中華民國第 55 屆中小學科學展覽會

作品說明書

高中組　數學科

第三名

040403

開關燈圖形變換

學校名稱：國立新竹高級中學

作者：	指導老師：
高二　李承駿 高二　曹立武	張世標

關鍵詞：$1_G(n)$、用 G_1 改變 G_2 、Möbius 反轉定理

摘要

我們將著名的開關燈問題轉為「給定格子數相同的圖G_1、G_2，圖中的格子為黑或白。若G_1的第 d 號格子為白，則G_2中每個編號為 d 的倍數的格子都要改變黑白狀態一次。則操作後，G_2中哪些格子為黑或白？」，稱上述操作為「用G_1改變G_2」。以此為基礎獲得了下列成果：

1. 令 H 是全黑的圖。給定圖G_2，可利用Möbius反轉定理求出G_1，使得 G_1 把 H 變成G_2。
2. 令 H 是全黑的圖。給定圖G_1，將 G_1 改變 H 得到新圖G_2，G_2又拿去改變 H 得到圖 G_3，……，如此重複操作，發現這一系列的圖會循環，為上述的1.提供不同解法。
3. 給定圖G，用G來改變G 得到G_1，又用G_1 改變G_1，……，如此重複操作，發現這一系列的圖會漸漸變黑而無法完全回復為G。
4. 將黑白兩色圖的性質推廣到質數種色並應用於密碼。

壹、研究動機

下述問題「有 100 顆全暗的燈泡,編號從 1 到 100。每個燈泡都有一個開關，按下任意編號的燈泡開關都會同時改變那些號碼為該編號倍數的燈泡的亮暗狀態。當所有編號的燈泡開關都被按一下後，哪些燈泡是亮的?」的答案廣為人知: 「亮著的燈泡號碼為完全平方數。」

我們被此饒富趣味的問題吸引。在嘗試進行了一些延伸探索後，在一個研習營的資料中看到下述發展方向：「若選定某些特定的編號，而只有在按下這些編號的燈泡開關時，才會改變那些號碼為該編號倍數的燈泡的亮暗狀態。那麼，最後哪些燈泡是亮的？反之，若先指定操作後的結果，那麼原先的特定編號為何？」，這的確令人好奇而讓我們躍躍欲試，希望不但能找出答案還能以此為起點而加以推廣或深入，於是就展開我們這個研究。

貳、研究目的

為了方便陳述，我們先列出底下的兩個定義。

定義1°：給定一組從1開始編號的燈泡，其中的燈泡有些亮、有些暗(可以全亮或全暗)。
我們乾脆就用黑格子來代表暗的燈泡、白格子來代表亮的燈泡，
因此就把這一組燈泡的亮暗狀態看成一個由黑白格子依編號排列而成的「圖」。
今若兩個圖G_1,G_2的格子數相同，我們稱下述操作:

「若G_1的第d 號燈泡是亮的，則G_2 中每個編號為d的倍數的燈泡都要改變亮暗狀態一次。」

為「用G_1 來改變G_2」，並用符號 $\hat{G}_1(G_2)$ 來表示G_2被這樣子操作後所獲得的新圖。

定義2°：符號$\boxed{0}$表示所有格子為全黑的圖。

我們的研究目的如下：

一、 釐清等式$\hat{G}_0(\boxed{0})=G_1$中的G_0和G_1如何互相推導，特別是如何從G_1反推回G_0。
(請注意，這其實相當於考慮研究動機中所提的問題：
若選定某些特定的編號，而只有在按下這些編號的燈泡開關時，
才會改變那些號碼為該編號倍數的燈泡的亮暗狀態。那麼，最後哪些燈泡是亮的？
反之，若先指定操作後的結果，那麼原先的特定編號為何？)

二、 探討當我們從給定的圖G開始，重複操作$\hat{G}(G),\hat{G}(\boxed{0}),\hat{G}(H)$(H是固定的圖)會有什麼性質。

三、 進一步的把黑白兩種顏色的研究心得推廣至質數種顏色的運算性質。

四、 將研究成果與密碼結合。

參、符號定義及預備知識

一、 圖的定義 :在我們這個研究裡，所謂的「圖」原本是指一群編號的燈泡$1,2,3,\ldots,n,\ldots$
其中每個燈泡的亮暗狀態皆已指定。但是為了表達上的方便，
我們以「白=亮，黑=暗」為原則，將燈泡轉成用格子的方式來呈現。例如
「一群編號1,2,3,4,5,6的燈泡，其中1,2,3號燈泡是亮的，4,5,6號燈泡是暗的。」
等同於
「一排編號1,2,3,4,5,6的格子，其中1,2,3號格子是白的，而4,5,6號格子是黑的。」

例1:「編號$1,2,3,\ldots,100$的格子，其中$1,2,\ldots,50$號格子是白的，而$51,52,\ldots,100$號格子是黑的。」是一個「圖」。

例2:「編號$1,2,3,\ldots$,(無限多個)的格子，其中$1,4,9,16,25,\ldots,n^2,\ldots\ldots$號格子是白的，其餘都是黑的。」也是一個「圖」。

而為了方便將兩種顏色狀態下時的性質推廣到質數種顏色，可以將原來只有黑白的兩種顏色擴增成第幾格第幾色的說法(配合參、三)，其中第幾色可以自行規定，但是要使用時必須確保使用者雙方的定義是相同的，例如: 現有一張七種顏色(紅橙黃綠藍靛紫)的圖，小明可以規定紅、橙、黃、綠、藍、靛、紫依序為第0、1、2、3、4、5、6色來使用此系統，但若小暗想以此圖形變換方式來跟小明傳遞圖片，那麼小暗就不能有任一色的規定和小明不同，像是紅為第6色就不行。

在建立此系統後，我們就改用「第幾格為第幾色」來描述一個圖，而不再使用燈泡來敘述了。

二、 $|G|$的定義:符號$|G|$表示圖G中的格子個數。(例如$|G|=18$表示G中共有18個格子，編號$1,2,3,\ldots,18$)。倘若G有無限多個格子，我們就說$|G|=\infty$。

三、 1_G的定義 給定圖G，在v種顏色的情況下，我們定義函數1_G為

$\forall 1 \le n \le |G|$，$1_G(n) = k$，若第 n 格為第 k 色(其中$0 \le k \le v-1$)。

而為了避免書寫上的重複，我們在探討2 種顏色的圖的時候一律定義:
$1_G(n) = 0$ 表示第 n 格是黑的，而$1_G(n) = 1$ 表示第 n 格是白的。

四、 若$|G_1| = |G_2|$，則下述命題顯然成立：$G_1 = G_2 \Leftrightarrow 1_{G_1} = 1_{G_2}$

這也就是說，在已知$|G|$的值的時候，我們可以用1_G來完整地描述G

五、 若圖 G 和 H 滿足$|G| = |H|$且$1_G(d_1), 1_G(d_2), 1_G(d_3), ..., 1_G(d_k), ...$都等於 1
我們以下述操作程序來定義「用 G 來改變 H」而得的圖$\hat{G}(H)$:

第一步：將 H 中編號為 d_1 的倍數的格子皆改變黑白之狀態一次；
第二步：將 H 中編號為 d_2 的倍數的格子皆改變黑白之狀態一次；
第三步：將 H 中編號為 d_3 的倍數的格子皆改變黑白之狀態一次；
⋮
第 k 步：將 H 中編號為 d_k 的倍數的格子皆改變黑白之狀態一次；
⋮

如此不斷操作，最後獲得的圖記為$\hat{G}(H)$。
例：設$|G| = |H| = \infty$，H為所有格子全黑的圖而又只有$1_G(1) = 1$，那麼$\hat{G}(H)$中每一個格子都是白的。

六、 $\boxed{1}$的定義: 代表每一個格子皆白的圖
$\boxed{0}$的定義: 代表每一個格子皆黑的圖
其中的格子個數，就等於「與其做運算的圖的格子個數」。
例如，若$|G| = 3$，則 $\hat{G}(\boxed{0})$中的$\boxed{0}$共有3個格子而這3個格子全黑。

七、 有時為了表達方便，我們會用符號$G_1 \rightleftarrows G_2$來表示$\hat{G}_1(\boxed{0}) = G_2$。
(對給定的圖 G_2，是否必有解和怎麼解出 G_1 來滿足$\hat{G}_1(\boxed{0}) = G_2$是一開始的研究主題。)

八、 在v種顏色的情況下，已知$|G_1| = |G_2|$，我們定義G_1、G_2的「**疊加**」運算：
G_1, G_2 的**疊加**$G_1 \oplus G_2$是一個圖滿足

$$1_{G_1 \oplus G_2}(n) \equiv 1_{G_1}(n) + 1_{G_2}(n) \pmod{v}，\forall 1 \le n \le |G_1| = |G_2|$$

九、為了敘述方便，對於$t \in \mathbb{N}$，我們將完全 t 次方數簡稱為完 t。

十、本研究的一組關鍵工具是 Möbius 函數及 Möbius 反轉定理(參考資料[1])，簡介如下。
定義：**Möbius 函數** $\mu(n)$ 定義為

$$\mu(n)=\begin{cases}1\ , & \text{若 } n=1\\ (-1)^r\ , & \text{若 } n \text{ 為 } r \text{ 個相異質數的乘積}\\ 0\ , & \text{其它情形}\end{cases}$$

定理(Möbius 反轉定理，參考 [1])：設F , G是定義在上ℕ的函數，則有

$$G(n)=\sum_{d\mid n}F(d)\ ,\ \forall n\in\mathbb{N}$$

$\Leftrightarrow$

$$F(n)=\sum_{d\mid n}\mu(\frac{n}{d})G(d)\ \ (=\sum_{d\mid n}\mu(d)G(\frac{n}{d})\ )\ ,\ \forall n\in\mathbb{N}$$

(其中$d\mid n$中的d為正整數)

附帶一提，因為「對於正整數n,d ，若$d\mid n$ ，則$d\le n$ 」，所以觀察上述的Möbius 反轉定理的形式可看出有下面的推論。

推論：

給定正整數k,若F和G都是定義在 {1 , 2 , 3k .的函數 則有

$$G(n)=\sum_{d\mid n}F(d)\ ,1\le n\le k$$

$\Leftrightarrow$

$$F(n)=\sum_{d\mid n}\mu(\frac{n}{d})G(d)\ =\sum_{d\mid n}\mu(d)G(\frac{n}{d})\ ,1\le n\le k$$

十一、 觀察$\hat{G}(H)$的定義可知，$\hat{G}(H)$的第 n 格的顏色只跟G, H的前 n 格的顏色有關。因此，若$|G_1|=|H_1|=m_1<m_2=|G_2|=|H_2|$且$G_1$,H_1分別為G_2 ,H_2的前 m_1 格所成的圖，則$\hat{G}_1(H_1)$就等於$\hat{G}_2(H_2)$的前m_1格所成的圖。由此可進一步知道，若$|H_1|=|K_1|=m_1<m_2=|H_2|=|K_2|$且$H_1$, K_1分別為H_2, K_2的前m_1格所成的圖，而又有$\hat{G}_1(H_1)=K_1$ ，$\hat{G}_2(H_2)=K_2$ 則 G_1 就是 G_2 的前 m_1 格所成的圖。總之，當我們把小圖擴展成大圖再進行上述運算時，原先的小圖的運算結果會原封不動地保留在大圖的相應範圍內。這給我們頗大的方便，例如我們可將對於有無限多個格子的圖的研究心得適當地運用到只有有限個格子的圖上。

肆、研究過程

原始問題:

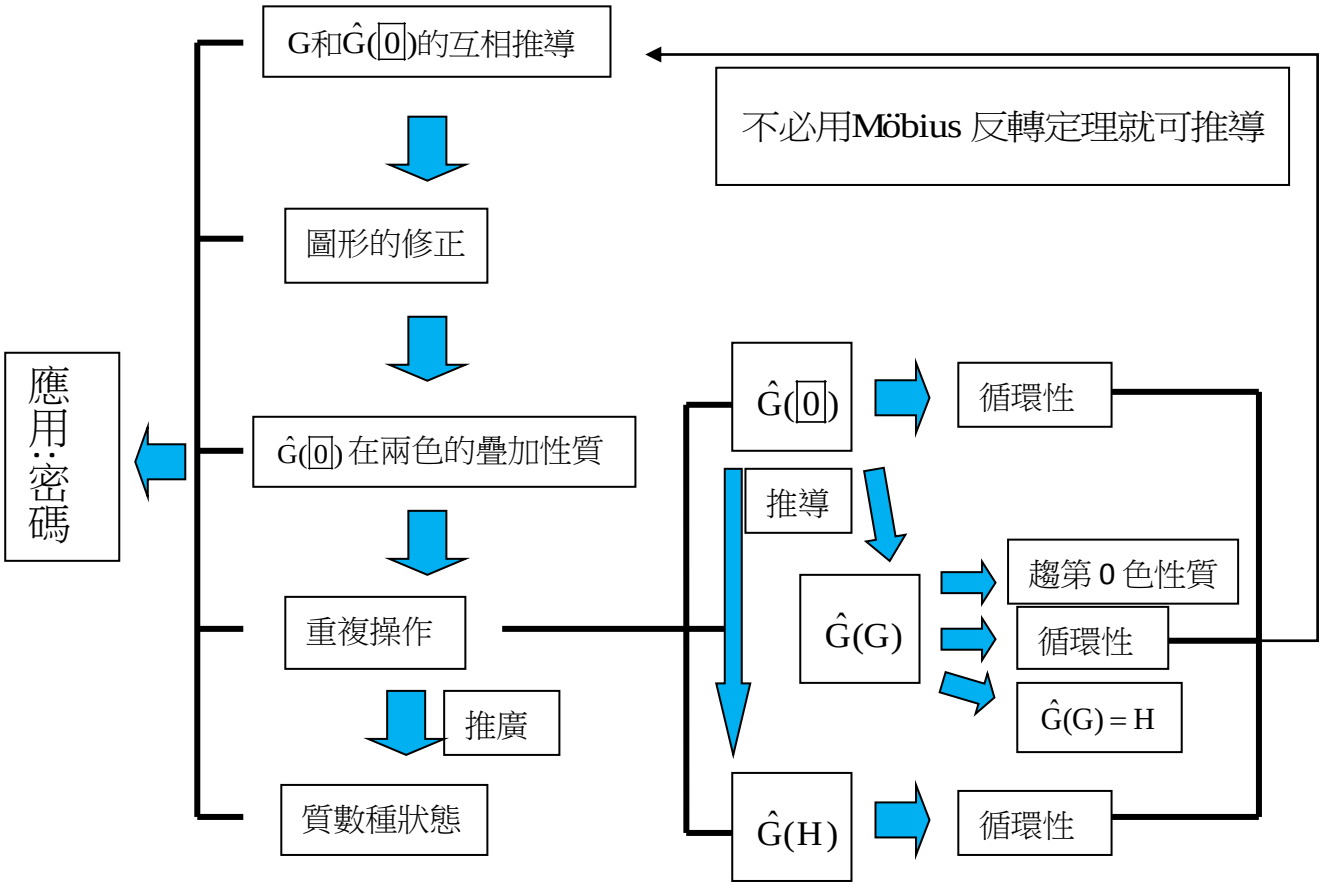
有 100 顆燈泡(目前都是暗的),編號從 1 到 100，
每個燈泡都有一個開關(一按即亮,再按即暗,再按又亮...)。
先將編號是 1 的倍數之燈泡開關都按一下，
再將編號是 2 的倍數之燈泡開關都按一下，
依此類推直到將所有編號 100 的倍數之燈泡開關都按一下。
試問最後哪些燈泡亮著?

解答:

剩下亮著的燈泡編號為完全平方數

說明:

根據原命題，只要遇到因數，就會改變一次狀態，
所以如果此燈泡編號有偶數個因數，則此燈必暗，
相反的，如果此燈泡編號有奇數個因數，則此燈必亮，
而所有數字中，符合有奇數個因數的數字只有完全平方數，
所以最後完全平方數會亮著。
根據原始問題，我們加以延伸而做了以下的探討(以流程圖表示):



一、 G 和 $\hat{G}(\boxed{0})$的互相推導 (即1_G和$1_{\hat{G}(\boxed{0})}$的互相推導)

(一)、給定G_0，如何求出 $\hat{G}_0(\boxed{0}) = G_1$

例 1:

設編號是 2 的倍數之格子都改變黑白狀態一次，則最後是白色的格子編號是哪些?

解答: 剩下是白色的格子編號為 2 的倍數

例 2:

設編號是 2 和 3 的倍數之格子分別改變黑白狀態一次,則最後白色的格子編號是哪些?

解答: 剩下白色的格子編號為 2 的倍數和 3 的倍數，但不為 6 的倍數

(二)、給定G_1，如何反求出$\hat{G}_0(\boxed{0}) = G_1$ 中的G_0

設$n \in \mathbb{N}$。由$G_1 = \hat{G}_0(\boxed{0})$的定義可知，若 d 為 n 的正因數且 d 的正因數且 $1_{G_0}(d) = 1$，則 $\boxed{0}$ 的第 n 號格子必須因為 d 而被改變狀態1次，否則就不須因為而被 d 改變狀態，所以 $\boxed{0}$ 的第 n 號格子共被改變了$\sum_{d|n} 1_{G_0}(d)$次。另外，注意到，

$\boxed{0}$ 的第 n 號格子最後變成白色 $\Leftrightarrow$ $\boxed{0}$ 的第 n 號格子共被改變了奇數次。

由以上這些分析，再加上$1_{G_1}(n)$的定義，即可得

$$1_{G_1}(n) \equiv \sum_{d \mid n} 1_{G_0}(d) \pmod 2 \qquad (1)$$

現在，我們想要由上面的(1)式著手來解出G_0。

為了方便排版，以下用函數$F(n)$表示$1_{G_1}(n)$，$f(d)$表示$1_{G_0}(d)$。

所以有以下結果:

$F(1) = f(1)$

$F(2) = f(1) + f(2)$

$F(3) = f(1) + f(3)$

$F(4) = f(1) + f(2) + f(4)$

$F(5) = f(1) + f(5)$

$F(6) = f(1) + f(2) + f(3) + f(6)$

$F(7) = f(1) + f(7)$

$F(8) = f(1) + f(2) + f(4) + f(8)$

$F(9) = f(1) + f(3) + f(9)$

$F(10) = f(1) + f(2) + f(5) + f(10)$

$F(11) = f(1) + f(11)$

$F(12) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$

接著，反求f 如何以F 表示出來:

$f(1) = F(1)$

$f(2) = F(2) - F(1)$

$f(3) = F(3) - F(1)$

$f(4) = F(4) - F(2)$

$f(5) = F(5) - F(1)$

$f(6) = F(6) - F(3) - F(2) + F(1)$

$f(7) = F(7) - F(1)$

$f(8) = F(8) - F(4)$

$f(9) = F(9) - F(3)$

$f(10) = F(10) - F(5) - F(2) + F(1)$

$f(11) = F(11) - F(1)$

$f(12) = F(12) - F(6) - F(4) + F(2)$

而我們由上觀察到，有些原本應該存在的正因數消失了，
且有些 F 前面的係數有 1 和 -1，所以我們想釐清 F 前面係數到底有何規律，
以下我們把它改寫成另一種形式:

$f(1)=F(1)$　　$f(7)=F(7)-F(\frac{7}{7})$

$f(2)=F(2)-F(\frac{2}{2})$　　$f(8)=F(8)-F(\frac{8}{2})+0F(\frac{8}{2^2})+0F(\frac{8}{2^3})$

$f(3)=F(3)-F(\frac{3}{3})$　　$f(9)=F(9)-F(\frac{9}{3})+0F(\frac{9}{3^2})$

$f(4)=F(4)-F(\frac{4}{2})+0F(\frac{4}{2^2})$　　$f(10)=F(10)-F(\frac{10}{2})-F(\frac{10}{5})+F(\frac{10}{2\times5})$

$f(5)=F(5)-F(\frac{5}{5})$　　$f(11)=F(11)-F(\frac{11}{11})$

$f(6)=F(6)-F(\frac{6}{2})-F(\frac{6}{3})+F(\frac{6}{2\times3})$　　$f(12)=F(12)-F(\frac{12}{2})-F(\frac{12}{3})+0F(\frac{12}{2^2})+F(\frac{12}{2\times3})+0F(\frac{12}{2\times3^2})$

我們觀察到，當分母的部分寫成標準分解式的形式後，
如果有質數的次方大於等於二次，那麼 F 前面的係數為 0 ;
如果是偶數個相異質數相乘，那麼 F 前面的係數為 1 ;
如果是奇數個相異質數相乘，那麼 F 前面的係數為 -1。

經過查資料後，發現這就是前面所提的Möbius反轉定理。
所以，由(1)式我們套用Möbius反轉定理，得:

$$1_{G_0}(n)\equiv\sum_{d\mid n}1_{G_1}(d)\mu(\frac{n}{d})\pmod 2 \qquad (2)$$

至於為甚麼可以在mod 2時使用Möbius反轉定理呢?這會不會影響到原公式的正確性呢?其實，我們可以由前面所列舉的F和f的運算過程發現，mod 2並不影響移項法則，故使用mod 2是沒問題的。

而我們要如何利用(2)式來將由G_1反求出G_0的問題看清楚呢?

根據 *Möbius* 函數的定義(見參 - 十)，若 $\frac{n}{d}$ 有質數平方為因數，則 $\mu(\frac{n}{d})=0$，

因此只須看 $\frac{n}{d}$ 沒有質數平方為因數的情形，即 $\frac{n}{d}=1$ 或 $\frac{n}{d}=r$ 個相異質數的乘積。

在此情形 $\mu(\frac{n}{d})=1$ 或 $\mu(\frac{n}{d})=-1$，但是 $-1\equiv1\pmod 2$，

所以 $\mu(\frac{n}{d})=1$ 和 $\mu(\frac{n}{d})=-1$ 在 mod 2 下都會得到 $\mu(\frac{n}{d})=1$。

另外，找出所有滿足此條件的 d 後，d 必須要是奇數個，

若 d 為偶數個，則在 $\sum$ 運算後，$1_{G_0}(n)\equiv0\pmod 2$，不合。

因此，我們得到以下結論:

定理一

在黑白兩色的狀態下，若$\hat{G}_0(\boxed{0})=G_1$且正整數$n\le|G_1|$，則有

「$1_{G_0}(n)=1\Leftrightarrow$ n 的正因數 d 中，形如「$1_{G_1}(d)=1$，且$\frac{n}{d}$沒有質數平方為因數」者共有奇數個

例 3：

設$1_{G_1}(n)=1 \Leftrightarrow n=k^2+1, k\in\mathbb{N}$，則$1_{G_0}(68)$是否等於1？

說明：

因為$68=1\times68=2\times34=4\times17$，其中2和17形如$k^2+1$，

又$68=2\times34$且34沒有質數平方為因數，所以2滿足條件，

又$68=17\times4$且$4=2^2$，所以17不滿足條件，

符合條件的只有1個數，為奇數個，所以$1_{G_0}(68)=1$

由上述方式可一個個推得:

$1_{G_0}(n)=1 \Leftrightarrow$ n 的正因數 d 中，滿足$d=k^2+1, k\in\mathbb{N}$,

且$\frac{n}{d}$沒有質數平方為因數者共有奇數個。

$n=2,4,5,6,10,12,14,15,17,22,25,28,30...$

接著把(1)、(2)兩式中的(mod 2)改成(mod v)就能夠加以推廣成v種顏色($v\in\mathbb{N}$)的形式：

$$1_{G_0}(n)\equiv 1_{G_1}(n)+\sum_{d|n\text{ 且 }d=r\text{個相異質數乘積}} 1_{G_1}(d)\cdot(-1)^r \pmod v$$

定理二 (在v種顏色的情況下，$v\in\mathbb{N}$)

若$\hat{G}_0(\boxed{0})=G_1$且正整數$n\le|G_1|$，則有

$$1_{G_0}(n)\equiv 1_{G_1}(n)+\sum_{d\mid n\text{ 且 }d=r\text{個相異質數乘積}} 1_{G_1}(d)\cdot(-1)^r \pmod v$$

二、 在黑白兩色的狀態下操作$\hat{G}_0(\boxed{0})=G_1$，並給定$1_{G_0}(n)$的狀態，若某些$1_{G_0}(k)$的值($k\in\mathbb{N}$)有改變，則會如何影響$1_{G_1}(n)$？

對於這個問題其實可以很直觀的看出答案，

由$1_{G_1}(n) \equiv \sum_{d \mid n} 1_{G_0}(d) \pmod 2$ 可知，

欲求出G_1的第 n 格是黑還是白的關鍵就在於

把 n 的正因數 d 的1_G函數值全部加起來再經 mod 2運算後，

得到的值如果是1，那第 n 格就是白的，

得到的值如果是0，那第 n 格就是黑的。

而如果每多讓一個$1_{G_0}(k)$的值+1，而 k 為 n 的正因數，則$1_{G_1}(n)$的值會$+1 \pmod 2$，

如果每多讓一個$1_{G_0}(k)$的值+1，而 k 不為 n 的正因數，則$1_{G_1}(n)$的值會不變，

如果每多讓一個$1_{G_0}(k)$的值-1，而 k 為 n 的正因數，則$1_{G_1}(n)$的值會$-1 \pmod 2$，

如果每多讓一個$1_{G_0}(k)$的值-1，而 k 不為 n 的正因數，則$1_{G_1}(n)$的值會不變，

又$1 \equiv -1 \pmod 2$，這表示在黑白兩色的情況下，增加一個值就等於減少這個值，

所以若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有偶數個，則$1_{G_1}(n)$不用改變黑白狀態；

若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有奇數個，則$1_{G_1}(n)$必須改變黑白狀態。

定理三

在黑白兩色的狀態下操作$\hat{G}_0(\boxed{0}) = G_1$，並給定$1_{G_0}(n)$的狀態。若某些$1_{G_0}(k)$的值$(k \in N)$有改變，

若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有偶數個，則$1_{G_1}(n)$不用改變黑白狀態；

若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有奇數個，則$1_{G_1}(n)$必須改變黑白狀態。

例4:

假設原$1_{G_0}(n)=1$的 n 中增加$23,27,33$且減少$11,12,26$，

而由G_0'操作得

$1_{G_1}(n)=1 \Leftrightarrow n=$ $11,12,22,24,26,33,34,37,43,44,45,46,47,48,52,$

$53,54,55,57,60,63,67,69,72,73,78,81,84,88,92,96$

如欲求原本應該得到的G_1，則需要觀察$11,12,23,26,27,33$此六數的倍數

根據定理二，得知原來的G_1應為

$1_{G_1}(n)=1 \Leftrightarrow n=$ $23,27,33,34,36,37,43,45,47,53,57,63,67,73,77$

上面我們已經得到了$\hat{G}_0(\boxed{0}) = G_1$中$G_0$和$G_1$互相推導的關係，

而這使我們想要進一步了解，如果有$\hat{G}_1(\boxed{0}) = H_1$、$\hat{G}_2(\boxed{0}) = H_2$這兩條關係式，

那麼G_1、G_2和H_1、H_2間有沒有什麼運算關係呢?

三、 在 v種顏色的情況下$(v \in \mathbb{N})$，若$\hat{G}_1(\boxed{0}) = H_1$且$\hat{G}_2(\boxed{0}) = H_2$，

則$G_1 \oplus G_2$和$H_1 \oplus H_2$的關係為何？

在 v色的情況下$(v\in\mathbb{N})$，令$G_1\oplus G_2=G$，$\hat{G}_1(\boxed{0})\oplus\hat{G}_2(\boxed{0})=H_1\oplus H_2=H$

因為$1_{\hat{G}(\boxed{0})}(n)=\sum_{d\mid n}1_G(d)\equiv\sum_{d\mid n}[1_{G_1}(d)+1_{G_2}(d)]$

$$\equiv\sum_{d\mid n}1_{G_1}(d)+\sum_{d\mid n}1_{G_2}(d)\equiv 1_{\hat{G}_1(\boxed{0})}(n)+1_{\hat{G}_2(\boxed{0})}(n)$$

$$\equiv 1_{\hat{G}_1(\boxed{0})\oplus\hat{G}_2(\boxed{0})}(n)\equiv 1_H(n)\pmod{v}$$

所以$\hat{G}(\boxed{0})=H\Rightarrow G\rightleftarrows H$

$\Rightarrow G_1\oplus G_2\rightleftarrows\hat{G}_1(\boxed{0})\oplus\hat{G}_2(\boxed{0})$

$\Rightarrow G_1\oplus G_2\rightleftarrows H_1\oplus H_2$

根據上述之推論，得知$G_1\oplus G_2\rightleftarrows H_1\oplus H_2$

定理四 (在 v 種顏色的情況下，$v\in\mathbb{N}$)

若$\hat{G}_1(\boxed{0})=H_1$且$\hat{G}_2(\boxed{0})=H_2$，則$G_1\oplus G_2\rightleftarrows H_1\oplus H_2$成立

根據定理四做以下的例子說明:

例5:

設滿足$1_{G_1}(n)=1$的$n=2,3,5,7,8,10,11,13,17$ (1)式

則滿足$1_{H_1}(n)=1$的$n=2,3,4,5,7,9,10,11,13,17,20,24,25,27,\ldots$ (2)式

設滿足$1_{G_2}(n)=1$的$n=3,4,6,7,8,9,12,14,15,16,19$ (3)式

則滿足$1_{H_2}(n)=1$的$n=3,4,7,16,18,19,20,24,28,30,32,33,35,36,\ldots$ (4)式

由上(1)、(3)式可知

滿足$1_G(n)=1$的$n=2,4,5,6,9,10,11,12,13,14,15,16,17,19$

而由G轉換而來的H為

滿足$1_H(n)=1$的$n=2,5,9,10,11,13,16,17,18,19,25,27,28,30,32,33,35,36,\ldots$

又由上(2)、(4)式知

滿足$1_{H_1\oplus H_2}(n)=1$的$n=2,5,9,10,11,13,16,17,18,19,25,27,28,30,32,33,35,36,\ldots$

所以$H=H_1\oplus H_2$，即$G\rightleftarrows H\Leftrightarrow G\rightleftarrows H_1\oplus H_2\Leftrightarrow G_1\oplus G_2\rightleftarrows H_1\oplus H_2$

而我們似乎可以由上述$1_{G_1}(n)=1,1_{H_1}(n)=1,1_{G_2}(n)=1,1_{H_2}(n)=1,1_G(n)=1,1_H(n)=1$

觀察到以下關係式:

1. $\hat{G}_1(H_2)=H_1\oplus H_2=H$
2. $\hat{G}_2(H_1)=H_1\oplus H_2=H$
3. 合併上述2式和定理四得$H_1\oplus H_2=\hat{G}_1(H_2)=\hat{G}_2(H_1)=H$

證明:

在 v 色的情況下，令$\hat{G}_1(\boxed{0}) = H_1$，$\hat{G}_2(\boxed{0}) = H_2$，$H_1 \oplus H_2 = H$。

則 $1_H(n) \equiv \sum_{d|n} 1_{G_1}(d) + \sum_{d|n} 1_{G_2}(d) \equiv \sum_{d|n} 1_{G_1}(d) + 1_{H_2}(n) \equiv \hat{G}_1(H_2)$

$$\equiv \sum_{d|n} 1_{G_2}(d) + 1_{H_1}(n) \equiv \hat{G}_2(H_1) \pmod{v}$$

因此就得到

定理五 (在 v 種顏色的情況下，$v \in \mathbb{N}$)

若$\hat{G}_1(\boxed{0}) = H_1$，$\hat{G}_2(\boxed{0}) = H_2$，則 $H = H_1 \oplus H_2 = \hat{G}_1(H_2) = \hat{G}_2(H_1)$。

四、 $\hat{G}(G)$在2種顏色時的性質探討

上述一、至三、的部分大致上都只對$\hat{G}_1(\boxed{0}) = G_2$ (即$G_1 \rightleftarrows G_2$)進行探討，
而這些結果我們都可以拿來套用在密碼上，
例如:有一張只有黑白兩色的圖G_1想要傳給別人，但是又怕被中途劫取，
此時就可以進行$\hat{G}_1(\boxed{0}) = G_2$的操作，再把圖$G_2$傳給對方，
並利用定理一的方式反推回圖G_1。
但是很明顯的，此種加密方式似乎很容易被破解，
所以我們就聯想到，如果將 $\boxed{0}$ 改為任意的圖，
那會不會有其它有趣的性質出現可以讓密碼的強度再增加呢?
我們考慮以下五種操作方式:

(一) 加密方式: 給定 G_0、G_1，$\hat{G}_0(G_1) = G_2$，$\hat{G}_2(G_1) = G_3$
將G_3這張圖傳出，而接收者已知G_2
破解方式: $\hat{G}_2(\hat{G}_2(G_1)) = G_1 \Rightarrow \hat{G}_2(G_3) = G_1$ ，

(二) 加密方式: 給定 G_0、G_1，$\hat{G}_0(G_1) = G_2$，$\hat{G}_2(G_1) = G_3$，$\hat{G}_3(G_2) = G_4$，
將G_4這張圖傳出，而接收者已知G_3
破解方式: $\hat{G}_3(G_4) = \hat{G}_3(\hat{G}_3(G_2)) = G_2$

(三) 加密方式: $\hat{G}_1(G_2) = G_3$，
將G_2、G_3這兩張圖傳出，而接收者想要知道G_1
破解方式: $(G_2 \oplus G_3) \rightleftarrows G_1$

(四) 加密方式: 給定G_1，$\hat{G}_1(G_1) = G_2$，$\hat{G}_2(G_2) = G_3$，$\hat{G}_3(G_3) = G_4$，.....
破解方式: 似乎難以用G_1、G_2、G_3、G_4、.....作運算得知

(五) 加密方式：給定$G_0, \hat{G}_0(\boxed{0}) = G_1, \hat{G}_1(\boxed{0}) = G_2, \hat{G}_2(\boxed{0}) = G_3$,..... , $\hat{G}_{n-1}(\boxed{0}) = G_n$

破解方式：似乎難以用G_1、G_2、G_3、G_4、.....作運算得知

綜上五種加密情形知道，應該是第(四)、(五)種的安全度較高，

故以下對此兩種加密方式進行研究。

五、 **在兩種顏色的狀態下，給 n 個格子且令 $G = \boxed{1}$，由$\hat{G}(\boxed{0}) = A$開始，**

接續操作$\hat{A}(A) = A_1$、 $\hat{A}_1(A_1) = A_2$、 $\hat{A}_2(A_2) = A_3$、...、$\hat{A}_t(A_t)$

由實驗結果我們推測：則對固定的前幾格而言，必有c，使得

在轉換 c 次後，保證這前幾格圖形會變成 $\boxed{0}$，且永遠為 $\boxed{0}$。

首先，我們進行下面的實驗。

(一) $\hat{G}(\boxed{0}) = A \Rightarrow A = \{1, 4, 9, 16, ..., 100, ...\}$ ⇒ 燈泡0個時圖會變為全黑

(二) $\hat{A}(A) = A_1$

(三) $\hat{A}_1(A_1) = A_2 \Rightarrow A_2 = \{4, 9, 25, 36, 49, 64, 100, ...\}$ ⇒ 燈泡3個 $= 3\times1$個時圖會變為全黑

(四) $\hat{A}_2(A_2) = A_3$

(五) $\hat{A}_3(A_3) = A_4 \Rightarrow A_4 = \{16, 64, 81, ...\}$ ⇒ 燈泡15個 $= 3\times5$個時圖會變為全黑

(六) $\hat{A}_4(A_4) = A_5$

(七) $\hat{A}_5(A_5) = A_6 \Rightarrow A_6 = \{64, ...\}$ ⇒ 燈泡63個 $= 3\times21$個時圖會變為全黑

觀察上面的實驗結果，我們猜測轉換奇數次時會有以下的一些規律：

轉換1次 ⇒ 格子0個 ⇒ 無意義,不討論

轉換3次 ⇒ 格子3×1個 ⇒ $3\times\left(2^0\right)$個

轉換5次 ⇒ 格子3×5個 ⇒ $3\times\left(2^0+2^2\right)$個

轉換7次 ⇒ 格子3×21個 ⇒ $3\times\left(2^0+2^2+2^4\right)$個

由上面的式子觀察，我們列出底下的算式:

$c = 2k+1(k \in \mathbb{N}) \Rightarrow c-1 = 2k \cdots (1\text{式})$

$n \le 3\times\left(2^0+2^2+2^4...+2^{2k-2}\right) = 2^{2k}-1(k \in \mathbb{N}) \cdots (2\text{式})$

(1式)代入(2式)中得 $n \le 2^{c-1}-1$

所以$n_{max} = 2^{c-1}-1$個燈泡

再根據以上結果推測，若已知 n 而欲求c，則由

$n \le 2^{c-1}-1$

$\Rightarrow (n+1) \le 2^{c-1}$

$\Rightarrow \log_2(n+1) \le c-1$

$\Rightarrow c \ge \log_2(n+1)+1$

因此我們就推測 c_{min}等於「不小於$\log_2(n+1)+1$的最小整數」，

不過，以上的推測，要如何證明呢？這引發了下面一連串的分析及計算。

六、 令G_0為起始圖，利用上述第四種的加密方式重複操作 u 次，
那麼G_u和G_0之間存在著甚麼關係呢?

首先，因為 $\hat{G}_0(\hat{G}_0)=G_1$，所以 $1_{G_1}(n)\equiv 1_{G_0}(n)+\sum_{d|n}1_{G_0}(d)(\mathrm{mod}\,2)$

其次，我們需要下面的引理:

引理一:(在2種顏色的情況下)

$$\sum_{d|n}\sum_{d'|d}1_{G_0}(d')\equiv\sum_{d'|n且\frac{n}{d'}為完平}1_{G_0}(d')\,(\mathrm{mod}\,2)$$

證明:

$$\sum_{d|n}\sum_{d'|d}1_{G_0}(d')\equiv\sum_{d'|n}\sum_{d'|d且d|n}1_{G_0}(d')\equiv\sum_{d'|n}1_{G_0}(d')\times(滿足d'|d且d|n的d之個數)\,(\mathrm{mod}\,2)$$

給定 n 的正因數 d'，令 $n=ad'$，$d=bd'\Rightarrow\frac{n}{d}=\frac{ad'}{bd'}=\frac{a}{b}$，即 $d|n\Leftrightarrow b|a\Leftrightarrow b|\frac{n}{d'}$。

為了讓 $(d'|d且d|n的d之個數)\equiv 1\,\mathrm{mod}\,2$

所以 b 必須有奇數個，也就是 $\frac{n}{d'}$ 有奇數個正因數，故 $\frac{n}{d'}$ 為完平。

引理二:(在2種顏色的情況下)

$$\sum_{d|n且\frac{n}{d}為完平}\ \sum_{d'|d且\frac{d}{d'}為完平}1_{G_0}(d')\equiv\sum_{d'|n且\frac{n}{d'}為完四}1_{G_0}(d')\,(\mathrm{mod}\,2)$$

證明:

$$\sum_{d|n且\frac{n}{d}為完平}\ \sum_{d'|d且\frac{d}{d'}為完平}1_{G_0}(d')\equiv\sum_{d'|n且\frac{n}{d'}為完平}\ \sum_{d|d且\frac{d}{d'}為完平且d|n且\frac{n}{d}為完平}1_{G_0}(d')$$

$$\equiv\sum_{d'|n且\frac{n}{d'}為完平}1_{G_0}(d')\times(滿足d'|d且\frac{d}{d'}為完平且\,d|n且\frac{n}{d}為完平的d之個數)\,(\mathrm{mod}\,2)$$

在上式中，因為 $\frac{n}{d}$ 和 $\frac{d}{d'}$ 為完平，所以 $\frac{n}{d'}$ 也必為完平 a^2。

故 $n=a^2d'$，又令 $d=b^2d'\Rightarrow\frac{n}{d}=\frac{a^2d'}{b^2d'}=\frac{a^2}{b^2}$，即 $d|n\Leftrightarrow b^2|a^2\Leftrightarrow b^2|\frac{n}{d'}$。

為了(使 $d'|d$ 且 $d|n$ 且 $\frac{n}{d}$ 和 $\frac{d}{d'}$ 皆為完平的d之個數) $\equiv 1\,(\mathrm{mod}\,2)$

所以 b 必須有奇數個，也就是(完平 $\frac{n}{d'}$)有奇數個完平的正因數，故 $\frac{n}{d'}$ 為完四。

根據引理一和引理二的推導方式，可類推出$\frac{n}{d'}$為完2^k，$k\in\mathbb{N}$ 的形式

再其次，我們發現到以下的運算都用到了同一個技巧

技巧一:

$$1_{G_u}(n)\equiv 1_{G_{u-1}}(n)+\sum_{d|n}1_{G_{u-1}}(d)$$

$$\equiv 1_{G_{u-2}}(n)+\sum_{d|n}1_{G_{u-2}}(d)+\sum_{d|n}[1_{G_{u-2}}(d)+\sum_{d'|d}1_{G_{u-2}}(d')]$$

$$\equiv 1_{G_{u-2}}(n)+\sum_{d|n}\sum_{d'|d}1_{G_{u-2}}(d')(\mathrm{mod}\,2)$$

觀察上式可知，在$\mathrm{mod}\,2$的系統下，第二行的$\sum_{d|n}1_{G_{u-2}}(d)+\sum_{d|n}1_{G_{u-2}}(d)$會被消掉，

利用這個特性，我們代換到最後就可以推出G_u和G_0的關係

以$1_{G_4}(n)$為例:

$$1_{G_4}(n)\equiv 1_{G_2}(n)+\sum_{d|n}\sum_{d'|d}1_{G_2}(d')$$

$$\equiv[1_{G_0}(n)+\sum_{d|n}\sum_{d'|d}1_{G_0}(d')]+\sum_{d|n}\sum_{d'|d}[1_{G_0}(d')+\sum_{d''|d'}\sum_{d'''|d''}1_{G_0}(d''')]$$

$$\equiv 1_{G_0}(n)+\sum_{d|n}\sum_{d'|d}\sum_{d''|d'}\sum_{d'''|d''}1_{G_0}(d''')(\mathrm{mod}\,2)$$

以下我們就直接套用這個技巧再配合引理推出G_u和G_0的關係

(一) G_1和G_0間的關係: $1_{G_1}(n)\equiv 1_{G_0}(n)+\sum_{d|n}1_{G_0}(d)\ (\mathrm{mod}\,2)$

(二) G_2和G_0間的關係: $1_{G_2}(n)\equiv 1_{G_0}(n)+\sum_{d|n且\frac{n}{d}為完平}1_{G_0}(d)(\mathrm{mod}\,2)$

(三) G_4和G_0間的關係: $1_{G_4}(n)\equiv 1_{G_0}(n)+\sum_{d|n且\frac{n}{d}為完四}1_{G_0}(d)(\mathrm{mod}\,2)$

(四) G_8和G_0間的關係: $1_{G_8}(n)\equiv 1_{G_0}(n)+\sum_{d|n且\frac{n}{d'}為完八}1_{G_0}(d)\ (\mathrm{mod}\,2)$

依此類推，可得G_{2^k}和G_0間的關係 : $1_{G_{2^k}}(n)\equiv 1_{G_0}(n)+\sum_{d|n為完\,2^k}1_{G_0}(d)\ (\mathrm{mod}\,2)$

同時就有以下的推論 : $1_{G_{2^k+m}}(n)\equiv 1_{G_{0+m}}(n)+\sum_{d|n為完\,2^k}1_{G_{0+m}}(d)\ (\mathrm{mod}\,2)$

定理六 (在2種顏色的情況下)

在$\hat{G}_0(G_0)=G_1$，$\hat{G}_1(G_1)=G_2$，...，$\hat{G}_{u-1}(G_{u-1})=G_u$，...的操作方式下，設 k 和 m 皆為正整數，則對於正整數 n

$$1_{G_{2k}}(n)\equiv 1_{G_0}(n)+\sum_{d|n\text{為完}2^k} 1_{G_0}(d)\pmod 2$$

$$1_{G_{2k+m}}(n)\equiv 1_{G_{0+m}}(n)+\sum_{d|n\text{為完}2^k} 1_{G_{0+m}}(d)\pmod 2$$

我們可用定理六來解釋固定的前幾格終將全黑的現象，如下:

以G_4為例來說明:

因為$1_{G_4}(n)\equiv 1_{G_0}(n)+\sum_{d|n\text{且}\frac{n}{d}\text{為完四}} 1_{G_0}(d)\pmod 2$，

所以如果$n\le 2^4-1$，則d 為了滿足($d\mid n$且$\frac{n}{d}$為完四)的條件，此時的d 必定只能是n，

因此得到以下式子:

$1_{G_4}(n)\equiv 1_{G_0}(n)+1_{G_0}(n)\equiv 0\pmod 2$。

同理(由定理六及上述推理方式)可知，若$n\le 2^{(2^k)}-1$，則$1_{G_{2^k}}(n)\equiv 1_{G_0}(n)+1_{G_0}(n)\equiv 0\pmod 2$。

定理七 (在2種顏色的情況下)

在$\hat{G}_0(G_0)=G_1$，$\hat{G}_1(G_1)=G_2$，...，$\hat{G}_{u-1}(G_{u-1})=G_u$，...的操作方式下，

若$n\le 2^{(2^k)}-1$且$k\in\mathbb{N}$，則$1_{G_{2^k}}(n)\equiv 0\pmod 2$。

這表示G_{2^k}的前$2^{(2^k)}-1$格必全黑。

其實我們可再進一步探討。

當 m 恰等於單獨一個質數的四次方時，

$1_{G_4}(m)\equiv 1_{G_0}(m)+1_{G_0}(1)+1_{G_0}(m)\equiv 1_{G_0}(1)\pmod 2$，$\sum_{d|m}1_{G_4}(d)\equiv 1_{G_0}(1)\pmod 2$

得知以上的結果後再觀察$1_{G_5}(m)\equiv 1_{G_4}(m)+\sum_{d|m}1_{G_4}(d)\equiv 1_{G_0}(1)+1_{G_0}(1)\equiv 0\pmod 2$

所以當m 恰等於單獨一個質數的四次方時，$1_{G_5}(m)\equiv 0\pmod 2$

利用上述的結論$1_{G_4}(m)\equiv 1_{G_0}(m)+1_{G_0}(1)+1_{G_0}(m)\equiv 1_{G_0}(1)\pmod 2$

我們發現到，在只有16個格子的狀況下，因為只有16為單獨一個質數的四次方，

所以1~15在1_{G_4}的情況下必為黑色，只有16可能會是白色，

所以若要使16個格子都保證為黑色，則共需轉換5次。

七、 令G_0為起始圖，利用上述第五種的加密方式重複操作 u 次，
那麼G_u和G_0之間存在著甚麼關係呢?

(一) G_1和G_0間的關係:

$$1_{G_1}(n) \equiv \sum_{d|n} 1_{G_0}(d) (\mathrm{mod}\, 2)$$

(二) G_2和G_0間的關係:

$$1_{G_2}(n) \equiv \sum_{d|n} 1_{G_1}(d) \equiv \sum_{d|n} \sum_{d'|d} 1_{G_0}(d') \equiv \sum_{d'|n且\frac{n}{d'}為完平} 1_{G_0}(d')$$

$$\equiv \sum_{d|n且\frac{n}{d}為完平} 1_{G_0}(d) (\mathrm{mod}\, 2)$$

(三) G_4和G_0間的關係:

$$1_{G_4}(n) \equiv \sum_{d|n且\frac{n}{d}為完平} 1_{G_2}(d) \equiv \sum_{d|n且\frac{n}{d}為完平} \sum_{d'|d且\frac{d}{d'}為完平} 1_{G_0}(d') \equiv \sum_{d'|n且\frac{n}{d'}為完四} 1_{G_0}(d')$$

$$\equiv \sum_{d|n且\frac{n}{d}為完四} 1_{G_0}(d) (\mathrm{mod}\, 2)$$

(四) G_8和G_0間的關係:

$$1_{G_8}(n) \equiv \sum_{d|n且\frac{n}{d}為完四} \sum_{d'|d且\frac{d}{d'}為完四} 1_{G_0}(d') \equiv \sum_{d'|n且\frac{n}{d'}為完八} 1_{G_0}(d')$$

$$\equiv \sum_{d|n且\frac{n}{d}為完八} 1_{G_0}(d) (\mathrm{mod}\, 2)$$

依此類推，可得 G_{2^k} 和 G_0 間的關係 :

$$1_{G_{2^k}}(n) \equiv \sum_{d|n為完2^k} 1_{G_0}(d) (\mathrm{mod}\, 2)$$

同時就有以下推論

$$1_{G_{2^k+m}}(n) \equiv \sum_{d|n為完2^k} 1_{G_{0+m}}(d) (\mathrm{mod}\, 2)$$

定理八 (在2種顏色的情況下)

在$\hat{G}_0(\boxed{0})=G_1$，$\hat{G}_1(\boxed{0})=G_2$，...，$\hat{G}_{u-1}(\boxed{0})=G_u$，...的操作方式下，

設 k 和 m 皆為正整數，則對於正整數 n

$$1_{G_{2^k}}(n)\equiv\sum_{d|n\text{為完}2^k}1_{G_0}(d)\pmod 2$$

$$1_{G_{2^k+m}}(n)\equiv\sum_{d|n\text{為完}2^k}1_{G_{0+m}}(d)\pmod 2$$

我們可用定理八來解釋固定的前幾格會有循環的現象，如下:

以G_4為例來說明:

因為$1_{G_4}(n)\equiv\sum_{d|n\text{且}\frac{n}{d}\text{為完四}}1_{G_0}(d)\pmod 2$，

所以如果$n\le 2^4-1$，則d 為了滿足($d\mid n$且$\frac{n}{d}$為完四)的條件，

此時的d 必定只能是 n，因此得到以下式子:

$1_{G_4}(n)\equiv 1_{G_0}(n)\pmod 2$。

同理(由定理八及上述推理方式)可知，若$n\le 2^{(2^k)}-1$，則$1_{G_{2^k}}(n)\equiv 1_{G_0}(n)\pmod 2$。

定理九 (在2種顏色的情況下)

在$\hat{G}_0(\boxed{0})=G_1$，$\hat{G}_1(\boxed{0})=G_2$，...，$\hat{G}_{u-1}(\boxed{0})=G_u$，...的操作方式下，

若$n\le 2^{(2^k)}-1$，且$k\in\mathbb{N}$，則$1_{G_{2^k}}(n)\equiv 1_{G_0}(n)\pmod 2$。

這表示G_{2^k}的前$2^{(2^k)}-1$格必全部回到原始狀態。

將定理九再加以分析:

已知$G_{2^k}=G_0$

若G_0之週期為m，也就是$G_0=G_{mt}=G_{2^k}(t\in\mathbb{N})$，則$m\le 2^k$。

今若$m\nmid 2^k$，則$mt+r=2^k(1\le r<m)$，又$G_{mt}=G_0$，

得到$G_r=G_{mt+r}=G_{2^k}=G_0$，

此時的 r 和G_0之週期為 m 矛盾，所以$m\mid 2^k$

$\Rightarrow m=2^h$，且$0\le h\le k$，$h\in\mathbb{Z}$

定理十 (在2種顏色的情況下)

設$|G_0| \le 2^{(p^k)}$ -1且$k \in \mathbb{N}$。則 $\hat{G}_0(\boxed{0}) = G_1$，$\hat{G}_1(\boxed{0}) = G_2$，...，$\hat{G}_{u-1}(\boxed{0}) = G_u$，... 的週期必為$2^h$，且$0 \le h \le k$。

例6. 令$|G_0| = 10$且$1_{G_0}(n)=1 \Leftrightarrow n=1,2,3,4,5,6,7,8,9,10$，

如定理十的方式重複操作，可得

$1_{G_1}(n)=1 \Leftrightarrow n=1,4,9$，$1_{G_2}(n)=1 \Leftrightarrow n=1,2,3,5,6,7,10$，

$1_{G_3}(n)=1 \Leftrightarrow n=1$，$1_{G_4}(n)=1 \Leftrightarrow n=1,2,3,4,5,6,7,8,9,10$，故得週期$=4=2^2$。

非常值得一提的是，因為$\hat{G}_{2^h-1}(\boxed{0}) = G_{2^h} = G_0$，這表示，對於給定有限格的$G_0$，

我們可以透過重複操作的方式，來找到G，滿足$\hat{G}(\boxed{0}) = G_0$；

而在這個演算過程中，沒有使用Möbius反轉公式！

於是我們獲得了求解$\hat{G}(\boxed{0}) = G_0$ 中的G 的另一種演算方法。

在掌握 2 種顏色的性質後，我們就想把它推廣到 2 種以上顏色的狀態。

八、 $\hat{G}(G)$在 v 種顏色時的性質探討

在2種以上顏色的情況時，因為$\sum$會一直重複出現，為了表達上的方便，

我們根據屢次運算累積起來的經驗，而發展出以下的形式運算符號：

(1)$1_{G_k}(n) = \alpha_k$，$\sum_{d_1|n} \sum_{d_2|d_1} \dots \sum_{d_q|d_{q-1}} 1_{G_k}(d_q) = \beta_k^q$，且$\alpha_k = \beta_k^0$

(2)$\beta_{k-1}^0 = \beta_{k-2}^0 + \beta_{k-2}^1$，$(\alpha_k)^b = \alpha_{k\times b}$，$(\beta_k^q)^s = \beta_k^{q\times s}$

例:$\alpha_k = 1_{G_k}(n) = 1_{G_{k-1}}(n) + \sum_{d_1|n} 1_{G_{k-1}}(d_1) = \beta_{k-1}^0 + \beta_{k-1}^1$

$= 1_{G_{k-2}}(n) + 2\sum_{d_1|n} 1_{G_{k-2}}(d_1) + \sum_{d_1|n} \sum_{d_2|d_1} 1_{G_{k-2}}(d_2) = \beta_{k-2}^0 + 2\beta_{k-2}^1 + \beta_{k-2}^2$

由上述舉例得知

$\alpha_k = \beta_{k-1}^0 + \beta_{k-1}^1$ [形式上將此式用$(\beta_{k-1}^0 + \beta_{k-1}^1)^1$表示]

$= \beta_{k-2}^0 + 2\beta_{k-2}^1 + \beta_{k-2}^2$ [形式上將此式用$(\beta_{k-2}^0 + \beta_{k-2}^1)^2$表示]

$= \beta_{k-3}^0 + 3\beta_{k-3}^1 + 3\beta_{k-3}^2 + \beta_{k-3}^3$ [形式上將此式用$(\beta_{k-3}^0 + \beta_{k-3}^1)^3$表示]

$\vdots$

$= C_0^m \beta_{k-m}^0 + C_1^m \beta_{k-m}^1 + \dots + C_m^m \beta_{k-m}^m$

[形式上將此式用$(\beta_{k-m}^0 + \beta_{k-m}^1)^m$表示]

$= C_0^m(\beta_{k-m-1}^0 + \beta_{k-m-1}^1) + C_1^m(\beta_{k-m-1}^1 + \beta_{k-m-1}^2) + \dots + C_m^m(\beta_{k-m-1}^m + \beta_{k-m-1}^{m+1})$

$= C_0^m \beta_{k-m-1}^0 + (C_0^m + C_1^m)\beta_{k-m-1}^1 + \dots + (C_{m-1}^m + C_m^m)\beta_{k-m-1}^m + C_m^m \beta_{k-m-1}^{m+1}$

$= C_0^{m+1} \beta_{k-m-1}^0 + C_1^{m+1} \beta_{k-m-1}^1 + \dots + C_m^{m+1} \beta_{k-m-1}^m + C_{m+1}^{m+1} \beta_{k-m-1}^{m+1}$

[形式上將此式用$(\beta_{k-m-1}^0 + \beta_{k-m-1}^1)^{m+1}$表示]

如此一直無窮的推導下去，可知$\alpha_k=(\beta_{k-q}^0+\beta_{k-q}^1)^q$的形式皆成立

$\Rightarrow (3)\alpha_k=(\beta_{k-q}^0+\beta_{k-q}^1)^q$

$$=C_0^q\beta_{k-q}^0+C_1^q\beta_{k-q}^1+C_2^q\beta_{k-q}^2+\ldots+C_{q-1}^q\beta_{k-q}^{q-1}+C_q^q\beta_{k-q}^q$$

當$q=k$時，$\alpha_k=(\beta_0^0+\beta_0^1)^k$

$\Rightarrow (4)\alpha_k=(\beta_0^0+\beta_0^1)^k=C_0^k\beta_0^0+C_1^k\beta_0^1+C_2^k\beta_0^2+\ldots+C_{k-1}^k\beta_0^{k-1}+C_k^k\beta_0^k$

$\Rightarrow$換成原式為$1_{G_k}(n)=1_{G_0}(n)+C_1^k\sum_{d_1|n}1_{G_0}(d_1)+C_2^k\sum_{d_1|n}\sum_{d_2|d_1}1_{G_0}(d_2)+\ldots+$

$$C_{k-1}^k\sum_{d_1|n}\sum_{d_2|d_1}\ldots\sum_{d_{k-1}|d_{k-2}}1_{G_0}(d_{k-1})+C_k^k\sum_{d_1|n}\sum_{d_2|d_1}\ldots\sum_{d_k|d_{k-1}}1_{G_0}(d_k)$$

(1)當p為質數時，$1_{G_p}(n)\equiv 1_{G_0}(n)+\sum_{d_1|n}\sum_{d_2|d_1}\ldots\sum_{d_p|d_{p-1}}1_{G_0}(d_p)\pmod p$

證明:

令 p 為質數

$\alpha_p=(\beta_0^0+\beta_0^1)^p$

$=C_0^p\beta_0^0+C_1^p\beta_0^1+C_2^p\beta_0^2+\ldots+C_{p-1}^p\beta_0^{p-1}+C_p^p\beta_0^p$

觀察$C_k^p=\frac{p!}{(k!)(p-k)!}=\frac{p(p-1)\ldots(p-k+1)}{k!}$

當$p>k>0$時，$(p-1)(p-2)\ldots(p-k+1)$整除k!(因為p為質數和k!互質，同時C_k^p為整數)

$\Rightarrow (p-1)(p-2)\ldots(p-k+1)=t(k!)$，$t\in\mathbb{N}$

此時$C_k^p=pt(k!)\equiv 0\pmod p$

$\Rightarrow$所以$\alpha_p\equiv\beta_0^0+\beta_0^p\pmod p$

換成原式為$1_{G_p}(n)\equiv 1_{G_0}(n)+\sum_{d_1|n}\sum_{d_2|d_1}\ldots\sum_{d_p|d_{p-1}}1_{G_0}(d_p)\pmod p$

(2)當p為質數時，$1_{G_{p^k}}(n)\equiv 1_{G_0}(n)+\sum_{d|n且\frac{n}{d}為完\ p^k}1_{G_0}(d)\pmod p$

求證$\alpha_{p^k}\equiv\beta_0^0+\beta_0^{p^k}\pmod p$

證明：

(i)已知$\alpha_p\equiv\beta_0^0+\beta_0^p\pmod p$成立，亦即$k=1$時上式成立。

(ii)設$k=w$時命題成立，即$\alpha_{p^w}\equiv\beta_0^0+\beta_0^{p^w}\pmod p$。

(iii)則$k=w+1$時，$\alpha_{p^{w+1}}\equiv(\alpha_{p^w})^p\equiv(\beta_0^0+\beta_0^{p^w})^p$

$$\equiv C_0^p(\beta_0^0)+C_1^p(\beta_0^{p^w})^1+C_2^p(\beta_0^{p^w})^2+\ldots+C_p^p(\beta_0^{p^w})^p$$

$$\equiv\beta_0^0+\beta_0^{p^{w+1}}\pmod p$$，命題也成立。

$\Rightarrow$根據數學歸納法得證$\alpha_{p^k}\equiv\beta_0^0+\beta_0^{p^k}\pmod p$。

於是再對β_0^p、$\beta_0^{p^k}$做深入探討，也就是以$\hat{G}(\boxed{0})$的形式來觀察質數種顏色下的結果。

九、 $\hat{G}(\boxed{0})$在質數種顏色時的性質探討

已知$\hat{G}(\boxed{0})$的運算形式為$1_{G_2}(n)=\sum_{d_1|n}\sum_{d_2|d_1}\cdots\cdots\sum_{d_p|d_{p-1}}1_{G_0}(d_p)$，

於是我們需要以下的引理來解釋

引理三:(在p色的情況下，p為質數)

$$1_{G_p}(n)\equiv\sum_{d_1|n}\sum_{d_2|d_1}\cdots\cdots\sum_{d_p|d_{p-1}}1_{G_0}(d_p)\equiv\sum_{d_p|n且\frac{n}{d_p}為完p}1_{G_0}(d_p)\pmod p$$

$$\Rightarrow 也就是\beta_0^p\equiv\sum_{d_p|n且\frac{n}{d_p}為完p}1_{G_0}(d_p)\pmod p$$

技巧二:

$$H_{b_1}^pH_{b_2}^p\cdots H_{b_m}^p=C_{b_1}^{p+b_1-1}C_{b_2}^{p+b_2-1}\cdots C_{b_m}^{p+b_m-1}=\prod_{j=1}^{m}\frac{(p+b_j-1)(p+b_j-2)\cdots(1+b_j)}{(p-1)!}$$

觀察$\frac{(p+b_j-1)(p+b_j-2)\cdots(1+b_j)}{(p-1)!}$在$(\mathrm{mod}\ p)$的狀態下，可知:

(i)設$b_j=pk+\alpha$，$\alpha=1,2,\ldots,p-1$且$k\in\mathbb{N}$，則$(p+b_j-1)(p+b_j-2)\cdots(1+b_j)\equiv 0(\mathrm{mod}\ p)$

於是可以令$(p+b_j-1)(p+b_j-2)\cdots(1+b_j)=ps$, $s\in\mathbb{N}$。

將之代回得$\frac{ps}{(p-1)!}$，且已知此數必為整數，同時因為p為質數和(p-1)!互質，

所以s可以整除$(p-1)!$，得到$\frac{s}{(p-1)!}=t$。

再將上述代回原式，得知$\frac{(p+b_j-1)(p+b_j-2)\cdots(1+b_j)}{(p-1)!}\equiv pt\equiv 0\ (\mathrm{mod}\ p)$

(ii)設$b_j=pk$，$k\in\mathbb{N}$，則$(p+b_j-1)(p+b_j-2)\cdots(1+b_j)\equiv(p-1)!\ (\mathrm{mod}\ p)$

於是可以令$(p+b_j-1)(p+b_j-2)\cdots(1+b_j)=ps+(p-1)!$，

將之代回得$\frac{ps+(p-1)!}{(p-1)!}=\frac{ps}{(p-1)!}+1$，且已知此數必為整數，同時因為p為質數和(p-1)!互質，

所以s可以整除$(p-1)!$，得到$\frac{s}{(p-1)!}=t$。

再將上述代回原式，得知$\frac{(p+b_j-1)(p+b_j-2)\cdots(1+b_j)}{(p-1)!}\equiv pt+1\equiv 1(\mathrm{mod}\ p)$

證明:

$$\sum_{d_1|n}\sum_{d_2|d_1}.....\sum_{d_p|d_{p-1}}1_{G_0}(d_p)\ \equiv \sum_{d_p|n}\ \sum_{d_1|n且d_2|d_1...且d_p|d_{p-1}}1_{G_0}(d_p)$$

$$\equiv \sum_{d_p|n}1_{G_0}(d_p)\times[滿足d_1\mid n且d_2\mid d_1...且d_p\mid d_{p-1}\ 的(d_{p-1},d_{p-2}...,d_1)之組數]\ (\mathrm{mod}\ p)$$

$$\begin{cases} n=c_1d_1 \\ d_1=c_2\ d_2 \\ \quad\vdots \\ d_{p-1}=c_p\ d_p \end{cases} \Leftrightarrow n=c_1c_2...c_pd_p \Leftrightarrow \frac{n}{d_p}=c_1c_2...c_p$$

設$\frac{n}{d_p}=a_1{}^{b_1}a_2{}^{b_2}...a_m{}^{b_m}$，其中$a_1,a_2,...,a_m$為質數，

則$\frac{n}{d_p}$是 p 個正整數相乘的方法，根據技巧二中的(i)和(ii)得知:

(1)當$b_j=pk+\alpha$時，$1_{G_p}(n)\equiv 0\ (\mathrm{mod}\ p)$

(2)當$b_j=pk$時，$\frac{n}{d_p}=a_1{}^{pk_1}a_2{}^{pk_2}...a_m{}^{pk_m}=(a_1{}^{k_1}a_2{}^{k_2}...a_m{}^{k_m})^p$，得知$\frac{n}{d_p}$為完全p次方數。

因此原式可改為$1_{G_p}(n)\equiv \sum_{d_p|n且\frac{n}{d_p}為完p}1_{G_0}(d_p)\times\prod_{j=1}^{m}\frac{(p+b_j-1)(p+b_j-2)...(1+b_j)}{(p-1)!}$,

再根據(ii)可再把式子改成$1_{G_p}(n)\equiv \sum_{d_p|n且\frac{n}{d_p}為完p}1_{G_0}(d_p)\times 1\equiv \sum_{d_p|n且\frac{n}{d_p}為完p}1_{G_0}(d_p)\ (\mathrm{mod}\ p)$

引理四:(在p色的情況下，p為質數)

$$1_{G_{p^2}}(n)\equiv \sum_{d_1|n且\frac{n}{d_1}為完\ p}\ \sum_{d_2|d_1且\frac{d_1}{d_2}為完\ p}\ .....\ \sum_{d_p|d_{p-1}且\frac{d_{p-1}}{d_p}為完\ p}1_{G_0}(d_p)\ \equiv \sum_{d_p|n且\frac{n}{d_p}為完\ p^2}1_{G_0}(d_p)\ (\mathrm{mod}\ p)$$

$$\Rightarrow 也就是(\beta_0^{\,p})^p\equiv\beta_0^{\,p^2}\equiv \sum_{d_p|n且\frac{n}{d_p}為完\ p^2}1_{G_0}(d_p)\ (\mathrm{mod}\ p)$$

證明:

$$\sum_{d_1|n且\frac{n}{d_1}為完\ p}\ \sum_{d_2|d_1且\frac{d_1}{d_2}為完\ p}\ .....\ \sum_{d_p|d_{p-1}且\frac{d_{p-1}}{d_p}為完\ p} 1_{G_0}(d_p) \equiv \sum_{d_p|n且\frac{n}{d_p}為完\ p^2} 1_{G_0}(d_p)$$

$$\equiv \sum_{d_p|n且\frac{n}{d_p}為完\ p} 1_{G_0}(d_p)\times[滿足 d_1 \mid n且 d_2 \mid d_1 ...且 d_p \mid d_{p-1} 的(d_{p-1}, d_{p-2}..., d_1)之組數] \pmod p$$

$$\begin{cases} n = c_1{}^p d_1 \\ d_1 = c_2{}^p\ d_2 \\ \quad\vdots \\ d_{p-1} = c_p{}^p\ d_p \end{cases}，且\frac{n}{d_p}為完\ p \Leftrightarrow n = c_1{}^p c_2{}^p ... c_p{}^p d_p，且\frac{n}{d_p} = r^p$$

$$\Leftrightarrow \frac{n}{d_p} = c_1{}^p c_2{}^p ... c_p{}^p = (c_1 c_2 ... c_p)^p = r^p \Leftrightarrow r = c_1 c_2 ... c_p$$

設 $r = a_1{}^{b_1} a_2{}^{b_2} ... a_m{}^{b_m}$，其中$a_1, a_2, ..., a_m$為質數，

則 r 是 p 個正整數相乘的方法，根據技巧二中的(i)和(ii)得知:

(1)當$b_j = pk + \alpha$ 時，$1_{G_p}(n) \equiv 0 \pmod p$

(2)當$b_j = pk$ 時，$r = a_1{}^{pk_1} a_2{}^{pk_2} ... a_m{}^{pk_m} = (a_1{}^{k_1} a_2{}^{k_2} ... a_m{}^{k_m})^p$

$\Rightarrow \frac{n}{d_p} = r^p = [(a_1{}^{k_1} a_2{}^{k_2} ... a_m{}^{k_m})^p]^p = (a_1{}^{k_1} a_2{}^{k_2} ... a_m{}^{k_m})^{p^2}$，得知$\frac{n}{d_p}$為完全$p^2$次方數。

因此原式可改為$1_{G_{p^2}}(n) \equiv \sum_{d_p|n且\frac{n}{d_p}為完p^2} 1_{G_0}(d_p) \times \prod_{j=1}^{m} \frac{(p+b_j-1)(p+b_j-2)...(1+b_j)}{(p-1)!}$,

再根據(ii)可再把式子改成$1_{G_{p^2}}(n) \equiv \sum_{d_p|n且\frac{n}{d_p}為完p^2} 1_{G_0}(d_p)\times 1 \equiv \sum_{d_p|n且\frac{n}{d_p}為完p^2} 1_{G_0}(d_p) \pmod p$

根據引理三和引理四的推導方式，可類推出$\frac{n}{d}$為完p^k，$k \in \mathbb{N}$ 的形式

同時也推出$\beta_0{}^{p^k} \equiv \sum_{d|n且\frac{n}{d}為完p^k} 1_{G_0}(d) \pmod p$

十、 $\hat{G}(G)$在質數種顏色時的性質探討

根據八、九、的結果，我們可針對質數種顏色做另類的探討:

$\hat{G}(G)$在質數種顏色時的操作為:

$1_{G_1}(n) \equiv 1_{G_0}(n) + \sum_{d|n} 1_{G_0}(d) \pmod p$，p為質數

由八、九、得知此式可化為$1_{G_{p^k}}(n) \equiv 1_{G_0}(n) + \sum_{d|n且\frac{n}{d}為完\ p^k} 1_{G_0}(d) \pmod p$，p為質數。

$|G_0| \le 2^{p^k}$ -1時，$\sum_{d|n且\frac{n}{d}為完\ p^k} 1_{G_0}(d) = 1_{G_0}(n)$，此時$1_{G_{p^k}}(n) \equiv 2 \times 1_{G_0}(n) \pmod p$，

也可表示為$\alpha_{p^k} \equiv 2\alpha_0 \pmod p$

$\Rightarrow$ 令$m \in \mathbb{N}$，$(\alpha_{p^k})^m \equiv (2\alpha_0)^m \equiv 2^m \alpha_0 \pmod p$，

根據費馬小定理得知$m = p-1$時必能使$2^m \equiv 1 \pmod p$成立，

而當此條件成立時，也就可以得知$(\alpha_{p^k})^{p-1} \equiv 2^{p-1}\alpha_0 \equiv \alpha_0 \pmod p$，

$\Rightarrow (\alpha_{p^k})^{p-1} = \alpha_{(p-1)p^k} \equiv \alpha_0 \pmod p \Rightarrow 1_{G_{(p-1)p^k}}(n) \equiv 1_{G_0}(n)$

所以在p種顏色下的$\hat{G}(G)$經過$(p-1)p^k$次操作時必回到原始圖形。

定理十一 (在 p 種顏色的情況下，p為質數)

設$|G_0| \le 2^{(p^k)}$ -1且$k \in \mathbb{N}$。則 $\hat{G}_0(G_0) = G_1$，$\hat{G}_1(G_1) = G_2$，$\hat{G}_2(G_2) = G_3$，

.....，$\hat{G}_{u-1}(G_{u-1}) = G_u$，..... 經過$(p-1)p^k$次操作時必回到原始圖形。

十一、 $\hat{G}(H)$在質數種顏色時的性質探討

上述十、是針對本身的圖形操作，於是我們想知道如果對任意固定的圖形操作會是什麼結果。

在p種顏色(p為質數)且$\hat{G}_0(H_0) = K_1$、$\hat{K}_1(H_0) = K_2$、...、$\hat{K}_u(H_0) = K_{u+1}$的操作模式下:

(1)$\hat{G}_0(H_0) = K_1 \Rightarrow \hat{G}_0(\boxed{0}) \oplus H_0 = G_1 \oplus H_0 = K_1$

(2)$\hat{K}_1(H_0) = K_2 \Rightarrow \hat{G}_1(\boxed{0}) \oplus \hat{H}_0(\boxed{0}) \oplus H_0 = G_2 \oplus H_1 \oplus H_0 = K_2$

(3)$\hat{K}_2(H_0) = K_3 \Rightarrow G_3 \oplus H_2 \oplus H_1 \oplus H_0 = K_3$

⋮

$(p^k)\hat{K}_{p^k-1}(H_0) = K_{p^k} \Rightarrow G_{p^k} \oplus H_{p^k-1} \oplus H_{p^k-2} \oplus ... \oplus H_1 \oplus H_0 = K_{p^k}$

$(p^k+1)\hat{K}_{p^k}(H_0) = K_{p^k+1} \Rightarrow G_{p^k+1} \oplus H_{p^k} \oplus H_{p^k-1} \oplus ... \oplus H_1 \oplus H_0 = K_{p^k+1}$

(其中$H_{p^k} = H_0$，因為經過p^k次操作過後一定會回來)

⋮

$(p \times p^k)\hat{K}_{p \times p^k\text{-}1}(H_0) = K_{p \times p^k} \Rightarrow G_{p \times p^k} \oplus H_{p \times p^k\text{-}1} \oplus H_{p \times p^k-2} \oplus ... \oplus H_1 \oplus H_0 = K_{p \times p^k}$

$\Rightarrow G_{p \times p^k} \oplus pH_0 \oplus pH_1 \oplus ... \oplus pH_{p^k-1} = K_{p \times p^k}$ (如上$G_{p \times p^k} = G_0$)

$\Rightarrow G_0 = K_{p \times p^k}$

所以經過p^{k+1}次操作過後，能在$\hat{G}_0(H_0)$的操作形式下回到原來給定的G_0。

定理十二 (在 p 種顏色的情況下，p為質數)

設$|G_0| \le 2^{(p^k)}$ -1 且$k \in \mathbb{N}$。則 $\hat{G}_0(H_0) = K_1$，$\hat{K}_1(H_0) = K_2$，$\hat{K}_2(H_0) = K_3$，...，$\hat{K}_{u-1}(H_0) = K_u$，... 經過p^{k+1}次操作時必回到原始圖形G_0。

十二、 $\underbrace{\hat{G}(\hat{G}(...\hat{G}}_{\text{p-1個}\hat{G}}(G)...))$在p種顏色(p為質數)時的性質探討

$\underbrace{\hat{G}(\hat{G}(\cdots\hat{G}}_{\text{p-1個}\hat{G}}(G)\cdots))$可以表達成:

$$1_{G_1}(n) \equiv 1_{G_0}(n) + (p-1)\sum_{d|n} 1_{G_0}(d) \Rightarrow \alpha_1 \equiv \alpha_0 + (p-1)\beta^1{}_0$$

$$\Rightarrow (\alpha_1)^{p^k} \equiv [\alpha_0 + (p-1)\beta^1{}_0]^{p^k}$$

$$\equiv C_0^{p^k}(p-1)^0\beta_0^0 + C_1^{p^k}(p-1)^1\beta_0^1 + ... + C_{p^k}^{p^k}(p-1)^{p^k}\beta_0^{p^k}$$

$$\equiv \beta_0^0 + (p-1)^{p^k}\beta_0^{p^k} \equiv \beta_0^0 + (-1)^{p^k}\beta_0^{p^k} \pmod p$$

其中p為質數，$(-1)^{p^k} \equiv (-1) \equiv p-1 \pmod p$(當$p=2$時依然成立，因為 $-1 \equiv 1 \pmod p$)

$$\Rightarrow \text{所以}\alpha_{p^k} \equiv \beta_0^0 + (p-1)\beta_0^{p^k} \pmod p \Rightarrow 1_{G_p}(n) \equiv 1_{G_0}(n) + (p-1)\sum_{d|n\text{且}\frac{n}{d}\text{為完}p^k} 1_{G_0}(d)$$

$$\equiv \sum_{d|n\text{且}\frac{n}{d}\text{為完}p^k\text{且}d\neq n} 1_{G_0}(d) \pmod p$$

十三、 在 p 種顏色的情況下，給定有限格的圖H，若有G滿足$\underbrace{\hat{G}(\hat{G}(...\hat{G}}_{\text{p-1個}\hat{G}}(G)...))$=H，是否可完整將G解出？又如何解出G？

由$1_H(n) \equiv 1_G(n) + (p-1)\sum_{d|n} 1_G(d) \equiv (p-1)\sum_{d|n\text{且}d\neq n} 1_G(d) \pmod p$

任意給定m，$2 \le m \le n$

由$1_H(2m) \equiv 1_G(2m) + (p-1)\sum_{d|2m} 1_G(d) \pmod p$

$$\Rightarrow 1_H(2m) + [(p-1)1_H(2m) + 1_G(m)]$$

$$\equiv 1_G(2m) + (p-1)\sum_{d|2m} 1_G(d) + [(p-1)1_H(2m) + 1_G(m)] \pmod p$$

可得$1_G(m) \equiv (p-1)1_H(2m) + (p-1)\sum_{d|2m\text{且}d\neq m,2m} 1_G(d)$

$$\equiv (-1)1_H(2m) + (-1)\sum_{d|2m\text{且}d\neq m,2m} 1_G(d) \pmod p$$

既然已知$1_G(1)\equiv(-1)1_H(2)(\text{mod } p)$ ，

故由上式配合數學歸納法可知我們可求出$1_G(1),1_G(2),...,1_G(n)$。

另一方面，若 $n+1\le m\le 2n$ ，則$2m>2n$，

故由 $1_H(2m)\equiv 1_G(2m)+(p-1)\sum_{d|2m}1_G(d)\ (\text{mod } p)$

可知如果我們只知道$1_H(1),1_H(2),...,1_H(2n)$

$\Rightarrow$則我們無法解出$1_G(m)$。

因此，如果只給定$1_H(1),1_H(2),...,1_H(2n)$的話，則我們只能解出$1_G(1),1_G(2),...,1_G(n)$。

所以得知經過$\underbrace{\hat{G}(\hat{G}(\cdots\hat{G}}_{p-1個\hat{G}}(G)\cdots))=H$ 的操作後，

給定有限格的圖H能確定推出的G必定只有前一半。

十四、 在 p 種顏色(p為質數)的情況下，若給定有限格的圖G_0，

不論在$\hat{G}_0(G_0)=G_1$、$\hat{G}_0(\hat{G}_0(G_0))=G_1$、$\hat{G}_0(\hat{G}_0(\hat{G}_0(G_0)))=G_1$、...、

$\underbrace{\hat{G}_0(\hat{G}_0(...\hat{G}_0}_{p-2個\hat{G}_0}(G_0)...))=G_1$ 的重複操作下有什麼性質?

我們可以將上述提到的所有運算方法化簡為

$1_{G_1}(n)\equiv 1_{G_0}(n)+(p-r)\sum_{d|n}1_{G_0}(d)\ (\text{mod } p)$，p為質數，$r=2,...,p-2,p-1$

(根據十二、可知r =1時無法回到原始圖形，故不在此處討論)

可再將此式化為$\alpha_{p^k}\equiv\beta_0^0+(p-r)\beta_0^{p^k}\ (\text{mod } p)\ (k\in\mathbb{N})$，

也就是$1_{G_{p^k}}(n)\equiv 1_{G_0}(n)+(p-r)\sum_{d|n且\frac{n}{d}為完p^k}1_{G_0}(d)\ (\text{mod } p)$

$\Rightarrow$當$|G_0|\le 2^{p^k}-1$時，$1_{G_{p^k}}(n)\equiv(p-r+1)1_{G_0}(n)\ (\text{mod } p)$

也可表示為$\alpha_{p^k}\equiv(p-r+1)\alpha_0(\text{mod } p)$，

再根據十、的推導方法$\Rightarrow(\alpha_{p^k})^m\equiv[(p-r+1)\alpha_0]^m\equiv(p-r+1)^m\alpha_0(\text{mod } p)$，

根據費馬小定理得知$m=p-1$時必能使$(p-r+1)^m\equiv 1(\text{mod } p)$成立(因為p會和$(p-r+1)$互質)，

而當此條件成立時，也就可以得知$(\alpha_{p^k})^{p-1}\equiv(p-r+1)^{p-1}\alpha_0\equiv\alpha_0(\text{mod } p)$，

$\Rightarrow(\alpha_{p^k})^{p-1}=\alpha_{(p-1)p^k}\equiv\alpha_0(\text{mod } p)\Rightarrow 1_{G_{(p-1)p^k}}(n)\equiv 1_{G_0}(n)$

所以在 p 種顏色下，這些類型經過$(p-1)p^k$次操作時必回到G_0。

而這種循環性有助於我們做反向的運算!

例如:在五種顏色的情況下，不管是$\hat{G}_0(G_0)=G_1$、$\hat{G}_0(\hat{G}_0(G_0))=G_1$、$\hat{G}_0(\hat{G}_0(\hat{G}_0(G_0)))=G_1$

哪一種運算，若給定了 G_1 這張圖，就一定可以由正向的重複操作找到原本 G_0 的解，

而這個過程似乎無法直接使用Möbius 反轉定理，卻可以用重複操作得到答案。

因為當重複操作到 G_1 再次出現後，它的前面那張圖就是 G_0 的一個解。

而比較可惜的是，目前還沒有辦法得知 G_0 是僅有一組解還是有多組的解，

不過至少已經確定了能找出 G_0 的其中一個解。

定理十三（在 p 種顏色的情況下，p為質數）

若給定有限格的圖G_0，在$\hat{G}_0(G_0)=G_1$、$\hat{G}_0(\hat{G}_0(G_0))=G_1$、$\hat{G}_0(\hat{G}_0(\hat{G}_0(G_0)))=G_1$、...、

$\underbrace{\hat{G}_0(\hat{G}_0(...\hat{G}_0}_{p-2個\hat{G}_0}(G_0)...))=G_1$ 的重複操作下，

有以下關係式：當$|G_0|\le 2^{p^k}-1$且$k\in\mathbb{N}$時，$1_{G_{p^k}}(n)\equiv(p-r+1)1_{G_0}(n)\pmod p$ $(r=2,3,...,p-1)$

且這些類型經過$(p-1)p^k$次操作時必回到G_0。

十五、 密碼上的應用

以下我們舉一個簡單密碼上的應用(假設使用者雙方已經先溝通好要使用此加密方式了)：

假設現在有一張三色的圖G_0上有SOS的字樣，且此圖總共有511格，

現在想要把這張圖傳出去，但是又怕被劫走，所以拿它來改變一張圖 H_0，

也就是進行$\hat{G}_0(H_0)$的操作，而 H_0 也是一張三色且總共有511格的圖，

操作後會得到一張圖 K_0，然後把 K_0 和 H_0 這兩張圖傳出去。

如果想要得到 G_0 這張圖，那就必須再進行$\hat{K}_0(H_0)=K_1$, $\hat{K}_1(H_0)=K_2$,...的操作26次才能獲得。

倘若中途有駭客攔截到了K_0 和 H_0 這兩張圖，那他很可能就認為正確的資訊就是這兩張圖，

而達到圖形加密的效果。

伍、研究成果

一、 若$\hat{G}_0(\boxed{0})=G_1$，則G_0和G_1之間的關係式為：

$$1_{G_1}(n)\equiv\sum_{d\mid n}1_{G_0}(d)\pmod v\quad v\in\mathbb{N}$$

$$1_{G_0}(n)\equiv\sum_{d\mid n}1_{G_1}(d)\,\mu(\frac{n}{d})\pmod v\quad v\in\mathbb{N}$$

二、 在 v 種顏色($v\in\mathbb{N}$)的情況下，若$\hat{G}_0(\boxed{0})=G_1$且正整數$n\le|G_1|$，則有

$$1_{G_0}(n)\equiv 1_{G_1}(n)+\sum_{d\mid n\text{ 且 }d=r\text{個相異質數乘積}}1_{G_1}(d)\cdot(-1)^r\pmod v$$

三、 在 v 種顏色($v\in\mathbb{N}$)的情況下，若$\hat{G}_1(\boxed{0})=H_1$且$\hat{G}_2(\boxed{0})=H_2$，則$G_1\oplus G_2\rightleftarrows H_1\oplus H_2$成立

四、 在2種顏色的情況下給定G_1，$\hat{G}_1(G_1)=G_2$，$\hat{G}_2(G_2)=G_3$，$\hat{G}_3(G_3)=G_4$，.....

則對固定前幾格而言，重複操作有限次之後必定全黑。

五、 在2種顏色的情況下，給定G_0，進行$\hat{G}_0(\boxed{0})=G_1$、$\hat{G}_1(\boxed{0})=G_2$、$\hat{G}_2(\boxed{0})=G_3$.....，
則可以找出之間的循環性。且其週期必為2^h(h為非負整數)之形式。

六、 根據上面的五、，給定有限格的圖H，可藉由重複操作而求出G來滿足 $\hat{G}(\boxed{0})=H$

七、 在 p 種顏色的情況下(p為質數)，設 $|G_0|\le 2^{(p^k)}-1$且$k\in\mathbb{N}$。
則 $\hat{G}_0(G_0)=G_1$，$\hat{G}_1(G_1)=G_2$，$\hat{G}_2(\boxed{0})=G_3$，...，$\hat{G}_{n-1}(G_{n-1})=G_n$，...
經過$(p-1)p^k$次操作時必回到原始圖形。

八、 在 p 種顏色的情況下(p為質數)，設 $|G_0|\le 2^{(p^k)}-1$ 且$k\in\mathbb{N}$。
則 $\hat{G}_0(H_0)=K_1$，$\hat{K}_1(H_0)=K_2$，$\hat{K}_2(H_0)=K_3$，...，$\hat{K}_{n-1}(H_0)=K_n$，...
經過 p^{k+1} 次操作時必回到原始圖形G_0。

九、 在 p 種顏色的情況下(p為質數)，給定有限格的圖 H，
若有 G 滿足$\underbrace{\hat{G}(\hat{G}(\cdots\hat{G}}_{p-1個\hat{G}}(G)\cdots))=H$，則只能夠解出 G 的前一半。

十、 在 p 種顏色(p為質數)的情況下，若給定有限格的圖G_0，
在$\hat{G}_0(G_0)=G_1$、$\hat{G}_0(\hat{G}_0(G_0))=G_1$、$\hat{G}_0(\hat{G}_0(\hat{G}_0(G_0)))=G_1$、...、
$\underbrace{\hat{G}_0(\hat{G}_0(...\hat{G}_0}_{p-2個\hat{G}_0}(G_0)...))=G_1$ 的重複操作下，
有以下關係式: 當$|G_0|\le 2^{p^k}-1$且$k\in\mathbb{N}$時，$1_{G_{p^k}}(n)\equiv(p-r+1)1_{G_0}(n)\ (\mathrm{mod}\ p)$
且這些類型經過$(p-1)p^k$次操作時必回到G_0。

陸、討論與未來展望

一、在循環的過程中發現與費馬小定理有相似之處，也就是我們能求出特定條件下幾次之內必定循環。

二、合數種顏色下的$\hat{G}(\boxed{0})$:

令A為合數，$1_{G_A}(n) \equiv \sum_{d_1|n} \sum_{d_2|d_1} ..... \sum_{d_A|d_{A-1}} 1_{G_0}(d_A) \pmod{A}$，其中證明方法可參考九、的技巧二，

但我們發現將此套用在技巧二中時，$\frac{(A+b_j-1)(A+b_j-2)...(1+b_j)}{(A-1)!}$在$(\mathrm{mod}\ A)$的狀態下，

由於A是合數的關係，無法像上述技巧二內容所提的進行化簡。因為當：

(i) 設$b_j = Ak+\alpha$，α=1, 2 ,..., A-1 且$k \in \mathbb{N}$，則$(A+b_j-1)(A+b_j-2)...(1+b_j) \equiv 0(\mathrm{mod}\ A)$

於是可以令$(A+b_j-1)(A+b_j-2)...(1+b_j)$=As , $s \in \mathbb{N}$。

將之代回得$\frac{As}{(A-1)!}$，如欲使$\frac{As}{(A-1)!} \equiv 0(\mathrm{mod}\ A)$，那麼$\frac{s}{(A-1)!}$一定要是個整數。

當$\frac{s}{(A-1)!}$是分數時，A×$\frac{s}{(A-1)!}$要是整數，而這個整數一定不是 A的倍數，

所以不能確定$\frac{As}{(A-1)!}$在$(\mathrm{mod}\ A)$的運算下同餘0，

故$\frac{(A+b_j-1)(A+b_j-2)...(1+b_j)}{(A-1)!}$在$b_j = Ak+\alpha$時無法化簡，也就無法得到漂亮的結果。

(ii) 設$b_j = Ak$，$k \in \mathbb{N}$，則$(A+b_j-1)(A+b_j-2)...(1+b_j) \equiv (A\text{-}1)!\ (\mathrm{mod}\ A)$

於是可以令$(A+b_j-1)(A+b_j-2)...(1+b_j)$= $As+(A\text{-}1)!$，

將之代回得$\frac{As+(A\text{-}1)!}{(A-1)!}$ = $\frac{As}{(A-1)!}$+1，同(i)可知此種條件也無法得到漂亮的結果。

三、 上面我們已經發現$\hat{G}(\boxed{0})$、$\hat{G}(G)$、$\hat{G}(H)$、$\hat{G}(\hat{G}(...\hat{G}(\hat{G}(G))\cdots))$的循環性質

下一步我們想研究的是，綜合以上所有的性質，將本研究的結果和多項式結合。

也就是把G看作常數項，$\hat{G}(G)$看作x^1，$\hat{G}(\hat{G}(G))$看作x^2...，依此類推，

然後我們可以針對一串多項式進行重複操作，觀察其是否有循環的性質出現。

例如:將$(2x^2+4x^1+2)$重複操作就等同於對$[2\hat{G}(\hat{G}(G))\oplus 4\hat{G}(G)\oplus 2G]$進行重複操作，

最後看是否能從多項式中再得出更一般化形式的結果。

四、 上述有些性質對合數也對，像定理三、定理四和Möbius反轉定理。

五、 上述定理三的地方，我們只針對兩種顏色的情況作討論，事實上，我們已經發現了多種顏色情況下的結果 ：

在 v 種顏色($v \in \mathbb{N}$)的情況下操作$\hat{G}_0(\boxed{0}) = G_1$，並給定$1_{G_0}(n)$的狀態。

若某些$1_{G_0}(k)$的值($k \in N$)有改變，

再加上若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有vk個，

則$1_{G_1}(n)$不用改變顏色狀態；

再加上若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有vk+1個，

則$1_{G_1}(n)$必須改變1次顏色狀態；

⋮

再加上若值有所改變的$1_{G_0}(k)$中，k 為 n 的正因數者共有vk+(v-1)個，

則$1_{G_1}(n)$必須改變(v-1)次顏色狀態。

明顯的這個結果並不漂亮，且沒有比較好利用的性質，所以沒有將它呈現在研究過程中。

柒、結論

由原始的開關燈問題轉化、推廣為$\hat{G}_1(G_2) = G_3$的圖形運算後，

除了如定理一那樣把原始的開關燈問題看得更清楚，

我們還可推算出兩種狀態下，$\hat{G}(G)$及$\hat{G}(\boxed{0})$的重複操作所引發的有趣現象。

還可以再進一步的把兩種顏色的性質推廣成質數種，

最後，利用$\hat{G}(\boxed{0})$的循環性，我們意外的發現，要想由$\hat{G}_1(\boxed{0}) = G_2$中的$G_2$來反推$G_1$，

除了可以如定理一所述用Möbius 反轉定理，也能夠藉由重複操作$\hat{G}(\boxed{0})$來達到目的。

而這種循環性及其應用又可推廣，

這讓我們感受這種圖形運算值得再更深入探討並思考其可能的應用(例如密碼)。

捌、參考文獻

1. 潘承洞 潘承彪，初等數論(第二版)，北京大學出版社(2006)

【評語】040403

本作品在 P=2 時得到相當的成果，P > 2 為質數時也有比較一般性的結果，定理 1, 2 與 Mobius 反轉定理連結是有趣的。比較可惜的部分是只做了簡單的部分，也沒有得到 P 為合數時的任何結果。

另外，定理 5 中一系列變換如果可以適當地採用群論中的記號與結果，將有助於使結果更為深刻與簡潔；定理 6～10 可以與平面關燈策略問題作一比較，加強立論的縱深。