第一章　预备知识

引理 6.9 设 $\sigma \in S_n$ 是长度为 k 的循环. 则 $\mathrm{ord}(\sigma) = k$.

证明. 设 $\sigma = (i_1 i_2 \dots i_k)$ 且 $m \in \{1, 2, \dots, k-1\}$, 则

$$\sigma^m(i_1) = i_{1+m}.$$

故 $\sigma^m \neq e$. 而 $\sigma^k(i_1) = i_1$. 注意到对任意 $\ell \in \{2, \dots, k\}$,

$$\sigma = (i_\ell i_{\ell+1} \dots i_k \dots i_1 \dots i_{\ell-1}).$$

故 $\sigma^k(i_\ell) = i_\ell$. 于是, $\sigma^k = e$. 我们得到 $\mathrm{ord}(\sigma) = k$. □

恒同映射也称为长度等于 1 的循环, 它是平凡的.

例 6.10 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. $\sigma = (198)(23)(67)$.

设 $\sigma \in S_n$. 定义 $M_\sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\}$.

例 6.11 我们有 $M_e = \emptyset$ 和 $M_{(i_1, \dots, i_k)} = \{i_1, \dots, i_k\}$.

引理 6.12 设 $\sigma \in S_n$ 且 $i \in M_\sigma$. 则 $\sigma(i) \in M_\sigma$.

证明. 假设设 $\sigma(i) \notin M_\sigma$. 则 $\sigma^2(i) = \sigma(i)$. 两边同时作用 σ^{-1} 得 $\sigma(i) = i$, 矛盾. □

定义 6.13 设 $\sigma, \tau \in S_n$. 如果 $M_\sigma \cap M_\tau = \emptyset$, 则称 σ 和 τ 是两个互不相交的置换.

命题 6.14 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. 设 $m = \mathrm{card}(M_\sigma)$. 我们对 m 归纳.

根据引理 6.12, $m>1$. 如果 $m=2$, 则设 $M_\sigma=\{i_1, i_2\}$. 再利用引理 6.12 可知 $\sigma=(i_1 i_2)$. 设 $m > 2$ 且对 $\mathrm{card}(M_\sigma) < m$ 结论都成立. 设 $i_1 \in M_\sigma$ 且 $p = \mathrm{ord}(\sigma)$. 则 $\sigma^p(i_1) = i_1$. 于是, 存在最小正整数 k 使得 $\sigma^k(i_1) = i_1$. 则

$$i_1,\, i_2 := \sigma(i_1),\, \ldots,\, i_k := \sigma^{k-1}(i_1) \tag{1}$$

两两不同. 否则, 存在 $r, s \in \{0, 1, \ldots, k-1\}$ 使得 $r < s$ 且 $\sigma^s(i_1) = \sigma^r(i_1)$. 则 $\sigma^{s-r}(i_1) = i_1$. 但 $0 < s - r < k$, 矛盾. 由 (1) 和 $\sigma(i_k) = \sigma^k(i_1) = i_1$ 可知, 循环 $\tau = (i_1 i_2, \ldots i_k)$ 满足 $\tau(i_1) = \sigma(i_1), \ldots, \tau(i_{k-1}) = \sigma(i_{k-1}), \tau(i_k) = i_1 = \sigma(i_k)$. 换言之,

$$\tau^{-1}\sigma(i_1) = i_1,\, \ldots,\, \tau^{-1}\sigma(i_{k-1}) = i_{k-1},\, \tau^{-1}\sigma(i_k) = i_k.$$

令 $\lambda=\tau^{-1}\sigma$. 则 $i_1,\ldots,i_k\notin M_\lambda$. 设 $j\in\{1,2,\ldots,n\}\backslash M_\sigma$. 则 $j\notin\{i_1,\ldots,i_k\}$. 故 $\lambda(j)=\tau^{-1}\sigma(j)=\tau^{-1}(j)=j$. 于是,

$$M_\lambda\subset M_\sigma\setminus\{i_1,\ldots,i_k\}\implies \operatorname{card}(M_\lambda)<m.$$

如果 $M_\lambda=\emptyset$, 则 $\lambda=e$. 故 $\sigma=\tau$ 是循环. 否则, 归纳假设蕴含 $\lambda=\lambda_1\cdots\lambda_s$, 其中 $\lambda_1,\ldots,\lambda_s$ 是两两互不相交的循环. 又因为 $i_1,\ldots,i_k\notin M_\lambda$, 所以每个循环 $\lambda_1,\ldots,\lambda_s$ 与 τ 都不相交. 从而 $\sigma=\tau\lambda=\tau\lambda_1\cdots\lambda_s$ 即为所求. $\square$

下面来证明上述定理中循环分解的唯一性.

引理 6.15 *设 $\sigma,\tau\in S_n$ 互不相交. 则 $\sigma\tau=\tau\sigma$.*

证明. 如果 $\sigma=e$ 或 $\tau=e$, 则结论显然成立.

设 $\sigma\neq e$ 和 $\tau\neq e$. 令 $i\in M_\sigma$. 则 $i\notin M_\tau$. 故 $\tau(i)=i$. 从而, $\sigma\tau(i)=\sigma(i)$. 另一方面, 引理 6.12 蕴含 $\sigma(i)\in M_\sigma$. 故 $\sigma(i)\notin M_\tau$. 我们有 $\tau\sigma(i)=\sigma(i)$. 于是, 对任意 $i\in M_\sigma$,

$$\sigma\tau(i)=\tau\sigma(i).$$

类似地, 对任意 $j\in M_\tau$, $\sigma\tau(j)=\tau\sigma(j)$.

而对任意 $k\in\{1,2,\ldots,n\}\setminus(M_\sigma\cup M_\tau)$,

$$\sigma\tau(k)=k=\tau\sigma(k)$$

显然成立. 综上所述, $\sigma\tau=\tau\sigma$. $\square$

定理 6.16 设 $\sigma \in S_n \setminus \{e\}$. 则在不计循环出现顺序的前提下, σ 可以唯一地写成有限个两两互不相交的(长度大于 1 的)循环之积.

证明. 分解的存在性见命题 6.19. 下面证明唯一性. 设

$$\sigma = \tau_1 \cdots \tau_p = \lambda_1 \cdots \lambda_q,$$

其中 $\tau_1, \ldots, \tau_p$ 是一组两两互不相交的循环, $\lambda_1, \ldots, \lambda_q$ 是另一组互不相交的循环. 我们要证明 $p = q$ 且适当调整下标后, $\tau_1 = \lambda_1, \ldots, \tau_p = \lambda_p$.

我们对 p 归纳. 设 $\tau_1 = (i_1 i_2 \ldots i_k)$. 则 $i_1 \in M_\sigma$, 故 i_1 会被唯一的一个第二组的循环移动. 由引理 6.15 可知, 不妨设 λ_1 移动 i_1. 则

$$\sigma(i_1) = \tau_1 \tau_2 \cdots \tau_p(i_1) = \tau_1(i_1) = i_2$$

且

$$\sigma(i_1) = \lambda_1 \lambda_2 \cdots \lambda_p(i_1) = \lambda_1(i_1).$$

故 $\lambda_1(i_1) = i_2$. 特别地, i_2 在循环 λ_1 中出现且不在其它循环中出现. 利用上述推理方式可得 $\lambda_1(i_2) = i_3$. 进而

$$\lambda_1(i_j) = i_{j+1},\ j \in \{3, \ldots, k-1\} \quad 且 \quad \lambda_1(i_k) = i_1.$$

于是, $\lambda_1 = \tau_1$. 特别地, 当 $p = 1$ 时, $\sigma = \tau_1 = \lambda_1$.

设 $p>1$ 且结论对 $p-1$ 成立. 则根据 $\tau_1=\lambda_1$, 我们有 $\tau_2\cdots\tau_p=\lambda_2\cdots\lambda_q$. 由归纳假设可知, $p=q$ 且在适当调整下标后, $\tau_2=\lambda_2,\ldots,\tau_p=\lambda_p$. $\square$

推论 6.17 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 $\ell_i=\mathrm{ord}(\tau_i)$, $i=1,\ldots,m$, $\ell=\mathrm{lcm}(\ell_1,\ldots,\ell_m)$. 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

$$\sigma^\ell=\tau_1^\ell\cdots\tau_m^\ell=\tau_1^{\ell_1k_1}\cdots\tau_m^{\ell_mk_m}=e.$$

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, $\ell_2|k$, $\ldots$, $\ell_m|k$. 故 k 也是 $\ell_1,\ldots,\ell_k$ 的公倍数. 再根据 $k|\ell$ 可知, $k=\ell$. $\square$

例 6.18 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. $\sigma=(134689)(25\underline{10}7)\implies\mathrm{ord}(\sigma)=\mathrm{lcm}(6,4)=12.$

命题 6.19 设 $\sigma, (i_1, \ldots, i_k) \in S_n$. 则

$$\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

证明. 我们只要证明 $\sigma(i_1, \ldots, i_k) = (\sigma(i_1), \ldots, \sigma(i_k))\sigma$.

设 $j \in \{1, \ldots, k-1\}$. 则

$$\sigma(i_1, \ldots, i_k)(i_j) = \sigma(i_{j+1}) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(i_j) = \sigma(i_{j+1}).$$

进而,

$$\sigma(i_1, \ldots, i_k)(i_k) = \sigma(i_1) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(i_k) = \sigma(i_1).$$

在设 $a \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. 则

$$\sigma(i_1, \ldots, i_k)(a) = \sigma(a) \quad \text{和} \quad (\sigma(i_1), \ldots, \sigma(i_k))\sigma(a) = \sigma(a).$$

综上所述, $\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$. □

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 6.20 任何一个循环都是若干个对换之积.

证明. 我们证明

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

其中 $k>2$. 令 $\sigma=(i_ki_{k-1})\cdots(i_ki_2)(i_ki_1)$.

设 $\ell\in\{1,2,\ldots,k-2\}$. 则

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

而

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

最后

$$\sigma(i_k)=\underbrace{(i_ki_{k-1})\cdots(i_ki_2)}\underbrace{(i_ki_1)}(i_k)=\underbrace{(i_ki_{k-1})\cdots(i_ki_2)}(i_1)=i_1.\square$$

例 6.21 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 6.22 设 $a,b,c\in\{1,2,\ldots,n\}$ 且两两不同, 则

$$(ac)(ab)(ac)=(bc).$$

证明. 注意到 $(ac)^{-1}=(ac)$. 再应用命题 6.19 即可. $\square$

引理 6.23 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 $\sigma' = (tu)$. 根据引理 6.22, $(st)(su)(st) = (tu)$. 故 $(su)(st) = (st)(tu)$. 取 $\sigma' = (tu)$ 和 $\tau' = (st)$ 即可.
情形 3. 设 $\tau = (tu)$. 则 $u \neq s$. 根据引理 6.22,

$$(tu)(st)(tu) = (su).$$

故 $(tu)(st) = (su)(tu)$. 取 $\tau' = (su)$ 和 $\sigma' = \tau$ 即可. □

引理 6.24 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 6.23, 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 6.23 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, 但 τ^*_{k-2} 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 6.25 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 6.16, σ 是若干循环之积. 由引理 6.20, 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 6.24 蕴含 $k+m$ 是偶数. 于是, k 和 m 的奇偶性相同. □

定义 6.26 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 6.27 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 6.28 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 6.29 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 6.30 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$\tau = (i_1 \ldots i_m)$. 根据引理6.20, $\tau = (i_m i_{m-1}) \cdots (i_m i_1)$. 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 6.31 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 $\pi = (1364\underline{10})(289)(57)$. 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 的正公因子. 如果任何 m, n 的公因子都整除 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

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

下面我们来验证 $g=\gcd(m,n)$. 根据 (2), 我们有

$$\begin{cases} r_0=q_2r_1+r_2\\ r_1=q_3r_2+r_3\\ \vdots\\ r_{k-4}=q_{k-2}r_{k-3}+r_{k-2}\\ r_{k-3}=q_{k-1}r_{k-2}+r_{k-1}\\ r_{k-2}=q_kr_{k-1}+r_k\\ r_{k-1}=q_{k+1}r_k \end{cases} \tag{3}$$

断言 *1.* 对 $j=2,3,\ldots,k$, $\gcd(r_{j-2},r_{j-1})=\gcd(r_{j-1},r_j)$.

断言 *1* **证明.** 我们有 $r_{j-2}=q_jr_{j-1}+r_j$. 根据引理 7.1, r_{j-2},r_{j-1} 的公因子都是 r_{j-1},r_j 的公因子, 反之也一样. 断言 1 成立.

由断言 1 可知, $\gcd(m,n)=\gcd(r_0,r_1)=\gcd(r_{k-1},r_k)$. 故 $\gcd(m,n)=r_k$.