§7 置换

记号 设 $n \in \mathbb{Z}^+$. X 是 n 个元素的集合. 不妨设 $X = \{1, 2, \cdots, n\}$

定义 $S_n = \{\sigma : X \to X \mid \sigma$ 是双射$\}$

称 σ 是 X 上的一个置换

把 σ 通过下列图表来表示

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

其中 $i_1, i_2, \cdots i_n \in X$ 两两不同

即 $\sigma(k) = i_k$, $k = 1, 2, \cdots n$

注 (S_n 中有 $n!$ 个元素)

§7.1 置换的积

设 $\sigma, \tau \in S_n$. 因为双射的复合仍是双射. 所以 $\sigma \circ \tau \in S_n$

把 $\sigma \circ \tau$ 简记为 $\sigma\tau$. 称之为 σ 和 τ 的积. ①

$\forall \sigma, \tau, \pi \in S_n$

$(\sigma\tau)\pi = \sigma(\tau\pi)$ 复合的结合律

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

$\sigma e = e\sigma = \sigma$ 乘法单位

$\sigma\sigma^{-1} = e$ 乘法逆

例 在 S_4 中. 设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

计算 $\sigma\tau$ 和 $\tau\sigma$

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

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

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

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

$\sigma\tau \neq \tau\sigma$

记号 设 $\sigma \in S_n$. $k \in \mathbb{Z}^+$

$$\sigma^k := \underbrace{\sigma \sigma \cdots \sigma}_{k} \qquad \sigma^{-k} = \underbrace{\sigma^{-1} \cdot \cdots \cdot \sigma^{-1}}_{k}$$

$$\sigma^0 = e$$

自己验证: $\sigma^i \sigma^j = \sigma^{i+j}$ $(\sigma^i)^j = \sigma^{ij}$

注: $(\sigma\tau)^2 = \sigma\tau\sigma\tau$ 一般不等于 $\sigma^2\tau^2$

引理 7.1 设 $\sigma \in S_n$. 则 $\exists k \in \mathbb{Z}^+$ 使得

$$\sigma^k = e$$

证明: 考虑无穷序列 $\sigma, \sigma^2, \sigma^3, \cdots$

每项都是 S_n 中的元素. 则

$\exists k, l \in \mathbb{Z}^+$, $k \neq l$, 使得 $\sigma^k = \sigma^l$

不妨设 $k < l$.

$$e = \sigma^{-k} \cdot \sigma^k = \sigma^{l-k}$$ $l-k \in \mathbb{Z}^+$

□

定义 设 $\sigma \in S_n$ 使得 $\sigma^k = e$ 成立的最小正整数 k. 称为 σ 的阶 (order), 记为 $\mathrm{ord}(\sigma)$.

设 $\mathrm{ord}(e) = 1$.

例: 设 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ 计算 $\mathrm{ord}(\sigma)$

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

$$\sigma^3 = \sigma^2 \cdot \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$$

$$\mathrm{ord}(\sigma) = 3.$$

引理 7.2 设 $\sigma \in S_n$, $\mathrm{ord}(\sigma) = k$, $m \in \mathbb{Z}$

则 $\sigma^m = e \iff k \mid m$

证: "$\Rightarrow$" 由带余除法 $m = qk + r$

其中 $q \in \mathbb{Z}$, $r \in \{0, 1, \cdots k-1\}$

"$\Leftarrow$" 若 $\sigma^m = \sigma^{qk+r} = (\sigma^k)^q \cdot \sigma^r$

$$= e^q \cdot \sigma^r = \sigma^r$$

由此可知 $\sigma^m = \sigma^r$ (*)

"$\Leftrightarrow$" $\sigma^m = e \overset{(*)}{\Longleftrightarrow} \sigma^r = e \overset{\text{阶的定义}}{\Longleftrightarrow} r = 0$

$\Leftrightarrow k \mid m$ ☒

定义：设 $i_1, \cdots, i_k \in \{1, \cdots n\}$ 两两不同

$\pi \in S_n$. 如果

$\pi(i_1) = i_2$, $\pi(i_2) = i_3, \cdots \pi(i_{k-1}) = i_k$

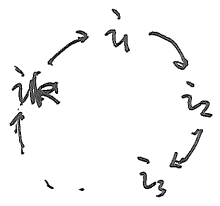
且 $\pi(i_k) = i_1$.

且 $\forall j \in X \setminus \{i_1, \cdots i_k\}$, $\pi(j) = j$.

则称 π 是一个循环 (cycle). 记为

$(i_1, \cdots i_k)$. k 称为 π 的长度

记为 $len(\pi)$.



$\pi = (i_1, i_2, \cdots i_k)$

$= (i_2, i_3 \cdots i_k i_1)$

$\cdots$

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

注. e 称为单位的循环

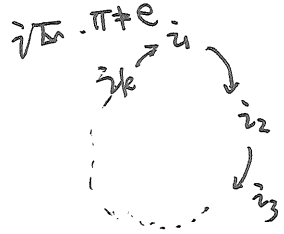
例：求 (123) 的阶

$ord(123) = 3$

引理 3.3 设 π 是 S_n 中的循环

则 $ord(\pi) = len(\pi)$

证. $\pi \neq e$



$\pi^1(i_1) = i_2$, $\pi^2(i_1) = i_3$

$\cdots \pi^{k-1}(i_1) = i_k$

$\pi^k(i_1) = \pi(i_k) = i_1$

同理 $\pi^k(i_s) = i_s$, $s = 2, \cdots k$

于是 $\pi^l \neq e$ $1 \leq l < k$. 但 $\pi^k = e$ ☒

定义：设 $\sigma = (i_1, \cdots i_k)$, $\tau = (j_1, \cdots j_l)$

是 S_n 中两个循环.

如果 $\{i_1, \cdots i_k\} \cap \{j_1, \cdots j_k\} = \emptyset$

则称 σ, τ 是不相交的.

引理 7.4. 设 $\sigma, \tau \in S_n$ 是两个不相交的循环

则 $\sigma\tau = \tau\sigma$

证: 设 $\sigma = (i_1 \cdots i_k)$, $\tau = (j_1 \cdots j_l)$

令 $I = (i_1 \cdots i_k)$. $J = \{j_1 \cdots j_l\}$

$\forall m \in X \setminus (I \cup J)$, $\sigma(m) = m$, $\tau(m) = m$

$\sigma\tau(m) = \sigma(\tau(m)) = \sigma(m) = m$

同理 $\tau\sigma(m) = m$

$\forall m \in I$ $\sigma\tau(m) = \sigma(m)$, $\tau\sigma(m) = \tau(\sigma(m))$
$= \sigma(m)$
$(\because \sigma(m) \in I)$

同理 $\forall m \in J$ $\sigma\tau(m) = \tau\sigma(m)$ ☒

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

写成若干互不相交的循环之积.

解 $\sigma = (198)(23)(67)$

定理 7.1 设 $\sigma \in S_n$ 则 σ 可以写为 ④
若干互不相交的循环之积.

证: 设 $\sigma \neq e$.

对 n 归纳. $n = 2$

$\sigma = (12)$

设当 $\sigma \in S_k$ 且 $k < n$ 时定理成立

设 $\sigma \in S_n$. 不妨设 $\sigma(i_1) = i_2$ 且 $i_1 \neq i_2$

断言 则从 i_1 出发我们可以得到循环

$(i_1, i_2, \cdots i_m)$

断言的证明: 考虑序列

$i_1, \sigma(i_1), \sigma^2(i_1) \cdots \cdots \in X$

$\exists k, l \in \mathbb{N}$ $k < l$ 使得

$\sigma^k(i_1) = \sigma^l(i_1) \Rightarrow \sigma^{-k}\sigma^k(i_1) = \sigma^{l-k}(i_1)$

$\Rightarrow \sigma^{l-k}(i_1) = i_1$

~~设 $l - k = s$~~

设 m 为最小的正整数使得 $\sigma^m(i_1) = i_1$

令 $i_2=\sigma(i_1),\ i_3=\sigma^2(i_1),\ \cdots\ i_m=\sigma^{m-1}(i_1)$

则 $i_1, i_2, \cdots i_m$ 两两不同

否则 $\exists\ 0\le k<l\le m-1$ 使得

$$\sigma^l(i_1)=\sigma^k(i_1)\Rightarrow \sigma^{l-k}(i_1)=i_1$$

但 $m>l-k>0$ $\rightarrow\leftarrow$.

于是 $\pi=(i_1,i_2,\cdots i_m)$ 是一个循环, 满足要求

如果 $m=n$., 则 $\sigma=(i_1,i_2,\cdots i_n)$

定理成立

设 $m<n$. 令 $J=X\setminus\{i_1,\cdots i_m\}$

π_1 是 $\{i_1,\cdots i_m\}$ 上的置换

$\sigma|_J$ 是 J 上的置换且阶

J 中元素 $<n$ 个.

由归纳假设

$$\sigma|_J=\tilde{\pi}_2\cdots\tilde{\pi}_s$$

其中 $\tilde{\pi}_2,\cdots,\tilde{\pi}_s$ 是 J 上互不相交的循环

对 $k=2,\cdots s$

令 $\pi_k: X\to X$

$$a\in J\mapsto \tilde{\pi}_k(j)$$

$$a\notin J\mapsto a$$

则 $\pi_2,\cdots\pi_s$ 是 X 上互不相交的循环

它们与 π_1 也不相交

验证: $\sigma=\pi_1\pi_2\cdots\pi_s$

设 $a\in\{i_1,\cdots i_s\}$. 则 $a\in J$

$$\pi_1\pi_2\cdots\pi_s(a)=\pi_1(a)=\sigma(a)$$

设 $a\notin\{i_1,\cdots i_s\}$ 则 $a\in J$

$$\sigma\pi_1\pi_2\cdots\pi_s=\pi_2\cdots\pi_s\pi_1(a)=\pi_2\cdots\pi_s(a)$$

$$=\sigma|_J(a)=\sigma(a).$$ 图

注: σ 互不相交循环是唯一的.

定理 7.2 设 $\sigma\in S_n$.

$$\sigma=\pi_1\cdots\pi_s$$

其中 $\pi_1,\cdots\pi_s$ 是两两互不相交的循环

则 $ord(\sigma)=lcm(len(\pi_1),\cdots len(\pi_s))$

↳ least common multiple.

例：

证：设 $m = \text{lcm}(\text{len}(\pi_1), \cdots \text{len}(\pi_s))$

令 $m_i = k_i \, \text{len}(\pi_i)$, $k_i \in \mathbb{Z}^+$ $i = 1, \cdots s$

由引理2.4 $\sigma^m = [\pi_1^{\text{len}(\pi_1)}]^{k_1} \cdots [\pi_s^{\text{len}(\pi_s)}]^{k_s}$

由引理题2.7.3 $= e$

设 $0 < m' < m$，则存在 $i \in \{1, \cdots s\}$

使得 $m' = q k_i + r$. 且 $r < k_i$

不妨设 $i = 1$ 则 $\pi_1^r \neq e$

则 $\sigma^{m'} = \pi_1^r \pi_2^{m'} \cdots \pi_s^{m'}$

设 $\pi_1^r(i) \neq i$ 因为 π_1 与 $\pi_2, \cdots \pi_s$ 互

不相交 $\pi_2^{m'} \cdots \pi_s^{m'}(i) = i$.

$\sigma^{m'}(i) = \pi_1^r(i) \neq i$.

于是 m 是 σ 的阶 ☒

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

的阶

$\sigma = (1\,3\,4\,6\,8\,9)(2\,5\,10\,7)$

$\text{ord}(\sigma) = \text{lcm}(6, 4) = 12$. ☒

定义：长度为2的循环称为对换

注：对换 $(i_1 i_2)$ 的逆是 (i_1, i_2)

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

σ τ

证：设 $\tau(i_1) = i_k$

设 $s \in \{1, \cdots k-1\}$

$\tau(i_s) = [(i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_{s+1})(i_1, i_s)](i_s)$

$= [(i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_{s+1})](i_1)$

$= [(i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_{s+2})](i_{s+1})$

$= i_{s+1}$

$\tau(i_k) = [(i_1, i_k)](i_k) = i_1$.

注：任何置换都是若干对换之积，但这些对换不一定两两不相交

引理7.5 设 $\alpha, \beta \in S_n$ 是两个对换且 $\alpha \neq \beta$

令 $\alpha = (st)$

则存在两个对换 $\alpha', \beta' \in S_n$

使得 $\beta\alpha = \alpha'\beta'$

满足 $\alpha'(s) \neq s$ ，$\beta'(s) = s$.

证：令 $\beta = (uv)$

$\{s,t\} \cap \{u,v\} = \emptyset$

情形1 令 $\alpha' = \alpha$, $\beta' = \beta$ 即可

$\beta\alpha = \alpha\beta$

情形2 $u = s$ $v \neq t$

$\beta = (sv)$

$\beta\alpha = (sv)(st) = (st)(vt)$

α' β'

直接验证

情形3 $u \neq s$ $v = t$

$\beta\alpha = (tv)(st) = (sv)(vt)$

情形4 $\beta = (st)$ 平凡 □

定理7.3 设 $\sigma = \lambda_1 \cdots \lambda_l = \mu_1 \cdots \mu_m$

其中 $\lambda_1, \cdots \lambda_l$, $\mu_1, \cdots \mu_m$ 都是对换

则 l 和 m 有相同的奇偶性

证：$\sigma^{-1} = \lambda_l \cdots \lambda_2 \lambda_1$

$\Rightarrow e = \lambda_l \cdots \lambda_2 \lambda_1 \sigma = \lambda_l \cdots \lambda_2 \lambda_1 \mu_1 \cdots \mu_m$

要证 l 和 m 有相同的奇偶性. 只要证 $l+m$ 是偶数. 为此

我们只要证下列特言

设 $e = \tau_1 \cdots \tau_k$，其中 $\tau_1 \cdots \tau_k$ 是对换

则 k 是偶数

显然 $k \geq 2$. 我们只要证 e 一定可以写为 $k-2$ 个对换即可

设 $\tau_k = (st)$. 如果 $\tau_{k-1} = \tau_k$. 则

$\tau_{k-1}\tau_k = e \Rightarrow e = \tau_1 \cdots \tau_{k-2}$. 结论成立

设 $\tau_{k-1} \neq \tau_k$. 由引理7.5

$e = \tau_1 \cdots \tau_{k-2} \tau_k' \tau_{k-1}'$

其中 τ_{k-1}', τ_k' 是对换且 $\tau_{k-1}'(s) = s$

$\tau_k'(s) \neq s$

对 τ_{k-2}, τ_k' 应用同样的推理可知

或者 e 可以写成 $k-2$ 个对换之积，

或者 $e = \tau_1 \cdots \tau_{k-3} \tau_k'' \tau_{k-2}' \tau_{k-1}'$

使得 $\tau_k''(s) \neq s$, $\tau_{k-2}'(s) = s$

如此从右至左推理可知，

e 总可以写成 $k-2$ 个对换之积

总之 $e = \pi \tau_1' \cdots \tau_{k-1}'$，使得

$\pi(s) \neq s$, $\tau_i'(s) = s$, $i = 1, \cdots k-1$

则 $e(s) = \pi(s) \neq s$ $\rightarrow\leftarrow$

于是 π 是 $k-2$ 个对换之积

同为 σ 不是对换，所以 k 是偶数 □

定义：设 $\sigma \in S_n$

$$\varepsilon_\sigma = \begin{cases} 1 & \text{如果 } \sigma \text{ 是偶数个对换之积，一定是} \\ -1 & \cdots\cdots \text{奇数} \cdots\cdots \text{一奇置换} \end{cases}$$

称 ε_σ 为 σ 的符号

定理 7.4 设 $\sigma \in S_n$ 且

$$\sigma = \pi_1 \cdots \pi_m,$$

其中 $\pi_1, \cdots, \pi_m$ 是互不相交的圈

则 $\varepsilon_\sigma = (-1)^{\sum_{i=1}^{m} [\mathrm{len}(\pi_i) - 1]}$

证：设 $\pi = (i_1 \cdots i_k)$ 则

$$\pi = (i_1 i_k) \cdots (i_1 i_2)$$

$$\varepsilon_\pi = (-1)^{\mathrm{len}(\pi) - 1}$$

$$\Rightarrow \varepsilon_\sigma = (-1)^{\sum_{i=1}^{m} [\mathrm{len}(\pi_i) - 1]}$$ □

注 $\boxed{\varepsilon_{\sigma\tau} = \varepsilon_\sigma \varepsilon_\tau}$

§8 整数的算术

定义：设 $a, b \in \mathbb{Z}\setminus\{0\}$，$c \in \mathbb{Z}\setminus\{0\}$

如果 $c|a$，$c|b$ 则称 c 是 a 和 b 的公因子

设 $g \in \mathbb{Z}^+$ 是 a, b 的公因子. 如果 a, b 的任何公因子都整除 g，则称 g 是 a, b 的最大公因子.

注：设 g_1, g_2 是 a, b 的最大公因子. 则

$g_1 | g_2$，$g_2 | g_1 \Rightarrow g_1 = \pm g_2 \Rightarrow g_1 = g_2$

于是 a, b 的最大公因子是唯一的，记为 $\gcd(a, b)$.

辗转相除法（Euclidean algorithm）

给定 $a, b \in \mathbb{Z}\setminus\{0\}$，计算 $\gcd(a, b)$

设 $r_0 = a$，$r_1 = b$

$r_0 = q_2 r_1 + r_2$，其中 $r_2 = \mathrm{rem}(r_0, r_1)$

如果 $r_2 \neq 0$ $r_1 = q_3 r_2 + r_3$，其中 $r_3 = \mathrm{rem}(r_1, r_2)$

如果 $r_3 \neq 0$ $r_2 = q_4 r_3 + r_4$，其中 $r_4 = \mathrm{rem}(r_2, r_3)$

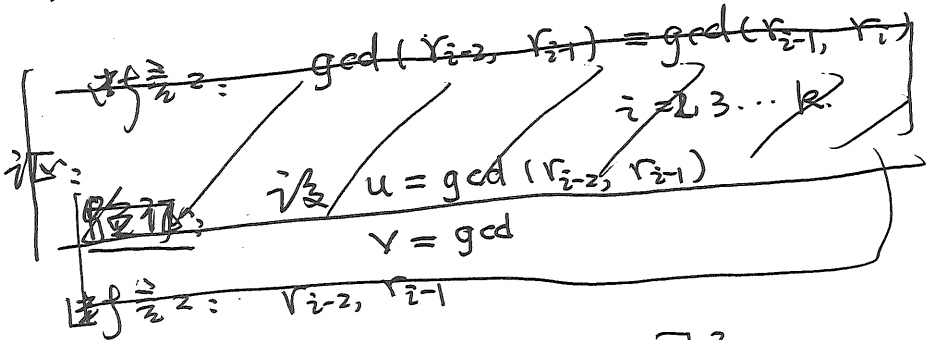
$\vdots$

$r_{k-2} = q_k r_{k-1} + r_k$ 其中 $r_k = \mathrm{rem}(r_{k-2}, r_{k-1})$

$r_{k-1} = q_{k+1} r_k$

断言1 上述的 k 必然存在 ①

证 $\because r_1 > r_2 > \cdots$ 是 $\mathbb{N}$ 中严格递减序列. 所以它只有有限项 □



断言2. c 是 r_{i-2}, r_{i-1} 的公因子

$\Leftrightarrow$ c 是 r_{i-1}, r_i 的公因子，$i = 2, 3, \cdots k$

证：由 $r_{i-2} = q_i r_{i-1} + r_i$ 可得

$c | r_{i-2}$，$c | r_i \Rightarrow c | r_{i-2}$

$c | r_{i-2}$，$c | r_{i-1} \Rightarrow c | r_i$ □

见关于整除的注：

断言3. r_k 是 a, b 的最大公因子

由 $r_{k-1} = q_{k+1} r_k \Rightarrow r_k$ 是 r_k, r_{k-1} 的公因子

$\Rightarrow r_k$ 是 r_{k-2}, r_{k-1} 的公因子 $\Rightarrow \cdots \Rightarrow$

r_k 是 r_0, r_1 的公因子 $\Rightarrow r_k$ 是 a, b 公因子

设 c 是 a, b 的公因子 $\Rightarrow c$ 是 r_0, r_1 的公因子

$\Rightarrow c$ 是 r_1, r_2 的公因子 $\Rightarrow \cdots \Rightarrow c$ 是 r_{k-1}, r_k 的公因子 $\Rightarrow c | r_k \Rightarrow r_k = \gcd(a, b)$.

断言4. $\exists u, v \in \mathbb{Z}$ 使得

$$ua + vb = \gcd(a,b)$$

证：对辗转相除次数作带余数法的次数归纳. 并做了 k 次除法.

当 $k=1$. $r_0 = q_2 r_1$, $\gcd(a,b) = r_1 = b$

$$0 \cdot a + 1 \cdot b = b$$

取 $u=0$, $v=1$ 即可

设做 $k-1$ 次除法时命题成立

则 $\exists u', v' \in \mathbb{Z}$ 使得

$$u' r_1 + v' r_2 = \gcd(r_1, r_2)$$

由断言2 $u' r_1 + v' r_2 = \gcd(a,b)$

因为 $r_0 = q_2 r_1 + r_2$

所以 $u' r_1 + v' r_2 = u' r_1 + v'(r_0 - q_2 r_1)$

$= v' r_0 + (u' - q_0 v') r_1 = \gcd(a,b)$ ☒

定理8.1 设 $a, b \in \mathbb{Z} \setminus \{0\}$. 则

(i) a, b 的最大公因子存在且唯一

(ii) $\exists u, v \in \mathbb{Z}$, $ua + vb = 1$ (Bezout 关系)

证：(i) 由断言3和关于唯一性的注解知 (10)

(ii) 是断言4

另证：设 $S = \{sa + tb \mid s, t \in \mathbb{Z}\}$

令 $g \in S \cap \mathbb{Z}$

令 g 为 $S \cap \mathbb{Z}^+$ 中最小的元素

则 存在 $u, v \in \mathbb{Z}$, 使得

$$ua + vb = g \qquad (*)$$

如果 $c|a$ 且 $c|b$, 则 $c|g$. 于是只须验证 $g|a$ 且 $g|b$ 即可. 假设 $g \nmid a$

则 $a = qg + r$ 其中 $r \in \{1, 2, \cdots g-1\}$

由此和 $(*)$ 得出

$$qua + qvb = qg = a - r$$

$$(qu-1)a + (qv)b = r$$

$\Rightarrow r \in S$ ← g的选择. ☒

于是 $g|a$. 同理 $s|b$ 于是 g 是 a,b 的公因子.

设 c 是 a 与 b 的公因子.

由 $c|a$, $c|b$ $\Rightarrow c|(ua+vb)$

$\Rightarrow c|g$

于是 g 是最大公因子 □

例: 计算 95 与 57 的最大公因子

$r_0=95$, $r_1=57$

$95 = 1\cdot 57 + 38$

$57 = 1\cdot 38 + 19$

$38 = 2\cdot 19.$

$\gcd(95,57)=19.$

求 $u,v\in\mathbb{Z}$, 使得

$u\cdot 95 + v\cdot 57 = 19$

$57 - 1\cdot 38 = 19$

$95 = 1\cdot 57 + 38$

$= 1\cdot 57 + 57 - 19$

$= 2\cdot 57 - 19$

$95 - 2\cdot 57 = -19$

$(-1)\cdot 95 + 2\cdot 57 = 19$

定义: 设 $a,b\in\mathbb{Z}\setminus\{0\}$.

如果 $\gcd(a,b)=1$. 则称 a,b 互素

定理 8.2 设 $a,b\in\mathbb{Z}\setminus\{0\}$

a,b 互素 $\Leftrightarrow \exists u,v\in\mathbb{Z}$ 使得

$ua+vb=1$

证: "$\Rightarrow$" 由定理 8.2 直接可得 □

"$\Leftarrow$" 设 $g=\gcd(a,b)$

由 $g|a$, $g|b \Rightarrow g|1 \Rightarrow g=1$ □

定义：设 $a,b\in\mathbb{Z}\setminus\{0\}$，$m\in\mathbb{Z}\setminus\{0\}$

如果 $a\mid m$，$b\mid m$，则称 m 是 a,b 的公倍数.

设 l 是 a,b 的正公倍数，如果 m 的任何公倍数都是 l 的倍数，则称 l 是 m 的正最小公倍数，记为 $lcm(a,b)$

注：a,b 的最小公倍数唯一.

引理 8.1 设 $a,b\in\mathbb{Z}\setminus\{0\}$，$a,b$ 互素，则 $lcm(a,b)=|a||b|$

证：设 $l=|a||b|$. 则 l 是 a,b 的公倍数.

∵ a,b 互素

∴ $\exists\, u,v\in\mathbb{Z}$ 使得

$$ua+vb=1$$

设 m 是 a,b 的公倍数

则 $m=sa=tb$，其中 $s,t\in\mathbb{Z}$

$$uam+vbm=m$$

$$ubab+vsab=m$$

$$ab(ut+vs)=m$$

$$|a||b|\mid|ut+vs|=m$$

$\Rightarrow |a|\mid m \Rightarrow l=lcm(a,b)$ ☒

定理 8.3 设 $a,b\in\mathbb{Z}\setminus\{0\}$

$$lcm(a,b)=\frac{|ab|}{gcd(a,b)}$$

证：由定理 8.2 $\exists\, u,v\in\mathbb{Z}$

$$ua+vb=g,\ \text{其中 } g=gcd(a,b)$$

且 $a=cg$ $b=dg$，其中 $c,d\in\mathbb{Z}$

$$ucg+vdg=g$$

$$uc+vd=1$$

由定理 8.2 和引理 8.1 $lcm(c,d)=|cd|$

令 $l=|cd|g=|d||a|=|c||b|$

$\Rightarrow l$ 是 a,b 的公倍式

设 m 是 a,b 的公倍式，则

$$m=\lambda a=\mu b,\ \lambda,\mu\in\mathbb{Z}$$

$$=\lambda cg=\mu dg$$

令 $w=\lambda c$，则 $m=\mu d$

于是 w 是 c,d 的公倍式，

$\Rightarrow |c||d|\mid w$

$\Rightarrow l\mid wg \Rightarrow l\mid m \Rightarrow l$ 是最小公倍式 □

例：计算 95 和 57 的最小公倍数

$$lcm(95,57)=\frac{95\times57}{19}=285.$$

定义：设 $m\in\mathbb{Z}^+\setminus\{1\}$，如果 m 不能写成两个小于 m 的正整数之积，则称 m 是素数 (prime)

定理 8.4 任何大于1的正整数都有限个素数之积。

证：设 $n\in\mathbb{Z}^+\setminus\{1\}$

如果 $n=2$，则定理成立（2是素数）

设当比 n 小的正整数时定理成立

如果 n 是素数，则定理显然成立

否则 $n=ml$，其中 $m,l\in\mathbb{Z}^+\setminus\{1\}$

且 $m<n$，$l<n$.

由归纳假设

m，l 都是若干个素数之积

从而 n 也是