和b 的最大公因数

设a,b是两个整数，$b\neq 0$，依次做带余数除法

$$a = bq_1 + r_1, 0 < r_1 < |b|$$

$$b = r_1 q_2 + r_2, 0 < r_2 < r_1$$

$$\vdots$$

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, 0 < r_{k+1} < r_k$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1}, r_{n+1} = 0$$

经过有限步运算，必然存在n使得 $r_{n+1}=0$，这是因为

$$0 \leq r_{n+1} < r_n < \cdots < r_1 < |b|$$

1.2 整数中的算法

定理1.2.1 设 a,b 是两个整数，不妨设 $a>b$ ，则 $\gcd(a,b)=r_n$，其中 r_n 是上述辗转相除法中得到的最后一个非零余数。

证明： 根据最大公因数的性质（5），有

$$
\begin{aligned}
\gcd(a,b) &= \gcd(b,r_1) \\
&= \gcd(r_1,r_2) \\
&\;\;\vdots \\
&= \gcd(r_{n-1},r_n) \\
&= r_n
\end{aligned}
$$

1.2 整数中的算法

例1.2.1　计算 $\gcd(4864, 3458)$。

$$
\begin{aligned}
4864 &= 1 \times 3458 + 1406, & q_1 &= 1, r_1 = 1406 \\
3458 &= 2 \times 1406 + 646, & q_2 &= 2, r_2 = 646 \\
1406 &= 2 \times 646 + 114, & q_3 &= 2, r_3 = 114 \\
646 &= 5 \times 114 + 76, & q_4 &= 5, r_4 = 76 \\
114 &= 1 \times 76 + 38, & q_5 &= 1, r_5 = 38 \\
76 &= 2 \times 38, & q_6 &= 2
\end{aligned}
$$

所以 $\gcd(4864, 3458) = r_5 = 38$ 。

1.2 整数中的算法

注意：当 a, b 中有负整数时，可根据最大公因数的性质（1）可将其中的负整数转变为正整数来求其最大公因数。

例1.2.2 用辗转相除法求 $\gcd(-123, 17)$。

解： $\gcd(-123, 17) = \gcd(123, 17)$

做辗转相除法：

$$
\begin{aligned}
123 &= 7 \times 17 + 4, \quad q_1 = 7, r_1 = 4, \\
17 &= 4 \times 4 + 1, \quad q_2 = 4, r_2 = 1, \\
4 &= 4 \times 1, \quad q_3 = 4
\end{aligned}
$$

因此， $\gcd(123, 17) = r_2 = 1$

1.2 整数中的算法

定理1.2.2 对于任意两个整数 a,b，存在整数 x,y 使得

$$\gcd(a,b) = xa + yb$$

证明 根据辗转相除法，有

$$r_1 = a - bq_1, r_2 = b - r_1q_2 = -q_2a + (1 + q_1q_2)b$$

一般地，对于任意的 r_i，都存在两个整数 x_i, y_i，使

$$r_i = x_ia + y_ib$$

x_i, y_i 可利用如下递推公式得到：

$$\begin{aligned} r_i &= r_{i-2} - q_ir_{i-1} \\ &= (x_{i-2}a + y_{i-2}b) - q_i(x_{i-1}a + y_{i-1}b) \\ &= (x_{i-2} - q_ix_{i-1})a + (y_{i-2} - q_iy_{i-1})b \end{aligned}$$

可见 $x_i = x_{i-2} - q_ix_{i-1}, y_i = y_{i-2} - q_iy_{i-1}, i = 1,2,3,\cdots$

1.2 整数中的算法

由式（1.2）可知

$$x_{-1}=1, x_0=0,$$

$$y_{-1}=0, y_0=1$$

利用这几个初值及递推关系式（1.3），就可依次计算出

$$(x_1,y_1)(x_2,y_2),\cdots,(x_n,y_n)$$

最后得到

$$\gcd(a,b)=r_n=x_na+y_nb$$

令 $x=x_n, y=y_n$，定理得证。

1.2 整数中的算法

例 求整数 x,y使得，$\gcd(17,26)=17x+26y$。

$$
\begin{aligned}
26 &= 17\times 1+9\\
17 &= 9\times 1+8\\
9 &= 8\times 1+1\\
8 &= 1\times 8
\end{aligned}
$$

$$
\begin{aligned}
1 &= 9-8\times 1\\
&= 9-(17-9\times 1)\\
&= 9\times 2-17\\
&= (26-17\times 1)\times 2-17\\
&= 26\times 2-17\times 3
\end{aligned}
$$

1.2 整数中的算法

例1.2.3 求整数 x, y ，使 $\gcd(4864, 3458) = 4864x + 3458y$ 。

解：回顾例1.2.1 中

$$
\begin{aligned}
4864 &= 1 \times 3458 + 1406, & q_1 &= 1, r_1 = 1406 \\
3458 &= 2 \times 1406 + 646, & q_2 &= 2, r_2 = 646 \\
1406 &= 2 \times 646 + 114, & q_3 &= 2, r_3 = 114 \\
646 &= 5 \times 114 + 76, & q_4 &= 5, r_4 = 76 \\
114 &= 1 \times 76 + 38, & q_5 &= 1, r_5 = 38 \\
76 &= 2 \times 38, & q_6 &= 2
\end{aligned}
$$

$$\gcd(4864, 3458) = r_5 = 38$$

根据例1.2.1，有

1.2 整数中的算法

$$
\begin{aligned}
1406 &= 4864 - 1 \times 3458 \\
646 &= 3458 - 2 \times 1406 \\
&= 3458 - 2 \times (4864 - 1 \times 3458) \\
&= 3 \times 3458 - 2 \times 4864 \\
114 &= 1406 - 2 \times 646 \\
&= 4864 - 1 \times 3458 - 2 \times (3 \times 3458 - 2 \times 4864) \\
&= 5 \times 4864 - 7 \times 3458 \\
76 &= 646 - 5 \times 114 \\
&= 3 \times 3458 - 2 \times 4864 - 5 \times (5 \times 4864 - 7 \times 3458) \\
&= 38 \times 3458 - 27 \times 4864 \\
38 &= 114 - 76 \\
&= 5 \times 4864 - 7 \times 3458 - (38 \times 3458 - 27 \times 4864) \\
&= 32 \times 4864 - 45 \times 3458
\end{aligned}
$$

1.2 整数中的算法

即：

$$
\begin{aligned}
38 &= 114 - 76 \\
&= 114 - (646 - 5 \times 114) \\
&= -646 + 6 \times (1406 - 2 \times 646) \\
&= 6 \times 1406 - 13 \times (3458 - 2 \times 1406) \\
&= -13 \times 3458 + 32 \times (4864 - 3458) \\
&= 32 \times 4864 - 45 \times 3458
\end{aligned}
$$

因此整数 $x = 32, y = -45$ 满足 $gcd(4864, 3458) = 4864x + 3458y$。

1.2 整数中的算法

定理1.2.3 设 a,b 是两个不全为0的整数，则 $\gcd(a,b)=1$ 当且仅当存在整数 u,v 使得

$$ua+vb=1$$

证明 必要性式定理 1.2.1 的特例。下证充分性。
如果存在整数 u,v，使得 $ua+vb=1$
则根据整除的性质有 $\gcd(a,b)|ua+vb$，即有 $\gcd(a,b)|1$，因此有 $\gcd(a,b)=1$ 。

推论1.2.1 设 a,b,c 为不等于0的整数，
（1）若 $c|ab, \gcd(a,c)=1$，则 $c|b$ ；

证明：因为 $\gcd(a,c)=1$ ，根据定理1.2.3存在整数 u,v，使得

$$ua+vc=1$$

两边同时乘以 b 可得 $uab+vcb=b$
由于 $c|uab+vcb$，因此 $c|b$ 。

1.2 整数中的算法

（2） 若 $a|c, b|c$ 且 $\gcd(a,b)=1$ ， 则 $ab|c$ ；

证明： 由 $\gcd(a,b)=1$可知存在整数u,v使得

$$ua+vb=1$$

两边同时乘以c ， 可得 $uac+vbc=c$

由于$a|c, b|c$ ， 所以 $ab|uac, ab|vbc$ 。因此有$ab|c$ 。

（3） 若 $\gcd(a,c)=1, \gcd(b,c)=1$ ， 则 $\gcd(ab,c)=1$ 。

证明： 根据定理1.2.3 ， 存在整数s,t 使得 $sa+tc=1$ 。

同理， 存在整数u,v， 使得 $ub+vc=1$ 于是有

$$(sa+tc)(ub+vc)=(su)ab+(sva+tub+tvc)c=1$$

根据定理1.2.3有 $\gcd(ab,c)=1$ 。

1.2 整数中的算法

推论1.2.2 设 a, b 是两个正整数，

（1）若a, b互素，则$lcm[a, b] = ab$

证明： 显然 ab 是 a, b 的公倍数。
设m为 a, b 的任意公倍数即 $a|m, b|m$ 。存在整数 k 使得 $m = ak$ 。由$b|m$，可知 $b|ak$，又 a, b 互素，由推论1.2.1可知 $b|k$。因此存在整数 t 使得 $k = bt$ ，所以 $m = abt$ 。故 $ab|m$。由此可知 ab 是 a, b 的公倍数中的最小正整数，即 $lcm[a, b] = ab$ 。

（2）$lcm[a, b] = \dfrac{ab}{\gcd(a, b)}$

证明： 显然 $a\left|\dfrac{ab}{\gcd(a,b)}\right.$，$b\left|\dfrac{ab}{\gcd(a,b)}\right.$，所以$\dfrac{ab}{\gcd(a,b)}$是$a,b$ 的公倍数。

设 $a=k_a\gcd(a,b), b=k_b\gcd(a,b)$,由定理1.1.3 可知$\gcd(k_a,k_b)=1$

设m 为 a,b 的任意公倍数即$a|m, b|m$。存在整数 q_a,q_b

使得$m=q_a a=q_b b$，于是 $m=q_a k_a\gcd(a,b)=q_b k_b\gcd(a,b)$

因此有$q_a k_a=q_b k_b$。由于 $\gcd(k_a,k_b)=1$，于是有

$$k_a|q_b \Rightarrow k_a b|q_b b \Rightarrow \frac{\gcd(a,b)k_a b}{\gcd(a,b)}\left|q_b b \Rightarrow \frac{ab}{\gcd(a,b)}\right|m$$

这表明 $\dfrac{ab}{\gcd(a,b)}$ 是a,b 的最小公倍数。

谢谢！