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

1.4 整除的进一步性质及最小公倍数

思考题

1. 设$a,\ b,\ c \neq 0$ 是三个整数. 若$c \mid a \cdot b$, 则一定有$c \mid a$ 或$c \mid b$ 吗?
2. 设p 是素数. 若$p \mid a \cdot b$, 则一定有$p \mid a$ 或$p \mid b$ 吗?
3. 设$a,\ b,\ c$ 是三个非零整数. 若$a \mid c,\ b \mid c$, 则一定有$a \cdot b \mid c$?
4. 最小公倍数$[a,\ b]$ 的数学表述是什么?
5. 最大公因数$(a,\ b)$ 与最小公倍数$[a,\ b]$ 的关系是什么?
6. 如何计算最小公倍数$[a,\ b]$?

1.4 整除的进一步性质及最小公倍数

1.4.1 整除的进一步性质

我们先讨论整除的性质.

定理1.4.1 设$a,\ b,\ c$是三个整数, 且$c \neq 0$. 如果$c \mid a\,b,\ (a, c) = 1$, 则$c \mid b$.

证一 根据假设条件和定理1.3.11, 我们有

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

从而$c \mid b$.

证二 (直接证明) 因为$(a, c) = 1$. 根据定理1.3.8 ,存在整数s, t 使得

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

两端同乘b, 得到 $s \cdot (a\,b) + (t\,b) \cdot c = b.$

根据定理1.1.3, 由$c \mid a\,b,\ c \mid c$, 我们得到

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

即$c \mid b$. 证毕

例1.4.1 因为$15 \mid 2 \cdot 75$, 又$(2, 15) = 1$, 所以$15 \mid 75$.

访问主页
标题页
目录页
第 3 页 共 12 页
返回
全屏显示
关闭
退出

我们再讨论素因数的性质.

定理1.4.2 设p 是素数. 若$p \mid a\,b$, 则$p \mid a$ 或$p \mid b$.

证一 若$p \nmid a$, 则根据例1.3.6, 有$(a, p) = 1$. 再根据定理**??**, 有$p \mid b$.

证二 (直接证明) 若$p \nmid a$, 则根据例1.3.6, 有$(a, p) = 1$. 再根据定理1.4.1 ,存在整数s, t 使得

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

两端同乘b, 得到

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

根据定理1.1.3, 由$p \mid a\,b,\ p \mid p$, 我们得到

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

即$p \mid b$. 证毕

例1.4.2 因为$5 \mid 3 \cdot 25$, 又$5 \nmid 3$ 及5 为素数, 所以$5 \mid 25$.

定理1.4.3 设$a_1,\ \ldots,\ a_n$ 是n 个整数, p 是素数. 若$p \mid a_1 \cdots a_n$, 则p 一定整除某一个$a_k,\ \ 1 \le k \le n$.

证 若$a_1,\ \ldots,\ a_n$ 都不能被p整除, 则根据例1.3.6, 有

$$(a_i, p) = 1, \qquad 1 \le i \le n.$$

而由定理1.3.12,

$$(a_1 \cdots a_n, p) = 1,$$

这与$p \mid a_1 \cdots a_n$ 矛盾. 证毕

1.4.2 最小公倍数

下面讨论整数的最小公倍数.

定义1.4.1 设$a_1,\ \ldots,\ a_n$ 是n 个整数. 若D 是这n 个数的倍数, 则D 叫做这n 数的**一个公倍数**. $a_1,\ \ldots,\ a_n$ 的所有公倍数中的最小正整数叫做**最小公倍数**, 记作$[a_1, \ldots, a_n]$.

注1 $D > 0$ 是$a_1,\ \ldots,\ a_n$的最小公倍数的数学表达式可叙述为:

i) $a_i \mid D, \quad 1 \le i \le n$;

ii) 若$a_i \mid D', \quad 1 \le i \le n$, 则$D \mid D'$.

我们将在定理1.4.5 中给予说明.

注2 a, b 的最小公倍数$D = [a, b]$ 是集合

$$\{c \mid c \in \mathbf{Z},\ a \mid c,\ b \mid c\}$$

中的最小正整数.

注3 $a_1,\ \ldots,\ a_n$ 的最小公倍数D 是集合

$$\{c \mid c \in \mathbf{Z},\ a_i \mid c,\ \ 1 \le i \le n\}$$

中的最小正整数.

例1.4.3 14 和21 的公倍数为$\{\pm 42,\ \pm 84, \ldots\}$, 最小公倍数为$[14, 21] = 42$.

定理1.4.4 设a, b是两个互素正整数. 则

i) 若$a \mid D$, $b \mid D$, 则$a \cdot b \mid D$;

ii) $[a, b] = a \cdot b$.

证一 i) 设$b \mid D$, 则存在整数q, 使得$D = q \cdot b$. 又$a \mid D$, 即$a \mid q \cdot b$, 以及$(a, b) = 1$, 根据定理1.3.11 之推论, 得到$a \mid q$. 因此存在整数q', 使得$q = q' \cdot a$, 进而, $D = q' \cdot (a \cdot b)$. 故$a \cdot b \mid D$. i)得证.

ii) 显然$a \cdot b$ 是a, b 的公倍数. 又由i) 知, $a \cdot b$ 是a, b的公倍数中最小正整数, 故$[a, b] = a \cdot b$.

i) 之直接证明 由$a \mid D$, $b \mid D$, 知存在q_1, q_2 使得$D = q_1 \cdot a$, $D = q_2\, b$. 从而, $b \cdot D = q_1 \cdot (a \cdot b)$, $a \cdot D = q_2\, (a \cdot b)$. 因为$(a, b) = 1$, 所以由广义欧几里得除法, 可找到整数$s, t$, 使得$s \cdot a + t \cdot b = (a, b) = 1$, 进而

$$D = (s \cdot a + t \cdot b) D = s \cdot (a \cdot D) + t \cdot (b \cdot D) = s \cdot q_2 \cdot (a \cdot b) + t \cdot q_1 \cdot (a \cdot b) = (s \cdot q_2 + t \cdot q_1)(a \cdot b)$$

故$a \cdot b \mid D$. 证毕

例1.4.4 设p, q 是两个不同的素数. 则$[p, q] = p \cdot q$.

1.4.3 最小公倍数与最大公因数

定理1.4.5 设a, b是两个正整数. 则

i) 若$a \mid D$, $b \mid D$, 则$[a,b] \mid D$;

ii) $[a,b] = \dfrac{a \cdot b}{(a,b)}$.

证 令$d = (a,b)$. 根据定理1.3.10, 我们有

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

又根据定理1.4.4,

$$\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{a}{d} \cdot \frac{b}{d},$$

进而$[a,b] = \dfrac{a \cdot b}{d}$, 即ii)成立.

再由

$$\frac{a}{d} \mid \frac{D}{d}, \qquad \frac{b}{d} \mid \frac{D}{d},$$

得到

$$\frac{a}{d} \cdot \frac{b}{d} \mid \frac{D}{d}.$$

从而$\dfrac{a \cdot b}{d} \mid D$, 即i)成立. 证毕

1.4.4 多个整数的最小公倍数

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

定理1.4.6 设$a_1,\ \ldots,\ a_n$ 是n 个整数. 令

$$[a_1, a_2] = D_2,\ [D_2, a_3] = D_3,\ \ldots,\ [D_{n-1}, a_n] = D_n.$$

则$[a_1, \ldots, a_n] = D_n$.

证 对n 作数学归纳法. $n = 2$ 时, 有$[a_1, a_2] = D_2$, 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$[a_1, a_2, \ldots, a_{n-1}] = D_{n-1}$.

对于n ,令$D = [a_1, a_2, \ldots, a_n]$, 有$a_1 \mid D,\ a_2 \mid D,\ \ldots,\ a_{n-1} \mid D,\ a_n \mid D$. 根据归纳假设: $[a_1, a_2, \ldots, a_{n-1}] = D_{n-1}$ 以及定理1.4.5, 有$D_{n-1} \mid D$ 以及$D_n = [D_{n-1}, a_n] \mid D$. 进而, $D_n \le D$.

另一方面, 由$[D_{n-1}, a_n] = D_n$, 得到$D_{n-1} \mid D_n$ 以及$a_n \mid D_n$. 进而,

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

即D_n 是$a_1,\ \ldots,\ a_n$ 的公倍数. 从而, $D \le D_n$. 故$D_n = D$, 结论成立. 证毕

例1.4.5 计算最小公倍数$[120,150,210,35]$.

解 因为

$$[120,150]=\frac{120\cdot 150}{(120,150)}=\frac{120\cdot 150}{30}=600,$$

$$[600,210]=\frac{600\cdot 210}{(600,210)}=\frac{600\cdot 210}{30}=4200,$$

$$[4200,35]=\frac{4200\cdot 35}{(4200,35)}=\frac{4200\cdot 35}{35}=4200.$$

所以最大公因数$[120,150,210,35]=4200$.

定理1.4.7 设$a_1,\ a_2,\ \dots,\ a_n$ 是正整数. 如果$a_1 \mid D,\ a_2 \mid D,\ \dots,\ a_n \mid D$, 则

$$[a_1, a_2, \dots, a_n] \mid D.$$

证 对n 作数学归纳法.
$n = 2$ 时命题就是定理1.4.5 i).
假设$n-1$ $(n \geq 3)$ 时, 命题成立. 即

$$D_{n-1} = [a_1, a_2, \dots, a_{n-1}] \mid D.$$

对于n, 根据归纳假设和定理1.4.5, 有$D_{n-1} \mid D$ 以及$[D_{n-1}, a_n] \mid D$. 再根据定理1.4.6, $[D_{n-1}, a_n] = [a_1, a_2, \dots, a_n]$ 得到

$$[a_1, a_2, \dots, a_n] \mid D.$$

因此, 命题对所有的n 成立. 证毕