群論在計數問題上之應用

關鍵字：群論、Burnside's Lemma

作者：陳柏諺、陳聖諦、廖崇澔
指導教授：卓士堯教授

壹、摘要

我們從一個既定的串珠題目出發，而後將其推廣至「容納 n 顆珠子，使用 k 種珠子」得到一條公式，再推廣此公式，使之對應到平面座標系，並研究其性質。

In the first part of the study, we tried to figure out how many different necklaces consisting in six beads can be formed by using five different kinds of beads considering rotation and reflection. We then explored the question by using n beads and k kinds of beads, which actually gives a formula. Extending the domain of the formula, we researched further into its properties.

貳、題目

給定兩自然數 n、k 表於一可串入 n 個珠子的環中，以 k 種相異種類的珠子進行排列。若旋轉或翻轉後相同視為同種樣式，試求此環所有可能之樣式數。

參、研究動機

某次討論時，教授提到了一個這樣的題目："Considering rotation and reflection, how many different necklaces consisting of six beads can be formed by using five different kinds of beads?"，我們嘗試使用高中數學排列組合的方法來解決這個問題，但是卻發現過程十分繁雜。於是教授便教授我們將群論運用在計數問題上的方法，讓我們成功解決這道題目，然而這樣的方法只能在珠子個數、種類數都是常數的時候使用。這讓我們十分好奇，如果珠子個數、種類都是變數的話，那麼將會有什麼一般化的公式能解決此問題呢？於是我們便決定展開一連串的研究以推廣這個運用群論解決組合問題的方法。

肆、定義及先備知識

一、群 *Group*

(一)群由一個集合及一個二元運算所組成。

(二)群具有以下性質：

1. 具有單位元素。
2. 對於每一元素，皆存在反元素。
3. 運算具有封閉性。
4. 運算具有結合律。

(三)若一群 G 包含 n 個元素，則稱其階(*Order*)$|G| = n$。

(四)舉例

1. 整數加法群 $(\mathbb{Z}, +)$

由整數集合及加法運算所構成的群。以下說明整數加法群，滿足群的所有條件：

(1) $\forall z \in \mathbb{Z}\ 0 + z = z + 0 = z$，故0為其單位元素。

(2) $\forall z \in \mathbb{Z}\ z + (-z) = (-z) + z = 0$，故對於集合中的每一元素，皆存在反元素。

(3) $\forall z_1, z_2 \in \mathbb{Z}\ \exists\ z_3 \in \mathbb{Z}\ s.t.\ z_1 + z_2 = z_3$，故整數加法運算具有封閉性。

(4) $\forall z_1, z_2, z_3 \in \mathbb{Z}\ z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$，故整數加法運算具有結合律。

2. 二面體群 *Dihedral group*

一正 n 邊形在平面上所有能夠使得原形狀不改變之旋轉及翻轉所構成的群，以 D_n 表示。

以 D_4 為例，D_4 以正方形之旋轉及翻轉構成，可表示為 $D_4 = \{1, \rho^1, \rho^2, \rho^3, \tau_1, \tau_2, \tau_3, \tau_4\}$。其中，$\rho$ 為逆時針旋轉 $\frac{\pi}{2}$，τ_1、τ_2、τ_3、τ_4 分別為以正方形四條相異的對稱軸翻轉。

二、群作用 *Group action*

令 X 為一集合，G 為一個群，則 G 在 X 的(左)群作用是一個映射 $*: G * X \to X$，且滿足：

(一) $\forall x \in X\ 1 * x = x$

(二) $\forall g_1, g_2 \in G\ \forall x \in X\ g_1 * (g_2 * x) = (g_1 * g_2) * x$

若 G 在 X 上作用，則稱 X 為一個 G-*set*。

三、*Stabilizer and orbit*

令 X 為一個 G-*set*，$x \in X$。

(一)定義 x 的 *Stabilizer* 為 $S(x) = \{a \in G \mid a * x = x\}$。

(二)定義 x 的 *Orbit* 為 $G * x = \{g * x \mid g \in G\}$。

Orbit-stabilizer 定理：若 X 是一個 *G-set*，則集合 X 可被所有 G 作用於 X 上的相異 *Orbits* 所分割，且有 $|S(x)| \cdot |G * x| = |G|$。

對於 $g \in G$，定義 $F(g) = \{x \in X \mid g * x = x\}$。

四、*Burnside's lemma*

若 n 為「群 G 作用於一 *G-set* 上之相異 *Orbits* 的數量」，則可求得：

$$n = \frac{1}{|G|}\sum_{g\in G}|F(g)|$$

證明：

令 G 為一群，X 為一 *G-set*。

令集合 $Y = \{(g,x) \in G * X \mid g * x = x\} \subseteq G * X$，則 $|Y| = \sum_{g\in G}|F(g)| = \sum_{x\in X}|S(x)|$。

若 $O_1, O_2, \cdots, O_n$ 是由 G 於 X 作用所分割出的 n 個相異 *Orbits*，則

$$\sum_{x\in X}|S(x)| = \sum_{i=1}^{n}\sum_{x\in O_i}|S(x)| = \sum_{i=1}^{n}\sum_{x\in O_i}\frac{|G|}{|G * x|} = \sum_{i=1}^{n}\sum_{x\in O_i}\frac{|G|}{|O_i|} = \sum_{i=1}^{n}\frac{|G|}{|O_i|} \times |O_i| = \sum_{i=1}^{n}|G| = |G| \times n$$

所以有

$$\sum_{g\in G}|F(g)| = \sum_{x\in X}|S(x)| = |G| \times n$$

故

$$n = \frac{1}{|G|}\sum_{g\in G}|F(g)| \blacksquare$$

五、*Euler's phi function*

對於一正整數 n，定義 $\varphi(n)$是小於或等於 n 中，與 n 互質的正整數數目。注意到其為積性函數，對於兩互質自然數 a、b，有 $\varphi(ab) = \varphi(a) \times \varphi(b)$。

(一)數值

若 n 可被質因數分解為 $n = {p_1}^{q_1} \times {p_2}^{q_2} \times \cdots \times {p_r}^{q_r}$，

$$\varphi(n) = n\prod_{i=1}^{r}\frac{p_i - 1}{p_i}$$

(二)性質

1. $\sum_{d|n}\varphi(d) = n$
2. $\varphi(2n) = \begin{cases} 2\varphi(n), & 2 \mid n \\ \varphi(n), & 2 \nmid n \end{cases}$

六、*Notations*

n：項鍊中珠子的數量。

k：項鍊中珠子的種類數。

ρ：為逆時鐘旋轉 $\frac{2\pi}{n}$，ρ^i即旋轉 i 次。

τ_i：以 n 邊形的某條對稱軸為軸翻轉。注意到 $\forall\tau_i\ \exists j \in \mathbb{N}\ s.t.\ \rho^j\tau_0 = \tau_i$，其中 τ_0 是以 n 邊形的中軸翻轉。

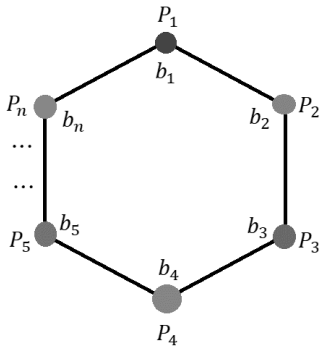
P_i：環形串珠中，編號 i 的珠子放置點。

b_i：位於P_i的珠子種類。

$\mathcal{A}(n,k)$：在一個可串入 n 個珠子的環中，以 k 種相異種類且數量足夠的珠子進行排列，考慮旋轉及翻轉，將此環所有可能之樣式數以 $\mathcal{A}(n,k)$ 表示。

伍、研究過程

若我們共有 k 種珠子，對於由 n 個珠子所構成的環型串珠 $P_1P_2\cdots P_n$，我們以右圖表示此串珠的排列方式（在此尚不考慮旋轉或翻轉）。



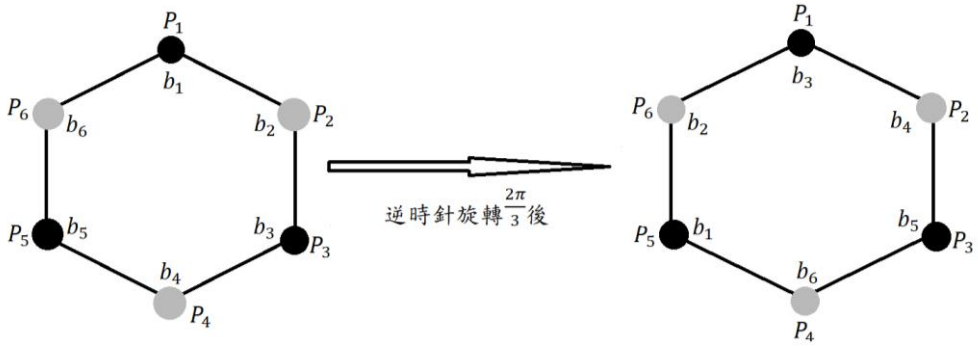
其中 $b_1, b_2, \cdots, b_n$ 皆為小於等於 k 之正整數，依序代表 $P_1, P_2, \cdots, P_n$ 各個頂點上所使用的珠子種類。任何依此方式構造的數列 $\langle b_i\rangle_{i=1}^{n}$ 皆可表示一種獨特的串珠排列方式。定義集合 $B_n = \{\langle b_i\rangle_{i=1}^{n} | b_i \in \mathbb{N}, b_i \in [1,k]\}$，則 B_n 可表示串珠在不考慮旋轉及翻轉下，所有排列方式的集合。顯然 $|B_n| = k^n$。

現在考慮所有可能的旋轉及翻轉，可以用一個二面體群 $D_n = \{1, \rho, \rho^2, \cdots\cdots, \rho^{n-1}, \tau_1, \tau_2, \ldots, \tau_n\}$ 表示此串珠所有可能的旋轉或翻轉，其中 ρ 表示將此 n 邊形逆時針旋轉 $\frac{2\pi}{n}$，$\tau_1, \tau_2, \cdots, \tau_n$ 分別表示將此 n 邊形以 n 條相異對稱軸進行翻轉。考慮 D_n 在集合 B_n 上的群作用，所求之樣式數 $\mathcal{A}(n,k)$ 即為集合 B_n 被 D_n 所分割出 *Orbits* 數量的總和。

由 *Burnside's lemma*，有 $\mathcal{A}(n,k) = \frac{1}{|D_n|}\sum_{g\in D_n}|F(g)|$。

以 $n=6$、ρ^2 為例，$B_6 = \{\langle b_i\rangle_{i=1}^{6} \big| b_i \in \mathbb{N}, b_i \in [1,k]\}$。對於任意 $x \in B_6$，若 x 滿足 $\rho^2 * x = x$，亦即 x 逆旋轉 $\frac{2\pi}{3}$ 後，各點 $P_1, P_2, \cdots, P_6$ 上的珠子種類沒有改變（即串珠排列方式相同），則 $x \in F(\rho^2)$。

如下圖所示，操作後可得知若旋轉前後串珠排列方式相同，則旋轉前 P_1, P_3, P_5 上的珠子種類必須相同，P_2, P_4, P_6 上的珠子種類也必須相同。若珠子種類有 k 種，$|F(\rho^2)| = k^2$。



以此類推，則若要計算 $n=6$，$k=5$ 的串珠樣式數，需考慮二面體群 $D_6 = \{1, \rho^1, \rho^2, \rho^3, \rho^4, \rho^5, \tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6\}$ 在 B_6 上的群作用構造出的所有相異 *Orbits*，亦即 $\mathcal{A}(6,5) = \frac{1}{12}[|F(1)| + |F(\rho^1)| + |F(\rho^2)| + |F(\rho^3)| + |F(\rho^4)| + |F(\rho^5)| + |F(\tau_1)| + |F(\tau_2)| + |F(\tau_3)| + |F(\tau_4)| + |F(\tau_5)| + |F(\tau_6)|]$。在此先將 τ_1、τ_2、τ_3 分別定義為以六邊形串珠過兩頂點的相異對稱軸進行翻轉，τ_4、τ_5、τ_6 分別定義為以六邊形串珠過兩對邊中點的相異對稱軸進行翻轉。則由前述的例子，我們可計算出：

$$\begin{cases} |F(1)| = k^n = 15625 \\ |F(\rho^1)| = |F(\rho^5)| = k^1 = 5 \\ |F(\rho^2)| = |F(\rho^4)| = k^2 = 25 \\ |F(\rho^3)| = k^3 = 125 \\ |F(\tau_1)| = |F(\tau_2)| = |F(\tau_3)| = k^4 = 625 \\ |F(\tau_4)| = |F(\tau_5)| = |F(\tau_6)| = k^3 = 125 \end{cases}$$

故 $\mathcal{A}(6,5) = (15625 + 5 + 25 + 125 + 25 + 5 + 625 \times 3 + 125 \times 3) \div 12$

$= 18060 \div 12 = 1505$

在可串入六顆串珠的環中，若使用五種珠子總共有 1505 種方法。

接著考慮 n 與 k 皆為變數的情況。

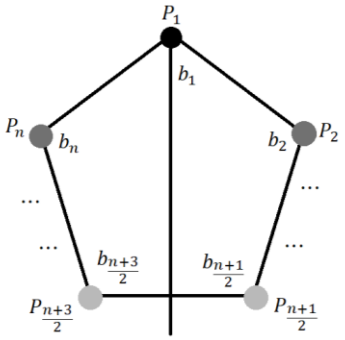
一、考慮串珠之翻轉

（一）n 為奇數

若 $2 \nmid n$，則此正 n 邊形的 n 條對稱軸各為一個頂點的角平分線，令 τ_i 是以 $\angle P_i$ 之角平分線為軸所進行的翻轉$(i = 1, 2, 3, \cdots, n)$。以 τ_1 為例，如右圖所示：

若以此為對稱軸翻轉後串珠排列方式相同，可得：

$$\begin{cases} b_1 = b_1 \\ b_2 = b_n \\ b_3 = b_{n-1} \\ \vdots \\ b_{\frac{n-1}{2}} = b_{\frac{n+5}{2}} \\ b_{\frac{n+1}{2}} = b_{\frac{n+3}{2}} \end{cases}$$



顯然$|F(\tau_i)| = k^{\frac{n+1}{2}}$，$i = 1,2,\cdots,n$。

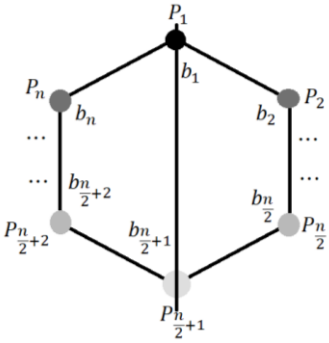
(二) n 為偶數

1. 以對角線為對稱軸

若 $2 \mid n$，則此正 n 邊形的 n 條對稱軸中有 $\frac{n}{2}$ 條過 2 個頂點，令 τ_i 是以$\overleftrightarrow{P_iP_{i+\frac{n}{2}}}$為軸所進行的翻轉$(i = 1,2,3,\cdots,\frac{n}{2})$。以 τ_1 為例，如右圖所示：

若以此為對稱軸翻轉後串珠排列方式相同，可得：

$$\begin{cases} b_1 = b_1 \\ b_2 = b_n \\ b_3 = b_{n-1} \\ \vdots \\ b_{\frac{n}{2}} = b_{\frac{n}{2}+2} \\ b_{\frac{n}{2}+1} = b_{\frac{n}{2}+1} \end{cases}$$



顯然$|F(\tau_i)| = k^{\frac{n}{2}+1}$，$i = 1,2,3,\cdots,\frac{n}{2}$。

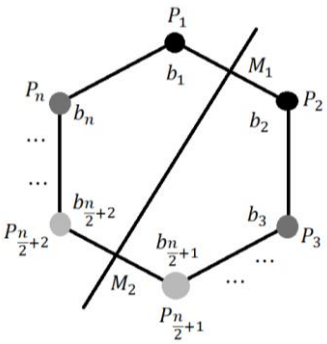
當 n 為偶數，以對角線為軸時，$\sum_{i=1}^{n/2}|F(\tau_i)| = \frac{n}{2}k^{\frac{n}{2}+1}$。

2. 以中線為對稱軸

另外 $\frac{n}{2}$ 條對稱軸經過 2 個對邊，令 M_j 為 $\overline{P_jP_{j+1}}$ 的中點$(j = 1,2,\cdots,n-1)$，M_n 為 $\overline{P_nP_1}$ 的中點，令 τ_i 是以 $\overleftrightarrow{M_{i-\frac{n}{2}}M_i}$ 為軸所進行的翻轉$(i = \frac{n}{2}+1,\frac{n}{2}+2,\cdots,n)$。以 τ_n 為例，如下頁圖片所示：

若以此對稱軸翻轉後串珠排列方式相同，可得：

$$\begin{cases} b_1 = b_n \\ b_2 = b_{n-1} \\ b_3 = b_{n-2} \\ \vdots \\ b_{\frac{n}{2}-1} = b_{\frac{n}{2}+2} \\ b_{\frac{n}{2}} = b_{\frac{n}{2}+1} \end{cases}$$



顯然$|F(\tau_i)| = k^{\frac{n}{2}}$，$i = \frac{n}{2}+1,\frac{n}{2}+2,\cdots,n$。

當 n 為偶數，以中線為軸時，$\sum_{i=\frac{n}{2}+1}^{n}|F(\tau_i)| = \frac{n}{2}k^{\frac{n}{2}}$。

(三)小結

1. 當 n 為奇數時，$\sum_{i=1}^{n}|F(\tau_i)| = nk^{\frac{n+1}{2}}$。

2. 當 n 為偶數時，$\sum_{i=1}^{n}|F(\tau_i)| = \frac{n}{2}(1+k)k^{\frac{n}{2}}$。

二、考慮串珠之旋轉

(一)引理 I

令 $a,i,n \in \mathbb{Z}$，$d = gcd(i,n)$，則

x 的同餘方程式 $i \cdot x \equiv a(mod\ n)$ 有整數解 $\Leftrightarrow d \mid a$

1. 證明

(⇐)： $\because d = gcd(i,n)$

$\therefore \exists\, x_0, y_0 \in \mathbb{Z}\ \text{s.t.}\ d = ix_0 + ny_0$

$\therefore \exists\, \ell \in \mathbb{Z}\ \text{s.t.}\ a = \ell d = \ell(ix_0 + ny_0)$

$\Rightarrow n(-y_0\ell) + a = (\ell x_0)\, i$

$\Rightarrow i\ (\ell x_0) \equiv a\ (mod\ n)$■

(⇒)： $\because i \cdot x \equiv a\ (mod\ n)$ 有整數解

$\therefore \exists\, x, y \in \mathbb{Z}\ \text{s.t.}\ ix = ny + a$

$\Rightarrow a = ix - ny$

$\because d = gcd(i,n)\ \therefore d \mid i, d \mid n$

$\Rightarrow d \mid ix - ny$

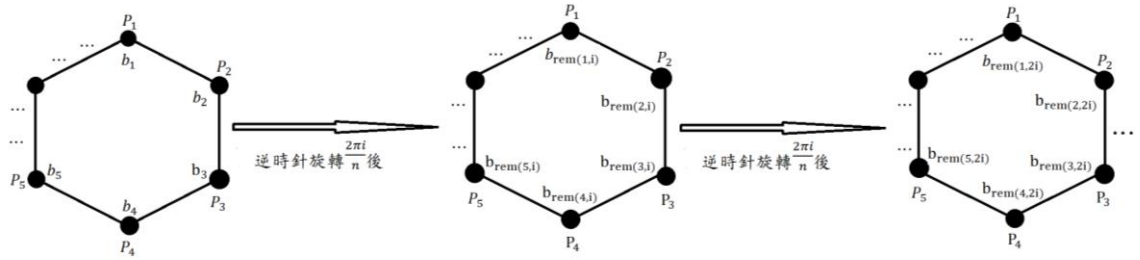
$\Rightarrow d \mid a$ ■

2. 推論

令 $d = gcd(n,i)$，$rem_n(p_1 + p_2) = (p_1 + p_2) \div n$ 之餘數。

因為在被 ρ^i 作用後，各點上的珠子種類沒有改變（如下圖所示），所以：

$$\begin{cases} b_1 = b_{rem_n(1+i)} = b_{rem_n(1+2i)} = b_{rem_n(1+3i)} = \cdots \\ b_2 = b_{rem_n(2+i)} = b_{rem_n(2+2i)} = b_{rem_n(2+3i)} = \cdots \\ \vdots \\ b_d = b_{rem_n(d+i)} = b_{rem_n(d+2i)} = b_{rem_n(d+3i)} = \cdots \end{cases}$$



由引理 I 可得所有 i 的倍數除以 n 所得的餘數集合便是所有小於 n 的 d 的倍數所構成的集合，故：

$$\begin{cases} 1, rem_n(1+i), rem_n(1+2i), rem_n(1+3i) \cdots \in \{1, d+1, 2d+1, \cdots, n-d+1\} \\ 2, rem_n(2+i), rem_n(2+2i), rem_n(2+3i) \cdots \in \{2, d+2, 2d+2, \cdots, n-d+2\} \\ \vdots \\ d, rem_n(d+i), rem_n(d+2i), rem_n(d+3i) \cdots \in \{d, 2d, 3d, \cdots, n\} \end{cases}$$

故

$$\begin{cases} b_1 = b_{d+1} = b_{2d+1} = \cdots = b_{n-d+1} \\ b_2 = b_{d+2} = b_{2d+2} = \cdots = b_{n-d+2} \\ \vdots \\ b_d = b_{2d} = b_{3d} = \cdots = b_n \end{cases}$$

$\therefore \left|F(\rho^i)\right| = k^d = k^{\gcd(n,i)}$

(二)引理 II

設 d 為正整數 n 的正因數，$i \in \{1, 2, \cdots, n\}$，則恰有 $\varphi(\frac{n}{d})$ 個 i 值滿足 $gcd(n,i) = d$。

1. 證明

若 $gcd(n,i) = d$，則 i 為 d 的倍數且 $\frac{n}{d}$ 與 $\frac{i}{d}$ 互質，亦即 $i \in \left\{d, 2d, \cdots, \left(\frac{n}{d}\right)d\right\}$ 且 $gcd\left(\frac{n}{d}, \frac{i}{d}\right) = 1$。因為 $\frac{i}{d} \in \left\{1, 2, \cdots, \frac{n}{d}\right\}$，而在此 $\frac{n}{d}$ 個正整數中有 $\varphi\left(\frac{n}{d}\right)$ 個數與 $\frac{n}{d}$ 互質，故恰有 $\varphi\left(\frac{n}{d}\right)$ 個 i 值滿足 $gcd(n,i) = d$。

2. 推論

由引理 II 可推得，對於所有 n 的正因數 d，皆存在 $\varphi\left(\frac{n}{d}\right)$ 個小於等於 n 的正整數使 $k^{gcd(n,i)} = k^d$，所以：

$$\sum_{i=0}^{n-1}\left|F(\rho^i)\right| = \sum_{i=1}^{n}\left|F(\rho^i)\right| = \sum_{i=1}^{n} k^{\gcd(n,i)} = \sum_{d|n}\varphi\left(\frac{n}{d}\right)k^d$$

三、總結

綜合以上，則對於 $n \in \mathbb{N}$，$k \in \mathbb{N}$，

$$\mathcal{A}(n,k) = \frac{1}{|D_n|}\sum_{g\in D_n}|F(g)| = \frac{1}{2n}\left[\sum_{i=0}^{n-1}\left|F(\rho^i)\right| + \sum_{i=1}^{n}|F(\tau_i)|\right]$$

$$= \begin{cases} \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n}}\varphi\left(\frac{n}{d}\right)k^d + \frac{n}{2}(1+k)k^{\frac{n}{2}}\right], & 2 \mid n \\ \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n}}\varphi\left(\frac{n}{d}\right)k^d + nk^{\frac{n+1}{2}}\right], & 2 \nmid n \end{cases}$$

陸、討論

一、定義

給定一正整數 n，對於 $\mathcal{A}(n,x)$ 可得一 x 的多項式。現若將 n 的定義域擴展至任意非 0 整數，x 的定義域擴展至任意實數，我們可以將 $\mathcal{A}(n,x)$ 重新定義並表示為以下連續函數：

$$y = a_n(x) = \begin{cases} \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)x^d + \frac{n}{2}(1+x)x^{\frac{n}{2}}\right], & 2 \mid n \\ \dfrac{1}{2n}\left[\displaystyle\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)x^d + nx^{\frac{n+1}{2}}\right], & 2 \nmid n \end{cases}$$

注意到當 $n < 0$ 時，$d < 0$。

二、性質

進一步觀察，$y = a_n(x)$ 具有以下性質：

（一）$\forall n > 0$，$a_n(0) = 0$。

（二）$a_n(1)$ 有兩種情形：

1. 當 $n > 0$，$a_n(1) = 1$。

證明：

因為 $\varphi(n)$ 有 $\sum_{d|n}\varphi(d) = n$。

故當 $n > 0$ 且 $2 \mid n$ 時，

$$a_n(1) = \frac{1}{2n}\left[\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)(1)^d + \frac{n}{2}(2)(1)^{\frac{n}{2}}\right] = \frac{1}{2n}(n+n) = 1$$

當 $n > 0$ 且 $2 \nmid n$ 時，

$$a_n(1) = \frac{1}{2n}\left[\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)(1)^d + n(1)^{\frac{n+1}{2}}\right] = \frac{1}{2n}(n+n) = 1$$

故得證。

2. 當 $n < 0$，$a_n(1) = 0$。

證明：

因為 $\varphi(n)$ 有 $\sum_{d|n}\varphi(d) = n$。

故當 $n < 0$ 且 $2 \mid n$ 時，

$$a_n(1) = \frac{1}{2n}\left[\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)(1)^d + \frac{n}{2}(2)(1)^{\frac{n}{2}}\right] = \frac{1}{2n}(-n+n) = 1$$

當 $n < 0$ 且 $2 \nmid n$ 時，

$$a_n(1) = \frac{1}{2n}\left[\sum_{d|\mathrm{n},dn>0}\varphi\left(\frac{n}{d}\right)(1)^d + n(1)^{\frac{n+1}{2}}\right] = \frac{1}{2n}(-n+n) = 1$$

故得證。

(三) $a_n(-1)$ 有五種情形：

1. 當 $2 \mid n$，$a_n(-1) = 0$。

證明：

若兩自然數 a, b 互質，有 $\varphi(ab) = \varphi(a) \times \varphi(b)$。

因為 $2 \mid n$，n 可被質因數分解為 $n = 2^{q_0} \times {p_1}^{q_1} \times {p_2}^{q_2} \times \cdots \times {p_r}^{q_r}$，其中對於所有 $i < r$ 的正整數，p_i 為 2 以外的質數。

令一 n 的因數 $d = 2^{m_0} \times {p_1}^{m_1} \times {p_2}^{m_2} \times \cdots \times {p_r}^{m_r}$，其中對於所有 $i < r$ 的正整數，$m_i < q_i$。令 $p_0 = 2$。

當 $m_0 > 0$，

$$\varphi\left(\frac{n}{d}\right)(-1)^d = \varphi\left(\prod_{i=0}^{r} {p_i}^{q_i - m_i}\right)(-1)^{2^{m_0} \times {p_1}^{m_1} \times {p_2}^{m_2} \times \cdots \times {p_r}^{m_r}}$$
$$= \varphi(2^{q_0 - m_0} \times {p_1}^{q_1 - m_1} \times {p_2}^{q_2 - m_2} \times \cdots \times {p_r}^{q_r - m_r})$$

當 $m_0 = 0$，

$$\varphi\left(\frac{n}{d}\right)(-1)^d = \varphi\left(\prod_{i=0}^{r} {p_i}^{q_i - m_i}\right)(-1)^{{p_1}^{m_1} \times {p_2}^{m_2} \times \cdots \times {p_r}^{m_r}}$$
$$= -\varphi(2^{q_0} \times {p_1}^{q_1 - m_1} \times {p_2}^{q_2 - m_2} \times \cdots \times {p_r}^{q_r - m_r})$$

又 $\varphi(2n) = \begin{cases} 2\varphi(n), & 2 \mid n \\ \varphi(n), & 2 \nmid n \end{cases}$，因此

$$\sum_{d \mid n, dn > 0} \varphi\left(\frac{n}{d}\right)(-1)^d$$
$$= [(\varphi(1) + \varphi(2) + \cdots + \varphi(2^{q_0 - 1}) - \varphi(2^{q_0})] \prod_{i=1}^{r} \left(\sum_{j=1}^{q_i - m_i} \varphi({p_i}^j) \right)$$
$$= [(1 + 2^0 + 2^1 + \cdots + 2^{q_0 - 2} - 2^{q_0 - 1}] \prod_{i=1}^{r} \left(\sum_{j=1}^{q_i - m_i} \varphi({p_i}^j) \right) = 0$$

∴ 若 $2 \mid n$，

$$a_n(-1) = \frac{1}{2n}\left[\sum_{d \mid n, dn > 0} \varphi\left(\frac{n}{d}\right)(-1)^d + \frac{n}{2}(0)(-1)^{\frac{n}{2}} \right] = \frac{0 + 0}{2n} = 0$$

故得證。

2. 當 $n \equiv 1 \ (mod\ 4)$時，若 $n > 0$，$a_n(-1) = -1$。

3. 當 $n \equiv 1 \ (mod\ 4)$時，若 $n < 0$，$a_n(-1) = 0$。

注意到對於情形 2、3，$y = a_n(x)$ 為奇函數。

4. 當 $n \equiv 3 \ (mod\ 4)$，$n > 0$，$a_n(-1) = 0$。

5. 當 $n \equiv 3 \ (mod\ 4)$，$n < 0$，$a_n(-1) = 1$。

證明：

因為 $\varphi(x)$ 有 $\sum_{d \mid n} \varphi(d) = n$。

當 $n \equiv 1 \ (mod\ 4)$ ，若 $n > 0$，

$$a_n(-1) = \frac{1}{2n}\left[\sum_{d \mid n, dn > 0} \varphi\left(\frac{n}{d}\right)(-1)^d + n(-1)^{\frac{n+1}{2}} \right]$$

因為 $n \equiv 1 \ (mod\ 4)$為一奇數，故 n 的因數 d 必為奇數。又 $\frac{n+1}{2}$ 為奇數，故

$$a_n(-1) = \frac{1}{2n}\left[\sum_{d \mid n, dn > 0} \varphi\left(\frac{n}{d}\right)(-1) + n(-1)^{\frac{n+1}{2}} \right] = \frac{-n - n}{2n} = -1$$

同理，若 $n < 0$，

$$a_n(-1) = \frac{1}{2n}\left[\sum_{d \mid n, dn > 0} -\varphi\left(\frac{n}{d}\right) + n(-1)^{\frac{n+1}{2}} \right] = \frac{-(-n) - n}{2n} = 0$$

又同理，當 $n \equiv 3 \ (mod\ 4)$

$$\begin{cases} \frac{1}{2n}\left[\sum_{d|n,dn>0}\varphi\left(\frac{n}{d}\right)(-1)+n(-1)^{\frac{n+1}{2}}\right]=\frac{-n+n}{2n}=0, & n>0 \\ \frac{1}{2n}\left[\sum_{d|n,dn>0}\varphi\left(\frac{n}{d}\right)(-1)+n(-1)^{\frac{n+1}{2}}\right]=\frac{n+n}{2n}=1, & n<0 \end{cases}$$

故得證。

（四）$y=a_n(x)=0$ 的解

1. 若 $2\mid n$，$n\neq 0$

$$y=a_n(x)=\frac{1}{2n}\left[\sum_{d|n}\varphi\left(\frac{n}{d}\right)x^d+\frac{n}{2}(1+x)x^{\frac{n}{2}}\right]$$

$$\text{解：}\begin{cases} n>0,\ \text{有二實數解}\ (0,0),(-1,0) \\ n=-2,-4,\ \text{有二實數解}\ (\pm1,0) \\ n\leq -6,\ \text{有三實數解}\ (\pm1,0),(\alpha,0),\alpha\in(0,1] \end{cases}$$

2. 對於 $n\equiv 1\ (mod\ 4)$

$$y=a_n(x)=\frac{1}{2n}\left[\sum_{d|n}\varphi\left(\frac{n}{d}\right)x^d+nx^{\frac{n+1}{2}}\right]$$

$$\text{解：}\begin{cases} n>0,\ \text{有一實數解}\ (0,0) \\ n=-3,\ \text{有二實數解}\ (\pm1,0) \\ n\leq -7,\ \text{有四實數解}\ (\pm1,0),(,\pm\alpha,0),\alpha\in(0,1) \end{cases}$$

3. 對於 $n\equiv 3\ (mod\ 4)$

$$y=a_n(x)=\frac{1}{2n}\left[\sum_{d|n}\varphi\left(\frac{n}{d}\right)x^d+nx^{\frac{n+1}{2}}\right]$$

$$\text{解：}\begin{cases} n>0,\ \text{有三實數解}\ (0,0),(-1,0),(\alpha,0),\alpha\in[-2,-1) \\ n=-1,\ \text{有一實數解}\ (1,0) \\ n\leq -5,\ \text{有二實數解}\ (1,0),(\alpha,0),\alpha\in(0,1) \end{cases}$$

特別的是，α 與 n 在上述各情形皆存在嚴格遞增關係。

基於以上各性質，我們推測 $a_n(x)$ 或許有特別的因式分解形式。

（五）對於大於 5 的質數 n，$a_n(x)=0$ 的複數根呈一正 $\frac{n-1}{2}$ 邊形。

說明：對於大於 2 的質數 n，有

$$a_n(x)=\frac{1}{2n}\left[x^n+(n-1)x+nx^{\frac{n+1}{2}}\right]$$

而其有一般性因式分解

$$\frac{1}{2n}\cdot x\cdot\left(x^{\frac{n-1}{2}}+1\right)\cdot\left[x^{\frac{n-1}{2}}+(n-1)\right]$$

顯然當 $n>5$ 時，$a_n(x)=0$ 之複根可形成一雙層正 $\frac{n-1}{2}$ 邊形。

三、整除

對於自然數 n，顯然在 x 為正整數時，由 Burnside's lemma，$a_n(x)$ 必然為整數。而我們發現當 x 為負整數時，$a_n(x)$ 亦為整數。以下嘗試以群論以外之觀點證明。

(一)定義

1. $a_n'(x)$

給定一正整數 n，定義

$$y=a_n'(x)=\begin{cases} \sum_{d|n}\varphi\left(\frac{n}{d}\right)x^d+\frac{n}{2}(1+x)x^{\frac{n}{2}}, & 2\mid n \\ \sum_{d|n}\varphi\left(\frac{n}{d}\right)x^d+nx^{\frac{n+1}{2}}, & 2\nmid n \end{cases}$$

2. 前項差分 Forward difference

令 $i \in \mathbb{N}$，則

(1)當 $i = 1$ 時，定義 $\Delta^i[a'_n](x) = a'_n(x+1) - a'_n(x)$。

(2)當 $i \geq 2$ 時，定義 $\Delta^i[a'_n](x) = \Delta^{i-1}[a'_n](x+1) - \Delta^{i-1}[a'_n](x)$。

注意到當 $1 \leq i \leq n$ 時，$deg(\Delta^i[a'_n](x)) = n - i$。

而當 $i > n$ 時，$\Delta^i[a'_n](x) = 0$。

(二)命題

$$\forall n \in \mathbb{N}\ \forall x \in \mathbb{Z}\ 2n \mid a'_n(x)$$

(三)證明

(1) 當 $n \geq 3$

根據性質一，$2n \mid a'_n(0) = 0$。則依歸納法，假設 $2n \mid a'_n(x)$，若 $2n \mid a'_n(x+1)$，則可證得命題為真。而其等價於 $2n \mid a'_n(x+1) - a'_n(x) = \Delta^1[a'_n](x)$。故若 $2n \mid \Delta^1[a'_n](x)$，可證得命題為真。若要證明 $2n \mid \Delta^1[a'_n](x)$，同理，必須證得 $2n \mid \Delta^1[a'_n](0)$ 且 $2n \mid \Delta^1[a'_n](x+1) - \Delta^1[a'_n](x) = \Delta^2[a'_n](x)$。

如此反覆，則若 $\forall i \in \mathbb{N} \cap [1,n]\ \forall n \in \mathbb{N}\ 2n \mid \Delta^i[a'_n](0)$ 且 $2n \mid \Delta^n[a'_n](x)$，可證得命題為真。顯然 $\Delta^n[a'_n](x)$ 為一常數函數，又根據二項式定理，有 $\Delta^n[a'_n](x) = C_1^n C_1^{n-1} \cdots C_1^1 = n!$，故 $2n$ 必然整除 $\Delta^n[a'_n](x)$。

因此若能證得 $\forall i \in \mathbb{N} \cap [1,n]\ \forall n \in \mathbb{N}\ 2n \mid \Delta^i[a'_n](0)$，即可證得命題為真。不過其仍有待進一步的證明。

(2) 對於 $n = 1$、$n = 2$

受翻轉項影響，$n = 1$、$n = 2$ 並不滿足前述 $\Delta^n[a'_n](x) = n!$ 之性質，須獨立討論。

當 $n = 1$ 時，$a_1(x) = 2x$，顯然 $\forall x \in \mathbb{Z}\ 2 \mid a_1(x)$，故得證。

當 $n = 2$ 時，$a_2(x) = 2x^2 + 2x$。已知 $4 \mid a_2(0) = 0$，又 $4 \mid \Delta^1[a_2](x) = 4x + 4$，故得證。

柒、結論

給定兩自然數 n、k 表於一可串入 n 個珠子的環中，以 k 種相異種類的珠子進行排列。若旋轉或翻轉後相同視為同種樣式，則此環所有可能之樣式數 $\mathcal{A}(n,k)$ 可以表示為：

$$\mathcal{A}(n,k) = \begin{cases} \dfrac{1}{2n}\left[\displaystyle\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) k^d + \frac{n}{2}(1+k)k^{\frac{n}{2}}\right], & 2 \mid n \\ \dfrac{1}{2n}\left[\displaystyle\sum_{d \mid n} \varphi\left(\frac{n}{d}\right) k^d + nk^{\frac{n+1}{2}}\right], & 2 \nmid n \end{cases}$$

捌、未來展望

一、更加地化簡 $\mathcal{A}(n,k)$。

二、完整證明 $2n \mid a'_n(x)$。

三、探討更多有關 $a_n(x)$ 的複數根及因式分解形式。

四、研究其他種類的環。

玖、參考資料

[1] Fraleigh, J. B. (2003). *A First Course in Abstract Algebra* (7th ed.). NJ: Pearson.

[2] Nicholson, W. K. (2012). *Introduction to Abstract Algebra* (4th ed.). NJ: John Wiley & Sons.

心得

數學確實是個神奇的存在，以嚴謹而天馬行空的思想，理直氣壯地開展出蟻穴般的世界觀。能夠抵達同樣一處的徑途太多，迂迴迤邐的求學路上，我們嘗試讓火把上的光照亮所有經過的地方，儘管總是有些角落裡岔路裡的黑並未被完全地抹上輕柔的映而依舊黯曖，繞了好多好多的圈卻也終於隱約看見前方寬闊得無所能及。

確實之必要，堅持之必要，想望之必要，數專之必要。日常裡埋怨時依然做著所厭惡之事之必要。

—陳柏諺

一開始，我認為這個題目十分的困難，在當時不管是用暴力窮舉的方式，又或者是高中教到的排列組合都難以解決這個問題，因為要考慮的因素實在是很多，所以就學習了一些更為高級的作法來解出這個問題；在這個過程中，我學習到了探就知識的精神，就是知識是沒有界限的，所以要勇於探索新的知識，還有面對困難挑戰的精神，遇到未知的挑戰時，不要放棄，只要有奮鬥不懈的意志，終有一天能克服難關。

—陳聖諦

在這次的專題研究中，我們一開始面對這個題目時毫無頭緒，不知如何下手，然而後來我們一步步擴展知識、深入鑽研，終於得到了一個令人滿意的成果。在這樣的過程中，我不僅體會到做研究時堅持不懈的奮鬥精神，更體會到了自己所知的有限與數學的無限，我們越是鑽研，越是發現仍有許多美麗的數學殿堂等待著我們進入探索，也領悟到自己所發現的結果，仍只是浩瀚無涯的數學領域中之一隅。希望未來我能持續秉持著初衷，探索那些我從未進入的數學殿堂，發掘那些美麗而永恆不朽的數學瑰寶。

—廖崇澔

教授與助教的勉勵

這次專題教給各位的群論雖然只是數學系大二代數課程的一小部分，但要學會這樣抽象的理論還是相當不容易。感覺大家都很用心在學習，吸收的狀況似乎也不錯，表現令人讚賞。藉由這次專題的機會各位得以一窺大學數學與高中數學的不同之處，如果你們其中有人覺得這樣的數學還蠻吸引人的，非常歡迎進入數學系繼續學習！

—卓士堯教授