第一章　预备知识

1　代数起源于解方程

2　线性方程组初步

3　集合

4　映射

5　等价关系和序关系

6　置换

6.1　置换的定义和乘法

6.2　循环分解

定理 6.12 设 $\sigma \in S_n \setminus \{e\}$. 则 σ 是有限个两两互不相交的长度大于 1 的循环之积.

证明. 对 n 归纳. 当 $n = 2$ 时, $\sigma = (12)$, 其本身是一个循环. 定理成立. 设 $n > 2$ 且定理对 S_m 中的置换都成立, 其中 $2 \leq m \leq n - 1$.

不妨设 $\sigma \in S_n$ 且 $\sigma(1) \neq 1$. 因为 $\sigma^{\mathrm{ord}(\sigma)} = e$, 所以存在最小的正整数 k 使得 $\sigma^k(1) = 1$ 且 $k > 1$. 则 $\{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$ 一定两两不同. 否则, 存在 $i, j \in \mathbb{N}$ 满足 $0 \leq i < j < k$ 使得 $\sigma^i(1) = \sigma^j(1)$. 于是, $\sigma^{j-i}(1) = 1$. 但我们有 $0 < j - i < k$, 矛盾.

不妨设 $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\ldots \sigma^{k-1}(1) = k$. 令 $\tau = (1, 2, \ldots, k) \in S_n$. 则 σ 和 τ 限制在 $\{1, 2, \ldots, k\}$ 上相同.
情形 1. 设 $\sigma = \tau$, 则 σ 是一个循环. 定理成立.
情形 2. 设 $\sigma \neq \tau$. 则 $k < n$.

$$\lambda = \sigma|_{\{k+1,\ldots,n\}}$$

是 $\{k+1, \ldots, n\}$ 上的一个非恒同置换. 根据归纳假设, $\lambda = \lambda_1 \cdots \lambda_\ell$ 是若干互不相交的循环之积. 设

$$\begin{aligned} \mu_i : \{1, 2, \ldots, n\} &\longrightarrow \{1, 2, \ldots, n\} \\ j &\mapsto \begin{cases} j, & j \in \{1, \ldots, k\} \\ \lambda_i(j), & j \in \{k+1, \ldots, n\} \end{cases} . \end{aligned}$$

则 $\mu_1, \ldots, \mu_\ell$ 是 S_ℓ 的循环. 则 $\sigma = \tau\mu_1 \cdots \mu_\ell$ 且 $\tau, \mu_1, \ldots, \mu_\ell$ 两两不相交. □

例 6.13 把

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 4 & 5 & 7 & 6 & 1 & 8 \end{pmatrix}$$

写成互不相交的循环之积.

解. $\sigma = (198)(23)(67)$.

推论 6.14 设 $\sigma \in S_n \setminus \{e\}$ 是互不相交的循环 $\tau_1, \ldots, \tau_m$ 之积. 则

$$\mathrm{ord}(\sigma) = \mathrm{lcm}(\mathrm{ord}(\tau_1), \ldots, \mathrm{ord}(\tau_m)).$$

证明. 设 $\ell_i = \mathrm{ord}(\tau_i)$, $i = 1, 2, \ldots, m$, $\ell = \mathrm{lcm}(\ell_1, \ldots, \ell_m)$. 令

$$\ell = k_i \ell_i,$$

其中 $k_i \in \mathbb{Z}^+$, $i = 1, 2, \ldots, m$. 第三讲引理 6.11 蕴含

$$\sigma^\ell = \tau_1^\ell \cdots \tau_m^\ell = \tau_1^{\ell_1 k_1} \cdots \tau_m^{\ell_m k_m} = e.$$

设 $k = \mathrm{ord}(\sigma)$. 根据第三讲命题 6.6, $k|\ell$. 我们有

$$\sigma^k = \tau_1^k \cdots \tau_m^k = e.$$

不妨设 $\tau_1(1) \neq 1$. 因为 τ_1 与 $\tau_2, \ldots, \tau_m$ 都不相交, 所以 $\tau_2(1) = \cdots = \tau_m(1) = 1$. 于是, $\tau_1^k(1) = 1$. 故 $\tau_1^k = e$. 根据第三讲命题 6.6, 我们得到 $\ell_1|k$. 同理, $\ell_2|k$, …, $\ell_m|k$. 故 k 也是 $\ell_1, \ldots, \ell_k$ 的公倍数. 再根据 $k|\ell$ 可知, $k = \ell$. □

例 6.15 计算

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 6 & 10 & 8 & 2 & 9 & 1 & 7 \end{pmatrix}$$

的阶.

解. $\sigma = (134689)(25\underline{10}7) \Longrightarrow \mathrm{ord}(\sigma) = \mathrm{lcm}(6,4) = 12.$

例 6.16 设 σ 的循环分解是 $\tau_1 \cdots \tau_k$. 由映射的穿衣脱衣规则可知,

$$\sigma^{-1} = \tau_k^{-1} \cdots \tau_1^{-1}.$$

根据第三讲例 *6.8*, 置换的逆可以通过循环分解直接得到.

6.3 偶置换和奇置换

长度等于 2 的循环称为对换(transposition). 对换的逆就是其本身.

引理 6.17 任何一个循环都是若干个对换之积.

证明. 我们来证明

$$(i_1 i_2 \cdots i_k) = (i_k i_{k-1}) \cdots (i_k i_2)(i_k i_1),$$

其中 $k > 2$. 令 $\sigma = (i_k i_{k-1}) \cdots (i_k i_2)(i_k i_1)$.

设 $\ell \in \{1, 2, \ldots, k-2\}$. 则

$$\begin{aligned}
\sigma(i_\ell) &= \underbrace{(i_k i_{k-1}) \cdots (i_k i_{\ell+2})}\underbrace{(i_k i_{\ell+1})(i_k i_\ell)}[i_\ell] \\
&= \underbrace{(i_k i_{k-1}) \cdots (i_k i_{\ell+2})}[i_{\ell+1}] \\
&= i_{\ell+1}.
\end{aligned}$$

而

$$\sigma(i_{k-1}) = \underbrace{(i_k i_{k-1})}[i_{k-1}] = i_k.$$

最后

$$\sigma(i_k) = \underbrace{(i_k i_{k-1}) \cdots (i_k i_2)}\ \underbrace{(i_k i_1)}[i_k] = \underbrace{(i_k i_{k-1}) \cdots (i_k i_2)}[i_1] = i_1.\square$$

例 6.18 把

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}$$

写成对换之积.

解. 由循环分解和上述引理可知:

$$\sigma = (124)(56) = (42)(41)(56).$$

引理 6.19 设 $\sigma, \tau \in S_n$ 两个对换, $\sigma = (st)$ 且 $\sigma \neq \tau$. 则 S_n 中存在两个对换 σ' 和 τ' 满足

$$\sigma'(s) = s,\ \tau'(s) \neq s \text{ 且 } \tau\sigma = \tau'\sigma'.$$

证明. 设 $\tau = (uv)$.

情形 *1.* 如果 $\{s,t\} \cap \{u,v\} = \emptyset$, 则令 $\tau' = \sigma$ 和 $\sigma' = \tau$. 由第三讲引理 6.11 可知, $\tau\sigma = \tau'\sigma'$.

情形 *2.* 设 $\tau = (su)$. 则 $u \neq t$. 令 $\tau' = \sigma$ 和 $\sigma' = (tu)$.

$$\begin{cases} \tau\sigma(s) = (su)(st)[s] = (su)[t] = t, \\ \tau\sigma(t) = (su)(st)[t] = (su)[s] = u, \\ \tau\sigma(u) = (su)(st)[u] = (su)[u] = s \end{cases}$$

和

$$\begin{cases} \tau'\sigma'(s) = (st)(tu)[s] = (st)[s] = t, \\ \tau'\sigma'(t) = (st)(tu)[t] = (st)[u] = u, \\ \tau'\sigma'(u) = (st)(tu)[u] = (st)[t] = s. \end{cases}$$

情形 *3*. 设 $\tau = (tu)$. 则 $u \neq s$. 令 $\tau' = (su)$ 和 $\sigma' = \tau$. 可类似地验证 $\tau\sigma = \tau'\sigma'$.

引理 6.20 设 $\tau_1, \ldots, \tau_k \in S_n$ 是对换. 如果 $\tau_1 \cdots \tau_k = e$, 则 k 是偶数.

证明. 我们先证明下列断言:

断言. 设 $k > 2$. 则 e 可以写成 $k-2$ 个对换之积.

断言的证明. 如果 $\tau_{k-1} = \tau_k$, 则 $\tau_{k-1}\tau_k = e$. 我们有 $\tau_1 \cdots \tau_{k-2} = e$. 断言成立.

否则 $\tau_{k-1} \neq \tau_k$. 设 $s \in \{1, 2, \ldots, n\}$ 满足 $\tau_k(s) \neq s$. 根据引理 6.19, 存在对换 $\tau'_{k-1}, \tau'_k \in S_n$ 满足 $\tau'_k(s) = s$, $\tau'_{k-1}(s) \neq s$ 且 $\tau'_{k-1}\tau'_k = \tau_{k-1}\tau_k$. 于是

$$e = \tau_1 \cdots \tau_{k-2}\tau'_{k-1}\tau'_k.$$

特别地, 最右侧的对换不移动 s.

下面考虑 τ_{k-2}, τ'_{k-1}. 如果 $\tau_{k-2}\tau'_{k-1} = e$, 则 e 是 $k-2$ 个对换之积. 否则, 引理 6.19 蕴含存在对换 τ^*_{k-2} 和 τ^*_{k-1} 满足 $\tau^*_{k-1}(s) = s$, $\tau^*_{k-2}(s) \neq s$ 和 $\tau_{k-2}\tau'_{k-1} = \tau^*_{k-2}\tau^*_{k-1}$. 于是

$$e = \tau_1 \cdots \tau^*_{k-2}\tau^*_{k-1}\tau'_k.$$

特别地, 最右侧的两个对换都不移动 s.

以此类推, 我们要么证明 e 是 $k-2$ 个对换之积; 要么得出 $e=\lambda_1\lambda_2\cdots\lambda_k$, 其中 $\lambda_1,\ldots,\lambda_k\in S_n$ 是对换, 满足

$$\lambda_1(s)\neq s,\ \text{且}\ \lambda_2(s)=\cdots\lambda_k(s)=s.$$

但这意味着 $e(s)\neq s$. 矛盾. 断言成立.

反复利用断言可知, k 是偶数. □

定理 6.21 设 $\sigma\in S_n$.

(i) σ 是有限个对换之积.

(ii) 设 $\sigma=\lambda_1\cdots\lambda_k=\mu_1\cdots\mu_m$, 其中 $\lambda_1,\ldots\lambda_k,\mu_1,\ldots,\mu_m$ 都是对换. 则 k 和 m 的奇偶性相同.

证明. (i) 根据定理 6.12, σ 是若干循环之积. 由引理 6.17, 每个循环都是若干对换之积. 故 σ 是有限个对换之积.

(ii) 由穿衣脱衣规则可知, $e=\lambda_1\cdots\lambda_k\mu_m^{-1}\cdots\mu_1^{-1}$. 因为对换的逆是其本身, 所以引理 6.20 蕴含 $k+m$ 是偶数. 于是, k 和 m 的奇偶性相同. □

定义 6.22 设 $\sigma\in S_n$. 如果 σ 可以写成奇数个对换之积, 则称 σ 是奇置换. 否则称为 偶置换. 特别地, e 是偶置换. 奇置换的符号定义为 -1, 偶置换的符号为 1. 置换 σ 的符号记为 ε_σ.

上述定理说明置换的符号是良定义的.

引理 6.23 设 $\sigma, \tau \in S_n$. 则 $\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau$.

证明. 注意到两个同号置换之积是偶置换, 而两个异号置换之积是奇置换. □

注解 6.24 反复应用上述定理可知, 对 $\sigma_1, \ldots, \sigma_k \in S_n$,

$$\epsilon_{\sigma_1 \cdots \sigma_k} = \epsilon_{\sigma_1} \cdots \epsilon_{\sigma_k}.$$

记号. 所有 S_n 中偶置换的集合记为 A_n.

例 6.25 设 $\sigma \in S_n$ 和 $\tau \in A_n$. 则 $\sigma^{-1}\tau\sigma \in A_n$.
证明. 上述注解蕴含:

$$\varepsilon_{\sigma^{-1}\tau\sigma} = \varepsilon_{\sigma^{-1}}\varepsilon_\tau\varepsilon_\sigma = \varepsilon_{\sigma^{-1}}\varepsilon_\sigma = \varepsilon_{\sigma^{-1}\sigma} = \varepsilon_e = 1. \quad \square$$

推论 6.26 设 $\sigma \in S_n$ 且 $\sigma = \tau_1 \cdots \tau_k$, 其中 $\tau_1, \ldots, \tau_k$ 是两两互不相交的循环. 则σ 的奇偶性与整数

$$\sum_{i=1}^{k} (\mathrm{ord}(\tau_i) - 1)$$

相同. 即

$$\epsilon_\sigma = (-1)^{\sum_{i=1}^{k} (\mathrm{ord}(\tau_i)-1)}.$$

证明. 设$\tau=(i_1\dots i_m)$. 根据引理6.17, $\tau=(i_m i_{m-1})\cdots(i_m i_1)$. 于是, $\epsilon_\tau=(-1)^{m-1}$. 再根据第三讲引理6.9可知, $m=\mathrm{ord}(\tau)$. 故$\epsilon_\tau=(-1)^{\mathrm{ord}(\tau)-1}$. 由上述引理和注解可知

$$\epsilon_\sigma=(-1)^{\sum_{i=1}^{k}(\mathrm{ord}(\tau_i)-1)}. \quad \square$$

例 6.27 确定下列置换的阶数并判定其奇偶性:

$$\pi=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&8&6&10&7&4&5&9&2&1\end{pmatrix}.$$

解. 计算得$\pi=(13641\underline{0})(289)(57)$. 于是

$$\mathrm{ord}(\pi)=\mathrm{lcm}(5,3,2)=30.$$

进而

$$\epsilon_\pi=(-1)^{4+2+1}=-1.$$

故π是奇置换.

7 整数的算数

7.1 最大公因子和最小公倍数

以下引理是整除的一个基本性质.

引理 7.1 设$m,n,d\in\mathbb{Z}$且$d\neq 0$. 如果$d|m$且$d|n$, 则对于任意$u,v\in\mathbb{Z}$, $d|(um+vn)$.

证明. 设 $a, b \in \mathbb{Z}$ 使得 $m = ad$ 和 $n = bd$. 则

$$um + vn = uad + vbd = (ua + vb)d.$$

于是, $d|(um + vn)$. □

设 $m, n, c \in \mathbb{Z}^+$. 如果 $c|m$ 且 $c|n$, 则称 c 是 m, n 的公因子. 设 g 是 m, n 的公因子. 如果任何 m, n 的公因子都不大于 g, 则称 g 是 m, n 的最大公因子.

注意到 1 是 m, n 的公因子. 于是 m, n 的最大公因子必然存在且唯一, 并记为 $\gcd(m, n)$.

对于两个非零整数 m, n, 它们的最大公因子定义为 $\gcd(|m|, |n|)$. 如果 $n = 0$, 则它们的最大公因子定义为 $|m|$. 下面我们描述两个计算正整数的最大公因子算法–辗转相除（*Euclidean*）算法.

定理 7.2 设 $m, n \in \mathbb{Z}^+$. 则下列算法在有限步内输出正整数 g, 和整数 u, v 使得

(i) $g = \gcd(m, n)$;

(ii) $um + vn = g$.

扩展的辗转相除法(Extended Euclidean Algorithm)

输入: $m, n \in \mathbb{Z}^+$

输出: $g \in \mathbb{Z}^+$, $u, v \in \mathbb{Z}$ 使得 $g = \gcd(m, n)$ 和 $um + vn = g$.

1. *[初始化]* 令 $r_0 := m;\ r_1 := n;\ i = 1;\ u_0 := 1; v_0 := 0;$ $u_1 = 0; v_1 := 1;$

2. *[循环] while* $r_i \neq 0$ *do*

   (a) $i := i + 1;$

   (b) $q_i := \mathrm{quo}(r_{i-2}, r_{i-1});\ r_i := \mathrm{rem}(r_{i-2}, r_{i-1});$

   (c) $u_i := u_{i-2} - q_i u_{i-1};\ v_i := v_{i-2} - q_i v_{i-1};$

   end do;

3. *[准备返回]* $g := r_{i-1};\ u := u_{i-1};\ v := v_{i-1};$

4. *[返回] return* $g, u, v;$

证明. 首先验证该算法在有限步内必然终止. 注意到算法中的循环产生一个关于余数的严格递减序列

$$r_1 > r_2 > \cdots .$$

因为余数都非负, 所以该余数序列有限步必然终止. 此时最后一项一定是零. 由此可知, 算法终止.

设 算法终止于 $r_{k+1} = 0$. 则算法输出为 $g = r_k$ 且 $\mathrm{rem}(r_{k-1}, r_k) = 0$. 事实上, 算法产生的商序列

$$q_2, \ldots, q_k, q_{k+1}.$$

两序列之间的关系如下

$$r_{i-2} = q_i r_{i-1} + r_i, \quad i = 2, 3, \ldots, k+1. \tag{1}$$

下面我们来验证 $g = \gcd(m, n)$. 根据 (1), 我们有

$$\begin{cases} r_0 = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \vdots \\ r_{k-4} = q_{k-2} r_{k-3} + r_{k-2} \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} = q_k r_{k-1} + r_k \\ r_{k-1} = q_{k+1} r_k \end{cases} \tag{2}$$

断言 *1.* 对 $j = 1, 2, \ldots, k$, $g | r_{k-j}$.

证明. 对 j 归纳. 当 $j = 1$ 时, 由 (2) 中最后一个方程可知, $g | r_{k-1}$. 设 $j > 1$ 且结论对 $1, 2, \ldots, j-1$ 都成立. 注意到 (2) 中的方程

$$r_{k-j} = q_{k-(j-2)} r_{k-(j-1)} + r_{k-(j-2)}.$$

根据归纳假设, 我们有 $g | r_{k-(j-2)}$ 和 $g | r_{k-(j-1)}$. 再根据上述方程和引理 7.1 可知, $g | r_{k-j}$. 断言 1 成立.

该断言蕴含 $g | r_0$ 和 $g | r_1$. 于是, g 是 r_0, r_1 的公因子.

再设 $d \in \mathbb{Z}^+$ 是 r_0 和 r_1 的公因子.

断言 *2.* 对 $j = 2, 3, \ldots, k$, $d | r_i$, $i = 2, 3, \ldots, k$.

证明. 对 i 归纳. 当 $i = 2$ 时, 由 (2) 中第一个方程和引理 7.1 可知, $d|r_2$. 设 $i > 2$ 且结论对 $2, 3, \ldots, i-1$ 都成立. 注意到 (2) 中的方程

$$r_{i-2} = q_i r_{i-1} + r_i.$$

根据归纳假设, 我们有 $d|r_{i-2}$ 和 $d|r_{i-1}$. 再根据上述方程和引理 7.1 可知, $d|r_i$. 断言 2 成立.

该断言蕴含 $d|r_k$. 于是, $d \leq g$. 我们得出 $g = \gcd(m, n)$.

最后验证 $um + nv = g$.

断言 *3.* 对 $i = 0, 1, \ldots, k$, $u_i m + v_i n = r_i$.

证明. 对 i 归纳. $i = 0, 1$ 时, u_0, v_0, r_0 和 u_1, v_1, r_1 初始值的设定可知, $u_0 m + v_0 n = r_0$ 和 $u_1 m + v_1 n = r_1$. 设 $i > 2$ 且结论对 $2, 3, \ldots, i-1$ 都成立. 由归纳假设可知:

$$u_{i-2} m + v_{i-2} n = r_{i-2} \quad \text{和} \quad u_{i-1} m + v_{i-1} n = r_{i-1}.$$

于是, $q_i u_{i-1} m + q_i v_{i-1} n = q_i r_{i-1}$. 由此得出,

$$(u_{i-2} - q_i u_{i-1}) m + (v_{i-2} - q_i v_{i-1}) n = r_{i-2} - q_i r_{i-1}.$$

根据扩展 Euclid 算法循环中第 (c) 步和 $r_i = \mathrm{rem}(r_{i-2}, r_{i-1})$ 可知:

$$u_i m + v_i n = r_i.$$

断言 3 成立.

在断言 3 中取 $i{=}k$ 得 $u_k m + v_k n{=}r_k$, 即 $um + vn{=}g$.

□

注解 7.3 如果我们只计算整数的最大公因子, 则在扩展的辗转相除法中无需计算序列 $q_2, q_3, \ldots$, $u_0, u_1, u_2, u_3, \ldots$, 和 $v_0, v_1, v_2, v_3, \ldots$,

例 7.4 计算 $\gcd(95, 57)$.

解. 设 $r_0 = 95, r_1 = 57$. 则

$$\begin{cases} r_2 = \mathrm{rem}(r_0, r_1) = \mathrm{rem}(95, 57) = 38, \\ r_3 = \mathrm{rem}(r_1, r_2) = \mathrm{rem}(57, 38) = 19, \\ r_4 = \mathrm{rem}(r_2, r_3) = \mathrm{rem}(38, 19) = 0. \end{cases}$$

于是, $r_3 = \gcd(95, 57) = 19$.

例 7.5 计算 $u, v \in \mathbb{Z}$ 使得 $u \times 95 + v \times 57 = \gcd(95, 57)$.

解. 设 $r_0 = 95, u_0 = 1, v_0 = 0, r_1 = 57, u_1 = 0, v_1 = 1$. 则

$$\begin{cases} r_2 = \mathrm{rem}(r_0, r_1) = \mathrm{rem}(95, 57) = 38, \\ q_2 = \mathrm{quo}(r_0, r_1) = \mathrm{quo}(95, 57) = 1 \\ u_2 = u_0 - q_2 u_1 = 1,\ v_2 = v_0 - q_2 v_1 = -1 \\ \\ r_3 = \mathrm{rem}(r_1, r_2) = \mathrm{rem}(57, 38) = 19, \\ q_3 = \mathrm{quo}(r_1, r_2) = \mathrm{quo}(57, 38) = 1 \\ u_3 = u_1 - q_3 u_2 = -1,\ v_3 = v_1 - q_3 v_2 = 2 \\ \\ r_4 = \mathrm{rem}(r_2, r_3) = \mathrm{rem}(38, 19) = 0. \end{cases}$$

于是, $\underbrace{(-1)}_{u} \times 95 + \underbrace{2}_{v} \times 57 = 19.$

例 7.6 定理 *7.2* 的另一个证明. 令:

$$S = \{am + bn | a, b \in \mathbb{Z}\}.$$

则 S 中有正整数. 令 g 是 S 中的最小正整数. 则存在 $u, v \in \mathbb{Z}$ 使得

$$um + vn = g.$$

下面我们验证 $g = \gcd(m, n)$. 设 d 是 m, n 的公因子. 根据引理 *7.1* 可知 $d|g$. 于是, $d \leq g$. 设 $r = \mathrm{rem}(m, g)$. 则存在 $q \in \mathbb{Z}$ 使得 $m = qg + r$. 于是,

$$qum + qvn = qg \implies qum + qvn = m - r \implies (1 - qu)m + (-qv)n = r.$$

由 g 的极小性和 $r \in \{0, 1, \ldots, g-1\}$ 可知, $r = 0$. 故 $g|m$. 同理 $g|n$. $\square$

定义 7.7 设 $m, n \in \mathbb{Z}$. 如果 $\gcd(m, n) = 1$, 则称 m 和 n 互素.

定理 7.8 设 $m, n \in \mathbb{Z}$. 则 m, n 互素当且仅当存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$.

证明. 设 m, n 互素. 则 $\gcd(m, n) = 1$. 由定理 7.2 可知, 存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$. 反之, 设存在 $u, v \in \mathbb{Z}$ 使得 $um + vn = 1$ 和 $g = \gcd(m, n)$. 因为 $g|m$ 和 $g|n$, 所以 $g|1$ (引理 7.1). 故 $g = 1$. $\square$

定义 7.9 设 $m, n, a \in \mathbb{Z} \setminus \{0\}$. 如果 $m|a$ 且 $n|a$, 则称 a 是 m, n 的公倍数. 它们的正公倍数中最小者称为最小公倍数, 记为 $\operatorname{lcm}(m, n)$.

定理 7.10 设 $m, n \in \mathbb{Z} \setminus \{0\}$. 则

$$\operatorname{lcm}(m, n) = \frac{|mn|}{\gcd(m, n)}.$$

证明. 不妨设 $m, n \in \mathbb{Z}^+$. 令 $g = \gcd(m, n)$. 则存在 $a, b \in \mathbb{Z}^+$ 使得 $m = ag$ 和 $n = bg$. 进而

$$\frac{|mn|}{\gcd(m, n)} = abg = an = bm.$$

故 abg 是 m, n 的公倍式. 因为 $g = \gcd(m, n)$, 所以 a, b 互素. 根据定理 7.8, 存在 $u, v \in \mathbb{Z}$ 使得

$$ua + vb = 1.$$

再设 k 是 m, n 的公倍式, 我们有 $k = pm = qn$, 其中 p, q 是整数. 故 $k = pag = qbg$. 由此得出

$$uak+vbk = k \implies ua(qbg)+vb(pag) = k \implies (abg)(uq+vp) = k.$$

于是, $(abg)|k$. 由此得出, abg 是 m 和 n 的最小公倍式. □

例 7.11

$$\mathrm{lcm}(95, 57) = \frac{95 \times 57}{19} = 285.$$