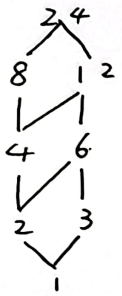
1.解：

循环分解 $\pi=(1\ 3\ 8\ 7\ 5)(2\ 6\ 4)(9\ 10)$

阶数 $ord(\pi)=lcm(5,3,2)=30$

置换符号 $\varepsilon_{\pi}=(-1)^{4+2+1}=(-1)^{7}=-1$

2. $24=2^3\times 3$ ，故 24的全体正因子为 $\{1,2,3,4,6,8,12,24\}$



3、置换 π ($\pi\in S_n$) 含有 m 个互不相交的循环，形式为

$$\pi=\pi_1\pi_2\cdots\pi_m,\quad l_i\text{为}\pi_i\text{的长度且 } l_i>1,\ i=1,2,\cdots m$$

令

$$m'=n-\sum_{k=1}^{m}l_k,$$

则π使 m' 个符号(或点)保持不变. 数 $d(\pi)=n-(m+m')$ 叫做置换π的减量. 验证

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

证明： $\varepsilon_\pi=(-1)^{\sum_{k=1}^{m}(l_k-1)}=(-1)^{\sum_{k=1}^{m}l_k-m}=(-1)^{n-m'-m}=(-1)^{n-(m+m')}=d(\pi)$.

π使 m' 个符号不变：~~由于~~ 令 $A=\{a\mid a\text{出现在}\pi_i\text{中}, i=1,2,\cdots m\}$，从而 $\{1,2,\cdots,n\}\setminus A$ 在π作用下保持不动，且由于 π_i 与 π_j 互不相交，故 $\forall a\in A$，$\exists!\ i\in\{1,2,\cdots,m\}$, s.t. a 在 π_i 中，从而 a 移动了.

故 π 使 m' 个符号保持不动.

4. 计算置换

$$\pi=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ n & n-1 & n-2 & \cdots & 2 & 1\end{pmatrix}\text{的符号.}$$

解：当n为偶数时，

$$\pi=(1,n)(2,n-1)\cdots\left(\frac{n}{2},\frac{n}{2}+1\right).$$

$$\varepsilon_\pi=(-1)^{\frac{n}{2}}$$

当n为奇数且 $n>1$ 时，

$$\pi=(1,n)(2,n-1)\cdots\left(\frac{n-1}{2},\frac{n+3}{2}\right)$$

$$\varepsilon_\pi=(-1)^{\frac{n-1}{2}}$$

$n=1$ 时， $\pi=(1)$， $\varepsilon_\pi=1$.

4. 证明：反身性：$\forall a\in\{1,2,\cdots,n\}$，$\exists 0\in\mathbb{Z}$，s.t $a=\sigma^0(a)$，故 $a\sim^\sigma a$.

对称性：$\forall a,b\in\{1,2,\cdots,n\}$ 满足 $a\sim^\sigma b$，则 $\exists i\in\mathbb{Z}$，s.t $a=\sigma^i(b)$

从而 $b=\sigma^{-i}(a)$，故 $b\sim^\sigma a$

传递性：$\forall a,b,c\in\{1,2,\cdots,n\}$. 满足 $a\sim^\sigma b$，$b\sim^\sigma c$，则 $\exists i,j\in\mathbb{Z}$，s.t

$a=\sigma^i(b)$，$b=\sigma^j(c)$，从而 $a=\sigma^i(b)=\sigma^{i+j}(c)$.，故 $a\sim^\sigma c$

5. 证明：$\forall \sigma\in S_n$，$\exists$ 互不相交的循环 $\pi_1,\pi_2,\cdots,\pi_m$（且 π_i 的长度大于1）. s.t

$\sigma=\pi_1\cdots\pi_m$.

设 π_i 的长度为 l_i，则 $\sum_{i=1}^{m} l_i\le n$

对每个循环 π_i，设 $\pi_1=(j_1\ j_2\cdots j_{l_1})$，则 $\pi_1=(j_1\ j_{l_1})(j_{l_1}\ j_{l_1-2})\cdots\cdots(j_{l_1}\ j_1)$，

即 π_1 可分解为 l_1-1 个对换之积，

类似地，π_i 可分解成 l_i-1 个对换之积.

从而 σ 可分解为 $\sum_{i=1}^{m}(l_i-1)$ 个对换之积

$\sum_{i=1}^{m}(l_i-1)=\sum_{i=1}^{m}l_i-m\le n-m\le n-1$.，故命题成立.

σ的互不相交循环分解

4. 补充：设 $\sigma=\sigma_1\cdots\sigma_s$.

$a\sim^\sigma b\Leftrightarrow \exists i\in\{1,2,\cdots,s\}$，

s.t a,b 落在同一个 σ_i 中

"⇒" $a\sim^\sigma b$，

$\exists r\in\mathbb{Z}$，s.t $\sigma^r(b)=a$

设 b 属于轮换 σ_i，则

$a=\sigma^r(b)=(\sigma_1\sigma_2\cdots\sigma_s)^r(b)$

$=\sigma_1^r\sigma_2^r\cdots\sigma_s^r(b)$

$=\sigma_i^r(b)$

$\Rightarrow a$ 也属于轮换 σ_i.

"⇐" 设 a,b 属于同一个轮换 σ_i，则

俏 $r\in\mathbb{Z}$，s.t $\sigma_i^r(b)=a$

$\Rightarrow a=\sigma_i^r(b)=(\sigma_1^r\cdots\sigma_s^r)(b)$

$=(\sigma_1\sigma_2\cdots\sigma_s)^r(b)=\sigma^r(b)$

$\Rightarrow a\sim b$.

补充：例

S_n 中任何置换都可以写成对换

(12)，(13)，(14)，$\cdots$，$(1,n-1)$，$(1,n)$.

的乘积，

证明：任何置换 π 皆可写成若干对换的乘积，又注意到 （自验证）

$(i,j)=(1\,i)(1\,j)(1\,i)$

$\Rightarrow$ 任意置换皆可表为 $(1,2),\cdots,(1,n)$ 的乘积

例 当 $n\ge3$ 时，证明：任何偶置换都可以写成 3-循环的乘积 （长度为3的循环）.

解：设 π 为偶置换，则存在对换 $\tau_1,\tau_2,\cdots,\tau_{2m-1},\tau_{2m}$，使得 $\pi=\tau_1\tau_2\cdots\tau_{2m-1}\tau_{2m}$

考虑相邻两个对换 $\tau_{2j-1}\tau_{2j}$，$j=1,2,\cdots,m$. 下证 $\tau_{2j-1}\tau_{2j}$ 总可以写成

3-循环乘积. 可设 $\tau_{2j-1}=(s,t)$，$\tau_{2j}=(s',t')$

① $\{s,t\}\cap\{s',t'\}\ne\emptyset$

若 $s=s'$，则 $(s,t)(s,t')=(s,t',t)$

若 $s=t'$，则 $(s,t)(s',s)=(s,s',t)$

情形 2. $\{s,t\}\cap\{s',t'\}=\emptyset$，则

$$(s,t)(s',t')=(s,t)e(s',t')=(s,t)(t,s')(t,s')(s',t').$$
$$=(t,s',s)(s',t',t).$$

由于每对 $\tau_{2j-1}\tau_j$ 都可以写成 3-循环乘积，则 π 亦可以。

扩展的辗转相除法

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 $um+vn=g$. Bezout 关系式

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) $q_i:=quo(r_{i-2},r_{i-1})$; $r_i:=rem(r_{i-2},r_{i-1})$.
   (c) $\boxed{u_i:=u_{i-2}-q_iu_{i-1};}$ $\boxed{v_i:=v_{i-2}-q_iv_{i-1};}$
   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;

注：
$\mathrm{lcm}(m,n)\gcd(m,n)=mn$.

例 利用扩展欧几里得算法求 161 和 253 的 gcd 和 lcm，且计算 $u,v\in\mathbb{Z}$，s.t $161u+253v=\gcd(161,253)$

解：$r_0:=253$，$r_1:=161$

$u_0=1$, $v_0=0$, $u_1=0$, $v_1=1$
$q_2=quo(r_0,r_1)=1$
$r_2=rem(r_0,r_1)=92.$
$u_2=u_0-q_2u_1=1-1\cdot 0=1$
$v_2=v_0-q_2v_1=0-1\cdot1=-1$
$q_3=quo(r_1,r_2)=1$
$r_3=rem(r_1,r_2)=69$
$u_3=u_1-q_3u_2=0-1\cdot1=-1$
$v_3=v_1-q_3v_2=1-1\cdot(-1)=2$
$q_4:=quo(r_2,r_3)=1$
$r_4=rem(r_2,r_3).=rem(92,69)=23$
$u_4=u_2-q_4u_3=1-1\cdot(-1)=2$
$v_4=v_2-q_4v_3=-1-1\cdot2=-3$
$r_5=rem(r_3,r_4)=0$

$\Rightarrow \gcd(253,161)=r_4=23.$
$u=u_4=2,$
$v=v_4=-3.$

$$\mathrm{lcm}(161,253)=\frac{253\times161}{23}.$$
$=253\times 7$
$=1771$

设 $a,b,c\in\mathbb{Z}$，a,b不全为0，求方程 $ax+by=c$ 的整数解.

解：设 $g=\gcd(a,b)$，$a'=\frac{a}{g}$，$b'=\frac{b}{g}$，则 $\gcd(a',b')=1$.

①若 $g\nmid c$，则方程无整数解.

②若 $g\mid c$，设 $c'=\frac{c}{g}$，则方程化为 $a'x+b'y=c'$

由 Bezout 定理式，$\exists\, u,v\in\mathbb{Z}$，s.t. $a'u+b'v=1$.

注：$(m,n$不全为0$)$，m,n互素 $\Leftrightarrow \exists\, u,v\in\mathbb{Z}$，s.t. $um+vn=1$.

$\Rightarrow a'uc'+b'vc'=c'$

$\Rightarrow \begin{cases} x_0=uc' \\ y_0=vc' \end{cases}$ 是方程的一组整数解

设 $(\tilde{x},\tilde{y})$ 是方程另一组整数解，即 $a'\tilde{x}+b'\tilde{y}=c'=a'x_0+b'y_0$

$\Rightarrow a'(\tilde{x}-x_0)=b'(y_0-\tilde{y})$

$\Rightarrow a'\mid b'(y_0-\tilde{y})$，

$\Rightarrow a'\mid y_0-\tilde{y}$ $(\because \gcd(a',b')=1)$.

同理 $b'\mid \tilde{x}-x_0$.

故可设 $\begin{cases} \tilde{y}=y_0-ka' \\ \tilde{x}=x_0+kb' \end{cases}$ (1)，$k\in\mathbb{Z}$.

经验证，(1)确为 $ax+by=c$ 的一组解.

$\Rightarrow \begin{cases} x=u\frac{c}{g}+k\frac{b}{g} \\ y=v\frac{c}{g}-k\frac{a}{g} \end{cases}$ $(k\in\mathbb{Z})$ 为方程的全部整数解.

gcd的一些性质.

$a,b,m,r\in\mathbb{Z}^+$. 证明：若 $b=am+r$，则 $\gcd(a,b)=\gcd(a,r)$.

解：方法一：令 $g_1=\gcd(a,b)$，$g_2=\gcd(a,r)$. 下证 $g_1=g_2$.

$g_1\mid a$，$g_1\mid b \Rightarrow g_1\mid b-am$，即 $g_1\mid r$

$\Rightarrow g_1$是a,r的公因子.

$\Rightarrow g_1\mid g_2$.

$g_2\mid a$，$g_2\mid r \Rightarrow g_2\mid am+r \Rightarrow g_2\mid b$.

$\Rightarrow g_2$是a,b的公因子 $\Rightarrow g_2\mid g_1$

$\Rightarrow g_1=g_2$.

(i) $\gcd(ma, mb) = m\gcd(a,b)$，$\forall n \in \mathbb{Z}^+$

(ii) 若 $\gcd(a,b)=1$，则 $\gcd(ab,m) = \gcd(a,m)\gcd(b,m)$，$\forall m \in \mathbb{Z}^+$.

解：(i) 设 $g = \gcd(a,b)$，$a = n_1 g$，$b = n_2 g$，其中 $\gcd(n_1, n_2) = 1$.

则 $ma = n_1 m g$，$mb = n_2 m g$.

$\Rightarrow \gcd(ma, mb) = mg = m\gcd(a,b)$.

(ii) 设 $g = \gcd(ab, m)$. $g_1 = \gcd(a,m)$，$g_2 = \gcd(b,m)$. 下证 $g = g_1 g_2$.

$g_1 \mid a,\ g_2 \mid b \Rightarrow g_1 g_2 \mid ab$

$\gcd(a,b)=1 \Rightarrow \gcd(g_1, g_2) = 1$

$g_1 \mid m,\ g_2 \mid m \Rightarrow g_1 g_2 \mid m$

$\Rightarrow$ $g_1 g_2$ 是 ab, m 的公因子，

$\Rightarrow g_1 g_2 \mid g$

另一方面，由 Bezout 关系式，$\exists u_1, u_2, v_1, v_2 \in \mathbb{Z}$, s.t. $u_1 a + v_1 m = g_1$，$u_2 b + v_2 m = g_2$.

$\Rightarrow g_1 g_2 = u_1 u_2 ab + (v_1 v_2 m + u_1 v_2 a + u_2 v_1 b) m$

$g \mid m$，$g \mid ab \Rightarrow g \mid g_1 g_1$

综上，$g = g_1 g_2$.

注：① $g_1 \mid m,\ g_2 \mid m \xRightarrow{\gcd(g_1,g_2)=1} g_1 g_2 \mid m$.

例 $2 \mid 12$，$4 \mid 12$，但 $8 \nmid 12$.

② 若 $\gcd(a,b) \neq 1$，则(ii)中等式不一定成立.

例 $a=2, b=4, m=6$，$\gcd(ab, m) = \gcd(8,6) = 2$，$\gcd(a,m)\gcd(b,m) = 2 \times 2 = 4 \neq \gcd(ab, m)$.

素数

prop ① p是素数，$a, b \in \mathbb{Z}$，若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$.

② p是素数，$k < p$，$k \in \mathbb{Z}^+$，则 $p \mid \binom{p}{k}$.

利用prop2.+二项式定理，可证：(费马小定理)

若p是素数，则 $n^p \equiv n \mod p$，$\forall n \in \mathbb{Z}$

解：首先利用数学归纳法证明 $\forall n\in\mathbb{Z}^+$，有 $p\mid n^p-n$.

① $n=1$ 时，$n^p-n=0$ ✓.

② 假设命题对 n 成立，下面来看 $n+1$ 时的情况

$$(n+1)^p-(n+1)=n^p+\binom{p}{1}n^{p-1}+\cdots+\binom{p}{p-1}n+1-(n+1)$$
$$=n^p-n+\binom{p}{1}n^{p-1}+\cdots+\binom{p}{p-1}n.$$

$\underbrace{p\mid\binom{p}{1},\ \cdots,\ p\mid\binom{p}{p-1}}_{(\text{Prop }12)}$，$\underline{p\mid n^p-p}$（归纳假设）

$\Rightarrow$ $p\mid(n+1)^p-(n+1)$

由①②可得，$\forall n\in\mathbb{Z}^+$，$p\mid n^p-n$.

$n=0$ 时，$p\mid n^p-n$ 显然成立.

$n<0$ 且 $n\in\mathbb{Z}$，有 $p\mid(-n)^p-(-n)$.

① $p=2$，$(-n)^p-(-n)=n^2+n=n(n+1)$，显然 $2\mid n(n+1)$

② $p\neq 2$ $(-n)^p-(-n)=-(n^p+n)$，$p\mid -(n^p+n)$.

$p\nmid -1\Rightarrow p\mid n^p+n$.

综上，$\forall n\in\mathbb{Z}$，$p\mid n^p-n$, i.e. $n^p\equiv n \bmod p$.

线性相关性

$$\mathbb{R}^n=\left\{\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}\middle|\ x_i\in\mathbb{R}\right\}.$$

设 $\vec{x}=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$，$\vec{y}=\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$

定义 $\vec{x}+\vec{y}=\begin{pmatrix}x_1+y_1\\ \vdots\\ x_n+y_n\end{pmatrix}$，数乘：$\lambda\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}\lambda x_1\\ \lambda x_2\\ \vdots\\ \lambda x_n\end{pmatrix}$.

加法

加法满足交换律，结合律，
$\forall\vec{x},\vec{y},\vec{z}\in\mathbb{R}^n$，

$\vec{x}+\vec{y}=\vec{y}+\vec{x}$

$(\vec{x}+\vec{y})+\vec{z}=\vec{x}+(\vec{y}+\vec{z})$

$\vec{x}+\vec{0}=\vec{0}+\vec{x}$

$\vec{x}+(-\vec{x})=\vec{0}$

数乘：$\lambda(\mu\vec{x})=\lambda(\mu\vec{x})$

$1\cdot\vec{x}=\vec{x}$

$\Rightarrow$ $\lambda(\vec{x}+\vec{y})=\lambda\vec{x}+\lambda\vec{y}$

$(\lambda+\mu)\vec{x}=\lambda\vec{x}+\mu\vec{x}$.

Def (线性组合). 设 $\vec{W}, \vec{V_1}, \cdots, \vec{V_k} \in \mathbb{R}^n$，如果∃ $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$, s.t

$$\vec{W} = \alpha_1 \vec{V_1} + \cdots + \alpha_k \vec{V_k}.$$

则称 $\vec{W}$ 是 $\vec{V_1}, \cdots, \vec{V_k}$（在 $\mathbb{R}$ 上）的线性组合

问题：给定 $\vec{W}, \vec{V_1}, \cdots, \vec{V_k} \in \mathbb{R}^n$，如何判断 W 是 $\vec{V_1}, \cdots, \vec{V_k}$ 的线性组合？

解决途径：令 $B = (A|\vec{W}) \in \mathbb{R}^{n\times(k+1)}$，其中 $A = (\vec{V_1}, \cdots, V_k) \in \mathbb{R}^{n\times k}$；判断以 B 为增广矩阵的 k 元线性方程组是否相容.（利用 Gauss 消元法）

Def 设 $\vec{V_1}, \cdots, \vec{V_k} \in \mathbb{R}^n$. 如果存在 $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$，不全为 0，使得

$$\alpha_1\vec{V_1} + \cdots + \alpha_k\vec{V_k} = \vec{0}.$$

则称 $\vec{V_1}, \cdots, \vec{V_k}$（在 $\mathbb{R}$）上线性相关. 否则，称 $\vec{V_1}, \cdots, \vec{V_k}$（在 $\mathbb{R}$）上线性无关.

Prop. 设 $\vec{V_1}, \cdots, \vec{V_k} \in \mathbb{R}^n$.

① ∃ $i \in \{1, \cdots, k\}$, s.t $\vec{V_1}, \cdots, \vec{V_i}$ 线性相关，则 $\vec{V_1}, \cdots, \vec{V_i}, \cdots, \vec{V_k}$ 也线性相关. 延长不改变线性相关性.

② $\vec{V_1}, \cdots, \vec{V_i}, \cdots, \vec{V_k}$ 线性无关，则对任意 $i \in \{1, \cdots, k\}$，使得 $\vec{V_1}, \cdots, \vec{V_i}$ 也线性无关

缩短不改变线性无关性.

③ $\vec{V} \in \mathbb{R}^n$ 且 $\vec{V_1}, \cdots, \vec{V_k}$ 线性无关，则 $\vec{V}, \vec{V_1}, \cdots, \vec{V_k}$ 线性相关 $\Longleftrightarrow$ ∃! $\alpha_1, \cdots, \alpha_k \in \mathbb{R}$, s.t $\vec{V} = \alpha_1\vec{V_1} + \cdots + \alpha_k\vec{V_k}$.

例. 设 $\vec{u_1}, \vec{u_2}, \vec{u_3} \in \mathbb{R}^n$，线性无关. 判断 $\vec{u_1} - \vec{u_2}, \vec{u_2} - \vec{u_3}, \vec{u_3} - \vec{u_1}$ 线性相关性？

解：设 ∃ $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, s.t $\alpha_1(\vec{u_1} - \vec{u_2}) + \alpha_2(\vec{u_2} - \vec{u_3}) + \alpha_3(\vec{u_3} - \vec{u_1}) = 0$. (1)

$$\Rightarrow (\alpha_1 - \alpha_3)\vec{u_1} + (\alpha_2 - \alpha_1)\vec{u_2} + (\alpha_3 - \alpha_2)\vec{u_3} = \vec{0}.$$

$\vec{u_1}, \vec{u_2}, \vec{u_3}$ 线性无关 $\Rightarrow \begin{cases} \alpha_1 - \alpha_3 = 0. \\ \alpha_2 - \alpha_1 = 0. \\ \alpha_3 - \alpha_1 = 0. \end{cases} \Rightarrow \alpha_1 = \alpha_2 = \alpha_3.$

$$\begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 0 \end{pmatrix}$$

令 $\alpha_1 = \alpha_2 = \alpha_3 = 1$，满足(1).

$\Rightarrow \vec{u_1} - \vec{u_2}, \vec{u_2} - \vec{u_3}, \vec{u_3} - \vec{u_1}$ 线性相关.