

回42: $\sigma \in S_n$, $X = \{1, 2, \dots, n\}$

$\forall a, b \in X$ $a \sim b$ 如果 $\exists k \in \mathbb{Z}$, 使得

~~$a = \sigma^k(b)$~~ $a = \sigma^k(b)$

验证: \sim 是等价关系

设商集 ~~X/\sim~~ $= \{O_1, O_2, \dots, O_m\}$

称等价类 O_i 是 X 中关于 σ 的一个轨道

(orbit). $i=1, \dots, m$

引理 7.3 设 O 是 X 中关于 σ 的一个轨道

且 $\text{card}(O) = l$. 则

$\forall a \in O$ $O = \{a, \sigma(a), \dots, \sigma^{l-1}(a)\}$

证: 考虑无穷序列

$a, \sigma(a), \sigma^2(a), \dots \in O$

因为 O 是有限集. 所以存在 $i, j \in \mathbb{Z}^+$, $i < j$

使得 $\sigma^i(a) = \sigma^j(a)$. 于是 $a = \sigma^{j-i}(a)$

即存在正整数 k 使得 $a = \sigma^k(a)$ (*)

不妨设 k 是最小的正整数使得 (*) 成立 ①

断言 1. $\forall b \in O$, $\exists m \in \{0, 1, \dots, k-1\}$

使得 $b = \sigma^m(a)$

断言 1 的证明 $\exists i \in \mathbb{Z}$, 使得 $b = \sigma^i(a)$

由带余除法, $i = qk + m$. $m \in \{0, 1, \dots, k-1\}$

$b = \sigma^i(a) = \sigma^{qk+m}(a) = \underbrace{\sigma^{qk}(a)}_{\sigma^m(\underbrace{\sigma^{qk}(a)}_a)}$ $q \geq 0$

$\sigma^{m(-q)}(\sigma^{qk}(a))$ $q < 0$

$= \sigma^m(a)$. ($\because \sigma^k(a) = \sigma^{-k}(a) = a$)

断言 1 成立

断言 2. $\{a, \sigma(a), \dots, \sigma^{m-1}(a)\}$ 中的元素两两

不同

断言 2 的证明 设 $i, j \in \{0, 1, \dots, m-1\}$

且 $\sigma^i(a) = \sigma^j(a)$, 则 $a = \sigma^{j-i}(a)$

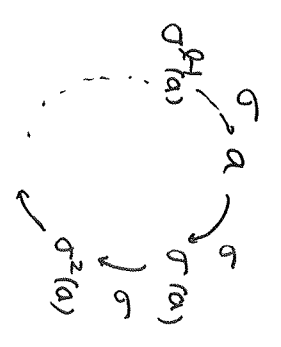
且 $0 \leq j-i < m$. 由 m 的最小性 $i=j$

由断言 1, 2 可知 $O = \{a, \sigma(a), \dots, \sigma^{m-1}(a)\}$

且 $l=m$



$$O = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$$



定义 设 $\{i_1, \dots, i_k\} \subset X, \sigma \in S_n$

如果 $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = \sigma(i_k) = i_1$
 $\sigma(i_{k-1}) = \sigma(i_k)$ 且 $\forall j \in X \setminus \{i_1, \dots, i_k\}$
 $\sigma(j) = j$.

则称 σ 是一个循环 (cycle).

此时 $\sigma = (i_1, i_2, \dots, i_{k-1}, i_k, i_1, \dots, i_k)$

简记为 (i_1, \dots, i_k) , 其长度为 k

记为 $\text{len}(\sigma) = k$. (length)

例 设 $X = \{1, 2, 3, \dots, 9\}$

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

确定 X/σ



$$(124875) \quad (36) \quad (9) = e$$



验证: $\sigma = (124875)(36)(9)(36)(124875)(9)$

定义: 设 $\sigma = (i_1, \dots, i_k), \tau = (j_1, \dots, j_m)$

是 X 上的两个循环. 如果

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_m\} = \emptyset$$

则称两个循环 σ, τ 互不相交

例: 设 $\sigma, \tau \in S_n$ 是两个互不相交的循环

则 $\sigma\tau = \tau\sigma$

设 $i \in \{i_1, \dots, i_k\}$ 则 $\sigma(i) \in \{i_1, \dots, i_k\}$ 且

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

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

同理 $\forall j \in \{j_1, \dots, j_m\} \quad \sigma\tau(j) = \tau\sigma(j)$

$\forall k \in X \setminus (\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_m\})$

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

□

定理 7.1 设 $\sigma \in S_n$ 则存在两两互不相交的循环 τ_1, \dots, τ_k . 使得

$$\sigma = \tau_1 \dots \tau_m \quad (**)$$

在不计顺序的前提下 (*) 是唯一的

证: 设 $X/\sigma = \{O_1, \dots, O_m\}$

由引理 7.3, 存在 $a_1, \dots, a_m \in X$ 使得

$$O_i = \{a_i, \sigma(a_i), \dots, \sigma^{l_i-1}(a_i)\}, \quad i=1, \dots, m$$

$$\text{令 } \tau_i = (a_i, \sigma(a_i), \dots, \sigma^{l_i-1}(a_i))$$

因为 O_1, \dots, O_m 两两不相交

所以 τ_1, \dots, τ_m 是两两不相交的循环

首先, 我们验证 (**) 成立

设 $a \in X$, 则存在唯一的 O_i 使得 $a = \sigma^{h_i}(a_i)$

$$\text{其中 } h_i \in \{0, 1, \dots, l_i-1\}$$

$$\tau_1 \dots \tau_m(a) = \tau_i(a) = \begin{cases} \sigma^{h_i+1}(a) & 0 \leq h_i < l_i-1 \\ a_i & h_i = l_i-1 \end{cases}$$

$$\sigma(a) = \sigma(\sigma^{h_i}(a_i)) = \sigma^{h_i+1}(a_i) = \begin{cases} \sigma^{h_i+1}(a_i) & 0 \leq h_i < l_i-1 \\ a_i & h_i = l_i-1 \end{cases}$$

(**) 成立.

唯一性 设 $\sigma = \alpha_1 \dots \alpha_s = \beta_1 \dots \beta_t$

其中 $\alpha_1, \dots, \alpha_s$ 是两两不相交的循环

β_1, \dots, β_t 是两两不相交的循环

设 $\alpha = (i_1, \dots, i_k) \in \{\alpha_1, \dots, \alpha_s\}$

则 $i_2 = \sigma(i_1), \dots, i_k = \sigma(i_{k-1}), \quad i_1 = \sigma(i_k)$

即 $\{i_1, \dots, i_k\}$ 是 ~~X~~ X 中的等价类 (轨道)

X 中关于 σ 的一个轨道. 于是

$\alpha_1, \dots, \alpha_s$ 对应 S 个不同的轨道 O_1, \dots, O_s

且 $X/\sigma = \{O_1, \dots, O_s\}$

且 $X/\sigma = \{O_1, \dots, O_t\}$. 于是 $s=t$

同理推的推论适用于 β_1, \dots, β_t . 于是

在适当调整顺序后可得

α_i, β_i 对应同样的轨道 $O_i, \quad i=1, \dots, s$

于是 $\alpha_i = \beta_i, \quad i=1, \dots, s$

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

$\sigma = (19)(256)(3874)(10)$

$= (10)(91)(8743)(625)$

例 设 $\sigma = (i_1 \dots i_k)$, 则 σ 的阶等于 k

证: $\{i_1, \dots, i_k\} = \{i_1, \sigma(i_1), \dots, \sigma^{k-1}(i_1)\}$
 $(i_2 = \sigma^2(i_1), \dots, i_{k-1} = \sigma^{k-2}(i_1))$

于是 σ 的阶 $\geq k$,

$\sigma^k(i_1) = \sigma(i_k) = i_1,$ ~~$\sigma^k(i_2) = \sigma^2(i_1)$~~

$\sigma^k(i_2) = \sigma^{k+1}(i_1) = \sigma^2(i_2) = \sigma(i_3) = i_2$

$\sigma^k(i_k) = \sigma^{k+1}(i_2) = \sigma^{k-1}(i_1) = i_k.$

$\sigma^k = e.$

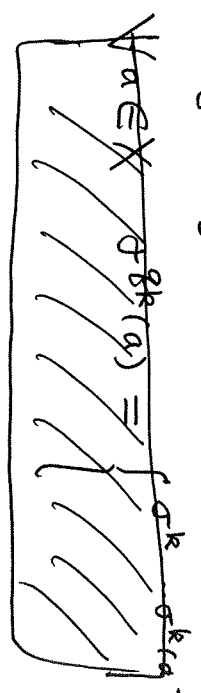
引理 7.4 设 $\sigma \in S_n$ k 是 σ 的阶, $m \in \mathbb{Z}$

r 是 m 关于 k 的余数

则 $\sigma^m = \sigma^r$, 特别地 $\sigma^m = e \iff k | m,$

证: 设 $m = qk + r$

$\sigma^m = \sigma^{qk+r} = \sigma^r \sigma^{qk} = \sigma^r (\sigma^k)^q = \sigma^r e^q = \sigma^r$



$= \sigma^r \quad (\because \sigma^k = \sigma^{-k} = e)$

$\sigma^m = e \iff \sigma^r = e \iff r = 0 \quad (r \in \{0, 1, \dots, k-1\}).$

证: $\sigma \in S_n$ 的阶记为 $\text{ord}(\sigma)$ (order)

定理 7.2 设 $\sigma \in S_n$, $\sigma = \tau_1 \dots \tau_k$ 其中 $\tau_1 \dots \tau_k$

是两两互不相交的循环,

则 $\text{ord}(\sigma) = \text{lcm}(\text{ord}(\tau_1), \dots, \text{ord}(\tau_k))$

其中 lcm 代表最小公倍数, 记为 (least common multiple)

证: 设 $m = \text{lcm}(\text{ord}(\tau_1), \dots, \text{ord}(\tau_k))$

$m = q_i \text{ord}(\tau_i), i = 1, \dots, k. \quad q_i \in \mathbb{Z}^+$

$\sigma^m = (\tau_1 \dots \tau_k)^m = \tau_1^m \dots \tau_k^m$ (互不相交的循环交换)

$$= \tau_1^{g_1 \text{ord}(\tau_1)} \dots \tau_k^{g_k \text{ord}(\tau_k)} = e \dots e = e$$

(3) (引理 7.4)

设 ρ 是 σ 的阶

$$e = \sigma^\rho = (\tau_1 \dots \tau_k)^\rho = \tau_1^\rho \dots \tau_k^\rho$$

由定理 7.1 的唯一性. $\tau_i^\rho = e, \dots, \tau_k^\rho = e$

由引理 7.4. $\text{ord}(\tau_i) \mid \rho, i=1, \dots, k$

$$\Rightarrow m \mid \rho \Rightarrow \rho = m. \quad \square$$

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

的阶

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

$$\text{ord}(\sigma) = \text{lcm}(2, 3, 4) = 12.$$

定义: 长度为 2 的循环称为对换 (5)

例: 阶为 $k > 1$ 的循环是 $k-1$ 个对换之积

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

注: 这些循环不一定两两不相交, 从而不一定交换

注: 由定理 7.2. 任何置换都是若干个对换之积

证: $(i_1 i_2)(i_2 i_3) = e.$

例: $(123) = (13)(12) = (23)(13) = (23)(12)(12)(13)$

定理 7.3 设 $\sigma \in S_n$. 则

$$\sigma = \lambda_1 \dots \lambda_k = \mu_1 \dots \mu_l, \text{ 其中 } \lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_l$$

都是对换. 则 k 和 l 有相同的奇偶性

证: $\because \lambda_1 \dots \lambda_k = \mu_1 \dots \mu_l$

$$\therefore \lambda_1 \dots \lambda_k \mu_l = e$$

要证明 k, l 有相同的奇偶性

引理 7.5 (换位引理)

设 $\alpha = (st)$ $\beta = (uv)$ 且 $\alpha \neq \beta$
 则存在对换 α', β' 使得

$$\beta\alpha = \alpha'\beta'$$

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

证: 情形 1 $\{s, t\} \cap \{u, v\} = \emptyset$

$$\beta\alpha = \alpha\beta \quad \text{另 } \alpha = \alpha', \beta = \beta' \quad \text{即可}$$

情形 2. $u = s, v \neq t$

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

$$\text{令 } \alpha' = \alpha, \beta' = (vt) \quad \text{即可}$$

情形 3 $u \neq t, v \neq s$

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

$$\text{令 } \alpha' = (sv), \beta = (vt) \quad \text{即可}$$

定理 7.3 设 $\sigma = \lambda_1 \dots \lambda_m = \mu_1 \dots \mu_m$

其中 $\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_m$ 都是对换

则 λ 和 μ 有相同奇偶性

证 由 $\lambda_1 \dots \lambda_r = \mu_1 \dots \mu_m$

可知 $\lambda_1 \dots \lambda_r \mu_m \dots \mu_1 = e$

λ, μ 有相同奇偶性 $\Leftrightarrow \lambda + \mu$ 是偶数
 于是我们的只要证明以下命题

设 $e = \tau_1 \tau_2 \dots \tau_k$, 其中 τ_1, \dots, τ_k

是对换. 则 k 是偶数. 为此只要证明
 以下命题: 设 $k > 0$. 则 e 可以写成

$k-2$ 个对换之积.

证: 设 $\tau_k = (st)$. 则 $e = \tau_1 \tau_2 \dots \tau_{k-2} \tau_k = (st)$. 则

设 $\tau_k = (st)$. 则 $e = \tau_1 \tau_2 \dots \tau_{k-2} \tau_k = (st)$. 则

否则. 由换位引理

$$e = \tau_1 \tau_2 \dots \tau_{k-2} \tau_k \tau_{k-1} \tau_{k-1}^{-1} \tau_k^{-1} \tau_k = s$$

如果 $\tau_{k-2} = \tau_k$, 则 $e = \tau_1 \tau_2 \dots \tau_{k-3} \tau_{k-1} \tau_{k-1}^{-1} \tau_k \tau_k^{-1} \tau_k = s$

否则 $e = \tau_1 \tau_2 \dots \tau_{k-3} \tau_k \tau_{k-2} \tau_{k-2}^{-1} \tau_k^{-1} \tau_k = s$

同样的推理说明. 那么命题成立. 那么

$$e = \tau_k^{(k-1)} \cdot \tau_1' \tau_2' \dots \tau_{k-1}'$$

满足 $\tau_k^{(k-1)}(s) \neq s, \tau_1' \tau_2' \dots \tau_{k-1}'(s) = s$

于是命题 $e(s) \neq s \rightarrow \leftarrow$ 定理成立

回忆：定理 7.3. 设 $\sigma = \lambda_1 \dots \lambda_g = \mu_1 \dots \mu_m$

其中 $\lambda_1, \dots, \lambda_g, \mu_1, \dots, \mu_m$ 都是对换.

则 λ 和 m 有相同的奇偶性.

更正：设 $\alpha, \beta \in S_n$

$$(\alpha\beta)^2 = (\alpha\beta)(\alpha\beta) = \alpha\beta\alpha\beta$$

$$\frac{1}{2} \beta\alpha = \alpha\beta \quad \alpha\beta\alpha\beta = \alpha\alpha\beta\beta = \alpha^2\beta^2$$

$$\text{当 } \frac{1}{2} \beta\alpha = \alpha\beta \text{ 时, } (\alpha\beta)^2 = \alpha^2\beta^2.$$

当 $\beta\alpha \neq \alpha\beta$ 时, $(\alpha\beta)^2 = \alpha^2\beta^2$ 一般不成立

补充：设 $\alpha_1, \dots, \alpha_s$ 是两两互不相交的循环

$$\sigma = \alpha_1 \dots \alpha_s$$

证明：如果 $\sigma^2 = e$, 则 $\forall i \in \{1, \dots, s\}, \alpha_i^2 = e$

证：假设 $\exists j \in \{1, \dots, s\}, \alpha_j^2 \neq e$. 则 $\exists a \in X$

使得 $\alpha_j(a) \neq a$. 于 $\alpha_j \alpha_j(a) \neq a$. 因为

α_j 与 $\alpha_i (i \neq j)$ 不相交. $\alpha_i(a) = a$

$$e = \sigma^2 = \alpha_1^2 \dots \alpha_s^2 = \alpha_j^2 \alpha_1^2 \dots \alpha_{j-1}^2 \alpha_{j+1}^2 \dots \alpha_s^2$$

$$\alpha = e(\alpha) = \alpha_j^2(\alpha) = \alpha_j^2(\alpha_1^2 \dots \alpha_j^2 \alpha_{j+1}^2 \dots \alpha_s^2)(\alpha) \\ = \alpha_j^2(m) \neq m \quad \rightarrow \leftarrow$$

定理 7.3 的证明

由 $\lambda_1 \dots \lambda_g = \mu_1 \dots \mu_m$

$$\Rightarrow \lambda_1 \dots \lambda_g \mu_m = \mu_1 \dots \mu_{m-1} \mu_m \mu_m \\ = \mu_1 \dots \mu_{m-1}$$

$$\Rightarrow \lambda_1 \dots \lambda_g \mu_m \mu_{m-1} \dots \mu_1 = e.$$

要证： λ, m 有相同的奇偶性，只要证 $\lambda + m$ 是偶数

换言之，只要证明下列命题

设 τ_1, \dots, τ_k 是对换 $\tau_1 \dots \tau_k = e$ (*)

则 k 是偶数. 为此只要证：

如果 (*) 成立且 $k > 0$. 则 e 可以写成 $k-2$

个对换之积. 设 $k > 0, \tau_k = (st)$ 则 (*) 成立

如果 $\tau_{k-1} = (st)$ 则 $\tau_1 \dots \tau_{k-2} = e$ 成立

否则由换位引理

$$e = \tau_1 \dots \tau_{k-2} \tau_k \tau_{k-1}, \text{ 其中 } \tau_k'(s) \neq s \\ \tau_{k-1}'(s) = s$$

如果 $\tau_{k-2} = \tau_k$. 则 e 是 $k-2$ 个对换之积.

否则再由换位引理 $e = \tau_1 \dots \tau_{k-3} \tau_k \tau_{k-2} \tau_{k-1}$

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

如该排列 或者 σ 可以写成 $k-2$ 个对换之积

或者 $\sigma = \tau_k^{(k-1)} \tau_{k-1} \dots \tau_1$ 其中

$$\tau_i^{(k-1)}(s) = s, \quad i=1, 2, \dots, k-1, \quad \tau_k^{(k-1)}(s) \neq s$$

$$s = \sigma(s) = \tau_k^{(k-1)} \tau_{k-1} \dots \tau_1(s) = \tau_k^{(k-1)}(s) \neq s$$

→ 于是 σ 必能写成 $k-2$ 个对换之积

证之积 □

定义. 设 $\sigma \in S_n$. 如果 σ 可以写成偶 (奇) 数个对换之积, 则称 σ 是偶 (奇) 置换

符号对换之积. 则当 σ 是偶置换

$$\varepsilon_\sigma := \begin{cases} 1 & \text{当 } \sigma \text{ 是奇置换} \\ -1 & \end{cases}$$

ε_σ 称为 σ 的符号. 也记为 $\text{sign}(\sigma)$ 或 $\text{sgn}(\sigma)$

例 设 $\sigma = (i_1 \dots i_k)$

证: $\varepsilon_\sigma = (-1)^{k-1}$

证: $\sigma = (i_1 i_2) (i_2 i_3) \dots (i_{k-1} i_k) \Rightarrow \varepsilon_\sigma = (-1)^{k-1}$

定理 7.4 设 $\sigma \in S_n, \sigma = \tau_1 \dots \tau_k$, 其中 ⑧

τ_1, \dots, τ_k 是两两互不相交的循环.

例 (i) $\text{ord}(\sigma) = \text{lcm}(\text{ord}(\tau_1), \dots, \text{ord}(\tau_k))$

(ii) $\varepsilon_\sigma = (-1)^{\text{ord}(\tau_1) + \dots + \text{ord}(\tau_k) - k}$

证 (i) 定理 7.3. (ii)

(iii) ε_σ 可以写成 $[\text{ord}(\tau_1) - 1] + \dots + [\text{ord}(\tau_k) - 1]$ 个对换之积 □

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

的符号和符号

$$\sigma = (1247)(36)(5) = (1247)(36)$$

$$\text{ord}(\sigma) = 4$$

$$\varepsilon_\sigma = (-1)^{4+2-2} = 1 \quad \text{偶置换}$$

§8 整数的运算

定义: 设 $a, d \in \mathbb{Z}$, 且 $d \neq 0$. 如果 $d | a$, 则称 d 是 a 的因子, a 是 d 的倍数.

(ii) 设 $b \in \mathbb{Z}$, 如果 $d | a$ 且 $d | b$, 则称 d 是 a, b 的公因子.

(iii) 设 g 是 a 和 b 的正公因子. 且对 a, b 的任何公因子 d , 都有 $d | g$. 则称 g 是 a, b 的最大公因子.

计算 a, b 的最大公因子

引理 8.1 设 $a, b \in \mathbb{Z}$, d 是 a, b 的公因子

$$\lambda, \mu \in \mathbb{Z}, \text{ 则 } d | (\lambda a + \mu b)$$

证: $d | a \Rightarrow \exists u \in \mathbb{Z} \quad a = ud$.

$$\text{同理 } \exists v \in \mathbb{Z}, \quad b = vd$$

$$\lambda a + \mu b = \lambda ud + \mu vd = (\lambda u + \mu v)d$$

$$\Rightarrow d | (\lambda a + \mu b). \quad \square$$

证 不考虑 $0, 0$ 的最大公因子

设 $a \in \mathbb{Z} \setminus \{0\}$. $\textcircled{1}$: a 的最大公因子当然是 $|a|$.

给定 $a, b \in \mathbb{Z} \setminus \{0\}$. 可以利用 Euclid 算法 (辗转相除法) 计算 a, b 的最大公因子如下

$$\text{令 } r_0 = a, \quad r_1 = b$$

$$r_0 = q_2 r_1 + r_2 \quad q_2 - \text{商}, \quad r_2 \text{ 余数}$$

$$0 \leq r_2 < r_1$$

$$\text{续 } r_1 > 0 \quad r_1 = q_3 r_2 + r_3 \quad q_3 - \text{商}, \quad r_3 \text{ 余数}$$

$$\vdots$$

$$r_{k-2} = q_k r_{k-1} + r_k$$

$$r_{k-1} = q_{k+1} r_k + 0$$

断言 r_k 是 a, b 的最大公因子.

断言的证明: $r_k | r_{k-1}$

$$\begin{aligned} \Rightarrow r_k | r_{k-2} &\xrightarrow{\text{引理 8.1}} r_k | r_{k-3} \Rightarrow \dots \\ \text{引理 8.1} & \end{aligned}$$

$$\Rightarrow r_k | r_3, r_k | r_2 \Rightarrow r_k | r_1 \Rightarrow r_k | r_0$$

$$\Rightarrow r_k \text{ 是 } a, b \text{ 的公因子.}$$

设 d 是 a, b 的公因子. $d | r_0, d | r_1 \Rightarrow d | r_2$

$$\Rightarrow d | r_3 \Rightarrow \dots \Rightarrow d | r_k \Rightarrow r_k \text{ 是 } a, b \text{ 的最大公因子.} \quad \square$$

设 $k > 1$ 且设 $k-1$ 降法时 定理成立

例 设 $\lambda', \mu' \in \mathbb{Z}$

$$\lambda' r_1 + \mu' r_2 = r_k = \gcd(a, b)$$

$$\text{且 } r_0 = g_2 r_1 + r_2$$

$$\lambda' r_1 + \mu' (r_0 - g_2 r_1) = \gcd(a, b)$$

$$\mu' r_0 + (\lambda' - \mu' g_2) r_1 = \gcd(a, b)$$

$$\text{令 } \lambda = \mu', \quad \mu = \lambda' - \mu' g_2 \quad \text{则}$$

$$\lambda a + \mu b = \gcd(a, b) \quad \square$$

证: 书上有一个优雅的办法.

定义: 设 $a, b \in \mathbb{Z}$. 称 $\gcd(a, b) = 1$

例称 a, b 互素

定理 8.2 设 $a, b \in \mathbb{Z}$. 则

a, b 互素 $\iff \exists \lambda, \mu \in \mathbb{Z}$, 使得

$$\lambda a + \mu b = 1 \quad (*)$$

于是 设 $a, b \in \mathbb{Z} \setminus \{0\}$. 不全为零 a, b 的公因子

存在. 设 g_1, g_2 是 a, b 的极大公因子

例 $g_1 | g_2$ 且 $g_2 | g_1$. 因为 $g_1, g_2 \in \mathbb{Z}^+$. 所以 $g_1 = g_2$

于是 极大公因子唯一.

记号: 设 $a, b \in \mathbb{Z}$ 不全为零. 则 a, b 的极大公因子 记为 $\gcd(a, b)$ [greatest common divisor]

定理 8.1 (Bezout's relation) 设 $a, b \in \mathbb{Z}$ 不全为零. 则存在 $\lambda, \mu \in \mathbb{Z}$ 使得

$$\lambda a + \mu b = \gcd(a, b).$$

证: 当 $a=0$ 时 $\gcd(a, b) = b$. 此时取

$$\lambda = 0, \mu = 1 \quad \text{即可.}$$

设在辗转相除法中通过 k 次除法 得到 $\gcd(a, b)$. 则 可归纳为

$$r_{k-1} = g_2 r_k \implies \gcd(a, b) = b$$

$$\text{取 } \lambda = 0, \mu = 1 \quad \text{即可}$$

证: " \Rightarrow " 由定理 8.1 直接得证

" \Leftarrow " 设 $(x, y) = d$, d 是 a, b 的正公因子

由引理 8.1, $d | 1 \Rightarrow d = 1 \Rightarrow \gcd(a, b) = 1$

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

则称 m 是 a, b 的公倍数. 设 $\lambda > 0$ 且

是 a, b 的公倍数. 则称 λ 是 a, b 的

公倍数的因子. 则称 λ 是 a, b 的

a, b 的最小公倍数.

证: 最小公倍数存在且唯一. 记为 $\text{lcm}(a, b)$

引理 8.2. 设 $a, b \in \mathbb{Z} \setminus \{0\}$, a, b 互素

$$\forall \lambda | \text{lcm}(a, b) = |\lambda| |ab|$$

证: 设 $\lambda = |\lambda| |ab|$. $\lambda | \lambda$ 是 a, b 的公倍数

设 m 是 a, b 的公倍数 $m = \mu a = \nu b$

由定理 8.2 $\exists \lambda, \mu \in \mathbb{Z}$, 使得

$$\lambda a + \mu b = 1$$

$$\lambda a m + \mu b m = \lambda m$$

$$\lambda a b + \mu b a = m$$

$$(\lambda \nu + \mu \mu) a b = m$$

$\lambda | a b \Rightarrow \lambda | m \Rightarrow \lambda$ 是 a, b 的公因子

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

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

证: 设 $g = \gcd(a, b)$ 则 $\exists c, d \in \mathbb{Z}$

使得 $a = cg, b = dg$

由 Bezout 系系 $\exists \lambda, \mu \in \mathbb{Z}$ 使得

$$\lambda a + \mu b = g$$

$$\lambda cg + \mu dg = g$$

$$\lambda c + \mu d = 1$$

$$|\text{lcm}(c, d)| = |cd| \quad (*)$$

即 c, d 互素. 由引理 8.2

$$\lambda c d g = a d = c b$$

设 m 是 a, b 的公倍数. 则 $m = \mu a = \nu b = (\nu c) g$

$$m = u c (= \nu d) \quad \text{则 } |w| \text{ 是 } c, d \text{ 的公因子}$$

$$w = t c d \quad t \in \mathbb{Z}$$

$$m = t c d g = t c d c b$$

$$\lambda | m \Rightarrow \lambda \text{ 是 } a, b \text{ 的公因子}$$

例：计算 95 和 57 的最小公倍数

$$95 = 1 \cdot 57 + 38$$

$$57 = 1 \cdot 38 + 19$$

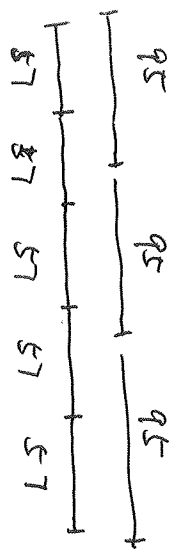
$$38 = 2 \cdot 19$$

$$\gcd(95, 57) = 19 \quad \text{lcm}(95, 57) = \frac{95 \cdot 57}{19} = 285$$

$$95 = 57 + 57 - 19$$

$$95 - 2 \times 57 = -19$$

$$\boxed{(-1) \times 95 + 2 \times 57 = 19}$$



定义：设 $p \in \mathbb{Z}^+ \setminus \{1\}$

如果 p 不能写成两个大于 1 的整数之积，

则称 p 是素数。在例 1 称之为合数。

又 3, 5, 7, 11, 13, 17, 19, ...

定理 8.4 每个大于 1 的整数都是若干个

素数之积。

证：假设 $\mathbb{Z}^+ \setminus \{1\}$ 中不能写成若干个素数之积的整数。设 n 为最小的这样的正整数。例 n 不是素数。于是 $\exists u, v \in \mathbb{Z}^+ \setminus \{1\}$ 使得

$$n = uv.$$

例 $1 < u < n, 1 < v < n$. 按 n 的最小性， u 是若干个素数之积， v 也是。从而 n 也是。 $\rightarrow \leftarrow$ \square

例：证明素数有无穷多个。

假设素数只有有限个 p_1, \dots, p_k . 令

$$n = p_1 p_2 \dots p_k + 1$$

由定理 8.4. n 是 p_1, p_2, \dots, p_k 中若干个素数之积。不妨设 $p_1 | n$. 由引理 8.1. $p_1 | 1 \rightarrow \leftarrow$.

例 设 p 是素数, $a, b \in \mathbb{Z} \setminus \{0\}$. ~~a, b 互素~~

证明 如果 $p | ab$ 则 $p | a$ 或 $p | b$

证：由 ~~Bézout 引理~~ ~~$\exists x, y \in \mathbb{Z}$~~

$$\cancel{x a + y b = 1} \quad \text{或}$$

证 $p \nmid a$. 则 $\cancel{a} = \gcd(a, b)$ 或

$1 \leq q < p$. 因为 p 是素数, q 可以 $q = 1$

由 Bezout 关系, $\exists \lambda, \mu \in \mathbb{Z}$

$$\lambda a + \mu p = 1$$

$$\lambda ab + \mu pb = b$$

$$p | ab, p | \mu pb \Rightarrow p | b \quad \square$$

例 ~~设 p 是小于 n 的素数~~ 设 p 是素数

$$\exists 0 < k < p, \quad \forall n | p | \binom{p}{k}$$

$$\binom{p}{k} = \frac{p!}{k! (p-k)!}$$

$$p! = k! (p-k)! \binom{p}{k} \quad \text{由上例}$$

$$p | k! \text{ 或 } p | (p-k)! \text{ 或 } p | \binom{p}{k}$$

$$\times \quad \times \quad \Rightarrow p | \binom{p}{k} \quad \square$$