信息安全数学基础

第一章 整除

熊虎
电子科技大学

第一章 整除

1.1 整除概念和基本性质

1.2 整数中的算法

1.3 素数、算数基本定理

1.1 整除概念和基本性质

定义 1.1.1（整除） a, b 是任意两个整数，$a \neq 0$，如果存在整数q ,使$b = aq$，称a整除b或b被a整除,记为 $a|b$ 。且称a为b的因数，b为a的倍数，否则a不能整除b或b不能被a整除,记$a \nmid b$ 。

0是任何整数的倍数。对于任意整数$a, \pm 1, \pm a$都是它的因数，称这四个因数为整数a的显然因数或平凡因数，整数a的其他因数称为非显然因数或非平凡因数。

1.1 整除概念和基本性质

例 1.1.1

（1） $28 = 4 \times 7$，因此 $4|28, 7|28$，4和7为28的因数，28为4和7的倍数。

（2）$-3|18$，因为 $18 = (-3) \times (-6)$。

（3）$173|0$，因为 $0 = 173 \times 0$。

1.1 整除概念和基本性质

定理1.1.1 （整除的性质）

对于任意 $a, b, c \in Z$ ，有：

(1)如果 $a|b$ 且 $b|c$ ，则有 $a|c$ 。

证明： $a|b$ 且 $b|c$，则存在整数 q_1 , q_2 ，使得 $b = aq_1, c = bq_2$，因此有 $c = aq_1q_2$，所以 $a|c$ 。

(2) $a|b$ 且 $a|c$ ，当且仅当对于任意 $x, y \in Z$ ，有 $a|bx + cy$ 。

证明： 必要性：$a|b$ 且 $a|c$ ，则存在整数 q_1 , q_2 ，使得 $b = aq_1, c = aq_2$。因此有 $bx + cy = a(q_1x + q_2y)$ ，所以 $a|bx + cy$ 。

充分性：分别取 $x = 1, y = 0$ 和 $x = 0, y = 1$，即可得 $a|b$ 且 $a|c$。

(3)设 $m \neq 0, a|b$ 当且仅当 $ma|mb$。

证明： 当 $m \neq 0$ 时，$b = aq \Leftrightarrow mb = (ma)q$ 。

(4)如果 $a|b$ 且 $b|a$，则 $a = \pm b$ 。

证明： $a|b$ 且 $b|a$，则存在整数 q_1, q_2，使得 $b = aq_1, a = bq_2$，因此有$a = a(q_1 q_2)$。又因为$a \neq 0$，所以$q_1 q_2 = 1$。由于q_1，q_2是整数，所以$q_1 = \pm 1$。故而$b = \pm a$。

定理1.1.2 （带余除法） 设 a, b 是两个给定的整数，$a \neq 0$，那么一定存在唯一的一对整数 q 和 r，满足

$$b = aq + r, 0 \leq r < |a|$$

因此，$a|b$ 的充要条件是 $r = 0$ 。

1.1 整除概念和基本性质

证明： 存在性。当 $a|b$ 时，取 $q=\frac{b}{a}, r=0$ 。当 $a\nmid b$ 时，考虑集合

$$T=\{b-ka, k=0,\pm 1,\pm 2,\cdots\}$$

容易看出，集合 T 中必有正整数，取 T' 为 T 的正整数子集。由于正整数集合的任一非空子集均有最小正整数。因此，T' 中必然存在一个最小正整数，设为

$$t_0=b-k_0a>0$$

下证 $t_0<|a|$ 。因为 $a\nmid b$，所 以 $t_0\neq|a|$ 。若 $t_0>|a|$ ，则有 $t_1=t_0-|a|\in T$ 且 $0<t_1<t_0$ 。这与 t_0 的极小性矛盾。因此有 $t_0<|a|$。取 $q=k_0, r=t_0$ 就满足要求。

1.1 整除概念和基本性质

定义1.1.2（公因数）设 a_1, a_2, d 是三个整数，若 $d|a_1, d|a_2$，则称 d 是整数 a_1, a_2 的公因数。一般地，设 $a_1, a_2, \cdots, a_k$ 是 k 个整数，若 $d|a_1, d|a_2, \cdots, d|a_k$，称 d 是整数 $a_1, a_2, \cdots, a_k$ 的公因数。

定义1.1.3（最大公因数）设 a_1, a_2 是两个不全为零的整数，把 a_1, a_2 的公因数中最大的一个称为整数 a_1, a_2 的最大公因数，记为 $\gcd(a_1, a_2)$。当 $\gcd(a_1, a_2) = 1$，称 a_1, a_2 互素。一般地，设 $a_1, a_2, \cdots, a_k$ 是 k 个不全为零的整数，把 $a_1, a_2, \cdots, a_k$ 的公因数中最大的整数称为 $a_1, a_2, \cdots, a_k$ 的最大公因数，记为 $\gcd(a_1, a_2, \cdots, a_k)$。当 $\gcd(a_1, a_2, \cdots, a_k) = 1$，称 $a_1, a_2, \cdots, a_k$ 互素。

例1.1.2

（1）12与18的公因数有 $\{\pm1,\pm2,\pm3,\pm6\}$，所以 $\gcd(12,18)=6$。

（2）-15与21的公因数有 $\{\pm1,\pm3\}$，所以 $\gcd(-15,21)=3$。

（3）25与12的公因数有 ±1，所以 $\gcd(25,12)=1$，

因此25与12互素。

1.1 整除概念和基本性质

定理1.1.3（最大公因数的性质）

对任意整数 a, b, c 有

（1）有 $\gcd(a,b)=\gcd(b,a)=\gcd(-a,b)=\gcd(a,-b)$

证明： 显然。

（2）若$a|b$ ，则 $\gcd(a,b)=a$ 。

证明： 显然。

（3）对于任意两个整数 a, b ，必有$\gcd(a,b)|ax+by$ ；

证明： 根据定理1.1.1整除的性质（2）易得出。

1.1 整除概念和基本性质

（4）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： 设 Z 是全体整数集合。做一个如下集合：

$S=\{|xa+yb||x,y\in Z\}$ 。S 中的元素显然大于等于0。

设 d 为 S 中的最小正整数，则 d 可表示为 a,b 的组合，设

$$d=ua+vb$$

现在我们证明 $d|a$ 且 $d|b$ 。

做带余除法：

$$a=qd+r,0\le r<d$$

于是

$$r=a-qd=a-q(ua+vb)=(1-qu)a-qvb$$

1.1 整除概念和基本性质

这说明 r 也可表示为 a,b 的组合，则 $r\in S$。由于 d 是 S 中的最小正整数，所以只有 $r=0$ 。故 $d|a$ 。同理 $d|b$ 。

设 c 是 a,b 的任意公因子，由 $c|a$ 和 $c|b$ 得 $c|d=ua+vb$ 。故 d 是 a,b 的最大公因子，证毕。

（5）若 $a=bq+c$ ，q 是一个整数，则有 $\gcd(a,b)=\gcd(b,c)$

证明： 很显然， $\gcd(a,b)|(a-bq)=c$ ，所以 $\gcd(a,b)|\gcd(b,c)$

反之，根据最大公因数的定义及整除的定义，$\gcd(b,c)|b$ ，

$\gcd(b,c)|c$,因而 $\gcd(b,c)|bq+c=a$ 。

所以，$\gcd(b,c)|\gcd(a,b)$ 。因此，$\gcd(a,b)=\gcd(b,c)$。

（6）若 $\gcd(a,c)=1$ ，$b|c$ ，则 $\gcd(a,b)=1$

证明： 设 $\gcd(a,b)=d$ ，则由 $d|b, b|c$ ，可得 $d|c$ ，又 $d|a$

所以$d|\gcd(a,c)$。由 $\gcd(a,c)=1$，可得 $d=1$ 即 $\gcd(a,b)=1$。

1.1 整除概念和基本性质

（7） $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$

证明： 设 $\gcd(a,b)=d$ ， $\gcd(\frac{a}{d}, \frac{b}{d}) = d'$ ，由 $d'|\frac{a}{d}, d'|\frac{b}{d}$ ，可得 $dd'|a, dd'|b$ ，根据最大公因数的性质可知 $dd'|d$ ，由此可得 $d'=1$ ，结论得证。

1.1 整除概念和基本性质

定义1.1.4（公倍数）设a_1,a_2,l是三个整数，若 $a_1|l,a_2|l$ ，则称 l 是整数 a_1,a_2的公倍数。一般地，设 $a_1,a_2,\cdots,a_k$ 是 k 个整数，若 $a_1|l,a_2|l,\cdots,a_k|l$ ，称 l 是整数$a_1,a_2,\cdots,a_k$ 的公倍数。

定义1.1.5（最小公倍数）设 a_1,a_2 是两个不全为零的整数，把 a_1,a_2 的所有公倍数中的最小正整数称为整数 a_1,a_2 的最小公倍数，记为 $lcm[a_1,a_2]$。一般地，设 $a_1,a_2,\cdots,a_k$是 k 个不全为零的整数，把$a_1,a_2,\cdots,a_k$的所有公倍数中的最小正整数称为整数 $a_1,a_2,\cdots,a_k$ 的最小公倍数，记为 $lcm[a_1,a_2,\cdots,a_k]$ 。

等价地，$lcm[a_1,a_2]$ 是能够被 a_1,a_2 同时整除的最小正整数。

1.1 整除概念和基本性质

定理1.1.4 设 a,b,m 是整数，$a|m, b|m$ ，则 $lcm[a,b]|m$ 。

证明： 不妨设 $m = qlcm[a,b]+r$ ，其中 q 是整数，$0 \le r < lcm[a,b]$ ，则 $r = m - qlcm[a,b]$ ，又 $a|m, b|m, a|lcm[a,b], b|lcm[a,b]$，由整除的性质可知 $a|r, b|r$ ，由 $lcm[a,b]$ 的最小性可知 $r=0$ 。因此有 $lcm[a,b]|m$。

谢谢！