2015 年臺灣國際科學展覽會
優勝作品專輯

作品編號　**010005**

參展科別　數學

作品名稱　環環相「扣」－奇偶性守恆與歸零的模式探究

得獎獎項　大會獎：一等獎

美國 ISEF 正選代表：美國第 66 屆國際科技展覽會

青少年科學獎

推薦參加英語測驗之指導教師

就讀學校　國立臺中第一高級中學

指導教師　蔡政樺

作者姓名　李嘉峻

關鍵字　奇偶性、同餘守恆數、同餘方程

作者簡介

我是李嘉峻，目前就讀台中一中二年級。平時靜如處子，動如脫兔。數學與文學為我的兩大愛好，我可以沉浸在文學的世界裡休憩，而數學卻引領我走向另一個簡潔而優雅的世界。參加本次國際科展，一路走來，我尤其享受那種由挫折和突破不斷交織混合而成的過程，更重要的是，從中對於數學的美又有了更深刻的體悟，以及探索的熱情。

摘要

本研究一開始在六邊形的六個頂點各填入一個數字後，作連續操作:擦去一個數，寫上其相鄰兩數之差的絕對值。從這些數字在環狀排列的設定條件下，探討其守恆的狀態或使之全數歸零的模式研究。在初步研究過程中我們建構了研究模型以及操作架構，找尋 n 邊形在「$|x-y|$型操作」下相對應的「理想 k 值」。在初始推廣階段，特別運用到了奇偶數的特性。

在延伸的變化形式探討上，則朝向同餘性守恆的方向發展，並給出了三種建構同餘守恆狀態的方法，對於「$x-y$型操作」與「$x-2y$型操作」的「同餘守恆數」與「同餘守恆模式」有深入的探究，並發現到跟盧卡斯數列與梅森數列有密切的相關。

我們目前已得到以下結果:

1. 在$|x-y|$型操作下:
   (1) 當 $3 \nmid n$ 時，則 n 邊形的「理想 k 值」為任意正整數。
   (2) 當 $3 \mid n$ 時，則 n 邊形的「理想 k 值」為所有的奇數和小於$\frac{2}{3}n$的偶數。

2. 在$x-y$型操作下:
   (1) 同餘守恆數:

n	ϕ_n	φ_{Mn}	φ_n
$4t$	$F_{\frac{n}{2}}$	$\frac{L_n-2}{\phi_n}$	φ_{Mn}的因數
$4t+2$	$L_{\frac{n}{2}}$		
$6t-3$	2	$\frac{L_n}{\phi_n}$	
$6t\pm1$	1		

*t為正整數

   (2) 同餘守恆模式:
   若n和φ_n皆為質數，則將所有基態列出後，恰好數字$1\sim\varphi_n-1$各出現一次。

3. 在$x-2y$型操作下:
   (1) 同餘守恆數:

n	ϕ_n	φ_{Mn}	φ_n
偶數	G_n	(無)	任何大於 2 的正整數
奇數	1	$2M_n$	φ_{Mn}的因數

   (2) 同餘守恆模式:
   a. 若n和φ_n皆為質數，則將所有基態列出後，恰好數字$1\sim\varphi_n-1$各出現一次。
   b. 若n和φ_n皆為奇數，且n個數照逆時針方向依序記為$a_1, a_2, \dots, a_n$，則有:

$$a_{k+1} \equiv 2a_k \pmod{\varphi_n}$$

   其中$k=1,2,\dots,n$且$a_{n+1}=a_1$。

Abstract

In the research, we fill numbers on six vertices of a hexagon at first, and perform the continuous operations: delete a number, and write the absolute difference of its two adjacent numbers. These numbers are arranged in circular permutation, and we aim at studying its conservation form and the model in which all numbers will return to zero. In the preliminary process of the research, we build a research model and operating architecture, finding the "ideal values k" related to different n-sided polygon in "$|x-y|$ operation mode". On the early stage, we especially apply the characteristics of odevity.

In the extensive investigation, our study is toward congruence conservation form, and we develop three ways to construct the congruence conservation form. We probe deeply into the congruence conservation number and conservation form of "$x-y$ operation mode" and "$x-2y$ operation mode", and we found that they are closely related to "Lucas sequence" and "Mersenne sequence".

We have got the following results:

1. In "$|x-y|$ operation condition" :
   (1) If *n* cannot be divided by 3, then the "ideal values k" of n-sided polygon are all positive integers.
   (2) If *n* can be divided by 3, then the "ideal values k" of n-sided polygon are all positive odd integers and all positive even integers less than $\frac{2}{3}n$.

2. In "$x-y$ operation condition" :
   (1) congruence conservation number:

n	ϕ_n	φ_{Mn}	φ_n
$4t$	$F_{\frac{n}{2}}$	$\frac{L_n-2}{\phi_n}$	factors of φ_{Mn}
$4t+2$	$L_{\frac{n}{2}}$		
$6t-3$	2	$\frac{L_n}{\phi_n}$	
$6t\pm1$	1		

   * t is a positive integer

   (2) congruence conservation form:
   Assume that n and φ_n are prime, and list all the possible "basis status", then the number from 1 to φ_n-1 will appear just right one time.

3. In "$x-2y$ operation condition" :
   (1) congruence conservation number:

n	ϕ_n	φ_{Mn}	φ_n

even	G_n	(none)	positive integers greater than 2
odd	1	$2M_n$	factors of φ_{Mn}

(2) congruence conservation form:

a. Assume that n and φ_n are prime, and list all the possible "basis status", then the number from 1 to $\varphi_n - 1$ will appear just right one time.

b. Assume that n and φ_n are odd numbers, and these n numbers are denoted by $a_1, a_2, \ldots, a_n$ in counterclockwise direction, then

$$a_{k+1} \equiv 2a_k \ (mod\ \varphi_n)$$

in which $k = 1, 2, \ldots, n$ and $a_{n+1} = a_1$.

一.前言

(一) 研究動機

在一次數學專題課中，研讀一本書籍《走向 IMO 數學奧林匹克試題集錦(2004)》，看到一道有趣的數學競賽題，題目敘述如下：
「在一個正六邊形的六個頂點上有六個非負整數(可以相同)，作如下操作：擦去一個數，寫上相鄰兩數之差的絕對值。問：對怎樣的正整數 k，使得只要六個頂點上的數之和為 k，總可以經過一系列操作，使得最終六個頂點上的數均變為 0?」

對於這題的解法，能直覺地感受到需要進行邏輯性的歸類與構想操作的巧思，於是我們便設想，是否能將原始操作條件稍做變化，然後再對原問題做更進一步的推廣。例如，若是在 n 邊形上操作、或是去除題目中取絕對值的條件、甚至是對相鄰兩數做線性的變化…等等相關延伸問題的探索。在初步的探究過程中，並跟指導老師討論與考慮之後，決定以原始問題以及相關延伸問題做為此次數學科展探究活動與獨立研究的題材。

(二) 研究目的

1. 尋找問題解決過程中有助於深入探究的數學模型。

2. 將初始條件推廣至 n 邊形，探討並找尋滿足條件的正整數 k 與 n 之間的關係。

3. 調整操作規則，針對相鄰兩頂點上的正整數做線性的變化，並找尋相對應滿足條件的「同餘守恆數φ」與其「同餘守恆模式」和 n 之間的關係。

二. 研究方法或過程

(一) 名詞、符號定義

1. $|x-y|$型操作：在一個 n 邊形的 n 個頂點上，填寫 n 個不盡相異之非負整數，依以下規則進行操作：擦去一個數，寫上相鄰兩數之差的絕對值。

2. $x-qy$型操作：在一個 n 邊形的 n 個頂點上，填寫 n 個不盡相異之非負整數，且這n個整數的最大公因數為 1，依以下規則進行操作：擦去一個數，寫上其相鄰兩數依照順時針方向前項減q倍後項之差。

3. 理想 k 值：若存在一正整數 k，使得只要 n 邊形的 n 個頂點上的數字之和為 k，總是可以經過一系列有限次操作後，使得最後 n 個頂點上的數均變為整數 0。則滿足此條件的 k 值，稱之為該 n 邊形在該操作模式下的「理想 k 值」。

4. 同餘守恆狀態、同餘守恆數：在一個 n 邊形的 n 個頂點上有 n 個整數，若存

在一正整數φ_n使得在某種操作狀態下，無論如何操作都不會改變此 n 個整數除以φ_n的餘數，則此時狀態稱之為「同餘守恆狀態」，同時稱φ_n是該 n 邊形在該操作狀態下的「同餘守恆數」，φ_n的最大值則稱為「最大同餘守恆數」，記為φ_{Mn}。

5. 本原守恆數：在$x - qy$操作模式下，若n邊形的n個頂點上的數字以逆時針排列依序為$a_1, a_2, \dots, a_n$，而且滿足遞迴關係$a_k = a_{k-1} + qa_{k-2}$ $(k = 3, 4, \dots, n)$，若只要a_1, a_2不全為0，則此狀態必為同餘守恆狀態且都有同餘守恆數ϕ_n，則稱ϕ_n是該n邊形在該操作模式下的「本原守恆數」。

6. 階：設正整數a、m互質且$m \geq 1$。使同餘方程$a^d \equiv 1 \ (mod\ m)$成立的最小正整數d稱為a對模m的階。

7. 符號 S 之定義：S 表示在某個操作狀態下，n 邊形上各頂點的數字總和。

8. 符號 *max* 之定義：*max* 表示 n 邊形上之各頂點數字中的最大者。

9. 符號 $MAX\{A, B\}$之定義：$MAX\{A, B\}$表示選取 A, B 兩數的最大者。

10. 符號$gcd(a_1, a_2, \dots, a_n)$之定義: $gcd(a_1, a_2, \dots, a_n)$表示$a_1, a_2, \dots, a_n$這$n$個數的最大公因數。

11. 符號$\varphi(m)$之定義：$\varphi(m)$表示尤拉函數，即小於m且與m互質的正整數個數。

12. 符號⊗之定義：K⊗L = M $(mod\ p)$ 表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合M之內。

13. 符號F_n之定義：F_n表示費氏數列< 1, 1, 2, 3, 5, 8, 13 … … >中的第 n 項。

14. 符號L_n之定義：L_n表示盧卡斯數列< 1, 3, 4, 7, 11, 18, 29 … … >中的第 n 項。

15. 符號G_n之定義：G_n表示 Jacobsthal 數列< 1, 1, 3, 5, 11, 21, 43 … … >中的第 n 項。

16. 符號M_n之定義:M_n表示梅森數列< 1, 3, 7, 15, 31, 63, 127 … … >中的第n項。

(二) 先備性質和定理：

【先備性質】

1. 費氏數列< F_n >：

(1) n 為 3 之倍數，若且唯若F_n為偶數。

(2) 相鄰兩項F_n, F_{n+1}必互質。

2. 盧卡斯數列$< L_n >$與費氏數列$< F_n >$之關係：$L_n = 2F_{n-1} + F_n$。

3. Jacobsthal 數列$< G_n >$：$\forall n \in N$，G_n為奇數。

4. 梅森數列$< M_n >$：當 n 為偶數時，若且唯若M_n為 3 的倍數。

【先備定理】

1. 完全剩餘系：已知k, m互質，且c為常數，若$\{a_1, a_2, a_3, \cdots, a_n\}$是模$m$的一組完全剩餘系，則$\{ka_1, ka_2, ka_3, \cdots, ka_n\}$，$\{a_1 + c, a_2 + c, a_3 + c, \cdots, a_n + c\}$也都是模$m$的一組完全剩餘系。

2. 設 p 為質數，$\varphi(m)$是尤拉函數，則對每一個正整數d，$d \mid (p-1)$，則在模 p 的一組最簡剩餘系中恰有$\varphi(d)$個數對模p的階為d。

3. 若$(a, m) = 1$，若k為a對模m的階，則$\{a^0, a^1, a^2, a^3, \cdots, a^k\}$對模$m$必兩兩不同餘。

4. 孫子定理：設$m_1,\ m_2, \ldots, m_n$是n個兩兩互質的正整數，那麼對於任意整數$a_1,\ a_2, \ldots, a_n$，一次同餘方程組

$$x \equiv a_k \ (mod\ m_k) \ (k = 1, 2, \ldots, n)$$

必有解，且解數為 1。

(三) 數學模型：

本作品將探究過程中所建構的數學模型，先整理如下：

1. 【數學模型一】：同餘

以$a_1\ \begin{matrix} a_n & \cdots & \cdots \\ a_2 & a_3 & \ldots \end{matrix}$的圖示來表示操作過程中的某個狀態，並且將相對應到的頂點數值取模的同餘數。(本作品在前半部分的推廣階段都是表示為$\mathrm{A}\ \begin{matrix} B & C \\ F & E \end{matrix}\ D$，而且取模 2 作同餘，亦即以奇偶性討論之。例如：$0\ \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}\ 0\ (mod\ 2)$

2. 【數學模型二】：交替循環

我們構造以下兩個操作步驟，作為「交替循環」的操作：

步驟Ⅰ：由 S 為奇數的狀態，轉變到只有一個奇數的狀態。

步驟Ⅱ：從只有一個奇數的狀態，轉變到 S 為奇數且 *max* 變小或為零的狀態。

【說明】

由於上述的操作步驟中，都不會增加 *max*，而每次操作步驟 II 後都會使 *max*

的值至少遞減1，最終變為零。所以我們只要說明以上的步驟是如何操作就行。

3. 【數學模型三】：遞迴累加

我們將兩個初始的非負整數記為α、β，在 $x-qy$ 型操作模式下，有以下狀態：

α	$qU_{n-2}\alpha+U_{n-1}\beta$	$qU_{n-3}\alpha+U_{n-2}\beta$	…	…
	β	$q\alpha+\beta$	$q\alpha+(1+q)\beta$	…

其中數列<U_n>滿足遞迴關係：$U_1=1$，$U_2=1$，　$U_{n+2}=U_{n+1}+qU_n$。

4. 【數學模型四】守恆三態

為了討論的方便性，我們將守恆的狀態分成以下三種：

(1) 遞迴累加態(以後簡稱累加態)：若n邊形上的n個數經過【遞迴累加】模型之操作後，滿足守恆狀態且各數間最大公因數為 1，則稱此狀態為遞迴累加態。

(2) 基準態(以後簡稱基態)：已知n邊形上的n個數在滿足守恆狀態的條件下，其同餘守恆數為φ_n，若這n個數都屬於mod φ_n的最小非負完全剩餘系且各數間最大公因數為 1，則稱此狀態為基準態。

(3) 循環群態(以後簡稱循環態)：已知n邊形上的n個數在滿足守恆狀態下，其同餘守恆數為φ_n，且這n個數恰成為一個mod φ_n的循環群，則稱此狀態為循環群態。

(四) 原問題的探究過程

以下分別依正整數 k 值的範圍與奇偶性，展開原問題的解決歷程：

1. 首先論述，當 $k\geqq 4$ 且 k 為偶數時：

事實上，當 $k\geqq 4$ 且 k 為偶數時，則 k 不滿足條件。因為若假設六個數依序為 1,1,0,1,k-3,0，可知每次操作後，六個數的奇偶性不變，依次為奇、奇、偶、奇、奇、偶。因此，不可能經過一系列有限次操作後，使得最後六個頂點上的數均變為整數 0。換言之，2 是 n = 6 在$|x-y|$型操作下的「同餘守恆數」。故當 $k\geqq 4$ 且 k 為偶數時，不滿足題目要求。

2. 其次說明，當 $k=2$ 或 k 為奇數時，此時 k 值就是理想 k 值

以下針對 $k=2$ 以及 k 為奇數等兩種情形探討：

(1) 當 k=2 時，令六個頂點上的值依序為 $a_1, a_2, a_3, a_4, a_5, a_6$，則 $\sum_{i=1}^{6} a_i = 2$。

不失一般性假設$a_1 = MAX\{a_1, a_2, \ldots, a_6\}$，則 a_1=1 或 a_1=2。

a. 若 $a_1=2$，則只要直接對 a_1 操作便可使全部的數歸零。

b. 若 $a_1=1$，且 $a_2=a_6=0$，那就先對 a_1 操作，再對另一個非 0 的數字操作亦可使全部的數歸零。

c. 若 $a_1=1$，$a_2=1$ 或 $a_6=1$，不妨假設 $a_2=1$，則依序對 a_3,a_2, a_1, a_3 操作即可使全部的數歸零。

綜上討論，2 為 n = 6 時在$|x-y|$型操作下的「理想 k 值」。

(2) 當 *k* 為奇數時：

為了方便討論，我們要對整體情況做一個操作模式之定義，並建構一個有助於後續探究的【數學模型二】(內容敘述如前(三)數學模型)。

接下來討論 *k* 為奇數的情形，並說明【數學模型二】中的步驟 I、Ⅱ是合理的。

首先考慮某個 S 為奇數的狀態 $A\begin{matrix}B&C\\F&E\end{matrix}D$，則 A+C+E 和 B+D+F 兩者中必有一者為奇數，因此不妨假設 A+C+E 為奇數。

a. 若 A, C, E 中只有一個數為奇數，假設為 A，則我們可以 D→B→F→A→F 的順序操作：

$$1\begin{matrix}B&0\\F&0\end{matrix}D \rightarrow 1\begin{matrix}B&0\\F&0\end{matrix}0 \rightarrow 1\begin{matrix}1&0\\F&0\end{matrix}0 \rightarrow 1\begin{matrix}1&0\\1&0\end{matrix}0 \rightarrow 0\begin{matrix}1&0\\1&0\end{matrix}0 \rightarrow 0\begin{matrix}1&0\\0&0\end{matrix}0 \pmod 2$$

因此將變為只有一個奇數的狀態。

b. 若 A.C.E 全是奇數，那就依照 D→B→F→C→E 的順序操作，完成後也會變到只有一個奇數的狀態：

$$1\begin{matrix}B&1\\F&1\end{matrix}D \rightarrow 1\begin{matrix}B&1\\F&1\end{matrix}0 \rightarrow 1\begin{matrix}0&1\\F&1\end{matrix}0 \rightarrow 1\begin{matrix}0&1\\0&1\end{matrix}0 \rightarrow 1\begin{matrix}0&0\\0&1\end{matrix}0 \rightarrow 1\begin{matrix}0&0\\0&0\end{matrix}0 \rightarrow 0\begin{matrix}0&0\\0&0\end{matrix}0 \ (mod\ 2)$$

以上 *a.*和 *b.*說明了步驟 I 是可行的。

c. 再來，我們考慮狀態 $A\begin{matrix}B&C\\F&E\end{matrix}D$ 中只有 A 是奇數，其他都是偶數的情形。我們希望變到某個使 *max* 更小的狀態，根據 *max* 的奇偶性，分成兩種情況討論：

(a) 當 *max* 是偶數，即 *B.C.D.E.F* 中的某一個數是 *max* 且 *A* <*max*。則我們可以依照 *B→C→D→E→F* 的順序操作，其奇偶性的變化如下：

$$1\begin{matrix}0&0\\0&0\end{matrix}0 \rightarrow 1\begin{matrix}1&0\\0&0\end{matrix}0 \rightarrow 1\begin{matrix}1&1\\0&0\end{matrix}0 \rightarrow 1\begin{matrix}1&1\\0&0\end{matrix}1 \rightarrow 1\begin{matrix}1&1\\0&1\end{matrix}1 \rightarrow 1\begin{matrix}1&1\\0&1\end{matrix}1 \pmod 2$$

我們將這個新的狀態記為 $A'\begin{matrix}B'&C'\\F'&E'\end{matrix}D'$，其 S 為奇數且$A',B',C',D',E'$都小於 *max*(因為它們是奇數而 *max* 是偶數)，同時$F'=|A'-E'|\leq$

$MAX\{A', E'\} < max$，因此 *max* 變小了。

(b) 當 *max* 是奇數，所以 *A* = *max*，而其餘的數皆小於 *max*。若 *C*＞0，則依照 *B*→*F*→*A*→*F* 的順序進行操作：

$$\begin{matrix}0&0\\1&\\0&0\end{matrix}0 \rightarrow \begin{matrix}1&0\\0&\\0&0\end{matrix}0 \rightarrow \begin{matrix}1&0\\1&\\0&0\end{matrix}0 \rightarrow \begin{matrix}1&0\\0&\\1&0\end{matrix}0 \rightarrow \begin{matrix}1&0\\0&\\0&0\end{matrix}0 \pmod 2$$

我們記這個新狀態為 $A'\begin{matrix}B'&C'\\&\\F'&E'\end{matrix}D'$，而 *max* 只有在$B' = A$時才不會變小，但這是不可能的，因為$B' = |A' - C'| < A$，因此又變到了一個 S 為奇數且 *max* 變小的狀態；若 *E*＞0，由於 *C, E* 的位置對稱，可以類似討論；

若 *C* = *E* = 0，則直接按照 *D*→*B*→*F*→*A*→*B*→*F* 的順序操作便可使全部的數字歸零。

以上說明步驟 II 也是可行的。

綜上所述，只要當 *k* = 2 或 *k* 為奇數時，總是可以經過一系列的操作使各頂點上的數字均變為零，也就是說當 *k* = 2 或 *k* 為奇數是當 n=6 在$|x - y|$型操作下的「理想 *k* 值」，而且所建構的數學模型是正確又有助於後續的探究。

原始問題之結果： 在一個正六邊形的六個頂點上有六個非負整數(可以相同)，作如下操作：擦去一個數，寫上其相鄰兩數之差的絕對值，則當 *k* = 2 或 *k* 為奇數時，只要此正六邊形的六個頂點上的數之和為 *k*，總是可以經過一系列操作，使得最終六個頂點上的數均變為零。

(五) 原問題的延伸與推廣

經過上述探討結果，並分析原問題的構造解法之脈絡後，我們嘗試將原問題的六邊形推廣至任意 *n* 邊形，並展開此延伸問題的探究以找尋在$|x - y|$型操作條件下相對應的「理想 *k* 值」。

1. 探究 *n* = 3 時的情況：

首先應用【數學模型一】中的同餘模式概念，即以 $A\overset{B}{\ }C$ 的圖示表示某操作過程中的三角形之三頂點所填入之數的狀態。

當 *k*=1 時，不妨假設 *A*=1，則直接對 *A* 進行操作後，顯然成立，即 1 是「理想 *k* 值」。

接下來，說明當 *k*≥2 時，皆不符合「理想 *k* 值」的條件。

由於 n=3 時的變化比較簡單，所以我們直接對三頂點的奇偶性做討論：

(1) A, B, C 皆為奇數時：

對任意一數操作後，都會產生有兩個奇數、一個偶數的狀態，顯然，之後的每次操作都不會再改變其奇偶性，因此這一狀態不符合題目要求。

(2) A, B, C 中有兩個數為奇數時：

同理於上述(1)的結果。

(3) 若 A, B, C 中僅有一數為奇數時：

不妨假設此奇數為 A，以下再分兩種情況：

a. 對 B 或 C 進行操作：由於對稱性，故兩者等價

$$1 \overset{0}{} 0 \ \rightarrow\ 1 \overset{1}{} 0 \pmod 2$$

由前面的討論知道這樣的狀況是沒有解的，即得不到三數均變為 0 的情況。

b. 對 A 進行操作：

$$1 \overset{0}{} 0 \ \rightarrow\ 0 \overset{0}{} 0 \pmod 2$$

最後，要說明三者皆為偶數的狀況也是無解的，討論如下：

在 A, B, C 三者皆為偶數時，必有一正整數 p 滿足 $2^p \mid (A, B, C)$ 且 $2^{p+1} \nmid (A, B, C)$，將 A, B, C 同除以 2^p，得到的新狀態記為 $A' \overset{B'}{} C'$，當中至少有一數為奇數，而從前面的討論知道，在有奇數的條件下，皆為無解。又狀態 $A' \overset{B'}{} C'$ 僅為狀態 $A \overset{B}{} C$ 提出公因數後的結果，並不影響數字間比例關係，亦即對 A', B', C' 三者操作實質上等價於對 A, B, C 操作。於是當 A, B, C 三者皆為偶數時，永遠無法使三數同時變為零。

綜上所述，當 n=3 時，僅當 k=1 時符合題目要求，即三角形在$|x-y|$型操作下的「理想 k 值」只有 1。

2. n=4 時的情況：

以圖示 $A \overset{B}{\underset{D}{}} C$ 表示某操作過程中的狀態，我們交替地操作【數學模型二】中的步驟 I 和步驟 II，並運用原問題的策略和方法進行分析與討論，如下：

(1) 當 k 為奇數時：

首先考慮某個 S 為奇數的狀態 $A\ {}^{B}_{D}\ C$ ，其中分為兩種狀況：

a. 如果只有一個奇數而其他皆為偶數，顯然已完成步驟 I；

b. 如果有三個奇數和一個偶數，不失一般性假設 *A* 為偶數，則依照 *C→B* 的順序操作即可變為只有一個奇數的狀態：

$$0\ {}^{1}_{1}\ 1 \ \rightarrow\ 0\ {}^{1}_{1}\ 0 \ \rightarrow\ 0\ {}^{0}_{1}\ 0 \pmod 2$$

以上說明了步驟 I 是可行的。

c. 再考慮狀態 $A\ {}^{B}_{D}\ C$ 中只有 A 為奇數，其餘皆為偶數的情況，依照 *max* 的奇偶性，再分兩種狀況做討論：

(a) 若 *max* 為偶數，即 B, C, D 中有一數為 *max* 且 A < *max*，則依照 B→C→D 的順序進行操作：

$$1\ {}^{0}_{0}\ 0 \ \rightarrow\ 1\ {}^{1}_{0}\ 0 \ \rightarrow\ 1\ {}^{1}_{0}\ 1 \ \rightarrow\ 1\ {}^{1}_{0}\ 1 \pmod 2$$

我們將此新的狀態記為 $A'\ {}^{B'}_{D'}\ C'$，其 S 為奇數且 A', B', C'都小於 *max*(因為它們是奇數而 *max* 是偶數)，同時 D'= │A' － C'│ ≦ *MAX*{A', C'} ＜ *max*，因此 *max* 變小了。

(b) 若 *max* 為奇數，即 *A* = *max*，而其餘的數皆小於 *max*。

若 C > 0，則依照 B→D→A→D 的順序進行操作：

$$1\ {}^{0}_{0}\ 0 \ \rightarrow\ 1\ {}^{1}_{0}\ 0 \rightarrow\ 1\ {}^{1}_{1}\ 0 \ \rightarrow\ 0\ {}^{1}_{1}\ 0 \ \rightarrow\ 0\ {}^{1}_{0}\ 0 \pmod 2$$

此時將此新的狀態記為 $A'\ {}^{B'}_{D'}\ C'$，其中 B'= │A － C│ <A，因此又變回 S 為奇數的狀態而且 *max* 變小。

若 C = 0，則依照 B→D→A→D→ B 的順序操作，可使全部的數歸零:

$$A\ {}^{B}_{D}\ 0 \ \rightarrow\ A\ {}^{A}_{D}\ 0 \ \rightarrow\ A\ {}^{A}_{A}\ 0 \ \rightarrow\ 0\ {}^{A}_{A}\ 0 \ \rightarrow\ 0\ {}^{0}_{A}\ 0 \ \rightarrow\ 0\ {}^{0}_{0}\ 0$$

(注意這裡的 0 代表數字 0 而非偶數)

以上說明了步驟 II 也是可行的。

因此，當 k 為奇數時，皆為四邊形在$|x-y|$型操作下的「理想k值」。

(2) 當 k 為偶數時：

在 A, B, C, D 四者中至少有一數為奇數時，都能經過簡單的操作導致某一 S 為奇數的狀態：

a. $\begin{matrix}1\\1\end{matrix}1 \rightarrow 1\begin{matrix}1\\1\end{matrix}0 \pmod 2$

b. $\begin{matrix}1\\0\end{matrix}0 \rightarrow 1\begin{matrix}1\\1\end{matrix}0 \pmod 2$

c. $\begin{matrix}0\\0\end{matrix}1 \rightarrow 1\begin{matrix}0\\0\end{matrix}0 \pmod 2$

接著就等同於上述在 k 為奇數時的討論。

同樣地，當 A, B, C, D 皆為偶數時，也可說明有解。

因為在 A, B, C, D 四者皆為偶數時，必有一正整數 p 滿足 $2^p \mid$ (A, B, C, D) 且 $2^{p+1} \nmid$ (A, B, C, D)，將 A, B, C, D 同除以 2^p，得到的新狀態記為 $A'\begin{matrix}B'\\D'\end{matrix}C'$，

當中至少有一數為奇數，從前面的討論知道，在有奇數的條件下，皆是有解的。

而同理上述 n=3 時之狀況討論，所以我們可以知道，對 *A', B', C', D'* 四者操作等價於對 *A, B, C, D* 操作，所以當 *A, B, C, D* 四者皆為偶數時，必可經過一系列的操作使得四數皆為零。

因此，當 k 為偶數時，也可符合題意要求。

綜上(1)(2)所述，當 n=4 時，k 為任意正整數，皆滿足題意要求，即四邊形在$|x-y|$型操作下的「理想k值」為任意正整數。

【心得一】

綜而言之，透過分析完 n=4 時的情況，發現到其實並不一定要將 k 值依照奇偶性做分類討論，因為除了各頂點皆為偶數的情況下，無論 k 為奇數或偶數，都能操作到只有一數為奇數的狀態，從而進行下一個步驟(將 *max* 的奇偶性做分類討論)，操作後又回到至少有一數為奇數且 *max* 變小的狀態。因此也不用顧慮 S 的奇偶性。另一方面，若初始條件中，各頂點皆為偶數，即可提出 2 的最高公因次，仍然可重複上階段的討論歷程。

3. n=5 時的情況：

以圖示 $A\begin{matrix}B & C\\ E & D\end{matrix}$ 表示某一操作過程中的狀態，並以剛才的分類構想進行討論。

(1) 在初始狀態下，*A, B, C, D, E* 五者中至少有一數為奇數的情況：

a. 不計對稱性的等價情況，一共有 7 種不同的奇偶分布狀態，而其皆可經過一系列固定的操作模式導致只有一個數為奇數的狀態：

$$1\begin{matrix}1 & 1\\ 1 & 1\end{matrix}\rightarrow 1\begin{matrix}0 & 1\\ 1 & 1\end{matrix}\rightarrow 1\begin{matrix}0 & 1\\ 0 & 1\end{matrix}\rightarrow 0\begin{matrix}0 & 1\\ 0 & 1\end{matrix}\rightarrow 0\begin{matrix}1 & 1\\ 0 & 1\end{matrix}\rightarrow 0\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\rightarrow 0\begin{matrix}0 & 0\\ 0 & 1\end{matrix}\ (mod\ 2)$$

以上表示可達成步驟 I 的目的，使得只剩一個數為奇數。

b. 考慮狀態 $A\begin{matrix}B & C\\ E & D\end{matrix}$ 中只有 *A* 為奇數，其餘皆為偶數的情況。再依據 *max* 的奇偶性進行討論：

(a) 當 *max* 為偶數，即 B, C, D, E 中有一數為 *max* 且 $A<max$，則依照 B→C→D→E 的順序進行操作：

$$1\begin{matrix}0 & 0\\ 0 & 0\end{matrix}\rightarrow 1\begin{matrix}1 & 0\\ 0 & 0\end{matrix}\rightarrow 1\begin{matrix}1 & 1\\ 0 & 0\end{matrix}\rightarrow 1\begin{matrix}1 & 1\\ 0 & 1\end{matrix}\rightarrow 1\begin{matrix}1 & 1\\ 0 & 1\end{matrix}\ (mod\ 2)$$

我們記此新的狀態為$A'\begin{matrix}B' & C'\\ E' & D'\end{matrix}$，其中$A', B', C', D'$都小於 *max*(因為它們是奇數而 *max* 是偶數)，同時 $E'=\left|A'-D'\right|\leqq MAX\{A', D'\}<max$，因此 *max* 變小了。

(b) 當 *max* 為奇數，即 $A=max$，而其餘的數皆小於 *max*。若 $C>0$，則依照 *B→E→A→E* 的順序進行操作：

$$1\begin{matrix}0 & 0\\ 0 & 0\end{matrix}\rightarrow 1\begin{matrix}1 & 0\\ 0 & 0\end{matrix}\rightarrow 1\begin{matrix}1 & 0\\ 1 & 0\end{matrix}\rightarrow 0\begin{matrix}1 & 0\\ 1 & 0\end{matrix}\rightarrow 0\begin{matrix}1 & 0\\ 0 & 0\end{matrix}\ (mod\ 2)$$

我們記此新的狀態為$A'\begin{matrix}B' & C'\\ E' & D'\end{matrix}$，其中 $B'=\left|A-C\right|<A$，因此又得到使 *max* 變小的狀態；若 $D>0$，由於對稱性，可得類似結果；若 $C=D=0$，則依照 *B→E→A→B→E* 的順序操作可使全部的數歸零。

以上說明了可保持至少有一數為奇數的狀態且使得 *max* 變小。

因此，當 *A, B, C, D, E* 不全為偶數時，可滿足條件要求。

(2) 當 *A, B, C, D, E* 皆為偶數時：

此亦同理於當 $n=4$ 且四數皆為偶數的情況，而由前面的討論知道只要有一數為奇數的所有情況都能滿足題目要求，故 *A, B, C, D, E* 皆為偶數時也可

滿足題目要求。

綜上所述，當 n=5 時，k 為任意正整數，皆能滿足題目要求，即五邊形在$|x-y|$型操作下的「理想 k 值」為任意正整數。

4. $n \geq 7$ 時的情況：

從 n=3, 4, 5, 6 的討論過程及結果來看，我們發現：

當 n 不是 3 的倍數時，任意整數 k 都是在$|x-y|$型操作下的「理想 k 值」。

因此我們透過演繹與猜測，進行以下的猜想一：

【猜想一】

在$|x-y|$型操作下，當 $3 \nmid n$ 時，則 n 邊形的「理想 k 值」為任意正整數。

為了要證明猜想一，我們仿照 n=5 時的討論模式，針對非 3 的倍數的正整數 n 建構一個一般性的操作模式，以作為證明猜想一的基本情境。

首先，我們要證明以下的引理一，作為此基本情境的探究開始，亦可作為猜想一的論證基礎。

【引理一】
在$|x-y|$型操作下，要使 n 邊形的各頂點數字之奇偶性經過任意操作後皆保持不變的情況，除了全是偶數之外，其狀態必須是唯一的，即在 n 必須為 3 的倍數的情況下，且各頂點上的數字必須以(奇、奇、偶、奇、奇、偶、…、奇、奇、偶)的順序方式排列，才能經過任意操作後皆保持奇偶性不變的情況。

【證明】
由於要使每個數字的奇偶性守恆，排除全是偶數的情況，則其中必有一數為奇數，只要確定那個奇數的相鄰一數的奇偶性，就能推導至後面所有數字的奇偶性：

以下所有證明皆以 1 代表奇數，以 0 代表偶數

11 → 110 → 1101 → 11011 → 110110 ……

10 → 101 → 1011 → 10110 → 101101 ……

我們可以簡單發現，以上兩者都是以奇、奇、偶、…的順序做規律的排列，因此若要以此排列規律完整接回第一項，只有在 n 是三的倍數的情況下才有可能，否則只要對第一個奇數進行操作就會使其變為偶數。亦即在有一個數是奇數的條件下，這種守恆的模式都是唯一的。得證。

接下來，我們就要分成以下兩種情況，討論當 $3 \nmid n$ 時，在$|x-y|$型操作下，n 邊形的「理想 k 值」：

(1) 初始狀態下，各頂點數字中至少有一個數字為奇數:

我們仿照之前的操作模式，即保持在只有一個奇數的狀態，不斷使 *max* 變小直到零。此時，我們只要說明這是如何操作的就可以得到合理結果。所以，要從初始狀態轉變成只有一個奇數的狀態，我們可以直接引入下面的引理二：

【引理二】

在填入 n 邊形的各頂點數字，其排列情形不符合奇偶性守恆的狀態下，則任意情況都可經過一系列的有限操作導致只剩一個頂點上的數字是奇數的狀態。

【證明】

由引理一，因此必定可以找到在一個偶數後面接兩個奇數以外的情況，我們簡單劃分為接一個奇數和接三個奇數以上的狀況，而兩者都可以經過簡單操作使得有連續兩個偶數接在一起的情況出現：

010...→ 000…→ 000…1

0111…→ 0101…→ 0001…

於是我們就有了一組奇偶性為(偶、偶、奇)的順序排列，再來我們討論接下來兩個數的奇偶性，一共有 2x2 共四種可能，這四種不同的排列順序也都可以經過簡單的操作遞進地產生一組新的(偶、偶、奇)排列：

<u>001</u>11…→ 00101…→ 00<u>001</u>…

<u>001</u>01…→ 00<u>001</u>…

<u>001</u>10…→ 01110…→ 01010 → 0<u>0010</u>…

<u>001</u>00…→ 00000…→ 00…<u>001</u>

於是我們可以再一次的進行反覆操作，直到操作中發現只剩下一個奇數的狀態為止。故對於任意不符合奇偶性守恆的狀態，我們都能操作到使之只剩一個奇數的狀態。得證。

由引理一，我們知道在 n 不為三的倍數的情況下是不會達成奇偶性守恆的狀態的(排除全為偶數的情況)，所以利用引理二，我們可以產生一個只有一個奇數的狀態，不妨假設此奇數為 A，其他偶數分別為 $A_1, A_2, \ldots\ldots,$

A_{n-1}，以圖示表示則為: $A\begin{matrix} A_1 & A_2 & A_3 & \cdots \\ A_{n-1} & A_{n-2} & A_{n-3} & \cdots \end{matrix}$，以下再按照 *max* 的奇偶性分成兩種情況：

(a) 當 *max* 為偶數，即 $A_1, A_2, \cdots, A_{n-1}$ 中有一數為 *max* 且 $A < max$，則依照 $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow \cdots \rightarrow A_{n-1}$ 的順序進行操作：

$$1\begin{matrix} 0\,0\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \rightarrow 1\begin{matrix} 1\,0\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \rightarrow 1\begin{matrix} 1\,1\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \rightarrow \cdots\cdots \rightarrow 1\begin{matrix} 1\,1\,1\cdots \\ 0\,1\,1\cdots \end{matrix} \pmod 2$$

我們記此新的狀態為 $A'\begin{matrix} A_1' & A_2' & A_3' & \cdots \\ A_{n-1}' & A_{n-2}' & A_{n-3}' & \cdots \end{matrix}$，其中 $A', A_1', A_2', \cdots\cdots A_{n-2}'$都小於 *max*(因為它們是奇數而 *max* 是偶數)，同時 $A_{n-1}' = |A' - A_{n-2}'| \leqq \mathrm{MAX}\{A', A_{n-2}'\} < max$，因此 *max* 變小了。

(b) 當 *max* 為奇數，即 $A = max$，而其餘的數皆小於 *max*。

若 $A_2 > 0$，則依照 $A_1 \rightarrow A_{n-1} \rightarrow A \rightarrow A_{n-1}$ 的順序進行操作：

$$1\begin{matrix} 0\,0\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \rightarrow 1\begin{matrix} 1\,0\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \rightarrow 1\begin{matrix} 1\,0\,0\cdots \\ 1\,0\,0\cdots \end{matrix} \rightarrow 0\begin{matrix} 1\,0\,0\cdots \\ 1\,0\,0\cdots \end{matrix} \rightarrow 0\begin{matrix} 1\,0\,0\cdots \\ 0\,0\,0\cdots \end{matrix} \pmod 2$$

我們記此新的狀態為 $A'\begin{matrix} A_1' & A_2' & A_3' & \cdots \\ A_{n-1}' & A_{n-2}' & A_{n-3}' & \cdots \end{matrix}$，其中 $A_1' = |A - A_2| < A$，因此又得到至少有一數為奇數且 *max* 變小的狀態；

若 $A_{n-2} > 0$，由於對稱性，可得類似結果；
若 $A_2 = A_{n-2} = 0$，可以依照 $A_1 \rightarrow A_{n-1} \rightarrow A \rightarrow A_1$ 的順序進行操作後，只要再引用下面的引理三，就可以直接使全部的數字歸零。得證。

> 【引理三】
>
> 在$|x-y|$型操作下，填入 n 邊形的各頂點數字，若只要有出現連續兩個零的排列狀態時，則可以經過一定的操作使得 n 邊形的各頂點數字都變為零。

【證明】

不妨假設各個數字依序為 $0, 0, B_1, B_2, \ldots, B_{n-2}$，因此整個狀態以圖示表示為：

$0\ \begin{matrix}0 & B_1 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix}$，現在我們建構一系列的操作步驟：

首先針對 B_1，我們有

$$0\ \begin{matrix}0 & B_1 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix} \rightarrow 0\ \begin{matrix}0 & B_2 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix} \rightarrow 0\ \begin{matrix}B_2 & B_2 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix} \rightarrow$$

$$0\ \begin{matrix}B_2 & 0 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix} \rightarrow 0\ \begin{matrix}0 & 0 & B_2 & \cdots \\ B_{n-2} & B_{n-3} & B_{n-4} & \cdots\end{matrix}$$

注意這裡的 0 都代表數字零，而非偶數。以上可以使得 B_1 變為零，以此類推，可以依序使 $B_2, B_3, \ldots, B_{n-2}$ 都變為零，也就是說，只要有連續兩項數字為零，我們總是可以使全部的數字都歸零。得證。

因此，上述討論說明了在各頂點不全為偶數的條件下，可以一直保持至少有一數為奇數的狀態，且使得 *max* 變小，也就是說，對於任何非三的倍數的 *n*，無論 k 值，只要初始狀態下有一個奇數，我們總是能經過一系列的操作使得各數字都歸零。

(2) 初始狀態下，各頂點數字全為偶數:

這樣的情況，在個別案例時我們都已經討論過了，但為了講究論證的嚴謹性，因此我們引進下一個引理四，以輔助論述並強化證明的嚴謹度：

【引理四】

若在 *n* 邊形的 *n* 個頂點數字至少有一數為奇數的條件下，存在滿足條件的「理想 *k* 值」(或不存在「理想 *k* 值」)時，則正 *n* 邊形的 *n* 個頂點數字都是偶數的情況仍然會有相同的「理想 *k* 值」(或不存在「理想 *k* 值」)。

【證明】

不妨假設各頂點數字分別為 $A_1, A_2, \ldots\ldots, A_n$，其中每一個數皆是偶數，因此我們必定能找到一個正整數 p 使得 $2^p \mid (A_1, A_2, \ldots\ldots, A_n)$且 $2^{p+1} \nmid (A_1, A_2, \ldots\ldots, A_n)$，我們將每個數字各除以 2^p，得到一個新的狀態，記其數字為 $A_1', A_2', \ldots\ldots, A_n'$，此狀態僅是初始狀態提出公因數的結果，並不會影響數字間的比例關係。

也就是說，對 $A_1', A_2', \ldots\ldots, A_n'$操作實質上會等價於對 $A_1, A_2, \ldots\ldots, A_n$ 操作。又 $A_1', A_2', \ldots\ldots, A_n'$這 *n* 個數當中必至少有一數為奇數，而已知在有一個奇數的條件下，皆存在滿足條件的「理想 *k* 值」(或不存在「理想 *k* 值」)，因此也說明了在各頂點皆為偶數的條件下，也存在滿足條件的相同之「理

想 k 值」(或不存在「理想 k 值」)。得證。

綜合以上所有討論，由引理一作為論證基礎出發，將初始狀態分為至少有一數為奇數或全為偶數的情況做討論，前者再以引理二導致只剩一個數是奇數的狀態，然後逐步遞減 *max* 直至零，當中有一特例情況運用到引理三的操作；後者則運用引理四推得和前者類似的操作過程。

於是我們透過上述的引理一至引理四，證明了猜想一的正確性，並將它整理而得到了以下的定理一：

【定理一】
在一個 n 邊形(n 不為 3 的倍數)的頂點上放上 n 個不盡相異的非負整數，做以下操作：擦去一個數，寫上其相鄰兩數之差的絕對值，則無論怎麼放置頂點上的數字，總是可以經過一系列的操作使得各頂點的數字歸零。

接下來，我們要討論當 n 為 3 的倍數時的情況，由引理一，於是我們知道要達成奇偶性守恆的最低條件要有 $\frac{2}{3}n$ 個奇數和 $\frac{1}{3}n$ 個偶數彼此規律排列，奇數都取 1，偶數都取 0，故 k 的最小值要為 $\frac{2}{3}n$。因此我們猜測：

【猜想二】

在 $|x-y|$ 型操作下，當 $3 \mid n$ 時，滿足條件的 k 為所有的奇數和小於 $\frac{2}{3}n$ 的偶數。

接下來我們再針對猜想二作論證，而要證明猜想二，其實可以類推到定理一的證明過程。

【證明】
由引理一，我們知道在 $|x-y|$ 型操作下的奇偶性守恆的模式是唯一的，只有在 $\frac{2}{3}n$ 個奇數和 $\frac{1}{3}n$ 個偶數彼此規律排列時才會達成，此狀態下，k 值為大於等於 $\frac{2}{3}n$ 的偶數。因此若 k 為奇數或小於 $\frac{2}{3}n$ 的偶數，一定不滿足守恆條件。
再由引理二，我們就能轉換到一個只有一個奇數的狀態，接下來的操作模式便完全等同於 n 不為三的倍數時的討論。唯一注意到的是，在其操作過程中，都會處在奇偶不守恆的情況，因此，不用顧慮會不小心進入守恆狀態。得證。

綜合以上，證明了猜想二的正確性，並將它整理而得到了以下的定理二。

【定理二】

在一個 n 邊形(n 為 3 的倍數)的頂點上放上 n 個不盡相異的非負整數，做以下操作：擦去一個數，寫上其相鄰兩數之差的絕對值，則只要頂點上的數字和是奇數或是小於 $\frac{2}{3}n$ 的偶數，總是可以經過一系列的操作使得各頂點的數字歸零。

(六) 原問題的再延伸變化之一——「$x-y$型」

將原題推廣至 n 邊形的討論結束後，我們不禁想問：

只將兩數差值的絕對值做探討是否過於狹隘？能不能將原始操作條件中的絕對值去除，即改以依照一個特定方向使兩數相減？

於是我們便開始了下一個階段的探討。

首先，我們必須要重新定義題目操作，將$|x-y|$操作改為$x-y$操作，並對於填入的數字也加入限制：這 n 個數的最大公因數為 1，論述如下：

「在一個 n 邊形的 n 個頂點上，填寫 n 個不盡相異之非負整數，且這 n 個數的最大公因數為 1。依以下規則進行操作：擦去一個數，寫上其相鄰兩數依照順時針或逆時針方向相減之差(本作品在以下探討過程中，皆是採順時針方向)。如此操作模式我們稱之為『$x-y$型操作』。」

我們在前面的(四)及(五)裡所探究的結果，得到在$|x-y|$型操作條件下的同餘守恆模式是奇偶性。

接下來，在這個階段的探討過程中，我們的首要目標是試著尋找在$x-y$型操作條件下的同餘守恆模式為何？以及此模式與n值之間的關係又為何？

雖然，原問題中乃針對「理想 k 值」進行歸零與奇偶性守恆模式之討論，然而，此階段的再延伸問題過於複雜，因此先僅就於同餘守恆模式方面進行探討，關於歸零的操作模式，僅是沿用其前面的概念，而先不在此延伸階段中進行深入討論。

1. n=3 時的狀況：

顯見，在 n=3 時也會有奇偶性守恆的狀態出現(即其同餘守恆數φ為 2)。事實上，n=3 時除了奇偶性守恆外，沒有其他的同餘守恆模式。嚴謹的證明會在後面作論述。

2. n=4 時的狀況：

(1) 在 n=4 時的探究過程中，由於不會出現奇偶性守恆的狀況，於是我們從

k=1,2, 3…的所有狀態開始逐數尋找「同餘守恆模式」。發現當 k 小於 10 時，都是「理想 k 值」，無論如何擺放數字都能操作到全數歸零，即不滿足守恆狀態；然而當 k=10 且四個頂點上的數依順時針方向以 1, 2, 4, 3 排列時，發現無論怎樣操作，都無法導致全數歸零的狀態。

【證明】

我們應用數學模型中同餘模數的概念，將各頂點的數以圖示表示:

$$1\begin{matrix}2\\3\end{matrix}4$$

仔細觀察，發現到對 1 和 3 進行操作並不改變其數值；而當對 2 和 4 進行操作時，所得新的數值都是原數值減 5:

$$1\begin{matrix}2\\3\end{matrix}4 \rightarrow 1\begin{matrix}-3\\3\end{matrix}4$$

$$1\begin{matrix}2\\3\end{matrix}4 \rightarrow 1\begin{matrix}2\\3\end{matrix}-1$$

由於我們是進行$x-y$型的線性操作，因此在之後的每一次操作後，各頂點的數值之間始終都會相差 5 的倍數，同時我們發現到，四個頂點除以五的餘數不全為零，而且無論怎麼操作都不會改變其模 5 的餘數，因此也不可能導致全數歸零的狀態。

亦即 5 是四邊形在$x-y$型操作下的「同餘守恆數」。得證。

【心得二】

根據上面的討論，可知 5 是四邊形在$x-y$型操作下的「同餘守恆數」。另一方面，在探究過程中，我們猜想：某種排列的數值在$x-y$操作模式下，出現模餘數不守恆，也可能無法達成歸零狀態。即**同餘守恆與歸零之間的因果關係只是單方向。**

(2) 發現到四邊形有一個同餘守恆數是 5，我們能依照同樣的方法證明當 n 為 4 的倍數時，5 皆為其 n 邊形的同餘守恆數。

【證明】

考慮當 n 為 4 的倍數時，如下的操作狀態：

$$1\begin{matrix}2\,4\,3\,1\,2\cdots\\3\,4\,2\,1\,3\cdots\end{matrix} \pmod 5$$

發現到，無論如何操作，每一個數字模 5 的餘數皆不會改變，亦即當 $4 \mid n$ 時，φ=5 為其「同餘守恆數」。得證。

3. n=5 時的狀況：

(1) 在探究 *n*=5 時，我們也發現了其同餘守恆數φ=11，守恆狀態則為

$$9\begin{matrix}5&4\\3&1\end{matrix} \pmod{11}$$

【證明】

證明其守恆的方法同於 n=4, φ=5 的情況，設初始數值狀態以圖示表示為

$$9\begin{matrix}5&4\\3&1\end{matrix}$$

首先注意到操作後會改變其原數值的僅有對 3 和 9 操作，而所得新數值皆為原數值減 11，操作情況如下：

$$9\begin{matrix}5&4\\3&1\end{matrix} \rightarrow 9\begin{matrix}5&4\\-8&1\end{matrix}$$

$$9\begin{matrix}5&4\\3&1\end{matrix} \rightarrow -2\begin{matrix}5&4\\3&1\end{matrix}$$

由於我們是進行$x-y$型的線性操作，因此在之後的每一次操作後，各頂點的數值之間始終都會相差 11 的倍數，無論怎麼操作都不會改變其模 11 的餘數，又由於各頂點模 11 的餘數不全為零，因此不可能導致全數歸零的狀態。

亦即 11 是五邊形在$x-y$型操作下的「同餘守恆數φ」。得證。

【進一步說明】

要證明同餘守恆性不難，然而問題在於如何找到守恆狀態。在 *n*=5 時，我們是以「化簡」的方式在做探索。首先以圖示表示操作狀態，如下：

$$A\begin{matrix}B&C\\E&D\end{matrix}$$

接著，我們希望透過一連串的步驟使得五個頂點只剩下比例關係，亦即消去四個字母，只剩下一個字母及其係數，如此一來，即可化簡成特殊情況，而若是有辦法繼續操作使之歸零，就說明任意情況皆有解；若是無法歸零即可能是產生守恆的狀態。

我們按照 B→D 的操作順序先消去 B, D，剩下 A, C, E 三種字母，如下：

$$A\begin{matrix}B&C\\E&D\end{matrix} \rightarrow A\begin{matrix}A-C&C\\E&C-E\end{matrix}$$

再來，我們按照 C→D→C→E 的操作順序消去 E，如下：

$$A\begin{matrix}A-C&C\\E&C-E\end{matrix} \rightarrow A\begin{matrix}A-C&C\\-2C&A-2C\end{matrix}$$

接著我們發現到 A 出現在三個頂點，而 C 出現在四個頂點，因此我們決定消去 A，依照 D→C→B→C→A 的順序操作，如下：

$$A\begin{matrix}A-C & C\\ -2C & A-2C\end{matrix} \rightarrow -6C\begin{matrix}4C & C\\ -2C & 3C\end{matrix}$$

最終化簡至使各頂點只剩下比例關係時，發現我們的守恆模式，如下：

$$-6C\begin{matrix}4C & C\\ -2C & 3C\end{matrix} \equiv -6\begin{matrix}4 & 1\\ -2 & 3\end{matrix} \equiv 5\begin{matrix}4 & 1\\ 9 & 3\end{matrix} \pmod{11}$$

事實上，當 n=4 時也能利用相同的方法發現其「同餘守恆數」，按照 B→D→A→B→A→C→B→D 的順序操作，以下以圖示表示，如下：

$$A\begin{matrix}B\\ D\end{matrix}C \rightarrow A\begin{matrix}2A\\ -2A\end{matrix}-A \equiv 1\begin{matrix}2\\ -2\end{matrix}-1 \equiv 1\begin{matrix}2\\ 3\end{matrix}4 \pmod{5}$$

(2) 找到 n=5 的同餘守恆數之後，我們可以仿照 n=4 時的情況，推廣至 n 為 5 的倍數的情況：

當 5 | n 時在$x-y$型操作條件下，都有同餘守恆數φ=11。

【證明】

當 n 為 5 的倍數時，考慮如下的操作狀態，如下：

$$9\begin{matrix}5\,4\,1\,3\,9\cdots\\ 3\,1\,4\,5\,9\cdots\end{matrix} \pmod{11}$$

顯然，無論對何數操作都不會改變其模 11 的餘數，因此此狀態可說明其「同餘守恆數」φ=11。

故當 5 | n 時在$x-y$型操作條件下，都有同餘守恆數φ=11。得證。

4. 發展找尋同餘守恆數更有效率的模式：

截至目前為止，我們初步有了方法來尋求同餘守恆模式，然而隨著 n 越來越大，這方法將會越來越繁複，而且無法說明唯一性，即同樣的 n 值或許有不同的同餘守恆數與同餘守恆狀態。

於是我們接下來要發展出一套有系統的方法作後續探討，首先考慮一個同餘守恆狀態:

$$a_1\begin{matrix}a_n & \cdots & \cdots\\ a_2 & a_3 & \ldots\end{matrix} (mod\ \varphi_n)$$

由守恆狀態的定義可以知道

$$a_k-(a_{k+1}-a_{k-1}) \equiv 0\ (mod\ \varphi_n)$$
$$\Rightarrow\ a_{k-1}+a_k \equiv a_{k+1}\ (mod\ \varphi_n)$$

其中$k = 1, 2, \dots, n$且令$a_{n+1} = a_1$。

於是我們便可建構出【數學模型三】(敘述於前(三))，這樣的遞迴累加方式，換言之其實就是**依照$x - qy$型的操作模式逆向填入數字，確保數字在經過操作後不會改變，使其依然維持守恆的狀態。**

但是注意到，依照這樣的模式填入，最後會有兩個數字經過操作後會改變其數值(分別為第一個和最後一個填入的數字)，而這兩個數字前後改變的差值的公因數就是我們要尋找的同餘守恆數，理由如同前述證明時的討論。

由於是探究$x - y$型的操作，若我們將初始的兩項非負整數記為α、β，便有以下狀態：

α	$F_{n-2}\alpha + F_{n-1}\beta$	$F_{n-3}\alpha + F_{n-2}\beta$	…	…	…
	β	$\alpha + \beta$	$\alpha + 2\beta$	$2\alpha + 3\beta$	…

當中的F_n表示費氏數列$< 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13 \dots\dots >$中的第 n 項。

我們令$\mathrm{P} = F_{n-3}\alpha + F_{n-2}\beta$；$\mathrm{Q} = F_{n-2}\alpha + F_{n-1}\beta$，即上述狀態最後填入的兩個數。而在上述狀態下經過一次操作後的數值會改變的數字為Q和α，以Q'和α'分別表示他們操作後的數值，則

$$\mathrm{Q}' = \alpha - P = \alpha - (F_{n-3}\alpha + F_{n-2}\beta) = (1 - F_{n-3})\alpha - F_{n-2}\beta$$
$$\alpha' = \beta - \mathrm{Q} = \beta - (F_{n-2}\alpha + F_{n-1}\beta) = -F_{n-2}\alpha + (1 - F_{n-1})\beta$$

他們與原數值的差分別為

$$\begin{aligned}\mathrm{Q} - \mathrm{Q}' &= (F_{n-2}\alpha + F_{n-1}\beta) - [(1 - F_{n-3})\alpha - F_{n-2}\beta] \\ &= (F_{n-2} + F_{n-3} - 1)\alpha + (F_{n-1} + F_{n-2})\beta \\ &= (F_{n-1} - 1)\alpha + F_n\beta \\ \alpha - \alpha' &= \alpha - [-F_{n-2}\alpha + (1 - F_{n-1})\beta] \\ &= (F_{n-2} + 1)\alpha + (F_{n-1} - 1)\beta\end{aligned}$$

這時我們要尋求的同餘守恆數φ即為這兩個差值的公因數，我們令函數

$$g(n) = gcd((F_{n-1} - 1)\alpha + F_n\beta,\ (F_{n-2} + 1)\alpha + (F_{n-1} - 1)\beta)$$

因此有$\varphi \mid g(n)$。

此外，注意到由於我們現在的初始狀態是遞迴累加的數字，根據操作定義，這n個數的最大公因數為 1，因此初始項α、β必須要互質。

【心得三】
比較一開始以「化簡」的方式在做探索，我們所建構出的這個數學模型三，明顯較有系統與邏輯。接下來只要討論由這個模型所推演出的函數$g(n)$，便能求出同餘守恆數和同餘守恆狀態的初始項，而後依據數學模型建構出整個

守恆狀態。

5. 同餘守恆數的分類與求ϕ_n值

由剛剛的討論，知道這個階段我們要討論函數$g(n)$。但由於函數$g(n)$的值牽涉到變數α、β的值與他們的係數關係，而對於α、β的取值討論較為複雜，因此這個階段我們先處理α、β的係數間的關係。

下表先列出了 *n* 從 3 到 20 所對應的 *g*(*n*):

n	$g(n)$	係數間的最大公因數
3	$\gcd(2\beta, 2\alpha)$	2
4	$\gcd(\alpha+3\beta, 2\alpha+\beta)$	1
5	$\gcd(2\alpha+5\beta, 3\alpha+2\beta)$	1
6	$\gcd(4\alpha+8\beta, 4\alpha+4\beta)$	4
7	$\gcd(7\alpha+13\beta, 6\alpha+7\beta)$	1
8	$\gcd(12\alpha+21\beta, 9\alpha+12\beta)$	3
9	$\gcd(20\alpha+34\beta, 14\alpha+20\beta)$	2
10	$\gcd(33\alpha+55\beta, 22\alpha+33\beta)$	11
11	$\gcd(54\alpha+89\beta, 35\alpha+54\beta)$	1
12	$\gcd(88\alpha+144\beta, 56\alpha+88\beta)$	8
13	$\gcd(143\alpha+233\beta, 90\alpha+143\beta)$	1
14	$\gcd(232\alpha+377\beta, 145\alpha+232\beta)$	29
15	$\gcd(376\alpha+610\beta, 234\alpha+376\beta)$	2
16	$\gcd(609\alpha+987\beta, 378\alpha+609\beta)$	21
17	$\gcd(986\alpha+1597\beta, 611\alpha+986\beta)$	1
18	$\gcd(1596\alpha+2584\beta, 988\alpha+1596\beta)$	76
19	$\gcd(2583\alpha+4181\beta, 1598\alpha+2583\beta)$	1
20	$\gcd(4180\alpha+6765\beta, 2585\alpha+4180\beta)$	55

首先從表中會發現到，對於某些特定的 *n* 值，*g*(*n*)可以先做初步的化簡，即提出係數間的最大公因數。這意味著，在這些情況下，只要確保互質，則可以**任取**α、β的值，然後按照【數學模型三】的方式將數字填滿各頂點，最後的狀態必為同餘守恆狀態，且這些由 *g*(*n*)做初步化簡所提出的公因數便為其同餘守恆數。我們將此提出的最大公因數稱為「本原守恆數」，以符號記為「ϕ_n」。

我們針對 *g*(*n*)以輾轉相除法作進一步的化簡，以求取ϕ_n的規律和數值:

$$g(n) = \gcd((F_{n-1}-1)\alpha + F_n\beta,\ (F_{n-2}+1)\alpha + (F_{n-1}-1)\beta)$$

$$= \gcd((F_{n-3}-2)\alpha+(F_{n-2}+1)\beta,\ (F_{n-2}+1)\alpha+(F_{n-1}-1)\beta)$$
$$= \gcd((F_{n-3}-2)\alpha+(F_{n-2}+1)\beta,\ (F_{n-4}+3)\alpha+(F_{n-3}-2)\beta)$$
$$\vdots$$
$$\vdots$$
$$= \gcd((F_{n-k}-F_k)\alpha+(F_{n-k+1}+F_{k-1})\beta,\ (F_{n-k+1}+F_{k-1})\alpha+(F_{n-k+2}-F_{k-2})\beta)$$
$$= \gcd((F_{n-k}-F_k)\alpha+(F_{n-k+1}+F_{k-1})\beta,\ (F_{n-k-1}+F_{k+1})\alpha+(F_{n-k}-F_k)\beta)$$

要特別注意的是這裡的 k 是奇數。

再來我們將 n 值分為四類，並分別證明以下定理三的各項：

【定理三】在「$x-y$型操作條件」下，則

(1)當 n 為 4 的倍數時，$\phi_n = F_{\frac{n}{2}}$

(2)當 n 為 2 的倍數但不為 4 的倍數時，$\phi_n = L_{\frac{n}{2}}$

(3)當 n 是奇數且為 3 的倍數時，$\phi_n = 2$

(4)當 n 是奇數且不為 3 的倍數時，$\phi_n = 1$

其中，「ϕ_n」為「本原守恆數」，F_n為費氏數列的第 n 項，L_n為盧卡斯數列的第 n 項。

【證明】

(1) 當 n 為 4 的倍數時，令$n = 4t$，$k = 2t+1$，其中 t 為正整數。則:

$$g(n) = \gcd((F_{n-k}-F_k)\alpha+(F_{n-k+1}+F_{k-1})\beta,\ (F_{n-k+1}+F_{k-1})\alpha+(F_{n-k+2}-F_{k-2})\beta)$$
$$= \gcd((F_{2t-1}-F_{2t+1})\alpha+(F_{2t}+F_{2t})\beta,\ (F_{2t}+F_{2t})\alpha+(F_{2t+1}-F_{2t-1})\beta)$$
$$= \gcd((-F_{2t})\alpha+(2F_{2t})\beta,\ (2F_{2t})\alpha+(F_{2t})\beta)$$
$$= F_{2t}\cdot\gcd(-\alpha+2\beta,\ \ 2\alpha+\beta)$$

$\Rightarrow \phi_n = F_{2t} = F_{\frac{n}{2}}$。得證。

(2) 當 n 為 2 的倍數但不為 4 的倍數時，令$n = 2t$，$k = t$，其中t為奇數。則:

$$g(n) = \gcd((F_{n-k}-F_k)\alpha+(F_{n-k+1}+F_{k-1})\beta,\ (F_{n-k-1}+F_{k+1})\alpha+(F_{n-k}-F_k)\beta)$$
$$= \gcd((F_t-F_t)\alpha+(F_{t+1}+F_{t-1})\beta,\ (F_{t-1}+F_{t+1})\alpha+(F_t-F_t)\beta)$$
$$= \gcd((F_{t+1}+F_{t-1})\beta,\ (F_{t-1}+F_{t+1})\alpha)$$
$$= (F_{t-1}+F_{t+1})\cdot\gcd(\beta,\alpha)$$

$\Rightarrow \phi_n = F_{t-1}+F_{t+1} = F_{\frac{n}{2}-1}+F_{\frac{n}{2}+1} = L_{\frac{n}{2}}$。得證。

(3) 當 n 是奇數且為 3 的倍數時，令$n = 6t-3$，$k = 3t-1$，其中 t 為偶數。則:

$$g(n) = \gcd((F_{n-k}-F_k)\alpha+(F_{n-k+1}+F_{k-1})\beta,\ (F_{n-k-1}+F_{k+1})\alpha+(F_{n-k}-F_k)\beta)$$

$= \gcd((F_{3t-2} - F_{3t-1})\alpha + (F_{3t-1} + F_{3t-2})\beta,\ (F_{3t-3} + F_{3t})\alpha + (F_{3t-2} - F_{3t-1})\beta)$

$= \gcd((-F_{3t-3})\alpha + (F_{3t})\beta,\ (F_{3t-3} + F_{3t})\alpha + (-F_{3t-3})\beta)$

$\Rightarrow \phi_n = \gcd(F_{3t},\ F_{3t-3})$

$= \gcd(2F_{3t-2} + F_{3t-3},\ F_{3t-3})$

$= \gcd(2F_{3t-2},\ F_{3t-3})$

$= 2$

若 t 為奇數，則取$k = 3t - 2$，可得同樣結果。得證。

(4) 當 n 是奇數且不為 3 的倍數時，又分兩種情況:

a. $n = 6t - 1$，令$k = 3t$，其中 t 為奇數。則:

$g(n) = \gcd((F_{n-k} - F_k)\alpha + (F_{n-k+1} + F_{k-1})\beta,\ (F_{n-k-1} + F_{k+1})\alpha + (F_{n-k} - F_k)\beta)$

$= \gcd((F_{3t-1} - F_{3t})\alpha + (F_{3t} + F_{3t-1})\beta,\ (F_{3t-2} + F_{3t+1})\alpha + (F_{3t-1} - F_{3t})\beta)$

$= \gcd((-F_{3t-2})\alpha + (F_{3t} + F_{3t-1})\beta,\ (F_{3t-2} + F_{3t+1})\alpha + (-F_{3t-2})\beta)$

$\Rightarrow \phi_n = \gcd(F_{3t+1},\ F_{3t-2})$

$= \gcd(2F_{3t-1} + F_{3t-2},\ F_{3t-2})$

$= \gcd(2F_{3t-1},\ F_{3t-2})$

$= 1$

若 t 為偶數，則取$k = 3t - 1$，可得同樣結果。

b. $n = 6t + 1$，令$k = 3t$，其中 t 為奇數。則:

$g(n) = \gcd((F_{n-k} - F_k)\alpha + (F_{n-k+1} + F_{k-1})\beta,\ (F_{n-k-1} + F_{k+1})\alpha + (F_{n-k} - F_k)\beta)$

$= \gcd((F_{3t+1} - F_{3t})\alpha + (F_{3t+2} + F_{3t-1})\beta,\ (F_{3t} + F_{3t+1})\alpha + (F_{3t+1} - F_{3t})\beta)$

$= \gcd((F_{3t-1})\alpha + (F_{3t+2} + F_{3t-1})\beta,\ (F_{3t+2})\alpha + (F_{3t-1})\beta)$

$\Rightarrow \phi_n = \gcd(F_{3t+2},\ F_{3t-1})$

$= \gcd(2F_{3t} + F_{3t-1},\ F_{3t-1})$

$= \gcd(2F_{3t},\ F_{3t-1})$

$= 1$

若 t 為偶數，則取$k = 3t + 1$，可得同樣結果。得證。

討論完了「本原守恆數ϕ_n」，對於函數$g(n)$的初步化簡和係數關係已經有了完整的結果，接下來我們便要針對函數中的變數(即α、β)做深入的探究。

6. 同餘守恆數的分類與求φ_n值

在意義上來說，所謂「本原守恆數ϕ_n」和我們現在要求的「同餘守恆數φ_n」，前者為後者的一個特例，兩者間最大的差異在於求取的過程: 前者是針對係數作探討，不討論變數α、β的取值，亦即此時的α、β就算任取也能保證守恆；而後者則是針對變數作探討，討論α、β的取值在甚麼情況下，函數$g(n)$才會有最大值(即同餘守恆數的最大值)，也就是我們現在要探究的目標。

【探討&化簡】

(1) 首先回到$g(n)$的原式：

$$\mathrm{g(n)} = \gcd((F_{n-1}-1)\alpha + F_n\beta,\ (F_{n-2}+1)\alpha + (F_{n-1}-1)\beta)$$

對於不同的α、β取值，g(n)會有不同的值，我們假設在g(n)有最大值的情況下，$\alpha = \alpha_0$ 、$\beta = \beta_0$，且令此最大值為M_g。則

$$M_g = \gcd((F_{n-1}-1)\alpha_0 + F_n\beta_0,\ (F_{n-2}+1)\alpha_0 + (F_{n-1}-1)\beta_0)$$

所以有

$M_g \mid (F_{n-1}-1)\alpha_0 + F_n\beta_0$
$M_g \mid (F_{n-2}+1)\alpha_0 + (F_{n-1}-1)\beta_0$

再來我們用加減消去法α_0使得只剩下一個未知數

$M_g \mid (F_{n-2}+1)[(F_{n-1}-1)\alpha_0 + F_n\beta_0] - (F_{n-1}-1)[(F_{n-2}+1)\alpha_0 + (F_{n-1}-1)\beta_0]$
$M_g \mid [(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2]\beta_0$ ——(1)

同理，也可以消去β_0
$M_g \mid (F_{n-1}-1)[(F_{n-1}-1)\alpha_0 + F_n\beta_0] - F_n[(F_{n-2}+1)\alpha_0 + (F_{n-1}-1)\beta_0]$
$M_g \mid -[(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2]\alpha_0$ ——(2)

由式(1)及式(2)，由於α_0和β_0互質，所以可得:
$M_g \mid [(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2]$

仔細觀察剛剛加減消去的過程中，事實上，我們可得M_g的最大值為

$\frac{(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2}{\gcd(F_{n-2}+1,\ F_{n-1}-1)}$，當中的分母恰為剛剛所求的"$\phi_n$"。

而α_0 、β_0也能仔細觀察後以參數式的形式簡單得出，即

$$\begin{cases} \alpha_0 = \frac{(F_{n-1}-1)-F_n t}{\phi_n} \\ \beta_0 = \frac{-(F_{n-2}+1)+(F_{n-1}-1)t}{\phi_n} \end{cases}, t\text{為整數}$$

此時$M_g = \frac{(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2}{\phi_n}$，

這便是我們所要求的同餘守恆數φ_n的最大值，記為"φ_{Mn}"。

(2) 我們將此結果作進一步的化簡：

由費氏數列的一般項: $F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$，為了方便起見，我們令

$a=\frac{1+\sqrt{5}}{2}$ 、$b=\frac{1-\sqrt{5}}{2}$。

$$
\begin{aligned}
&(F_{n-2}+1)\cdot F_n-(F_{n-1}-1)^2\\
&=\left[\frac{1}{\sqrt{5}}(a^{n-2}-b^{n-2})+1\right]\cdot\frac{1}{\sqrt{5}}(a^n-b^n)-\left[\frac{1}{\sqrt{5}}(a^{n-1}-b^{n-1})\right]^2\\
&=\left[\frac{1}{5}(a^n-b^n)(a^{n-2}-b^{n-2})+\frac{1}{\sqrt{5}}(a^n-b^n)\right]\\
&\quad-\left[\frac{1}{5}(a^{2n-2}-2a^{n-1}b^{n-1}+b^{2n-2})-\frac{2}{\sqrt{5}}(a^{n-1}-b^{n-1})+1\right]\\
&=\left\{\frac{1}{5}[a^{2n-2}+b^{2n-2}-a^{n-2}b^{n-2}(a^2+b^2)]+\frac{1}{\sqrt{5}}(a^n-b^n)\right\}\\
&\quad-\left[\frac{1}{5}(a^{2n-2}-2a^{n-1}b^{n-1}+b^{2n-2})-\frac{2}{\sqrt{5}}(a^{n-1}-b^{n-1})+1\right]\\
&=F_n+2F_{n-1}+\frac{1}{5}[-3(ab)^{n-2}+2(ab)^{n-1}]-1\\
&=F_n+2F_{n-1}+[(-1)^{n-1}]-1\\
&=\begin{cases}L_n,\ \text{若}n\text{為奇數}\\ L_n-2,\ \text{若}n\text{為偶數}\end{cases}
\end{aligned}
$$

這裡的L_n表示盧卡斯數列$<1,\ 3,\ 4,\ 7,\ 11,\ 18\ldots\ldots>$中的第$n$項。

(下文中所有L_n皆表示盧卡斯數列的第 n 項)

由以上的探討與論證結果，我們整理得到了以下的定理四：

【定理四】在「$x-y$型操作條件」下，n邊形的最大同餘守恆數

$\begin{cases}\varphi_{Mn}=\frac{L_n}{\phi_n}\ ,\ \text{若}n\text{為奇數}\\ \varphi_{Mn}=\frac{L_n-2}{\phi_n}\ ,\ \text{若}n\text{為偶數}\end{cases}$，且此時在遞迴累加模型中的初始兩項為

$\begin{cases}\alpha_0=\frac{(F_{n-1}-1)-F_nt}{\phi_n}\\ \beta_0=\frac{-(F_{n-2}+1)+(F_{n-1}-1)t}{\phi_n}\end{cases}$，$t$為整數

7. 同餘守恆數的統整：

(1) 截至目前為止，我們已經探討完了「本原守恆數ϕ_n」和「最大同餘守恆數φ_{Mn}」，也知道其他的同餘守恆數φ_n都是φ_{Mn}的因數。然而我們想問: 是否存在這樣的情況，使得某數φ_n為該條件下的同餘守恆數，而φ_{Mn}卻不是。

舉例來說，以$n=12$時為例，其本原守恆數為 2，最大同餘守恆數為 40，下面列出了它的所有七個同餘守恆數的一個守恆狀態，如下：

$33\ \begin{matrix}11 & 22 & 29 & 33 & 36\\ 4 & 37 & 1 & 38 & 39\end{matrix}\ 37 \pmod{40}$　　$13\ \begin{matrix}11 & 2 & 9 & 13 & 16\\ 4 & 17 & 1 & 18 & 19\end{matrix}\ 17 \pmod{20}$

$3\ \begin{matrix}1 & 2 & 9 & 3 & 6\\ 4 & 7 & 1 & 8 & 9\end{matrix}\ 7 \pmod{10}$　　$1\ \begin{matrix}3 & 6 & 5 & 1 & 4\\ 4 & 5 & 1 & 6 & 7\end{matrix}\ 5 \pmod{10}$

$3\ \begin{matrix}1 & 2 & 4 & 3 & 1\\ 4 & 2 & 1 & 3 & 4\end{matrix}\ 2 \pmod{5}$　　$1\ \begin{matrix}3 & 2 & 1 & 1 & 0\\ 0 & 1 & 1 & 2 & 3\end{matrix}\ 1 \pmod{4}$

$1\ \begin{matrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 1 & 0 & 1\end{matrix}\ 1 \pmod{2}$

由此可知，結果是可以的。

而對於所有的 n 值是否都能成立，答案也是肯定的。以下將論證:

【定理五】

在「$x-y$型操作條件」下，假設其n邊形的最大同餘守恆數為φ_{Mn}且$d \mid \varphi_{Mn}$，則我們必可找到一個狀態，滿足:此狀態各數間的最大公因數為 1，且d是這個狀態的最大同餘守恆數。

【證明】

假設有n個數為守恆狀態時，而且有最大同餘守恆數為φ_{Mn}，以圖示表示:

$$a_1\ \begin{matrix}a_n & a_{n-1} & \cdots\\ a_2 & a_3 & \cdots\end{matrix}\ \cdots \pmod{\varphi_{Mn}}$$

再來，我們考慮正整數d使得$d \mid \varphi_{Mn}$，令$b_k \equiv a_k \pmod{d}$ $(k = 1,\ 2, \dots, m)$且b_k屬於mod d的最小非負完全剩餘系，即$0 \le b_k \le d-1$。因此b_k的值是被唯一確定的。

接著，以b_k替換原狀態中的a_k:

$$b_1\ \begin{matrix}b_n & b_{n-1} & \cdots\\ b_2 & b_3 & \cdots\end{matrix}\ \cdots \pmod{d}$$

然後我們看各個數字操作前後的差值，令為b'_k，則:

$$\begin{aligned} b'_k &= b_k - (b_{k+1} - b_{k-1})\\ &= b_{k-1} + b_k - b_{k+1}\\ &\quad (\text{令} b_{n+1} = b_1)\end{aligned}$$

而從原守恆狀態，令a'_k表示a_k操作前後的差值，則我們知道:

$$\varphi_{Mn} \mid a'_k$$

即

$$\begin{aligned} a'_k &= a_k - (a_{k+1} - a_{k-1})\\ &= a_{k-1} + a_k - a_{k+1}\\ &= \varphi_{Mn} \cdot t_k\\ &\quad (\text{令} a_{n+1} = a_1)\end{aligned}$$

其中t_k為整數。又因為

$$b_k \equiv a_k \ (\text{mod d})$$
$$\Rightarrow b_k = a_k - d \cdot l_k \ \ (l_k \in Z)$$

所以我們可以重新改寫b'_k:

$$\begin{aligned} b'_k &= b_{k-1} + b_k - b_{k+1} \\ &= (a_{k-1} - l_{k-1} \cdot d) + (a_k - l_k \cdot d) - (a_{k+1} - l_{k+1} \cdot d) \\ &= (a_{k-1} + a_k - a_{k+1}) - d(l_{k-1} + l_k - l_{k+1}) \\ &= t_k \cdot \varphi_{Mn} - d \cdot l'_k \ \ (l'_k \in Z) \\ &= d \cdot t'_k \end{aligned}$$

其中t'_k為整數。

因此我們知道，b_k操作前後模d的值不變，即d為新狀態下的同餘守恆數。

又注意到，因為$0 \le b_k \le d-1$，所以

$$\begin{aligned} b'_k &= d \cdot t'_k \\ &= b_{k-1} + b_k - b_{k+1} \\ &\le 2(d-1) \\ &< 2\text{d} \end{aligned}$$

t'_k被迫只能為 0 或 1。亦即d是在新狀態下的最大同餘守恆數。

另一方面，由操作定義，各數間必須要為互質，

於是假設

$$gcd(b_1, b_2, \dots\dots, b_n) = r$$

那麼

$$gcd(d, r) = 1$$

因為如果d和r有公因數，由式子

$$b_k = a_k - d \cdot l_k$$

可以推得$a_1, a_2, \dots\dots, a_n$也有公因數$r$，即原始狀態下各數不互質，與定義不合，所以$d$和$r$必定互質。而$r$又是各數間的最大公因數，所以此狀態必有同餘守恆數$dr$，同時我們已知$d$是在新狀態下的最大同餘守恆數，故$r = 1$，即在新狀態下，各數間最大公因數為1。

因此，只要我們選定d值，就能透過以上方法導致我們要的狀態，而且保證各數間最大公因數為 1，且d為該狀態下的最大同餘守恆數。得證。

(2) 下表統整了目前的結果:

n	ϕ_n	φ_{Mn}	φ_n
$4t$	$F_{\frac{n}{2}}$		

$4t+2$	$L_{\frac{n}{2}}$	$\frac{L_n-2}{\phi_n}$	φ_{Mn}的因數
$6t-3$	2	$\frac{L_n}{\phi_n}$	
$6t\pm1$	1		

*t為正整數

(七) 同餘守恆模式之探究過程

在找尋完了同餘守恆數的數值之後，我們想要知道同餘守恆的「狀態」是否有特殊的性質，舉例來說，我們發現到$n=5$時，除了前面提到過的一種守恆狀態，如下：

$$1\ \begin{matrix}3 & 9\\ 4 & 5\end{matrix}\ (\text{mod } 11)$$

以外，還有另一種守恆狀態，如下：

$$2\ \begin{matrix}6 & 7\\ 8 & 10\end{matrix}\ (\text{mod } 11)$$

而這兩種狀態內的數字恰好是將數字 1~10 沒有重複的填入，更甚者，我們還發現到其實第一種守恆狀態內的數字 1、3、4、5、9 也恰好就是 11 的二次剩餘!。因此就開啟了我們這個階段的探討。

對於【數學模型四】中的前兩個狀態(累加態和基態)，於前述討論時可大略觀之，而循環群態在前述討論中並未出現，其主要論述部分在會在後面呈現。

1. 在這個階段中，我們首先定義好了守恆狀態的分類後，便要開始探討其性質。我們將分為n是質數或合數兩種情況討論。

   (1) 針對n為質數時進行觀察：

   a. 當$n=3$時，情況只有$1\ \begin{matrix}1\\0\end{matrix}\ (\text{mod } 2)$ 一種狀態，沒有討論空間。

   b. 當$n=5$時，有兩種守恆狀態:

   $$1\ \begin{matrix}3 & 9\\ 4 & 5\end{matrix}\ (\text{mod } 11) \qquad 2\ \begin{matrix}6 & 7\\ 8 & 10\end{matrix}\ (\text{mod } 11)$$

   注意到由於$11\equiv 1\ (\text{mod } 5)$，於是數字 1~10 便恰好能不重複的出現在兩個狀態中。而在仔細觀察後還會發現到其中一個狀態內的數字恰為 11 的二次剩餘，另一個狀態內的數字則為 11 的二次非剩餘。

   c. 當$n=7$時，有四種守恆狀態，如下：

$$23\begin{matrix}7 & 16 & 20\\ 1 & 24 & 25\end{matrix}\ (mod\ 29) \qquad 17\begin{matrix}14 & 3 & 11\\ 2 & 19 & 21\end{matrix}\ (mod\ 29)$$

$$5\begin{matrix}28 & 6 & 22\\ 4 & 9 & 13\end{matrix}\ (mod\ 29) \qquad 10\begin{matrix}27 & 12 & 15\\ 8 & 18 & 26\end{matrix}\ (mod\ 29)$$

恰好也是將數字從 1~28 不重複的填入。

但由於分成了四種狀態，所以沒辦法像$n = 5$時將數字簡單劃分為二次剩餘和二次非剩餘，但是我們仍舊發現到，這四組數字之間也有類似於二次剩餘和二次非剩餘之間的關係，為了更清楚的說明，我們定義符號

$$\mathbf{K}\otimes\mathbf{L} = \mathbf{M}\ (\boldsymbol{mod\ p})$$

表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合M之內。

若舉剛剛$n = 5$時的情況為例，將第一個狀態內的數字(1,3,4,5,9)記為集合 A，另一組數字(2,6,7,8,10)記為集合 B，那我們便有

$\mathrm{A}\otimes\mathrm{A} = \mathrm{A}\ (\mathrm{mod}\ 11)$　$\mathrm{A}\otimes\mathrm{B} = \mathrm{B}\ (\mathrm{mod}\ 11)$　$\mathrm{B}\otimes\mathrm{B} = \mathrm{A}\ (\mathrm{mod}\ 11)$

這其實就是二次剩餘和二次非剩餘之間的關係，只是我們以符號來表徵。

再回到$n = 7$的狀況，若我們將以上狀態內的數字分為四組，如下：

$$\mathrm{A} = \{1, 7, 16, 20, 23, 24, 25\}$$
$$\mathrm{B} = \{2, 3, 11, 14, 17, 19, 21\}$$
$$\mathrm{C} = \{4, 5, 6, 9, 13, 22, 28\}$$
$$\mathrm{D} = \{8, 10, 12, 15, 18, 26, 27\}$$

則我們可以得到以下關係:

$\mathrm{A}\otimes\mathrm{A} = \mathrm{A}\ (\mathrm{mod}\ 29)$　$\mathrm{A}\otimes\mathrm{B} = \mathrm{B}\ (\mathrm{mod}\ 29)$　$\mathrm{A}\otimes\mathrm{C} = \mathrm{C}\ (\mathrm{mod}\ 29)$

$\mathrm{A}\otimes\mathrm{D} = \mathrm{D}\ (\mathrm{mod}\ 29)$　$\mathrm{B}\otimes\mathrm{B} = \mathrm{C}\ (\mathrm{mod}\ 29)$　$\mathrm{B}\otimes\mathrm{C} = \mathrm{C}\ (\mathrm{mod}\ 29)$

$\mathrm{B}\otimes\mathrm{D} = \mathrm{A}\ (\mathrm{mod}\ 29)$　$\mathrm{C}\otimes\mathrm{C} = \mathrm{A}\ (\mathrm{mod}\ 29)$　$\mathrm{C}\otimes\mathrm{D} = \mathrm{B}\ (\mathrm{mod}\ 29)$

$\mathrm{A}\otimes\mathrm{B} = \mathrm{B}\ (\mathrm{mod}\ 29)$

【心得四】

觀察$n = 7$的情況，除了狀態間的數字都不會重複出現以外，數字間出現了「乘法」的結構。在還不清楚數字間的內部結構時，這樣的運算性質顯得有些複雜，於是有以下幾點可能要考量的：

1. 是否能找到另一種比較簡單的等價情況，依然能表述這十個運算性質。事實上，這樣的等價情況是有的，在經過嘗試與尋找之後，我們發現上述運算性質可以簡化為 5 的最簡剩餘類，如下：

   $\mathrm{A}' = 1\ \mathrm{mod}\ 5$　$\mathrm{B}' = 2\ \mathrm{mod}\ 5$　$\mathrm{C}' = 4\ \mathrm{mod}\ 5$　$\mathrm{D}' = 3\ \mathrm{mod}\ 5$

若將上述關係中的X(X = A 或 B 或 C 或 D)替換為X′，則等式關係仍然成立。

2. 同時，又注意到當我們簡化為 5 的剩餘類時，A′組和C′組為 5 的二次剩餘，而原狀態中的A組和C組就是 29 的二次剩餘。

d. 當$n = 11$時，可以得到和$n = 7$時類似的性質:

(a) 一共可分為 18 種不同的基態，恰好將數字 1~198 不重複的填入；

(b) 這 18 組數字間兩兩有關於符號⊗的等式關係，並且可以簡化為 19 的剩餘類

(c) 其中歸類為 19 的二次剩餘的 9 組數字，恰好就是 199 的二次剩餘。

(2) 針對n為質數時構造不同狀態之說明：

在證明剛剛所發現到的所有性質之前，我們先解釋如何得到那些不同的基態。

舉$n = 7$為例，按照我們在「同餘守恆數的分類與求φ_n值」時的討論，我們是利用【數學模型三】的方式建構狀態，並且求得初始項:

$$\begin{cases} \alpha_0 = \dfrac{(F_{n-1} - 1) - F_n t}{\phi_n} \\ \beta_0 = \dfrac{-(F_{n-2} + 1) + (F_{n-1} - 1)t}{\phi_n} \end{cases}，t為整數$$

又因為當$n = 7$時，$\phi_n = 1$，所以:

$$\begin{cases} \alpha_0 = (F_6 - 1) - F_7 t = 7 - 13t \\ \beta_0 = -(F_5 + 1) + (F_6 - 1)t = -6 + 7t \end{cases}，t為整數$$

由於只要固定初始項，就能唯一產生一個累加態，然後轉為相對應的基態。所以要產生不同的基態，初始項的取值就得不同，也就是讓上式中的t取不同的值。

理論上，t要遍取 29 的一組完全剩餘系，才能保證求出所有狀態；然而實際上，我們只要求出四種不同的狀態就能說明求出了所有守恆狀態$((29 - 1) \div 7 = 4)$，這樣的方式立論於所有狀態中出現過的數字都不會重複。以下將會給出證明。

(3) 針對n為質數時，守恆狀態特性的證明

在這一個部份，我們要給出剛剛觀察時所發現到的所有性質的證明。這裡還得假設同餘守恆數φ_n為質數，則我們有以下的定理六、定理七：

【定理六】
在「$x-y$型操作條件」下，若n與其同餘守恆數φ_n皆為質數，將所有可能的基態列出後，恰好數字1~(φ_n-1)各出現一遍。

【證明】

此證明將分為三個部份，分別標記a. b. c.：

a. 在之前的討論裡我們知道，當n為質數時，以【數學模型三】的構造方式，可得初始項參數式為

$$\begin{cases} \alpha_0 = (F_{n-1}-1) - F_n t \ \ (mod\ L_n) \\ \beta_0 = -(F_{n-2}+1) + (F_{n-1}-1)t \ \ (mod\ L_n) \end{cases}，t為整數$$

再利用【定理五】的證明方法，由於$\varphi_n | L_n$，所以上述參數式可以替換為

$$\begin{cases} \alpha_0 = (F_{n-1}-1) - F_n t \ \ (mod\ \varphi_n) \\ \beta_0 = -(F_{n-2}+1) + (F_{n-1}-1)t \ \ (mod\ \varphi_n) \end{cases}，t為整數$$

假設$gcd(\varphi_n,\ F_n) = m$，因為φ_n為L_n的質因數，所以

$$m |\ gcd(L_n,\ F_n)$$
$$\Rightarrow\ m |\ gcd(\ F_n + \ 2F_{n-1},\ F_n)$$
$$\Rightarrow\ m |\ gcd(\ 2F_{n-1},\ F_n)$$

$\because\ gcd(\ F_{n-1},\ F_n) = 1$且$2 \nmid\ F_n\ \ (\because\ 3 \nmid n)$
$\therefore m = 1$，即φ_n、F_n互質。
由【先備定理一】
$\Rightarrow 0,\ F_n, 2\ F_n, \dots\dots, (\varphi_n-1)F_n$ 恰為一組模φ_n的完全剩餘系
$\Rightarrow (F_{n-1}-1), (F_{n-1}-1)-F_n, (F_{n-1}-1)-2\ F_n, \dots\dots, (F_{n-1}-1)-(\varphi_n-1)F_n$
亦為一組模φ_n的完全剩餘系，即**α_0可以有φ_n種不同的值**，而且一一對應到不同的t值$(mod\ \varphi_n)$。因此，

只要確定了α_0的值，也就確定了的β_0的值，則整個狀態就被唯一確定了。

b. 但若$\alpha_0 \equiv 0\ (mod\ \varphi_n)$，則$\beta_0$亦會同餘 $0(mod\ \varphi_n)$。假設$\beta_0 \equiv b \not\equiv 0\ (mod\ \varphi_n)$，則整個累加態以圖示表示即為:

$$\begin{matrix} 0 & F_{n-1}b & F_{n-2}b & F_{n-3}b & \cdots \\ & b & b & 2b & \cdots \end{matrix}$$

此狀態的最大同餘守恆數為

$$gcd(\ (F_{n-1}-1)b,\ F_n b) = b \cdot gcd(\ F_{n-1}-1,\ F_n) = b \cdot \phi_n = b$$

即$b = \varphi_n \equiv 0\ \ (mod\ \varphi_n)$，矛盾，所以$\beta_0 \equiv 0\ (mod\ \varphi_n)$，從而這$n$個數皆為零，換句話說，

若有一個狀態有出現一個0，則此狀態全部的數都會是0。

而我們不討論這種情況。因此，實際上α_0只能夠有$(\varphi_n - 1)$種不同的值，恰好是模φ_n的一組最簡剩餘系。

c. 再者，由於只要確定了第一個數字(初始項α_0)，就能唯一確定後面所有數字。因此，若是一個狀態內有重複的數字出現，則一定有重複的數列完整排序，否則對於某個重複出現的數值，使它在狀態內出現的不同位置分別成為初始項後，所得到的狀態會不一樣，因為我們知道，確定一個初始項後，整個狀態便是唯一確定了。若以圖示表示則為:

$$\begin{matrix} & a_t & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & \cdots & a_t & a_1 & a_2 & \cdots \end{matrix} \ (mod\ \varphi_n)$$

但是已知n為質數，不可能由數個重複數列完整排序構成守恆狀態，故

整個狀態內不會有重複的數字出現。

綜合以上$a.b.c.$三點，首先初始項α_0的值可以為$1, 2, \ldots\ldots, \varphi_n - 1$(若為0，則全部的數都會為0，我們不討論)；而只要確定了初始值，就能唯一確定後面所有的數；最後，一個狀態內不可能會有重複的數字出現。得證。

同時，也可以論證得到同餘守恆數與模數n之間的同餘等量關係存在，如下：

$$\varphi_n \equiv 1\ (mod\ n)。$$

【定理七】
在「$x - y$型操作條件」下，這n個數為守恆狀態，且符號⊗的運算定義如下：

$$\mathrm{K}\otimes\mathrm{L} = \mathrm{M}\ (\mathrm{mod}\ \varphi_n)$$

表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合M之內。

則若一種狀態內的n個數字構成一個集合，共有 k 個集合，滿足$gcd(n, k) = 1$，則這 k 個集合間兩兩有滿足符號⊗的運算關係。

【證明】

由於牽涉到乘積的關係，於是我們勢必得找到另外一種構造同餘守恆模式的方式(亦即從內部結構觀察)，然後再證明它與遞迴累加模式是等價的關係。換句話說，此定理的證明將分為兩個部份。

a. 首先，由定理六的證明，我們知道$n|\varphi_n - 1$，所以我們令

$$\varphi_n - 1 = kn \ \ (k \in N)$$

再來，考慮兩個高次同餘方程

$$\begin{cases} a^n \equiv 1 \ (mod \ \varphi_n) & \text{——(1)} \\ b^k \equiv 1 \ (mod \ \varphi_n) & \text{——(2)} \end{cases}$$

由【先備定理二】，我們知道這兩個方程式有解，而且方程式(1)恰有$\varphi(n)$個數對模φ_n的階為n。方程式(2)恰有$\varphi(k)$個數對模φ_n的階為k。
於是我們從式(1)的那$\varphi(n)$個解中任選一個不為 1 的解，記為a_0；也從式(2)的那$\varphi(k)$個解中任選一個不為 1 的解，記為b_0。
然後考慮下列k個集合，其中每個集合都有n個元素，而且每個元素都屬於$mod \ \varphi_n$的最小非負完全剩餘系:

$$A_1 = \{a_0 b_0, \ {a_0}^2 b_0, \ {a_0}^3 b_0, \dots\dots, \ {a_0}^n b_0\} \ (mod \ \varphi_n)$$
$$A_2 = \{a_0 {b_0}^2, \ {a_0}^2 {b_0}^2, \ {a_0}^3 {b_0}^2, \dots\dots, \ {a_0}^n {b_0}^2\} \ (mod \ \varphi_n)$$
$$A_3 = \{a_0 {b_0}^3, \ {a_0}^2 {b_0}^3, \ {a_0}^3 {b_0}^3, \dots\dots, \ {a_0}^n {b_0}^3\} \ (mod \ \varphi_n)$$
$$\vdots$$
$$\vdots$$
$$A_k = \{a_0 {b_0}^k, \ {a_0}^2 {b_0}^k, \ {a_0}^3 {b_0}^k, \dots\dots, \ {a_0}^n {b_0}^k\} \ (mod \ \varphi_n)$$

由【先備定理三】，可以推得: 無論a_0和b_0的取值，所得出的k個集合是一樣的。
而且以下將要說明: 這kn個元素模φ_n必定兩兩相異。

利用反證法，假設有兩個數模φ_n同餘，即

$${a_0}^{i_1} {b_0}^{j_1} \equiv {a_0}^{i_2} {b_0}^{j_2} \ \ (mod \ \varphi_n) \ \ (1 \le i_1, i_2 \le n, 1 \le j_1, j_2 \le k)$$

令 $\text{MAX}\{i_1, i_2\} = i_M$，$\text{MIN}\{i_1, i_2\} = i_m$
$\text{MAX}\{j_1, j_2\} = j_M$，$\text{MIN}\{j_1, j_2\} = j_m$
若 $(i_1 \ge i_2 \ \text{且} \ j_1 \ge j_2) \ \text{或} \ (i_1 \le i_2 \ \text{且} \ j_1 \le j_2)$
$\Rightarrow \quad {a_0}^{i_m} {b_0}^{j_m} \left({a_0}^{i_M - i_m} {b_0}^{j_M - j_m} - 1\right) \equiv 0 \ \ (mod \ \varphi_n)$
$\because \ {a_0}^{i_m} {b_0}^{j_m} \not\equiv 0 \ \ (mod \ \varphi_n)$
$\therefore \ {a_0}^{i_M - i_m} {b_0}^{j_M - j_m} \equiv 1 \ \ (mod \ \varphi_n)$
兩邊同乘n次方，
$\Rightarrow \quad ({a_0}^{i_M - i_m})^n ({b_0}^{j_M - j_m})^n \equiv 1 \ \ (mod \ \varphi_n)$
$\Rightarrow \quad ({a_0}^n)^{i_M - i_m} ({b_0}^{j_M - j_m})^n \equiv 1 \ \ (mod \ \varphi_n)$
$\Rightarrow \quad ({b_0}^{j_M - j_m})^n \equiv 1 \ \ (mod \ \varphi_n)$
$\because \quad 0 \le j_M - j_m \le k - 1 \ \text{且} \ gcd(n, k) = 1$
$\therefore \quad j_M - j_m = 0$

$\Rightarrow \quad j_M = j_m$

$\Rightarrow \quad j_1 = j_2$

同理，$i_1 = i_2$，

即 $a_0{}^{i_1} b_0{}^{j_1} = a_0{}^{i_2} b_0{}^{j_2}$

若 $(i_1 \geq i_2$ 且 $j_1 \leq j_2)$ 或 $(i_1 \leq i_2$ 且 $j_1 \geq j_2)$

$\Rightarrow \quad a_0{}^{i_m} b_0{}^{j_m} \left(a_0{}^{i_M - i_m} - b_0{}^{j_M - j_m}\right) \equiv 0 \pmod{\varphi_n}$

$\because \quad a_0{}^{i_m} b_0{}^{j_m} \not\equiv 0 \pmod{\varphi_n}$

$\therefore \quad a_0{}^{i_M - i_m} \equiv b_0{}^{j_M - j_m} \pmod{\varphi_n}$

兩邊同乘n次方，

$\Rightarrow \quad 1 \equiv b_0{}^{j_M - j_m} \pmod{\varphi_n}$

以下等同於剛才的情況，

即 $a_0{}^{i_1} b_0{}^{j_1} = a_0{}^{i_2} b_0{}^{j_2}$

因此這kn個元素模φ_n兩兩相異。得證。

b. 接下來我們要說明，每一個集合內的n個元素都能以特定方式排列，構成一個同餘守恆的狀態。

在遞迴累加的模式中，我們是以逆時針方向累加，且滿足每一項等於前兩項之和，現在觀察每一個集合，發現到如果要滿足這樣的條件，只要說明從$a_0,\ a_0{}^2,\ a_0{}^3, \ldots\ldots, a_0{}^{n-1}$這$n-1$這數字中，有一數滿足同餘方程

$$x^2 \equiv x + 1 \pmod{\varphi_n} \quad \text{——(1)}$$

即可構成守恆狀態。或反過來說，同餘方程(1)的某一個根會滿足

$$x^n \equiv 1 \pmod{\varphi_n} \quad \text{——(2)}$$

假設為x_0，那我們便可構造守恆狀態，以圖示表示為:

$$\begin{matrix} b_0^i & b_0^i x_0^{n-1} & b_0^i x_0^{n-2} \cdots \\ & b_0^i x_0 & b_0^i x_0^2 \quad \cdots \end{matrix} \pmod{\varphi_n}$$

其中$i = 1, 2, \ldots\ldots, k$。

以下就要說明x_0的存在性。首先說明式(1)有解，因為$2 \nmid \varphi_n$，所以式(1)等價於

$$4x^2 - 4x - 4 \equiv 0 \pmod{\varphi_n}$$

接著可以以代換法變為

$$y^2 \equiv 5 \pmod{\varphi_n} \quad \text{——(3)}$$

其中

$$\mathrm{y} \equiv 2\mathrm{x} - 1 \pmod{\varphi_n} \quad \text{——(4)}$$

又由於

$$L_n^2 - L_{n-1}L_{n+1} = 5 \cdot (-1)^n$$

(這由公式$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$展開化簡即得證)

令

$$p = n + 1$$

為偶數，

$$\Rightarrow\ L_{n+1}^2 - L_n L_{n+2} = 5$$
$$\Rightarrow\ L_{n+1}^2 \equiv 5\ (mod\ L_n)$$
$$\Rightarrow\ L_{n+1}^2 \equiv 5\ (mod\ \varphi_n)$$

說明了式(3)有解，而且有兩個解，分別為$y_1 \equiv L_{n+1}(mod\ \varphi_n)$和$y_2 \equiv -L_{n+1}\ (mod\ \varphi_n)$；從而由式(4)的變換，式(1)也對應到兩個解，我們記為x_1和$x_2\ (mod\ \varphi_n)$。所以有

$$\begin{cases} x_1^2 - x_1 - 1 \equiv 0\ (mod\ \varphi_n) \\ x_2^2 - x_2 - 1 \equiv 0\ (mod\ \varphi_n) \end{cases}$$
$$\Rightarrow \begin{cases} x_1 + x_2 \equiv 1\ \ (mod\ \varphi_n) \\ x_1 x_2 \equiv -1\ \ (mod\ \varphi_n) \end{cases}$$

令

$$T_k = {x_1}^k + {x_2}^k$$

則

$$\begin{cases} T_0 \equiv 2\ (mod\ \varphi_n) \\ T_1 \equiv 1\ (mod\ \varphi_n) \\ T_k \equiv T_{k-1} + T_{k-2}\ (mod\ \varphi_n) \end{cases}$$

因此發現到，實際上

$$T_k \equiv 0\ (mod\ L_k)$$
$$\Longrightarrow T_k \equiv 0\ (mod\ \varphi_n)$$

所以

$$\begin{cases} {x_1}^n + {x_2}^n \equiv T_k \equiv 0\ (mod\ \varphi_n) \\ {x_1}^n {x_2}^n \equiv -1\ (mod\ \varphi_n) \end{cases}$$
$$\Rightarrow \begin{cases} {x_1}^n \equiv 1\ (mod\ \varphi_n) \\ {x_2}^n \equiv -1\ (mod\ \varphi_n) \end{cases}$$

於是x_0的存在性便得證($x_0 \equiv x_1\ (mod\ \varphi_n)$)，由乘法關係所構成的守恆狀態即成立。

而由剛剛定理六的證明過程，我們可以簡單推得守恆狀態的唯一性，定理七只是刻劃了各數字間的結構關係，換句話說，以遞迴累加的構造模式和上述乘積構造的模式是**同構**的。因此，可以完整的解釋有關符號⊗的運算關係。得證。

【心得五】
在上述的證明過程中，k個集合中每個集合都有n個元素，而且每個元素都屬於$mod\ \varphi_n$的最簡剩餘系，甚至此kn個元素模φ_n均兩兩相異，因此我們可稱此k個集合為$mod\ \varphi_n$的最簡剩餘系之一個「分割集合」。

【進一步說明】
由以上的證明過程中，注意到其中有一個守恆狀態，以圖示表示:

$$\begin{matrix} 1 & x_1^{n-1} & x_1^{n-2} & \cdots \\ & x_1 & x_1^2 & \cdots \end{matrix}\ (mod\ \varphi_n)$$

這n個數恰恰構成一個循環群(x_1即為它的生成元)，也就是【數學模型四】裡第三種守恆狀態的分類「循環態」。

而這種「循環態」,正能夠以同餘方程$x^2 \equiv x+1\ (mod\ \varphi_n)$的根構造出來。

特別注意到這個方程式的兩根，會剛好滿足$\begin{cases} {x_1}^n \equiv 1\ (mod\ \varphi_n) \\ {x_2}^n \equiv -1\ (mod\ \varphi_n) \end{cases}$，這表示可以構造出兩個循環態,初始項分別為$1$、$x_1$和$1$、$x_2$,前者狀態內會有$n$個數(便是我們剛剛所要證明的目標)，而後者則會有$2n$個數。
事實上，若n為質數，而φ_n為合數的情況下，也能透過這種方式建構出循環態，而且方程式的解數還跟φ_n的質因數個數有關，這個部分，我們要說明以下定理八:

【定理八】
在「$x-y$型操作條件」下，若n為質數，已知它的最大同餘守恆數為L_n。假設有一數φ_n為L_n的因數，且φ_n有p個質因數，則同餘方程$x^2 \equiv x+1\ (mod\ \varphi_n)$的解數為$2^p$。若將其根依序記為$x_1, x_2, \dots, x_{2^p}$，則必有${x_1}^n \equiv 1\ (mod\ \varphi_n)$和${x_k}^{2n} \equiv 1\ (mod\ \varphi_n)$ 且${x_k}^n \not\equiv 1\ (mod\ \varphi_n)\ (k = 2, 3, \dots, 2^p)$。亦即此$n$邊形有且僅有一個循環態$(mod\ \varphi_n)$，而$2n$邊形有$2^p$個循環態$(mod\ \varphi_n)$。

【證明】
設

$$\varphi_n = \varphi_1 \times \varphi_2 \times \dots \times \varphi_p$$

為φ_n的標準分解式。
所以同餘方程

$$x^2 \equiv x+1\ (mod\ \varphi_n) \quad \text{——(1)}$$

的解，實際上就等同於同餘方程組

$$\begin{cases} x^2 \equiv x+1\ (mod\ \varphi_1) \\ x^2 \equiv x+1\ (mod\ \varphi_2) \\ \vdots \\ x^2 \equiv x+1\ (mod\ \varphi_p) \end{cases}$$

的解，而由【定理七】的證明過程中，我們知道上述每一個同餘方程

$$x^2 \equiv x+1 \ (mod\ \varphi_m) \ (m=1,2,\dots,p)$$

皆有兩個解，若記為$\varphi_{m,1}$和$\varphi_{m,2}$，於是原方程式的解，便為一次方程組

$$\begin{cases} x \equiv \varphi_{1,t_1} \ (mod\ \varphi_1) \\ x \equiv \varphi_{2,t_2} \ (mod\ \varphi_2) \\ \quad\vdots \\ x \equiv \varphi_{p,t_p} \ (mod\ \varphi_p) \end{cases}$$

的解，其中t_m可以為 1 或 2 $(m=1,2,\dots,p)$，所以一共有2^p個一次方程組，由【先備定理四】，於是知道原方程式的解數共有2^p個。

又由【定理七】的證明過程中，知道可以假設

$$\begin{cases} {\varphi_{m,1}}^n \equiv 1 \ (mod\ \varphi_m) \\ {\varphi_{m,2}}^n \equiv -1 \ (mod\ \varphi_m) \end{cases} \quad (m=1,2,\dots,p)$$

我們又假設原方程式的一個解x_1是滿足同餘方程

$$\begin{cases} x \equiv \varphi_{1,1} \ (mod\ \varphi_1) \\ x \equiv \varphi_{2,1} \ (mod\ \varphi_2) \\ \quad\vdots \\ x \equiv \varphi_{p,1} \ (mod\ \varphi_p) \end{cases}$$

的解，所以

$$\begin{cases} x_1^n \equiv \varphi_{1,1}^n \equiv 1 \ (mod\ \varphi_1) \\ x_1^n \equiv \varphi_{2,1}^n \equiv 1 \ (mod\ \varphi_2) \\ \quad\vdots \\ x_1^n \equiv \varphi_{p,1}^n \equiv 1 \ (mod\ \varphi_p) \end{cases}$$

$$\Rightarrow \ x_1^n \equiv 1 \ (mod\ \varphi_n) \qquad \text{——(2)}$$

而原方程式的其他2^p-1個根，若將對應到的同餘方程組以同樣形式寫出，則至少會有一個同餘式是同餘-1，而其他的同餘式都同餘1。因此，可簡單推得

$$x_k^{2n} \equiv 1 \ (mod\ \varphi_n) \ (k=2,3,\dots,2^p) \qquad \text{——(3)}$$

且

$$x_k^n \not\equiv 1 \ (mod\ \varphi_n) \ (k=2,3,\dots,2^p) \qquad \text{——(4)}$$

又由於$x_1, x_2, \dots, x_{2^p}$是滿足同餘方程(1)的全部的解，再由式(2)和式(3)和式(4)，我們便能構造出循環態:

$$1 \quad \begin{matrix} x_1^{n-1} & x_1^{n-2} & \dots \\ x_1 & x_1^2 & \dots \end{matrix} \ (mod\ \varphi_n)$$

和

$$1 \quad \begin{matrix} x_m^{2n-1} & x_m^{2n-2} & \dots \\ x_m & x_m^2 & \dots \end{matrix} \ (mod\ \varphi_n)$$

其中$m = 1, 2, \dots, p$。定理七得證。

【心得六】
由定理七之證明過程，我們其實建構出了一種新的構造同餘守恆狀態的方式，簡而言之，即是解同餘方程$x^2 \equiv x + 1 \ (mod\ \varphi_n)$，所得到的兩個解剛好會滿足$\begin{cases} {x_1}^n \equiv 1 \ (mod\ \varphi_n) \\ {x_2}^n \equiv -1 \ (mod\ \varphi_n) \end{cases}$。另一方面，對於數字間的結構關係，我們也有了完整的結果(在φ_n為質數的情況)，由這些結構會推演出許多性質，其中【心得四】的描述只是我們在探究過程中的發現，可想見，除此之外還會有其它的性質，然後最重要的還是如同定理七的證明過程中所描述的數字本身的結構。

(4) 針對n為合數時構造守恆狀態之方法：

當n為合數時，如同是質數的情況一樣，也能以遞迴累加的模式構造守恆狀態；或是解同餘方程(在守恆數為質數的情況下)，構造出循環態。

其中特別注意到，當守恆數不為質數時，除了最基本的，以參數式構造所有守恆狀態的方法外，我們還有其他的方法，但是最根本的原理和參數式是一樣的，以下將證明：

【定理九】
在「$x - y$型操作條件」下，若這n個數滿足守恆狀態，且其同餘守恆數為φ_n，則將整個狀態乘以某數d，再轉為相對應的基態，則這個基態的最大同餘守恆數必為$\frac{\varphi_n}{gcd(d, \varphi_n)}$。

【證明】

我們還希望透過此方法構造出所有守恆狀態，因此不妨假設這n個數有最大同餘守恆數φ_{Mn}。令這n個數依照逆時針方向依序為$a_1, a_2, \dots\dots, a_n$，因此有

$$\begin{cases} a_1 + a_2 \equiv a_3 \ (mod\ \varphi_{Mn}) \\ a_2 + a_3 \equiv a_4 \ (mod\ \varphi_{Mn}) \\ \qquad\qquad \vdots \\ a_{n-1} + a_n \equiv a_1 \ (mod\ \varphi_{Mn}) \\ a_n + a_1 \equiv a_2 \ (mod\ \varphi_{Mn}) \end{cases}$$

且

$$gcd(a_1, a_2, \dots\dots, a_n) = 1$$

若將各數乘以d倍，可得一新的狀態:

$$da_1 \ \begin{matrix} da_n & \cdots & \cdots \\ da_2 & da_3 & \cdots \end{matrix} \ (mod\ d\varphi_{Mn})$$

將此狀態轉為$mod\ \varphi_{Mn}$的狀態:

$$b_1 \begin{matrix} b_n & \cdots & \cdots \\ b_2 & b_3 & \ldots \end{matrix} \quad (mod\ \varphi_{Mn})$$

其中

$$0 \le da_i - \varphi_{Mn} t_i = b_i \le \varphi_{Mn} - 1 \quad (i = 1, 2, \ldots\ldots, n\ ;\ t_i \in N) \quad \text{——(1)}$$

假設

$$gcd(d, \varphi_n) = k$$

則由式(1)，可知

$$k | b_i$$

即新的$mod\ \varphi_{Mn}$的狀態間有一公因數k，我們要得到基態，則各數間必須要互質，所以我們假設各數間除了k以外，還有最大公因數s，即

$$b_i = ksc_i \quad (i = 1, 2, \ldots\ldots, n) \quad \text{——(2)}$$

且

$$gcd(c_1, c_2, \ldots\ldots, c_n) = 1$$

因此剛剛所得的狀態便可表示為

$$ksc_1 \begin{matrix} ksc_n & \cdots & \cdots \\ ksc_2 & ksc_3 & \ldots \end{matrix} (mod\ \varphi_{Mn})$$

$$\Rightarrow\ sc_1 \begin{matrix} sc_n & \cdots & \cdots \\ sc_2 & sc_3 & \ldots \end{matrix} (mod\ \frac{\varphi_{Mn}}{k})$$

因此有

$$\begin{cases} sc_1 + sc_2 \equiv sc_3 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ sc_2 + sc_3 \equiv sc_4 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ \vdots \\ sc_{n-1} + sc_n \equiv sc_1 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ sc_n + sc_1 \equiv sc_2 \ (mod\ \frac{\varphi_{Mn}}{k}) \end{cases}$$

再假設

$$gcd(s, \varphi_n) = r$$

若$r \ge 2$，由式(1)可推得

$$gcd(a_1, a_2, \ldots\ldots, a_n) = r \ge 2$$

與原本敘述矛盾，因此$r = 1$，即s和φ_n互質，所以c_i的關係又可簡化為

$$\begin{cases} c_1 + c_2 \equiv c_3 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ c_2 + c_3 \equiv c_4 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ \vdots \\ c_{n-1} + c_n \equiv c_1 \ (mod\ \frac{\varphi_{Mn}}{k}) \\ c_n + c_1 \equiv c_2 \ (mod\ \frac{\varphi_{Mn}}{k}) \end{cases}$$

再由式(1)及式(2)，若$s \geq 2$，則

$$0 \leq c_i \leq \frac{\varphi_{Mn}}{ks} \leq \frac{\varphi_{Mn}}{2k}$$

$$\Rightarrow \ 0 \leq c_i + c_{i+1} \leq \frac{\varphi_{Mn}}{k}$$

所以c_i的關係又可進一步寫為

$$\begin{cases} c_1 + c_2 = c_3 \\ c_2 + c_3 = c_4 \\ \vdots \\ c_{n-1} + c_n = c_1 \\ c_n + c_1 = c_2 \end{cases}$$

注意到這裡的同餘關係已經變為等號了，將這n個式子相加

$$\Rightarrow \sum_{i=1}^{n} c_i = 0$$

$$\Rightarrow c_1 = c_2 = \cdots = c_n = 0$$

式(1)即可寫為

$$da_i = \varphi_{Mn} t_i$$
$$\Longrightarrow gcd(a_1, a_2, \ldots\ldots, a_n) > 1$$

除非$\varphi_{Mn} | d$，而這種情況是無意義的，從而s必須等於 1。

即經過如此操作後的狀態$(mod\ \frac{\varphi_{Mn}}{k})$，其各數必定互質，因此滿足了基態的條件，故原命題得證。

【心得七】

1. 我們能簡單推得，當乘數d從$1, 2, \ldots \varphi_{Mn} - 1$一一帶入計算後，會有$\varphi(k)$個數使得最後轉變成的基態的最大同餘守恆數為$\frac{\varphi_{Mn}}{k}$，這裡的$k$同於上述的證明，是$\varphi_{Mn}$的因數。
   這樣的結果也能由尤拉公式：

$$\sum_{d|m} \varphi(d) = m$$

解釋之。

2. 事實上，這樣的構造方式也能用於當同餘守恆數φ_n為質數的情況，而且在計算方面會比用參數式快一點。然而，我們對於當φ_n為合數時的總守恆狀態數尚未進行深入的探討，目前只能由構造出所有守恆狀態來計算。

2. 驚奇發現：另一種產生最簡剩餘系之分割集合的方法：同序方格

所謂「同序方格」，係指在m列n行的方格中，將符號$a_1, a_2, \dots a_{mn}$(可重複)從第一、二、三列由左而右依序填入，直到填完最後一列(第m列)。則符號順序$a_1, a_2, \dots a_{mn}$會等同於從第n 、$n-1$ 、$n-2$行由上往下排序，直到最後一行(第一行)。若以圖示表示:

a_1	a_2	a_3	$\cdots$	a_{n-1}	a_n
a_{n+1}	a_{n+2}	a_{n+3}	$\cdots$	a_{2n-1}	a_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$a_{(m-1)n+1}$	$a_{(m-1)n+2}$	$a_{(m-1)n+3}$	$\cdots$	a_{mn-1}	a_{mn}

則序列

$a_1, a_2, \dots, a_{n-1}, a_n, a_{n+1}, \dots, a_{(m-1)n+1}, a_{(m-1)n+2}, \dots, a_{mn}$

會完全等同於序列

$a_n, a_{2n}, \dots, a_{(m-1)n}, a_{mn}, a_{n-1}, \dots, a_1, a_{n+1}, a_{(m-1)n+1}$

實際上在當初探究各守恆狀態中不同數字的關係時，我們便嘗試將數字(以所在的集合表示)填入一個n × k的方格裡，觀察有何特性。

舉$n = 7$時為例:

$\mathrm{A} = \{1, 7, 16, 20, 23, 24, 25\}$

$\mathrm{B} = \{2, 3, 11, 14, 17, 19, 21\}$

$\mathrm{C} = \{4, 5, 6, 9, 13, 22, 28\}$

$\mathrm{D} = \{8, 10, 12, 15, 18, 26, 27\}$

接著我們將一個7×4的方格編號:

1	2	3	4	5	6	7
8	9	10	11	12	13	14

15	16	17	18	19	20	21
22	23	24	25	26	27	28

然後把數字所在的集合標上集合字母:

→

A	B	B	C	C	C	A
D	C	D	B	D	C	B
D	A	B	D	B	A	B
C	A	A	A	D	D	C

↓

仔細觀察後，發現這就是一個同序方格，即依照箭頭順序列出字母，所得到的序列是一樣的:

A, B, B, C, C, C, A, D, C, D, B, D, C, B, D, A, B, D, B, A, B, C, A, A, A, D, D, C

【證明】

若我們以得到的結果反向操作，以下便是我們依序填入字母的順序:

$$\text{A: } 1 \to 7 \to 20 \to 24 \to 23 \to 16 \to 25 \to 1 \text{ (循環)}$$
$$\text{B: } 2 \to 14 \to 11 \to 19 \to 17 \to 3 \to 21 \to 2 \text{ (循環)}$$
$$\text{C: } 4 \to 28 \to 22 \to 9 \to 5 \to 6 \to 13 \to 4 \text{ (循環)}$$
$$\text{D: } 8 \to 27 \to 15 \to 18 \to 10 \to 12 \to 26 \to 8 \text{ (循環)}$$

假設有個字母填在編號x的地方，則依據x的位置，下一個填入的字母的編號就記為$f(x)$，我們便有以下關係:

$$x = 4q + r \quad (q \in N^*; 1 \le r < 4)$$
$$\Rightarrow f(x) = 7(r-1) + 7 - q$$
$$= 7r - q$$
$$\equiv 7x \ (mod\ 29)$$

因為$7^7 \equiv 1 \ (mod\ 29)$，所以每個字母只要填七個位置後就會開始循環。

又由於我們當初可以透過定理七的論證模式構造出四個集合，恰好7為方程式

$$a^7 \equiv 1 \ (mod\ 29)$$

的一根，表示這四個集合中，每個集合裡的數字可以以7的冪次乘以某定數得出，於是便有以上同序方格的性質。

【進一步說明】

當初發現到這樣的性質後，以為在所有n和φ_n皆為質數下的情況都能成立，然而實際上，這樣的性質並不根屬於守恆狀態，只有少數滿足方程式

$$n^n \equiv 1 \ (mod\ \varphi_n)$$

的n值才會產生這種特殊的同序方格。

不過有個例外情況是當

$$n^n \equiv -1 \ (mod\ \varphi_n)$$

時，從左上角開始往右排序和從左下角開始往上排序會一樣，證明的方法和剛才一樣。

但是另一方面，若我們放寬方格的長寬限制，不一定要為$n \times k$時，此時即可透過此方法找到滿足方程式

$$d^x \equiv 1 \ (mod\ \varphi_n)$$

的最小正整數解，其中$d|\varphi_n - 1$為方格的行數(如同上例中的n)。

【心得八】
結果當初發現到的這個特殊性質只對特定的n值成立，然而這樣的模式或許能夠和循環態建構起關係，但詳細的模式還有待深入探究，尤其當φ_n為合數時，情況會變得相當複雜。

3. 同餘守恆狀態的統整:

截至目前為止，我們有了數個構造同餘守恆模式的方法，其中針對n、φ_n的值又分為質數和合數進行討論，以得出不同的性質或定理。除了【定理七】的證明所描述的以外的構造方法，都是普遍適用於任何情況。下面給出了這個階段探討的總整理:

(1) 構造同餘守恆狀態的方法:

a. 以參數式構造：
由【數學模型三】所推演出的初始項參數式

$$\begin{cases} \alpha_0 = (F_{n-1} - 1) - F_n t \ (mod\ \varphi_n) \\ \beta_0 = -(F_{n-2} + 1) + (F_{n-1} - 1)t \ (mod\ \varphi_n) \end{cases}, t\text{為整數}$$

帶入不同的t值以求得不同的守恆狀態。適用於任何情況。

b. 以同餘方程構造：
解同餘方程$x^2 \equiv x + 1 \ (mod\ \varphi_n)$，以其根作為生成元構造出循環態。適用於當$n$為質數時，詳細說明如【定理七】及【定理八】。

c. 以倍數法構造：
以參數式法構造出任意一組守恆狀態後，將整個狀態乘以某數d再轉為對應的基態。適用於任何情況。詳細說明如【定理九】

(2) 特殊情況：

a. 當n、φ_n皆為質數時，有【定理六】和【定理七】所描述的性質。

b. 當n為質數，φ_n為合數時，有【定理八】所描述的性質。

(3) 其他發現到的性質：

見「2. 驚奇發現：另一種產生最簡剩餘系之分割集合的方法」

(八) 原問題的再延伸變化之二——「$x-2y$型」

在探究完了x − y型操作模式的基本性質後，我們想要接著探討x − 2y型操作模式，觀察是否有類似的性質，並且希望能推廣到$x-qy$型。

論述$x-2y$型操作模式，如下：

「在一個 n 邊形的 n 個頂點上，填寫 n 個不盡相異之非負整數，且這n個整數的最大公因數為 1，依以下規則進行操作：擦去一個數，寫上其相鄰兩數依照順時針方向前項減兩倍後項之差。。如此操作模式我們稱之為『$x-2y$型操作』。」

1. x − 2y型操作模式下的同餘守恆數:

(1) 本原守恆數ϕ_n:

仿照x − y型的做法，首先我們依照【數學模型三】構造出一個遞迴累加的初始狀態，再利用操作前後差值的最大公因數來求得同餘守恆數。由於是x − 2y型的操作，其逆向操作即是按照逆時針方向且滿足關係式

$$a_k = a_{k-1} + 2a_{k-2}$$

假設初始兩項為α、β，則整個狀態以圖示表示為:

$$\begin{matrix} & Q & P & \cdots & \cdots \\ \alpha & \beta & 2\alpha+\beta & 2\alpha+3\beta & \cdots \end{matrix}$$

令最後兩項為P、Q，則

$$\begin{cases} P = 2G_{n-3}\alpha + G_{n-2}\beta \\ Q = 2G_{n-2}\alpha + G_{n-1}\beta \end{cases}$$

其中G_n滿足

$$\begin{cases} G_1 = 1 \\ G_2 = 1 \\ G_n = G_{n-1} + 2G_{n-2} \end{cases}$$

事實上，G_n即是 Jacobsthal 數列$< 1,\ 1,\ 3,\ 5,\ 11,\ 21,\ 43 \ldots\ldots >$。

由於經過第一次操作後會改變其數值的僅有Q和α，所以我們令Q'和α'分別表示他們操作後的數值，則

$$\mathrm{Q}' = \alpha - 2P = \alpha - 2(2G_{n-3}\alpha + G_{n-2}\beta) = (1 - 4G_{n-3})\alpha - 2G_{n-2}\beta$$

$$\alpha' = \beta - 2\mathrm{Q} = \beta - 2(2G_{n-2}\alpha + G_{n-1}\beta) = -4G_{n-2}\alpha + (1 - 2G_{n-1})\beta$$

他們與原數值的差分別為:

$$\begin{aligned} \mathrm{Q} - \mathrm{Q}' &= (2G_{n-2}\alpha + G_{n-1}\beta) - [(1 - 4G_{n-3})\alpha - 2G_{n-2}\beta] \\ &= (2G_{n-2} + 4G_{n-3} - 1)\alpha + (G_{n-1} + 2G_{n-2})\beta \\ &= (2G_{n-1} - 1)\alpha + G_n\beta \end{aligned}$$

$$\alpha - \alpha' = \alpha - [-4G_{n-2}\alpha + (1 - 2G_{n-1})\beta]$$
$$= (4G_{n-2} + 1)\alpha + (2G_{n-1} - 1)\beta$$

這兩個差值的公因數即為我們要求的同餘守恆數，令函數

$$h(n) = gcd((2G_{n-1} - 1)\alpha + G_n\beta, (4G_{n-2} + 1)\alpha + (2G_{n-1} - 1)\beta)$$

所以有

$$\varphi_n | h(n)$$

而$h(n)$又可以繼續化簡，由於G_n為一個二次遞迴式，可以解得其公式為

$$G_n = \frac{1}{3}[2^n - (-1)^n]$$

於是又可以簡單推得

$$\begin{cases} G_n = 2G_{n-1} + 1 \text{，若} n \text{為奇數} \\ G_n = 2G_{n-1} - 1 \text{，若} n \text{為偶數} \end{cases}$$

所以最後可以化簡得到:

$$h(n) = \begin{cases} \gcd\big((G_n - 2)\alpha + G_n\beta, (G_n + 2)\alpha + (G_n - 2)\beta\big) \text{，若} n \text{為奇數} \\ gcd(G_n\alpha + G_n\beta, G_n\alpha + G_n\beta) = G_n(\alpha + \beta) \text{，若} n \text{為偶數} \end{cases}$$

以下再依n的奇偶性分別討論:

a. 當n為偶數時，情況比較簡單，由上式中可以直接推得其本原守恆數為G_n，這代表說在$x - 2y$型操作模式下，若n為偶數，那麼只要固定初始兩項α、β為互質，以遞迴累加的方式填完所有數字，就必為守恆的狀態，而且此時G_n為其同餘守恆數。

b. 當n為奇數時，由G_n的遞迴式可以知道$2 \nmid G_n$，再觀察上式，可以簡單得知此時的本原守恆數(係數間可先提出的最大公因數)為1。

整理得到定理十:

【定理十】
在「$x - 2y$型操作條件」下，則
(1) 當n為偶數時，$\phi_n = G_n$
(2) 當n為奇數時，$\phi_n = 1$

(2) 同餘守恆數φ_n:

探討完了本原守恆數ϕ_n之後，我們要接著探討「$x - 2y$型操作條件」下的同餘守恆數φ_n。這個部分也是依照n的奇偶性分別討論:

a. 當n為偶數時:

(a) 若依照遞迴累加的模式，決定好初始兩項後(假設為α、β)，由上面的討論

可以知道，此時的最大同餘守恆數就等於$G_n(\alpha+\beta)$。但由於α、β的值可以任取(只要保證互質)，所以其同餘守恆數便能任意大，表示**在$\mathbf{x-2y}$型操作模式下，n為偶數時沒有最大同餘守恆數。**

(b) 事實上，若不考慮遞迴累加的模型，**對於每一個偶數$n\geq 4$，任何正整數$\varphi\geq 2$都可成為它的同餘守恆數**，我們考慮以下狀態:

$$\alpha\ \begin{matrix}\beta & \alpha & \cdots\\ \beta & \alpha & \cdots\end{matrix}\ \cdots\ (mod\ \alpha+\beta)$$

其中α和β互質。顯然這是一個同餘守恆狀態，且此時的最大同餘守恆數為$\alpha+\beta$。

b. 當n為奇數時:

(a) 由【定理十】知道其本原守恆數$\phi_n=1$，於是我們假設$h(n)$有最大值為M_g，且此時$\alpha=\alpha_0$、$\beta=\beta_0$，則

$$M_g=gcd\big((G_n-2)\alpha_0+G_n\beta_0,(G_n+2)\alpha_0+(G_n-2)\beta_0\big)$$

所以有

$M_g\mid(G_n-2)\alpha_0+G_n\beta_0$

$M_g\mid(G_n+2)\alpha_0+(G_n-2)\beta_0$

再來我們用加減消去法消去α_0使得只剩下一個未知數:

$\Rightarrow$

$M_g\mid(G_n+2)[(G_n-2)\alpha_0+G_n\beta_0]-(G_n-2)[(G_n+2)\alpha_0+(G_n-2)\beta_0]$

$M_g\mid[(G_n+2)\cdot G_n-(G_n-2)^2]\beta_0$ ——(1)

同理，也可以消去β_0，得到

$M_g\mid-[(G_n+2)\cdot G_n-(G_n-2)^2]\alpha_0$ ——(2)

由式(1)及式(2)，由於α_0、β_0互質，所以

$M_g\mid[(G_n+2)\cdot G_n-(G_n-2)^2]$

$\Rightarrow M_g\mid 6G_n-4$

$\Rightarrow M_g\mid 6\cdot\frac{1}{3}[2^n+1]-4$

$\Rightarrow M_g\mid 2[2^n-1]$

$\Rightarrow M_g\mid 2M_n$

這裡的M_n代表Mersenne數。

而此時可得$M_g=2M_n$，$\begin{cases}\alpha_0=(G_n-2)-G_nt\\ \beta_0=-(G_n+2)+(G_n-2)t\end{cases}$，$t$為整數

於是我們求出了在$\mathrm{x}-2\mathrm{y}$型操作模式下，當n為奇數時的最大同餘守恆數

$$\varphi_{Mn}=2M_n$$

整理為定理十一:

【定理十一】在「$x-2y$型操作條件」下，

若n為奇數，則n邊形的最大同餘守恆數

$$\varphi_{Mn}=2M_n$$

若n為偶數，則n邊形沒有最大同餘守恆數。

(b) 在求出了最大同餘守恆數φ_{Mn}之後，如同$x-y$型的討論，我們依然想問，是否存在這樣的情況，使得某數φ_n為φ_{Mn}的因數，且為該狀態下的同餘守恆數，而φ_{Mn}卻不是。

事實上，這是可以的，以下便為【定理十二】，而證明方法大致上也和討論$x-y$型時一樣:

【定理十二】

在「$x-2y$型操作條件」下，假設其n邊形有最大同餘守恆數為φ_{Mn}且$d \mid \varphi_{Mn}$，則我們必可找到一個狀態，滿足：此狀態各數間的最大公因數為 1，且d是這個狀態的最大同餘守恆數。

【證明】

假設有n個數為守恆狀態，而且此時有最大同餘守恆數為φ_{Mn}，由【定理十一】知道n必為奇數，以圖示表示:

$$\begin{matrix} a_1 & \begin{matrix} a_n & a_{n-1} & \cdots \\ a_2 & a_3 & \cdots \end{matrix} \end{matrix} \pmod{\varphi_{Mn}}$$

再來，我們考慮正整數d使得$d \mid \varphi_{Mn}$，令$b_k \equiv a_k \ (mod\ d)\ (k=1,\ 2,\ \dots,\ n)$且$b_k$屬於$mod\ d$的最小非負完全剩餘系，即$0 \le b_k \le d-1$。因此$b_k$的值是被唯一確定的。

接著，以b_k替換原狀態中的a_k:

$$\begin{matrix} b_1 & \begin{matrix} b_n & b_{n-1} & \cdots \\ b_2 & b_3 & \cdots \end{matrix} \end{matrix} \ (mod\ d)$$

然後我們看各個數字操作前後的差值，令為b_k'，則:

$$\begin{aligned} b_k' &= b_k-(b_{k+1}-2b_{k-1}) \\ &= 2b_{k-1}+b_k-b_{k+1} \\ &(\text{令} b_{n+1}=b_1) \end{aligned}$$

而從原守恆狀態，令a_k'表示a_k操作前後的差值，則我們知道:

$$\varphi_{Mn} \mid a_k'$$

即

$$\begin{aligned} a'_k &= a_k - (a_{k+1} - 2a_{k-1}) \\ &= 2a_{k-1} + a_k - a_{k+1} \\ &= \varphi_{Mn} \cdot t_k \\ &(\text{令} a_{n+1} = a_1) \end{aligned}$$

其中t_k為整數。又因為

$$\begin{aligned} b_k &\equiv a_k \ (mod\ d) \\ \Rightarrow b_k &= a_k - d \cdot l_k \ \ (l_k \in Z) \end{aligned}$$

所以我們可以重新改寫b'_k:

$$\begin{aligned} b'_k &= 2b_{k-1} + b_k - b_{k+1} \\ &= 2(a_{k-1} - l_{k-1} \cdot d) + (a_k - l_k \cdot d) - (a_{k+1} - l_{k+1} \cdot d) \\ &= (2a_{k-1} + a_k - a_{k+1}) - d(2l_{k-1} + l_k - l_{k+1}) \\ &= t_k \cdot \varphi_{Mn} - d \cdot l'_k \ \ (l'_k \in Z) \\ &= d \cdot t'_k \end{aligned}$$

其中t'_k為整數。

因此我們知道，b_k操作前後模d的值不變，即d為新狀態下的同餘守恆數。同時假設

$$gcd(b_1, b_2, \dots\dots, b_n) = r$$

則

$$gcd(d, r) = 1$$

因為如果d和r有公因數，由式子

$$b_k = a_k - d \cdot l_k$$

可以推得$a_1, a_2, \dots\dots, a_n$也有公因數，即原始狀態下各數不互質，與定義不合，所以d和r必定要互質。

又因為

$$\begin{aligned} b'_k &= d \cdot t'_k \\ &= 2b_{k-1} + b_k - b_{k+1} \\ &\leq 3(d-1) < 3d \end{aligned}$$

因此t'_k可能等於 2，然而，除了$r = 2$以外，這種情形是不存在的。這種情況我們會在後面的【定理十四】補述。

此時，我們便能保證一個各數互質且同餘守恆數為d的狀態:

$$\begin{matrix} & c_n & c_{n-1} & \cdots \\ c_1 & c_2 & c_3 & \cdots \end{matrix} \cdots \ (mod\ d)$$

其中$c_k = \frac{b_k}{r} \ \ (k = 1,\ 2, \dots,\ n)$。得證。

【心得九】
和討論$x - y$型時的證明比較起來，證明的架構基本上是一樣的，但是

其中唯一不同的地方，在於: 在$x-y$型操作條件下，將原狀態各數取$mod\ d$之後，各數即會互質；然而在$x-2y$型操作條件下，卻可能有公因數 2，此時便要再把此公因數 2 除掉(即上述證明中最後一個步驟)，才會得到我們想要的基態。

(3) 下表統整了目前的結果:

n	ϕ_n	φ_{Mn}	φ_n
偶數	G_n	(無)	任何大於 2 的正整數
奇數	1	$2M_n$	φ_{Mn}的因數

2. $x-2y$型操作模式下的同餘守恆狀態:

在這個階段中，我們試著沿用在$\mathrm{x}-\mathrm{y}$型所討論的方式來構造同餘守恆狀態，然而透過剛才的探討，知道在n為偶數的情況下，可以任意的選定初始值，構造守恆狀態。因此，以下皆針對n為奇數時的情況進行探討，亦即在有最大同餘守恆數的限制條件下，該如何構造守恆狀態? 而其中的狀態又有何性質?

在**n為奇數**的前提下，以下將分為同餘守恆數φ_n為奇數或偶數以及特殊情況(n為質數)三部份分別論述:

(1) 當φ_n為奇數時:

這個部分，我們要證明:

【定理十三】

在「$x-2y$型操作條件」下，假設其n邊形最大同餘守恆數為φ_n。若n和φ_n皆為奇數，且這n個數照逆時針方向依序記為$a_1, a_2, \dots, a_n$，則有:

$$a_{k+1} \equiv 2a_k \ (mod\ \varphi_n)$$

其中$k = 1, 2, \dots, n$且$a_{n+1} = a_1$。

【證明】

由守恆定義可以知道

$$\begin{cases} 2a_1 + a_2 \equiv a_3 \ (mod\ \varphi_n) \\ 2a_2 + a_3 \equiv a_4 \ (mod\ \varphi_n) \\ \vdots \\ 2a_{n-1} + a_n \equiv a_1 \ (mod\ \varphi_n) \\ 2a_n + a_1 \equiv a_2 \ (mod\ \varphi_n) \end{cases}$$

將以上n個等式相加，得到

$$2\sum_{k=1}^{n} a_k \equiv 0 \ (mod\ \varphi_n)$$

因為$2 \nmid \varphi_n$，所以

$$\sum_{k=1}^{n} a_k \equiv 0 \ (mod\ \varphi_n) \quad \text{——(1)}$$

然後我們再依據剛剛已知的n個式子，保留第奇數條式子

$$\begin{cases} 2a_1 + a_2 \equiv a_3 \ (mod\ \varphi_n) \\ 2a_3 + a_4 \equiv a_5 \ (mod\ \varphi_n) \\ \vdots \\ 2a_{n-2} + a_{n-1} \equiv a_n \ (mod\ \varphi_n) \\ 2a_n + a_1 \equiv a_2 \ (mod\ \varphi_n) \end{cases}$$

將這$\frac{n-1}{2}$個式子相加:

$$2a_1 + a_2 + a_3 + a_4 + \cdots + a_{n-1} \equiv a_n \ (mod\ \varphi_n) \quad \text{——(2)}$$

由式(1)與式(2)，可得

$$a_1 \equiv 2a_n \ (mod\ \varphi_n)$$

由於這n個數是環狀結構，所以

$$a_{k+1} \equiv 2a_k \ (mod\ \varphi_n)$$

其中$k = 1, 2, \ldots, n$且$a_{n+1} = a_1$。得證。

因此，【定理十三】即說明了：**在「$x - 2y$型操作條件」下，若n與其同餘守恆數φ_n皆為奇數，只要確定一個初始項，則整個狀態就被唯一確定了。**

(2) 當φ_n為偶數時:

這個部分，我們要證明:

【定理十四】
在「$x - 2y$型操作條件」下，假設這n個數為**基態**且同餘守恆數為φ_n，若n為奇數且φ_n為偶數，則這n個數當中必至少有一個數大於$\frac{\varphi_n}{2}$。

【證明】
首先沿用【定理十三】的證明過程，但其中φ_n為偶數，假設$\varphi_n = 2d$，則式(1)和式(2)便可改寫為:

$$2\sum_{k=1}^{n} a_k \equiv 0 \ (mod\ 2d) \quad \text{——(1)}$$

$$a_1 + \sum_{k=1}^{n} a_k \equiv 2a_n \ (mod\ 2d) \quad \text{——(2)}$$

於是就有以下兩種可能:

a. $\sum_{k=1}^{n} a_k \equiv 0 \pmod{2d}$

在此情況下，式(2)即等於

$$a_1 \equiv 2a_n \pmod{2d}$$

又由於這n個數是以環狀結構排列，不妨假設$a_1 \equiv \alpha \pmod{2d}$，則整個狀態以圖示表示便為:

$$\alpha \begin{matrix} 2^{n-1}\alpha & \cdots & \cdots \\ 2\alpha & 4\alpha & \cdots \end{matrix} \pmod{2d}$$

此時的最大同餘守恆數為$(2^n-1)\alpha$，即

$$2d|(2^n-1)\alpha$$

又因為$2d$為 $2M_n$的因數，即$d|(2^n-1)$，所以

$$2|\alpha$$

表示在此狀態下各數間有公因數 2，而轉為$2d$的基態後，仍然會有此公因數，與定義不合，矛盾。表示這種情況不存在。

b. $\sum_{k=1}^{n} a_k \equiv d \pmod{2d}$

在此情況下，式(2)即等於

$$a_1 + d \equiv 2a_n \pmod{2d}$$

又因為這n個數是以環狀結構排列，所以由上式可同理為

$$a_k + d \equiv 2a_{k-1} \pmod{2d}$$

其中$k = 1, 2, \dots, n$且$a_{n+1} = a_1$。

又因為d是$2^n - 1$的因數為奇數，所以由上式關係可以知道在此狀態下每個數皆為奇數，接著，仔細觀察上式，由於目前的狀態是基態，即

$$0 \le a_k < d$$

因此若我們令

$$a_1 = d - 2x \ \left(1 \le x \le \frac{d-1}{2} \ ，x \in N\right)$$

便可依序得到

$$\begin{cases} a_2 \equiv d - 4x \pmod{2d} \\ a_3 \equiv d - 8x \pmod{2d} \\ \vdots \\ a_n \equiv d - 2^n x \pmod{2d} \end{cases}$$

由於$\mathrm{d} \le 2^n - 1$，所以$d - 2^n x < 0$，因此我們可以假設

$$\begin{cases} d - 2^t x \equiv a_t \ge 0 \pmod{2d} \\ d - 2^{t+1} x \equiv a_{t+1} < 0 \pmod{2d} \end{cases}$$

$\Rightarrow \ 2^t x \le d < 2^{t+1} x$

$\Rightarrow \ -d \le -2^t x \le d - 2^{t+1} x < 0$

$\Rightarrow \ d \le a_{t+1} < 2d$

$\Rightarrow \ \frac{\varphi_n}{2} \le a_{t+1} < \varphi_n$

得證。

【心得十】
【定理十四】其實是做為【定理十二】的後半部分論證，解決了在$x-2y$型操作模式會遇到的問題，並且使【定理十二】的證明方法得到了完整的論證基礎。

(3) 特殊情況: 當n為質數時:

這個階段，在有了【定理十二】的證明過程和【定理十四】的補述證明後，我們便能證明：

【定理十五】
在「$x-2y$型操作條件」下，**若n與其同餘守恆數φ_n為質數**，則將所有可能的基態列出後，恰好數字1~(φ_n-1)各出現一遍。

【證明】

此證明幾乎同於【定理六】的證明，將分為三個部份，分別標記a. b. c.：

a. 由之前的探究過程，我們知道，當n為質數時，以【數學模型三】的構造方式，可得初始項參數式為

$$\begin{cases} \alpha_0 = (G_n-2)-G_n t \ \ (mod\ 2M_n) \\ \beta_0 = -(G_n+2)+(G_n-2)t \ \ (mod\ 2M_n) \end{cases}，t為整數$$

利用【定理十二】的證明過程與【定理十四】，由於$\varphi_n | M_n$而且φ_n為奇數，所以上述參數式可以替換為

$$\begin{cases} \alpha_0 = (G_n-2)-G_n t \ \ (mod\ \varphi_n) \\ \beta_0 = -(G_n+2)+(G_n-2)t \ \ (mod\ \varphi_n) \end{cases}，t為整數$$

此時所構造出的同餘守恆狀態，其各數間最大公因數必為 1 且最大同餘守恆數為φ_n

假設$gcd(\varphi_n,\ G_n)=m$，因為φ_n為$2M_n$的質因數，所以

$$m|\ gcd(M_n,\ G_n)$$

$$\Rightarrow\ m|\ gcd\left(2^n-1, \frac{1}{3}[2^n+1]\right)$$

由【先備性質四】

$$\Rightarrow\ m|\ gcd(2^n-1, 2^n+1)$$

$$\Rightarrow\ \ m=1$$

即φ_n、G_n互質。

再由【先備定理一】

$\Rightarrow 0,\ G_n, 2\ G_n, \dots\dots, (\varphi_n-1)G_n$ 恰為一組模φ_n的完全剩餘系

$\Rightarrow (G_n-2),(G_n-2)-G_n,(G_n-2)-2\,G_n,\ldots\ldots,(G_n-2)-(\varphi_n-1)G_n$ 亦為一組模φ_n的完全剩餘系，即**α_0可以有φ_n種不同的值**，而且一一對應到不同的t值$(mod\ \varphi_n)$。因此，

只要確定了α_0的值，也就確定了的β_0的值，則整個狀態就被唯一確定了。

b. 但若$\alpha_0 \equiv 0\ (mod\ \varphi_n)$，則$\beta_0$亦會同餘 $0(mod\ \varphi_n)$。假設$\beta_0 \equiv b \not\equiv 0\ (mod\ \varphi_n)$，則整個累加態以圖示表示即為:

$$\begin{matrix} & G_{n-1}b & G_{n-2}b & G_{n-3}b & \cdots \\ 0 & b & b & 3b & \cdots \end{matrix}$$

此狀態的最大同餘守恆數為

$$gcd(\ (2G_{n-1}-1)b,\ G_nb) = b\cdot gcd(2\ G_{n-1}-1,\ G_n) = b\cdot \phi_n = b$$

即$b=\varphi_n \equiv 0\ \ (mod\ \varphi_n)$，矛盾，所以$\beta_0 \equiv 0\ (mod\ \varphi_n)$，從而這$n$個數皆為零，換句話說，

若有一個狀態有出現一個0，則此狀態全部的數都會是0。

而我們不討論這種情況。因此，實際上α_0只能夠有(φ_n-1)種不同的值，恰好是模φ_n的一組剩餘系。

c. 再者，由於只要確定了第一個數字(初始項α_0)，就能唯一確定後面所有數字。因此，若是一個狀態內有重複的數字出現，則一定有重複的數列完整排序，否則對於某個重複出現的數值，使它在狀態內出現的不同位置分別成為初始項後，所得到的狀態會不一樣，因為我們知道，確定一個初始項後，整個狀態便是唯一確定了。若以圖示表示則為:

$$\begin{matrix} & a_t & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_1 & a_2 & \cdots & a_t & a_1 & a_2 & \cdots \end{matrix}\ (mod\ \varphi_n)$$

但是已知n為質數，不可能由數個重複數列完整排序構成守恆狀態，故

整個狀態內不會有重複的數字出現。

綜合以上$a.b.c.$三點，首先初始項α_0的值可以為$1,2,\ldots\ldots,\varphi_n-1$(若為0，則全部的數都會為0，我們不討論)；而只要確定了初始值，就能唯一確定後面所有的數；最後，一個狀態內不可能會有重複的數字出現。定理十二因此得證。

由此，還另外證明了同餘守恆數與模數n之間的同餘關係:

$$\varphi_n \equiv 1\ \ (mod\ n)$$

【心得十一】

由$mod\ 2M_n$的累加態轉為$mod\ \varphi_n$的基態時，由於可能會產生【心得九】所描述的問題，此時若將最大公因數 2 除掉，雖然還是能得到一個$mod\ \varphi_n$的守恆狀態，但是在上述【定理十五】證明過程的 *a.*部分，α_0就無法一一對應到不同的t值$(mod\ \varphi_n)$，從而整個定理就不會成立。
所以才要先證明【定理十四】，說明這種情況是不可能發生的。

再來，若仿照$x-y$型的探究過程，則我們也可證明:

【定理十六】
在「$x-2y$型操作條件」下，這n個數為守恆狀態且其同餘守恆數為φ_n，且符號⊗的運算定義如下：

$$\mathrm{K}\otimes\mathrm{L}=\mathrm{M}\ (\mathrm{mod}\ p)$$

表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合M之內。

假設n和φ_n皆為質數，若一種狀態內的n個數字構成一個集合，共有 k 個集合，滿足$gcd(n,k)=1$，則這 k 個集合間兩兩有滿足符號⊗的運算關係。

【證明】
由$x-y$型的討論中，我們知道，在$x-2y$型中，事實上就是要討論同餘方程

$$x^2\equiv x+2\ \ (\mathrm{mod}\ \varphi_n)\quad\text{——(1)}$$

的根有沒有辦法滿足

$$x^n\equiv 1\ \ (\mathrm{mod}\ \varphi_n)\quad\text{——(2)}$$

而這在$x-2y$型中，其實是個顯然的情況，式(1)中的兩個解顯然為

$$\begin{cases} x_1\equiv 2\ \ (\mathrm{mod}\ \varphi_n)\\ x_2\equiv -1\ \ (\mathrm{mod}\ \varphi_n)\end{cases}$$

又

$$\varphi_n|2M_n$$
$$\Rightarrow\ \ \varphi_n|2^n-1\quad\text{——(3)}$$

於是將x_1帶入式(2)中的x，則

$$2^n\equiv 1\ \ (\mathrm{mod}\ \varphi_n)$$

顯然為真。

再來我們令

$$\varphi_n-1=nk$$

於是我們便可考慮一個高次同餘方程

$$b^k\equiv 1\ \ (\mathrm{mod}\ \varphi_n)\quad\text{——(4)}$$

由【先備定理二】，知道方程式(4)中有$\varphi(k)$個解對模φ_n的階為k。於是我們從那$\varphi(k)$個解中任意挑一個，記為b_0。然後考慮以下k個集合:

$$A_1 = \{b_0,\ 2b_0,\ 4b_0, \dots\dots,\ 2^{n-1}b_0\}\ (mod\ \varphi_n)$$
$$A_2 = \{{b_0}^2,\ 2{b_0}^2,\ 4{b_0}^2, \dots\dots,\ 2^{n-1}{b_0}^2\}\ (mod\ \varphi_n)$$
$$A_3 = \{{b_0}^3,\ 2{b_0}^3,\ 4{b_0}^3, \dots\dots,\ 2^{n-1}{b_0}^3\}\ (mod\ \varphi_n)$$
$$\vdots$$
$$\vdots$$
$$A_k = \{{b_0}^k,\ 2{b_0}^k,\ 4{b_0}^k, \dots\dots,\ 2^{n-1}{b_0}^k\}\ (mod\ \varphi_n)$$

由【先備定理三】，可知無論b_0所選擇的解，所得的這k個集合是一樣的。
而且這nk個數$mod\ \varphi_n$均兩兩相異，證明過程同【定理六】裡的證明。
於是這k個集合便可各自排列成一個同餘守恆狀態:

$$\begin{matrix} b_0^i & 2^{n-1}b_0^i & \cdots & \cdots \\ & 2b_0^i & 4b_0^i & \cdots \end{matrix} \pmod{\varphi_n}$$

其中$i = 1, 2, \dots, n$。
又由【定理十五】的證明結果，知道守恆狀態的唯一性，亦即由遞迴累加模式所建構的守恆狀態和解同餘方程所得到的守恆狀態是同構的。因此可以完整的解釋符號⊗的運算關係。得證。

【進一步說明】
事實上，對於φ_n為奇合數的情況，我們有:

【定理十七】
在「$x - 2y$型操作條件」下，若n為質數，已知它的最大同餘守恆數為$2M_n$。假設有一數φ_n為M_n的因數，且φ_n有p個質因數，則同餘方程$x^2 \equiv x + 2\ (mod\ \varphi_n)$的解數為$2^p$。若將其根依序記為$x_1, x_2, \dots, x_{2^p}$，則必有${x_1}^n \equiv 1\ (mod\ \varphi_n)$和${x_k}^{2n} \equiv 1\ (mod\ \varphi_n)$且${x_k}^n \not\equiv 1\ (mod\ \varphi_n)\ (k = 2, 3, \dots, 2^p)$。亦即此$n$邊形有且僅有一個循環態$(mod\ \varphi_n)$。

證明方法同於【定理八】的陳述。

此外對於φ_n為奇合數的情況，我們有以下定理十六，也能建構守恆狀態:

【定理十八】
在「$x - 2y$型操作條件」下，若這n個數滿足守恆狀態且其同餘守恆數為φ_n，若n和φ_n皆為奇數，則將整個狀態乘以某數d，再轉為相對應的基態，則這個基態的最大同餘守恆數必為$\frac{\varphi_n}{gcd(d,\varphi_n)}$。

【證明】

令這n個數依照逆時針方向依序為$a_1, a_2, \dots\dots, a_n$，因此有

$$\begin{cases} 2a_1 + a_2 \equiv a_3 \ (mod\ \varphi_n) \\ 2a_2 + a_3 \equiv a_4 \ (mod\ \varphi_n) \\ \vdots \\ 2a_{n-1} + a_n \equiv a_1 \ (mod\ \varphi_n) \\ 2a_n + a_1 \equiv a_2 \ (mod\ \varphi_n) \end{cases}$$

且

$$gcd(a_1, a_2, \dots\dots, a_n) = 1$$

若將各數乘以d倍，可得一新的狀態:

$$da_1 \ \begin{matrix} da_n & \cdots & \cdots \\ da_2 & da_3 & \dots \end{matrix} \ (mod\ d\varphi_n)$$

將此狀態轉為$mod\ \varphi_n$的狀態:

$$b_1 \ \begin{matrix} b_n & \cdots & \cdots \\ b_2 & b_3 & \dots \end{matrix} \ (mod\ \varphi_n)$$

其中

$$0 \le da_i - \varphi_n t_i = b_i \le \varphi_n - 1 \quad \left(i = 1, 2, \dots\dots, n\ ;\ t_i \in N\right) \quad \text{——(1)}$$

假設

$$gcd(d, \varphi_n) = k$$

則由式(1)，可知

$$k | b_i$$

即新的$mod\ \varphi_n$的狀態間有一公因數k，我們要得到基態，則各數間必須要互質，所以我們假設各數間除了k以外，還有最大公因數s，即

$$b_i = ksc_i \quad (i = 1, 2, \dots\dots, n) \quad \text{——(2)}$$

且

$$gcd(c_1, c_2, \dots\dots, c_n) = 1$$

因此剛剛所得的狀態便可表示為

$$ksc_1 \ \begin{matrix} ksc_n & \cdots & \cdots \\ ksc_2 & ksc_3 & \dots \end{matrix} \ (mod\ \varphi_n)$$

$$\Rightarrow \ sc_1 \ \begin{matrix} sc_n & \cdots & \cdots \\ sc_2 & sc_3 & \dots \end{matrix} \ (mod\ \frac{\varphi_n}{k})$$

再由式(1)及式(2)，因為φ_n為奇數，所以$s \neq 2$，若$s \ge 3$，則

$$0 \le c_i \le \frac{\varphi_n}{ks} \le \frac{\varphi_n}{3k}$$

$$\Rightarrow \ 0 \le 2c_i + c_{i+1} \le \frac{\varphi_{Mn}}{k}$$

所以c_i的關係又可進一步寫為

$$\begin{cases} 2c_1 + c_2 = c_3 \\ 2c_2 + c_3 = c_4 \\ \vdots \\ 2c_{n-1} + c_n = c_1 \\ 2c_n + c_1 = c_2 \end{cases}$$

注意到這裡的同餘關係已經變為等號了，將這n個式子相加

$$\Rightarrow \sum_{i=1}^{n} c_i = 0$$

$$\Rightarrow c_1 = c_2 = \cdots = c_n = 0$$

式(1)即可寫為

$$da_i = \varphi_{Mn} t_i$$
$$\Longrightarrow gcd(a_1, a_2, \ldots\ldots, a_n) > 1$$

除非$\varphi_{Mn} | d$，而這種情況是無意義的，從而s必須等於 1。

即經過如此操作後的狀態$(mod\ \frac{\varphi_{Mn}}{k})$，其各數必定互質，因此滿足了基態的條件，故原命題得證。

三.研究結果與討論

1. 數學模型

(1) 【數學模型一】：同餘

以$a_1\ \begin{matrix} a_n & \cdots & \cdots \\ a_2 & a_3 & \ldots \end{matrix}$的圖示來表示操作過程中的某個狀態，並且將相對應到的頂點數值取模的同餘數。(本作品在前半部分的推廣階段都是表示為A $\begin{matrix} B & C \\ F & E \end{matrix}\ D$，而且取模 2 作同餘，亦即以奇偶性討論之。例如： $0\ \begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}\ 0\ (mod\ 2)$

(2) 【數學模型二】：交替循環

我們構造以下兩個操作步驟，作為「交替循環」的操作：

步驟Ⅰ：由 S 為奇數的狀態，轉變到只有一個奇數的狀態。

步驟Ⅱ：從只有一個奇數的狀態，轉變到 S 為奇數且 *max* 變小或為零的狀態。

【說明】

由於上述的操作步驟中，都不會增加 *max*，而每次操作步驟 II 後都會使 *max* 的值至少遞減 1，最終變為零。所以我們只要說明以上的步驟是如何操作就行。

(3) 【數學模型三】：遞迴累加

我們將兩個初始的非負整數記為α、β，在 $x - qy$ 操作模式下，有以下狀態：

$$\begin{array}{cccc} \alpha & U_{n-2}q\alpha + U_{n-1}\beta & U_{n-3}q\alpha + U_{n-2}\beta & \cdots & \cdots \\ & \beta & q\alpha + \beta & q\alpha + (1+q)\beta & \cdots \end{array}$$

其中數列<U_n>滿足遞迴關係：$U_1 = 1$，$U_2 = 1$，　$U_{n+2} = U_{n+1} + qU_n$。

【說明】

這是在$x - qy$操作模式下的逆向操作，以保證每個數在$x - qy$的第一次操作下，其數值不會改變，但在此遞迴累加模式中仍必須保留起始項與最末兩項的關係，符合$x - qy$的操作模式，以確保整體操作模式的一致性。

(4) 【數學模型四】守恆三態

為了討論的方便性，我們將守恆的狀態分成以下三種：

a. 遞迴累加態(以後簡稱累加態)：若n邊形上的n個數經過【遞迴累加】模型之操作後，滿足守恆狀態且各數間最大公因數為 1，則稱此狀態為遞迴累加態。

b. 基準態(以後簡稱基態)：已知n邊形上的n個數在滿足守恆狀態的條件下，其同餘守恆數為φ_n，若這n個數都屬於mod φ_n的最小非負完全剩餘系且各數間最大公因數為 1，則稱此狀態為基準態。

c. 循環群態(以後簡稱循環態)：已知n邊形上的n個數在滿足守恆狀態下，其同餘守恆數為φ_n，且這n個數恰成為一個mod φ_n的循環群，則稱此狀態為循環群態。

2. 引理與定理

(1) 【引理一】

在$|x - y|$型操作下，要使 n 邊形的各頂點數字之奇偶性經過任意操作後皆保持不變的情況，除了全是偶數之外，其狀態必須是唯一的，即在 n 必須為 3 的倍數的情況下，且各頂點上的數字必須以(奇、奇、偶、奇、奇、偶、…、奇、奇、偶)的順序方式排列，才能經過任意操作後皆保持奇偶性不變的情況。

(2) 【引理二】

在填入 n 邊形的各頂點數字，其排列情形不符合奇偶性守恆的狀態下，則任意情況都可經過一系列的有限操作導致只剩一個頂點上的數字是奇數的狀態。

(3) 【引理三】

在$|x - y|$型操作下，填入 n 邊形的各頂點數字，若只要有出現連續兩個零的排列狀態時，則可以經過一定的操作使得正 n 邊形的各頂點數字都變為零。

(4) 【引理四】

若在 n 邊形的 n 個頂點數字至少有一數為奇數的條件下，存在滿足條件的「理想 k 值」(或不存在「理想 k 值」)時，則正 n 邊形的 n 個頂點數字都是偶數的情況仍然會有相同的「理想 k 值」(或不存在「理想 k 值」)。

(5) 【定理一】

在一個 n 邊形(n 不為 3 的倍數)的頂點上放上 n 個不盡相異的非負整數，做以下操作：擦去一個數，寫上其相鄰兩數之差的絕對值，則無論怎麼放置頂點上的數字，總是可以經過一系列的操作使得各頂點的數字歸零。

(6) 【定理二】

在一個 n 邊形(n 為 3 的倍數)的頂點上放上 n 個不盡相異的非負整數，做以下操作：擦去一個數，寫上其相鄰兩數之差的絕對值，則只要頂點上的數字和是奇數或是小於$\frac{2}{3}n$的偶數，總是可以經過一系列的操作使得各頂點的數字歸零。

(7) 【定理三】

在「$x-y$型操作條件」下，則

(1)當 n 為 4 的倍數時，$\phi_n = F_{\frac{n}{2}}$

(2)當 n 為 2 的倍數但不為 4 的倍數時，$\phi_n = L_{\frac{n}{2}}$

(3)當 n 是奇數且為 3 的倍數時，$\phi_n = 2$

(4)當 n 是奇數且不為 3 的倍數時，$\phi_n = 1$，其中，「ϕ_n」為本原守恆數」，F_n為費氏數列的第 n 項，L_n為盧卡斯數列的第 n 項。

(8) 【定理四】

在「$x-y$型操作條件」下，則n邊形的最大同餘守恆數

$$\begin{cases} \varphi_{Mn} = \frac{L_n}{\phi_n}，若n為奇數 \\ \varphi_{Mn} = \frac{L_n-2}{\phi_n}，若n為偶數 \end{cases}$$，且此時在遞迴累加模型中的初始兩項為

$$\begin{cases} \alpha_0 = \frac{(F_{n-1}-1)-F_n t}{\phi_n} \\ \beta_0 = \frac{-(F_{n-2}+1)+(F_{n-1}-1)t}{\phi_n} \end{cases}，t為整數$$

(9) 【定理五】

在「$x-y$型操作條件」下，假設其n邊形的最大同餘守恆數為φ_{Mn}且$d \mid \varphi_{Mn}$，則我們必可找到一個狀態，滿足:此狀態各數間的最大公因數為 1，且d是這個狀態的最大同餘守恆數。

(10)【定理六】

在「$x-y$型操作條件」下，若給定其同餘守恆數φ_n，且n與φ_n皆為質數，將所有可能的基態列出後，恰好數字$1\sim(\varphi_n-1)$各出現一遍。

(11)【定理七】

在「$x-y$型操作條件」下，假設這n個數為守恆狀態且其同餘守恆數為φ_n。符號⊗的運算定義如下：

$$\mathrm{K}\otimes\mathrm{L} = \mathrm{M}\ (\mathrm{mod}\ \varphi_n)$$

表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合

M之內。

在n與φ_n皆為質數的情況下，若一種守恆狀態內的n個數字構成一個集合，共有 k 個集合，滿足$gcd(n,k)=1$，則這 k 個集合間兩兩有滿足符號⊗的運算關係。

(12)【定理八】

在「$x-y$型操作條件」下，若n為質數，已知它的最大同餘守恆數為L_n。假設有一數φ_n為L_n的因數，且φ_n有p個質因數，則同餘方程$x^2 \equiv x+1 \ (mod\ \varphi_n)$的解數為$2^p$。若將其根依序記為$x_1, x_2, \dots, x_{2^p}$，則必有${x_1}^n \equiv 1 \ (mod\ \varphi_n)$和${x_k}^{2n} \equiv 1 \ (mod\ \varphi_n)$ 且${x_k}^n \not\equiv 1 \ (mod\ \varphi_n) \ (k=2,3,\dots,2^p)$。亦即此$n$邊形有且僅有一個循環態$(mod\ \varphi_n)$，而$2n$邊形有$2^p$個循環態$(mod\ \varphi_n)$。

(13)【定理九】

在「$x-y$型操作條件」下，若這n個數滿足守恆狀態，且其同餘守恆數為φ_n，則將整個狀態乘以某數d，再轉為相對應的基態，則這個基態的最大同餘守恆數必為$\frac{\varphi_n}{gcd(d,\varphi_n)}$。

(14)【定理十】

在「$x-2y$型操作條件」下，則

(1) 當n為偶數時，$\phi_n = G_n$

(2) 當n為奇數時，$\phi_n = 1$

其中，G_n為 Jacobsthal 數列中的第n項。

(15)【定理十一】

在「$x-2y$型操作條件」下，

若n為奇數，則n邊形的最大同餘守恆數$\varphi_{Mn} = 2M_n$，且此時在遞迴累加模型中的初始兩項為

$$\begin{cases} \alpha_0 = (G_n-2) - G_n t \ (mod\ \varphi_n) \\ \beta_0 = -(G_n+2) + (G_n-2)t \ (mod\ \varphi_n) \end{cases}，t\text{為整數}$$

若n為偶數，則n邊形沒有最大同餘守恆數。

(16)【定理十二】

在「$x-2y$型操作條件」下，假設其n邊形的最大同餘守恆數為φ_{Mn}且$d \mid \varphi_{Mn}$，則我們必可找到一個狀態，滿足：此狀態各數間的最大公因數為 1，且d是這個狀態的最大同餘守恆數。

(17)【定理十三】

在「$x-2y$型操作條件」下，這n個數為守恆狀態且其同餘守恆數為φ_n。若n和φ_n皆為奇數，且這n個數照逆時針方向依序記為$a_1, a_2, \dots, a_n$，則有:

$$a_{k+1} \equiv 2a_k \ (mod\ \varphi_n)$$

其中$k = 1, 2, \dots, n$且$a_{n+1} = a_1$。

(18)【定理十四】

在「$x-2y$型操作條件」下，假設這n個數為基態且同餘守恆數為φ_n，若n為奇數且φ_n為偶數，則這n個數當中必至少有一個數大於$\frac{\varphi_n}{2}$。

(19)【定理十五】

在「$x-2y$型操作條件」下，若給定其同餘守恆數φ_n，且n與φ_n皆為質數，將所有可能的基態列出後，恰好數字1~(φ_n-1)各出現一遍。

(20)【定理十六】

在「$x-2y$型操作條件」下，這n個數為守恆狀態且其同餘守恆數為φ_n，且符號⊗的運算定義如下：

$$\mathrm{K}\otimes\mathrm{L}=\mathrm{M}\ (\mathrm{mod}\ p)$$

表示集合K內任一元素乘以集合L內任一元素再除以p的餘數皆會落在集合M之內。

假設n和φ_n皆為質數，若一種狀態內的n個數字構成一個集合，共有 k 個集合，滿足$gcd(n,k)=1$，則這 k 個集合間兩兩有滿足符號⊗的運算關係。

(21)【定理十七】

在「$x-2y$型操作條件」下，若n為質數，已知它的最大同餘守恆數為$2M_n$。假設有一數φ_n為M_n的因數，且φ_n有p個質因數，則同餘方程$x^2\equiv x+2\ (mod\ \varphi_n)$的解數為$2^p$。若將其根依序記為$x_1,x_2,\dots,x_{2^p}$，則必有${x_1}^n\equiv 1\ (mod\ \varphi_n)$和${x_k}^{2n}\equiv 1\ (mod\ \varphi_n)$且${x_k}^n\not\equiv 1\ (mod\ \varphi_n)\ (k=2,3,\dots,2^p)$。亦即此$n$邊形有且僅有一個循環態$(mod\ \varphi_n)$。

(22)【定理十八】

在「$x-2y$型操作條件」下，若這n個數滿足守恆狀態且其同餘守恆數為φ_n，若n和φ_n皆為奇數，則將整個狀態乘以某數d，再轉為相對應的基態，則這個基態的最大同餘守恆數必為$\frac{\varphi_n}{gcd(d,\varphi_n)}$。

3. 討論

(1) 在$x-y$型與$x-2y$型中，φ_n為合數的情況，目前僅給出了建構所有守恆狀態的方法，然而對於其狀態內的結構關係尚待進一步的探究。

(2) 對於「同序方格」長寬的值不同時，其產生的狀態目前還無法確切知道，尤其是當φ_n為合數的情況，所填入的符號關係會變得相當複雜。推論是和二項同餘方程$x^d\equiv 1\ (mod\ p)$有密切相關。

(3) 僅就討論同餘守恆數時，若推廣至$x-qy$型，對於其本原守恆數若仿照【定理三】的探究過程，可得到

$$\phi_n=\gcd(q^{k+1}U_{n-k+1}+U_{k+1},\quad q^kU_{n-k}-U_k)$$

其中<U_n>滿足遞迴關係：$U_1 = 1$，$U_2 = 1$，$U_{n+2} = U_{n+1} + qU_n$

然而目前卻沒有一個較好的辦法化簡上式，將其直接計算後一一列出，所觀察到的規律也有一定的複雜程度。

(4) 對於$x - qy$型的推廣，其同餘守恆數若仿照【定理四】的化簡，針對不同的q值，則我們可以得到不同的數列:

$$Q_n = |V_n - [(-q)^n + 1]|$$

其中<V_n>滿足遞迴關係：$V_0 = 2$，$V_1 = 1$，$V_{n+2} = V_{n+1} + qV_n$

則$\varphi_{Mn} = \frac{Q_n}{\phi_n}$。

特別地，若對<Q_n>的每一項作質因數分解，會發現若p為質數，而且$p|Q_n$且$p \nmid Q_m \; \forall \, m < n$，則有$p \equiv 1 \pmod n$若$p > n$。

我們推論這個性質和定理六及定理十五所陳述的內容相關，只是我們發現到，這個性質對於n為合數時也成立。這將會是我們未來研究一個值得深入探索的地方。

(5) 其實我們也有簡單對$x - qy$型與$px - y$型進行比較與探究，發現兩者的狀態存在某些共通性，只是由於整段探究還不完整，因此列於討論部分。這將會是我們未來研究的另一個方向。

(6) 事實上，若是僅單純討論同餘守恆模式，其實我們也可以探究$px + qy$型；而當初會以$px - qy$型做為推廣目標是為了探究歸零的模式，但本研究後期都聚焦在同餘守恆模式，因此這也可能成為我們未來的研究方向。

四.結論與應用

1. 結論：

(1) 在探究的過程中，我們透過所建構的同餘性與交替循環性之數學模型，針對 *n* 邊形在$|x - y|$型操作條件下之情形都已探討出具體的結果。

(2) 針對延伸問題之一——「$x - y$型」:

a. 在同餘守恆數方面，有了完整的結果。

b. 在同餘守恆模式方面，我們得出了三種不同的方式建構同餘守恆狀態，並可應用於其他的操作模式。

c. 其中針對n與φ_n皆為質數的情況，有完整的特殊性質探討。

(3) 針對延伸問題之二——「$x - 2y$型」:

a. 在同餘守恆數方面，有了完整的結果。

b. 在同餘守恆模式方面，對於n為偶數的情況，可以任意的建構同餘守恆狀態；對於n為奇數的情況，φ_n為奇數時的守恆模式有完整的解釋、φ_n為偶數時的守

恆模式尚待進一步探究。

c. 其中針對n與φ_n皆為質數的情況，有完整的特殊性質探討。

(4) 在心得四中初步得到兩個觀察結果，事實上，若進一步對於所陳述的集合與⊗運算關係作深入探討，發現若 $k+1$ 為質數，則可以將各集合等價的一一對應為質數 $k+1$ 的k個最簡剩餘類；甚至，對於此結論所陳述的對應剩餘類再做延伸討論，亦可發現若某集合對應到 $k+1$ 的二次剩餘，則此集合內的數字即為φ_n的二次剩餘。(此部分的論證，將置於後面的附錄)

2. 應用：

本研究是在探討環型排列的數字其守恆狀態及全數歸零的模式：

(1) 歸零模式的操作與設計可以發展成某些得運用策略型態的遊戲。

(2) 守恆狀態中運用的同餘性質概念，可以用於通訊傳遞或加密資料。

(3) 本研究可望為當中涉及到的一些數列(如盧卡斯數列、梅森數列)提供另一種角度的探究。

五.參考文獻

1. 2004 年 IMO 中國國家集訓隊教練組等編。數學奧林匹克試題集錦(2004)。一版。華東師範大學出版社。P.139~P.141。2004 年
2. 景琰杰。高次剩餘理論及二項同餘方程求解的研究初探。
3. 潘承洞、潘承彪著。簡明數論。一版。九章出版社。P.100~P.129, P.143~P.226。2002 年。
4. Verner E.Hoggatt.Jr. "Fibonacci and Lucas Numbers”The Fibbonacci Association. 1969.
5. Zhi-Hong-Sun. 24 February 2009. “Congruence for Fibonacci Numbers”.

※附錄

一、【結論(4)中的證明】

在一個 n 邊形的 n 個頂點上，填寫 n 個不盡相異之非負整數，且這 n 個數的最大公因數為 1 時，在「$x-y$型操作條件」下，且符號⊗的運算定義如下：

$$\mathrm{K}\otimes\mathrm{L}=\mathrm{M}\ (\mathrm{mod}\ \varphi_n)$$

則

(1)若 k+1 為質數，則可以將各集合等價的一一對應為質數 k+1 的k個剩餘類。

(2)對於(1)點所陳述的對應剩餘類，若某集合對應到 k+1 的二次剩餘，則此集合內的數字即為φ_n的二次剩餘。

【證明】

(1)

∵ 已知$k+1$為質數，又沿用【定理七】的證明過程 a.部分，知道b_0為$k+1$的原根。再由【先備定理四】，知道

$$b_0, {b_0}^2, {b_0}^3, \dots\dots, {b_0}^k$$

一一對應到一組模$k+1$的剩餘類，令

$${b_0}^j \equiv a_i \ \ (mod\ k+1)\ \ (1\le i,j\le \mathrm{k})$$

所以

$$a_1, a_2, \dots, a_k$$

也一一對應到一組模$k+1$的剩餘類，再來考慮集合

$$A_i=\left\{a_0{b_0}^j,\ \ {a_0}^2{b_0}^j,\ \ {a_0}^3{b_0}^j, \dots\dots,\ \ {a_0}^n{b_0}^j\right\}\ \ (mod\ \varphi_n)$$

使之對應到一組$k+1$的剩餘類$a_i\ mod\ k+1$，則性質(3)可立即推出:

$$A_i\otimes A_{i'}=A_{i\times i'}\ \ (mod\ \varphi_n)$$

(2)

承接性質(1)的證明過程，考慮以下命題: 若j為偶數，若且唯若a_i為$k+1$的二次剩餘。

此命題的順敘述顯然成立，又因為$k+1$的二次剩餘僅有$\frac{k}{2}$個，而 $j=1,2,\dots,k$當中也恰有$\frac{k}{2}$個偶數，且a_i值兩兩相異，所以逆敘述也被迫成立。

於是考慮a_i為$k+1$的二次剩餘的情況下，集合

$$A_i=\left\{a_0{b_0}^j,\ \ {a_0}^2{b_0}^j,\ \ {a_0}^3{b_0}^j, \dots\dots,\ \ {a_0}^n{b_0}^j\right\}\ \ (mod\ \varphi_n)$$

內的元素可寫為

$${a_0}^s{b_0}^j\ \ (1\le s\le n)$$

若s為偶數，則此元素顯然為φ_n的二次剩餘(因為s,j皆為偶數)。

若s為奇數，此元素亦為φ_n的二次剩餘，因為

${a_0}^s{b_0}^j\equiv{a_0}^{s+n}{b_0}^j\equiv\left({a_0}^{\frac{s+n}{2}}{b_0}^{\frac{j}{2}}\right)^2\ \ (mod\ \varphi_n)$。得證。

二、【最大同餘守恆數與其質因數分解表】($x-y$型)

n	ϕ_n	φ_{Mn}	φ_{Mn}之因數分解
3	2	2	2
4	1	5	5
5	1	11	11
6	4	4	2^2
7	1	29	29
8	3	15	3× 5
9	2	38	2 ×19
10	11	11	11
11	1	199	199
12	8	40	$2^3 \times 5$
13	1	521	521
14	29	29	29
15	2	682	2 × 11 ×31
16	21	105	3 × 5 ×7
17	1	3571	3571
18	76	76	$2^2 \times 19$
19	1	9349	9349
20	55	55	5 × 11
21	2	12238	2 × 29 ×211
22	199	199	199
23	1	64079	139×461
24	144	720	$2^4 \times 3 \times 5$
25	1	167761	11 ×101×151
26	521	521	521
27	2	5779	5779
28	377	1885	5 ×13× 29
29	1	1149851	59×19489
30	1364	1364	$2^2 \times 11 \times 31$

*標有框框表示之前沒有出現過的質因數

附註: $x-2y$型即為大家所熟知的梅森數列，故不特別於附錄列出。

Abstract

This research is a study of dynamic graph labeling on the vertices of a polygon. We start the labeling by using a set of integers and continually perform the following operation: *choose the label of a vertex and replace it by the linear combination of the labels from its adjacent vertices.*

There exists a number such that, if all labels remain unchanged after any operation under modulo by that number, then the stable representation of the labels is called a *Congruence Conservation Form*, and the number we take for congruence is referred to as the corresponding *Congruence Conservation Number.*

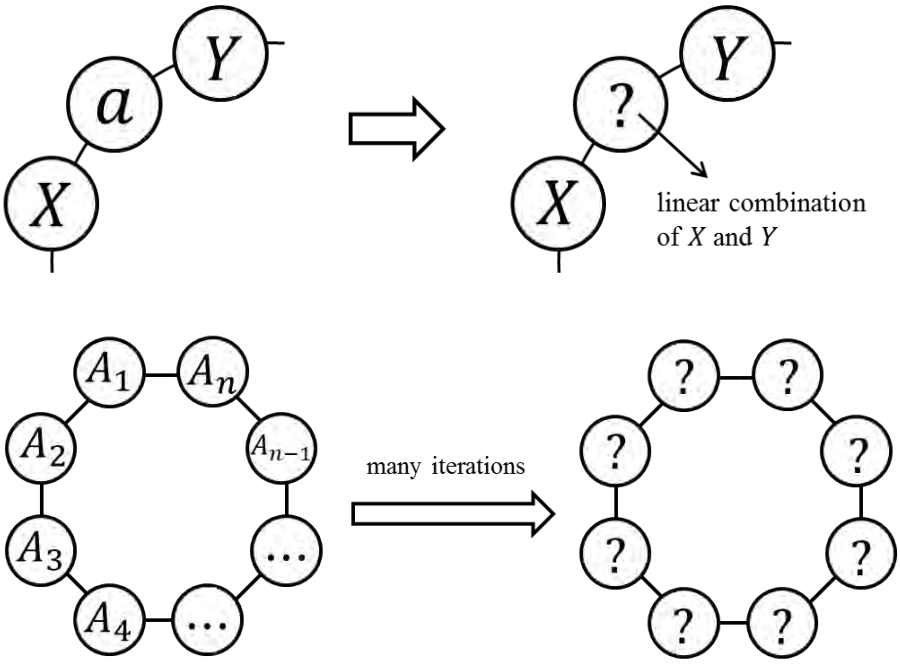
In this research proposal, by using a mathematical model and solving particular congruence equations, we are able to obtain many interesting Congruence Conservation Forms and their corresponding numbers. Moreover, we discover the secret hidden inside this special type of labeling.

As a consequence of this study, we have developed three ways to construct the Congruence Conservation Forms. Surprisingly, we also find a series of new sequences which are derived from the Congruence Conservation Number. As a matter of fact, they are closely related to the well-known sequences such as Lucas sequence etc., and the congruence properties of these new sequences can be explained by the Congruence Conservation Form. In the final part of this study, we conclude it with showing the fact that the set of labels used in a Congruence Conservation Form does form a cyclic group under multiplication operation.

I. Introduction

There are many games in graph labeling by using a set of integers, and one of them is to label the vertices of a polygon and continually perform given operation where **a label is changed and the changed value depends on the labels from its adjacent vertices.**

One needs to study the properties of the remaining numbers after many iterations.



II. Research Problem

The purpose of this study is to generalize these games into the problem of dynamic labeling on the vertices of a polygon. For a given n-gon, we want to find the ***conservation forms*** in which all labels remain unchanged after any operation (under specific condition), and explore their mathematical properties.

III. Basic Methods

A. Definitions

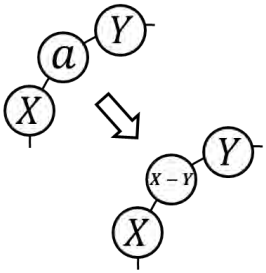
1. Congruence Conservation Form:

There exists a number such that, if all labels remain unchanged after any operation under modulo by that number, then the stable representation of the labels is called a *Congruence Conservation Form.*

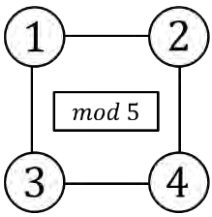
2. Congruence Conservation Number:

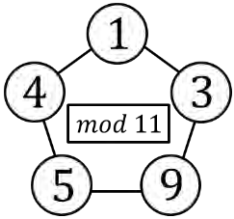
The number we take for congruence is referred to as the corresponding *Congruence Conservation Number.*

❒ *Examples*:



- Let us illustrate with relabeling a vertex by taking direct difference of the labels from two adjacent vertices in a clockwise direction.
- Observe the changed value of every label after performing an operation (left figure): $\mathbf{1 \to 1}$ $\mathbf{2 \to -3}$ $\mathbf{4 \to -1}$ $\mathbf{3 \to 3}$
- Notice that all labels remain unchanged under modulo 5, and thus the representation is regarded as a *Congruence Conservation Form*.
- The right figure is the other *Congruence Conservation Form* by labeling a pentagon.





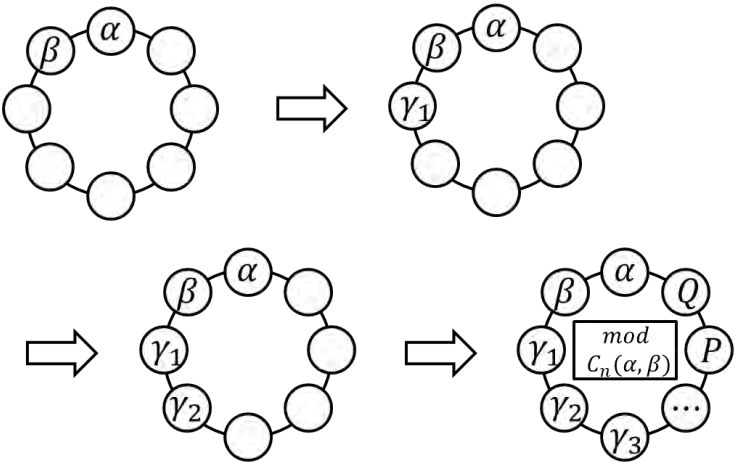
B. Mathematical Model

1. We can use reversal operations to reconstruct a *Congruence Conservation Form* step by step with two assumed initial labels α and β.

2. Suppose P and Q are the last two labels, owing to the circular structure, we can obtain a system of congruence equations.

3. We denote the maximal *Congruence Conservation Number* by "$C_n(\alpha,\ \beta)$" in this *Congruence Conservation Form*, and the maximal value of $C_n(\alpha,\ \beta)$ is abbreviated as "C_n" for simplicity. Only the factors of C_n can be the *Congruence Conservation Numbers.*

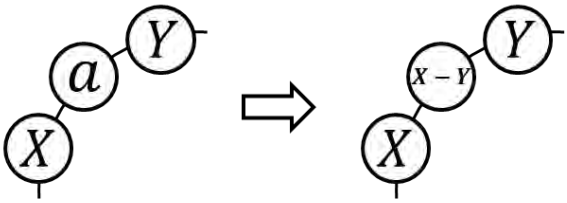
4. Suppose a number k satisfies the condition that no matter what values of α and β we choose, k can definitely be the *Congruence Conservation Number*, then we denote the maximal value of k by "D_n".



IV. Process & Results

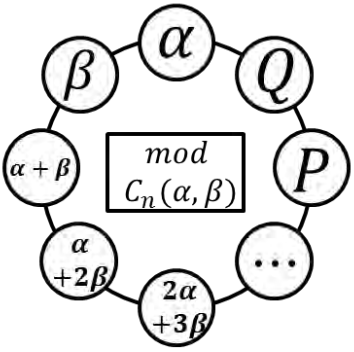
A. $X - Y$ Operation Mode

1. Operation:



2. Finding the value of the Congruence Conservation Number:

Applying the mathematical model, we can obtain a system of congruence equations:



$$\begin{cases} Q \equiv \alpha - P \ (mod\ C_n(\alpha,\ \beta)) \\ \alpha \equiv \beta - Q \ (mod\ C_n(\alpha,\ \beta)) \end{cases}$$

in which

$$\begin{cases} P = F_{n-3}\alpha + F_{n-2}\beta \\ Q = F_{n-2}\alpha + F_{n-1}\beta \end{cases}$$

(F_n is the Fibonacci number)

$$\Rightarrow \begin{cases} (\boldsymbol{F_{n-1} - 1})\boldsymbol{\alpha} + \boldsymbol{F_n\beta} \equiv \boldsymbol{0} \ (\boldsymbol{mod\ C_n(\alpha,\ \beta)}) \\ (\boldsymbol{F_{n-2} + 1})\boldsymbol{\alpha} + (\boldsymbol{F_{n-1} - 1})\boldsymbol{\beta} \equiv \boldsymbol{0} \ (\boldsymbol{mod\ C_n(\alpha,\ \beta)}) \end{cases}$$

➢ **Value of D_n**

According to the definition of D_n, we can infer that:

$$\begin{aligned} D_n &= gcd\left(F_{n-1} - 1,\ F_n\ ,\ F_{n-2} + 1\right) \\ &= gcd\left(F_{n-1} - 1,\ F_n\right) \\ &= gcd\left(F_{n-1} - 1,\ F_{n-2} + 1\right) \\ &= gcd\left(F_{n-3} - 2,\ F_{n-2} + 1\right) \\ &\quad\ \vdots \\ &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \qquad (k\ is\ odd) \end{aligned}$$

We then prove the following statements respectively:

(1) If $n = 4t$, then $D_n = F_{n/2}$
(2) If $n = 4t + 2$, then $D_n = L_{n/2}$
(3) If $n = 6t - 3$, then $D_n = 2$
(4) If $n = 6t \pm 1$, then $D_n = 1$
(Here t is a positive integer, and L_n is the Lucas number.)

Proof.

(1) $n = 4t$, let $k = 2t + 1$, then

$$\begin{aligned} D_n &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \\ &= gcd\left(F_{2t-1} - F_{2t+1},\ F_{2t} + F_{2t}\right) \\ &= gcd\left(-F_{2t},\ 2F_{2t}\right) \\ &= F_{2t} = F_{n/2} \end{aligned}$$

(2) $n = 4t + 2$, let $k = 2t + 1$, then

$$\begin{aligned} D_n &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \\ &= gcd\left(F_{2t+1} - F_{2t+1},\ F_{2t+2} + F_{2t}\right) \\ &= F_{2t+2} + F_{2t} = L_{2t+1} = L_{n/2} \end{aligned}$$

(3) $n = 6\mathrm{t} - 3$, let $k = 3t - 2$ (t is odd), then

$$\begin{aligned} D_n &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \\ &= gcd\left(F_{3t-1} - F_{3t-2},\ F_{3t} + F_{3t-3}\right) \\ &= gcd\left(F_{3t-3},\ 2F_{3t-2} + 2F_{3t-3}\right) \\ &= gcd\left(F_{3t-3},\ 2F_{3t-2}\right) = 2 \end{aligned}$$

If t is even, then let $k = 3t - 1$. The result is the same.

(4) $n = 6\mathrm{t} \pm 1$,

a. $n = 6\mathrm{t} - 1$, let $k = 3t$ (t is even), then

$$\begin{aligned} D_n &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \\ &= gcd\left(F_{3t-1} - F_{3t},\ F_{3t} + F_{3t-1}\right) \\ &= gcd\left(-F_{3t-2},\ 2F_{3t-1} + F_{3t-2}\right) \\ &= gcd\left(F_{3t-2},\ 2F_{3t-1}\right) = 1 \end{aligned}$$

If t is even, then let $k = 3t - 1$. The result is the same.

b. $n = 6\mathrm{t} + 1$, let $k = 3t$ (t is odd), then

$$\begin{aligned} D_n &= gcd\left(F_{n-k} - F_k,\ F_{n-k+1} + F_{k-1}\right) \\ &= gcd\left(F_{3t+1} - F_{3t},\ F_{3t+2} + F_{3t-1}\right) \\ &= gcd\left(F_{3t-1},\ 2F_{3t} + 2F_{3t-1}\right) \\ &= gcd\left(F_{3t-1},\ 2F_{3t}\right) = 1 \end{aligned}$$

If t is even, then let $k = 3t - 1$. The result is the same. ■

➢ **Value of C_n**

We are going to prove:

$$C_n = \begin{cases} \dfrac{L_n - 2}{D_n}, & n \text{ is even} \\ \dfrac{L_n}{D_n}, & n \text{ is odd} \end{cases}$$

Proof.

According to the system of congruence equations derived from the mathematical model, we know:

$$\begin{cases} (F_{n-1} - 1)\alpha + F_n\beta \equiv 0 \left(mod\ C_n(\alpha,\ \beta)\right) \\ (F_{n-2} + 1)\alpha + (F_{n-1} - 1)\beta \equiv 0\ (mod\ C_n(\alpha,\ \beta)) \end{cases}$$

Suppose $C_n(\alpha,\ \beta)$ has the maximal value C_n when $\alpha = \alpha_0$, $\beta = \beta_0$, then

$$\begin{cases} C_n | (F_{n-1} - 1)\alpha_0 + F_n\beta_0 \\ C_n | (F_{n-2} + 1)\alpha_0 + (F_{n-1} - 1)\beta_0 \end{cases}$$

Use elimination by addition or subtraction,

$$\begin{cases} C_n | [(F_{n-2} + 1) \cdot F_n - (F_{n-1} - 1)^2]\beta_0 \\ C_n | [(F_{n-2} + 1) \cdot F_n - (F_{n-1} - 1)^2]\alpha_0 \end{cases}$$

$$\Rightarrow\ C_n | [(F_{n-2} + 1) \cdot F_n - (F_{n-1} - 1)^2]$$

Notice that the greatest common divisor of the coefficient of α_0 and β_0 must be divided during elimination by addition or subtraction.

Therefore,

$$\boldsymbol{C_n = \frac{(F_{n-2}+1)\cdot F_n - (F_{n-1}-1)^2}{D_n}}$$

In the meantime, the determinant of this system of equations is zero, and thus we can derive the parametric form of α_0 and β_0:

$$\begin{cases} \boldsymbol{\alpha_0 = \frac{(F_{n-1}-1) - F_n \cdot t}{D_n}} \\ \boldsymbol{\beta_0 = \frac{-(F_{n-2}+1) + (F_{n-1}-1)\cdot t}{D_n}} \end{cases}$$

(Here t is an integer.)

We further simplify the value of C_n by the formula for the n[th] Fibonacci number:

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Finally, we can obtain:

$$C_n = \frac{F_n + 2F_{n-1} + [(-1)^{n-1}] - 1}{D_n}$$

$$= \begin{cases} \frac{L_n - 2}{D_n}, & n\ is\ even \\ \frac{L_n}{D_n}, & n\ is\ odd \end{cases}$$

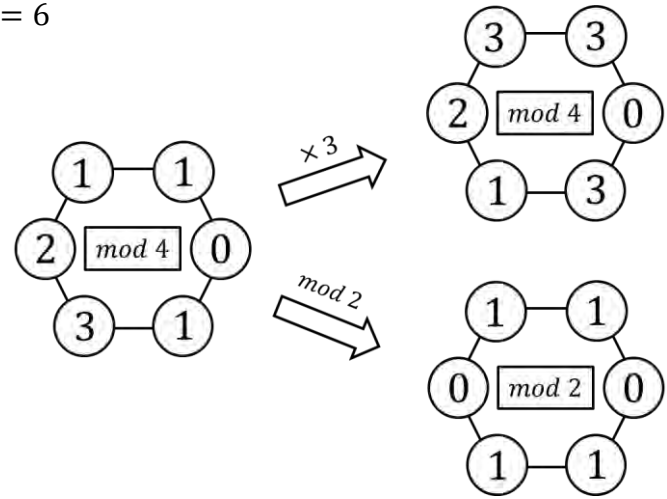
■

3. Constructing all Congruence Conservation Forms:

Now we are going to interpret how to construct all *Congruence Conservation Forms*. We have to introduce the aiding method —— **Supposing a *Congruence Conservation Form* is achieved, and then multiply all labels by an integer coprime to the *Congruence Conservation Number*, or modulo by a factor of the *Congruence Conservation Number.* A new *Congruence Conservation Form* will be constructed.** This method is valid for all situations.

❒ *Example:*

$n = 6$



By using the mathematical model and this method, for a given n-gon, we can construct its all *Congruence Conservation Forms*.

4. Investigating the properties of the Congruence Conservation Form:

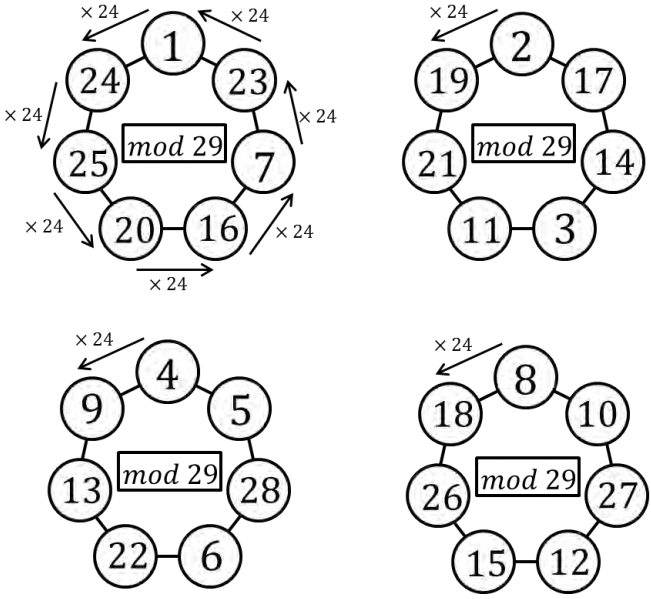
We have found two interesting properties of the *Congruence Conservation Form* when both the values of n and the corresponding *Congruence Conservation Number* are **prime**.

(1) The labels used in the *Congruence Conservation Form* does form a **cyclic group** under multiplication operation. In addition, it can be shown that the generator is given by $\frac{L_{n+1}+1}{2}$.

(2) All numerical factors of C_n are congruent to 1 modulo n.

❒ *Example:*

$n = 7$



Proof.

(1)

According to the formula for the *Congruence Conservation Number*, when n is a prime, we know

$$C_n = L_n$$

Suppose the corresponding *Congruence Conservation Number* is C'_n, which is a prime, and we know

$$C'_n | L_n$$

Now, we have to prove that there exists an integer satisfies the system of equations:

$$\begin{cases} x^2 \equiv x + 1 \ (mod\ C'_n) & \text{—— (1)} \\ x^n \equiv 1 \ (mod\ C'_n) & \text{—— (2)} \end{cases}$$

Using method of substitution, we suppose $y \equiv 2x - 1 \ (mod\ C'_n)$, and then equation (1) can be rewritten by

$$y^2 \equiv 5 \ (mod\ C'_n)$$

By the following identical equation:

$$L_p^2 - L_{p-1}L_{p+1} = 5 \cdot (-1)^p$$

Let $p = n + 1$ be even, we can infer that

$$y = \pm L_{n+1}$$

Its corresponding values of x are:

$$\begin{cases} x_1 = \dfrac{L_{n+1} + 1}{2} \\ x_2 = \dfrac{-L_{n+1} + 1}{2} \end{cases}$$

They are the roots of equation (1), thus

$$\begin{cases} x_1 + x_2 \equiv 1 \ (mod\ C'_n) \\ x_1 \cdot x_2 \equiv -1 \ (mod\ C'_n) \end{cases}$$

Suppose $T_k = x_1^k + x_1^2$, then

$$\begin{cases} T_0 \equiv 2 \ \ (mod\ C'_n) \\ T_1 \equiv 1 \ \ (mod\ C'_n) \\ T_k \equiv T_{k-1} + T_{k-2} \ \ (mod\ C'_n) \end{cases}$$

$$\Rightarrow T_k \equiv L_k \equiv 0 \ (mod\ C'_n)$$

So

$$\begin{cases} {x_1}^n + {x_2}^n \equiv T_k \equiv 0 \ \ (mod\ C'_n) \\ {x_1}^n \cdot {x_2}^n \equiv -1 \ \ (mod\ C'_n) \end{cases}$$

Hence, we know that either x_1 or x_2 satisfies equation (1) and (2) simultaneously. Now, we are going to prove that x_1 is the root.

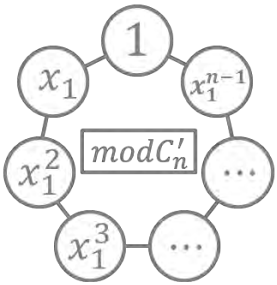
$$\begin{aligned} & x_1^2 \equiv x_1 + 1 \ (mod\ C'_n) \\ \Rightarrow\ & x_1^n \equiv F_n \cdot x_1 + F_{n-1} \ (mod\ C'_n) \\ \Rightarrow\ & 2x_1^n \equiv F_n \cdot (2x_1 - 1) \equiv F_n \cdot L_{n+1} \equiv 2 \ (mod\ C'_n) \end{aligned}$$

(by the identical equation $F_{n+1} \cdot L_n - F_n \cdot L_{n+1} = (-1)^n \cdot 2$)

$$\Rightarrow\ x_1^n \equiv 1 \ (mod\ C'_n)$$ ■

(2)

By property (1), we can construct a *Congruence Conservation Form*. (shown as the right figure)



Suppose set A_1 as follows:

$$\boldsymbol{A_1 = \{1,\ x_1,\ x_1^2,\ \cdots,\ x_1^{n-1}\}\ (mod\ C_n')}$$

A_1 is a cyclic group and its elements are the labels used in the above *Congruence Conservation Form*. Now consider its cosets:

$$\boldsymbol{A_k = \{k, kx_1, kx_1^2, \cdots, kx_1^{n-1}\}\ (mod\ C_n')}$$
$$\boldsymbol{(k\ is\ an\ integer, k \not\equiv 1\ (mod\ C_n'))}$$

They can also construct a *Congruence Conservation Form*. Besides, we can infer that:

a. **Any two of these sets (including A_1) have no intersection**

b. **The union of these sets are: $\{1, 2, 3, \ldots, C_n' - 1\}$**

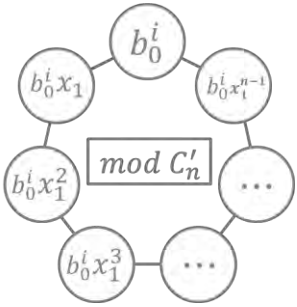
Thus, C_n' must be congruent to 1 modulo n. ■

In fact, suppose $C_n' - 1 = n \cdot k_0$ and b_0 is one of the roots of the equation:

$$x^{k_0} \equiv 1\ (mod\ C_n')$$

and satisfies that k_0 is the index of 1 to the base b_0 modulo C_n'.

Then those sets can be given by

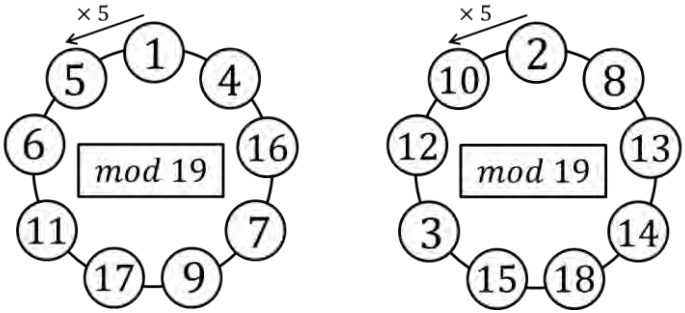


$$A_1 = \{1, x_1, x_1^2, \cdots, x_1^{n-1}\}\ (mod\ C_n')$$
$$A_2 = \{b_0, b_0 x_1, b_0 x_1^2, \cdots, b_0 x_1^{n-1}\}\ (mod\ C_n')$$
$$A_3 = \{b_0^2, b_0^2 x_1, b_0^2 x_1^2, \cdots, b_0^2 x_1^{n-1}\}\ (mod\ C_n')$$
$$\vdots$$
$$\vdots$$
$$A_{k_0} = \{b_0^{k_0-1}, b_0^{k_0-1} x_1, b_0^{k_0-1} x_1^2, \cdots, b_0^{k_0-1} x_1^{n-1}\}\ (mod\ C_n')$$

So far, we have developed the other different method to construct the *Congruence Conservation Form* by forming a cyclic group, and this method is definitely valid when n and the corresponding *Congruence Conservation Number* are both prime. For the other situations, we have observed that as long as the *Congruence Conservation Number* is congruent to 1 modulo n, then a cyclic group can also be formed.

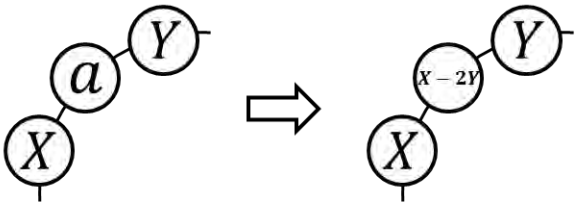
❒ *Example:*

$n = 9$



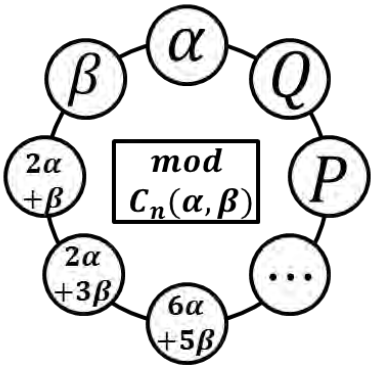
B. $X-2Y$ Operation Mode

1. Operation:



2. Finding the value of the Congruence Conservation Number:

As the method we used in the "$X-Y$ Operation Mode", we can obtain a system of congruence equations by applying the mathematical model:



$$\begin{cases} Q \equiv \alpha - 2P \ (mod\ C_n(\alpha,\ \beta)) \\ \alpha \equiv \beta - 2Q \ (mod\ C_n(\alpha,\ \beta)) \end{cases}$$

in which

$$\begin{cases} P = J_{n-3}\alpha + J_{n-2}\beta \\ Q = J_{n-2}\alpha + J_{n-1}\beta \end{cases}$$

(J_n is the Jacobsthal number)

$$\Rightarrow \begin{cases} (2\boldsymbol{J_{n-1}-1})\boldsymbol{\alpha} + \boldsymbol{J_n\beta} \equiv \boldsymbol{0}\ \left(\boldsymbol{mod\ C_n(\alpha,\ \beta)}\right) \\ (\boldsymbol{4J_{n-2}+1})\boldsymbol{\alpha} + (\boldsymbol{2J_{n-1}-1})\boldsymbol{\beta} \equiv \boldsymbol{0}\ (\boldsymbol{mod\ C_n(\alpha,\ \beta)}) \end{cases}$$

➢ **Value of D_n**

We are going to prove that

$$\boldsymbol{D_n = \begin{cases} J_n, & \boldsymbol{n\ is\ even} \\ \mathbf{1}, & \boldsymbol{n\ is\ odd} \end{cases}}$$

Proof.

By the formula

$$\begin{cases} J_n = 2J_{n-1} - 1, & n\ is\ even \\ J_n = 2J_{n-1} + 1, & n\ is\ odd \end{cases}$$

We can simply infer that

$$D_n = gcd\left(2J_{n-1} - 1,\ J_n\ ,\ 4J_{n-2} + 1\right)$$

$$= \begin{cases} gcd\left(J_n,\ J_n\ ,\ J_n\right), & n\ is\ even \\ gcd\left(J_n - 2,\ J_n\ ,\ J_n + 2\right), & n\ is\ odd \end{cases}$$

$$= \begin{cases} J_n, & n\ is\ even \\ 1, & n\ is\ odd \end{cases}$$

■

➢ **Value of C_n**

we are going to prove the following statements respectively:

(1) If n is even, then C_n has no maximal value.

(2) If n is odd, then $C_n = 2M_n$.

(M_n is the Mersenne number)

Proof.

(1)

Observing the proof of the value of D_n, we can find that when n is even, then

$$C_n(\alpha, \beta) = J_n(\alpha + \beta)$$

Since the values of α and β can be arbitrarily given, their sum can be arbitrarily large, and thus C_n has no maximal value.

(2)

When n is odd,

$$\begin{cases} (J_n - 2)\alpha + J_n\beta \equiv 0 \ (mod\ C_n(\alpha, \beta)) \\ (J_n + 2)\alpha + (J_n - 2)\beta \equiv 0 \ (mod\ C_n(\alpha, \beta)) \end{cases}$$

Suppose $C_n(\alpha, \beta)$ has the maximal value C_n when $\alpha = \alpha_0$, $\beta = \beta_0$, then

$$\begin{cases} C_n | (J_n - 2)\alpha_0 + J_n\beta_0 \\ C_n | (J_n + 2)\alpha_0 + (J_n - 2)\beta_0 \end{cases}$$

Using elimination by addition or subtraction, we can get:

$$C_n = (J_n + 2) \cdot J_n - (J_n - 2)^2$$

Simplify it,

$$\boldsymbol{C_n = 2M_n}$$

In the meantime,

$$\begin{cases} \boldsymbol{\alpha_0 = (J_n - 2) - J_n \cdot t} \\ \boldsymbol{\beta_0 = -(J_n + 2) + (J_n - 2) \cdot t} \end{cases}$$

(Here t is an integer.) ■

3. Constructing all Congruence Conservation Forms:

By using the aiding method we introduced in the "$X - Y$ Operation Mode" and the above results, we can also construct all *Congruence Conservation Forms* for a given n-gon (n is odd).

4. Investigating the properties of the Congruence Conservation Form:

In the "$X-2Y$ Operation Mode", the properties of the *Congruence Conservation Form* are the same as those in the "$X-Y$ Operation Mode" (a cyclic group structure and congruence relations between n and the *Congruence Conservation Number*). The only difference is that the generator in this operation mode is 2.

Obviously, 2 is the root of the system of equations:

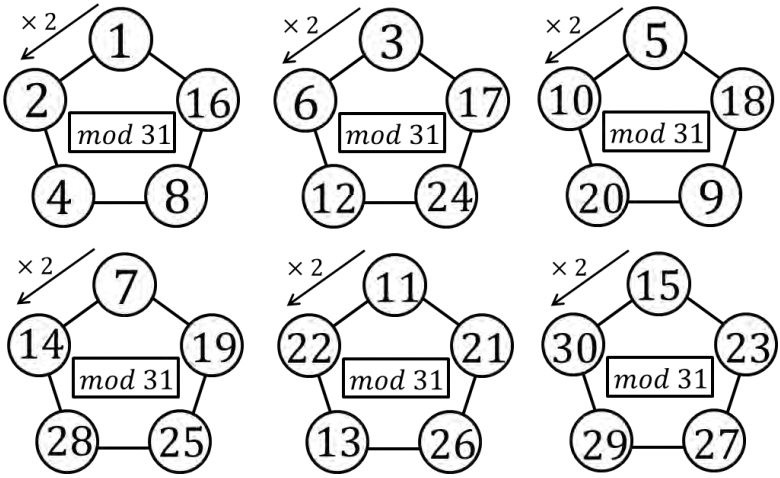
$$\begin{cases} x^2 \equiv x+2 \\ x^n \equiv 1\ (mod\ C_n') \end{cases}$$

in which C_n' is an odd prime *Congruence Conservation Number* and satisfies

$$C_n' | 2M_n$$

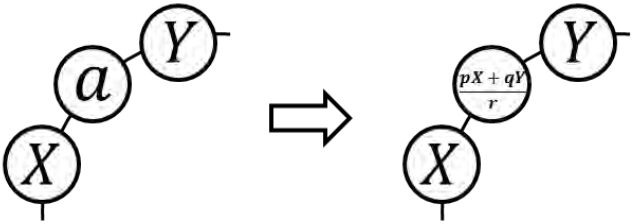
❒ *Example:*

$n=5$



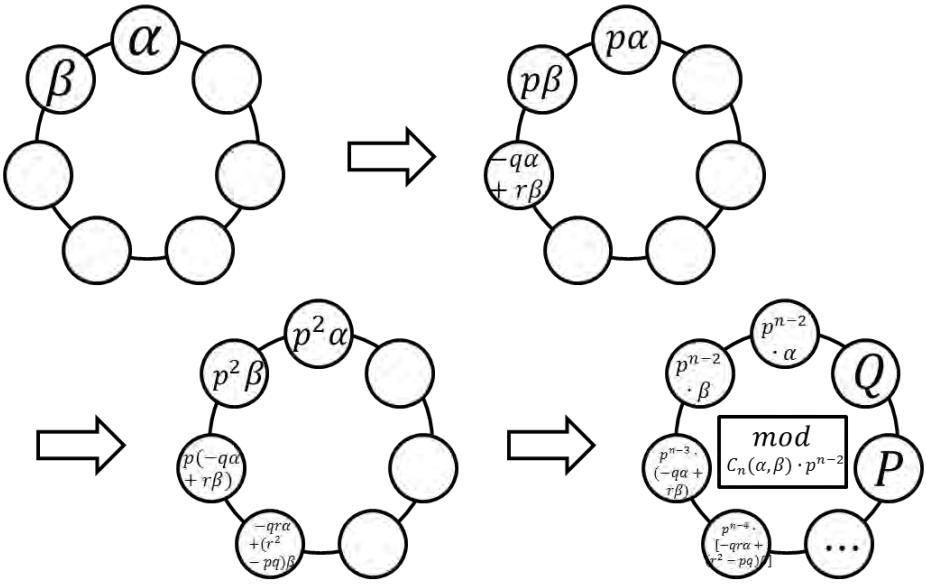
C. $\frac{1}{r}(pX + qY)$ *Operation Mode*

1. Operation: $(p, q, r \in \mathbb{Z}\ and\ gcd(p, q, r) = 1)$



2. Finding the value of the Congruence Conservation Number:

We apply the mathematical model in this operation mode to construct the *Congruence Conservation Form* step by step in **counterclockwise** direction:



and obtain a corresponding system of congruence equations:

$$\begin{cases} rQ \equiv p^{n-1}\alpha + qP \ (mod\ C_n(\alpha,\ \beta) \cdot p^{n-2}) \\ rp^{n-2}\alpha \equiv p^{n-1}\beta + qQ \ (mod\ C_n(\alpha,\ \beta) \cdot p^{n-2}) \end{cases}$$

in which

$$\begin{cases} P = p(-U_{n-3}\alpha + U_{n-2}\beta) \\ Q = -U_{n-2}\alpha + U_{n-1}\beta \end{cases}$$

and U_n satisfies the recurrence relation:

$$\begin{cases} U_0 = 0 \\ U_1 = 1 \\ U_n = rU_{n-1} - pqU_{n-2} \end{cases}$$

Simplify the system of equations, and we can get:

$$\begin{cases} \boldsymbol{(qU_{n-1} + p^{n-1})\alpha - U_n\beta \equiv 0 \ (C_n(\alpha,\ \beta) \cdot p^{n-2})} \\ \boldsymbol{(q^2U_{n-2} + rp^{n-2})\alpha - (qU_{n-1} + p^{n-1})\beta \equiv 0 \ (C_n(\alpha,\ \beta) \cdot p^{n-2})} \end{cases}$$

Then we are going to use similar method of the former operation mode to find the values of D_n and C_n. Besides, the sequence V_n in the next part is defined as follows:

$$\begin{cases} V_0 = 2 \\ V_1 = r \\ V_n = rV_{n-1} - pqV_{n-2} \end{cases}$$

➢ **Value of D_n**

$$\boldsymbol{D_n = gcd(qU_{n-1} + p^{n-1}, U_n, q^2U_{n-2} + rp^{n-2})}$$

We have found the formula for D_n under particular conditions:

(1) If $p + q - r = 0$, then $D_n = U_n$

(2) If $p + q + r = 0$, then $D_n = \begin{cases} U_n, & n \equiv 0 \ (mod\ 2) \\ 1, & n \equiv 1 \ (mod\ 2) \end{cases}$

(3) If $p + q = 0$, then

$$D_n = \begin{cases} U_{\frac{n}{2}}, & n \equiv 0 \ (mod\ 4) \\ V_{\frac{n}{2}}, & n \equiv 2 \ (mod\ 4) \\ 2, & n \equiv 3 \ (mod\ 6),\ k - r \equiv 0 \ (mod\ 2) \\ 1, & n \equiv 3 \ (mod\ 6),\ k - r \equiv 1 \ (mod\ 2) \\ 1, & n \equiv \pm 1 \ (mod\ 6) \end{cases}$$

Proof.

(1) $p + q - r = 0$, we can simply infer that

$$U_n = \frac{p^n - q^n}{p - q}$$

$$\begin{aligned} \Rightarrow D_n &= gcd(qU_{n-1} + p^{n-1},\ U_n,\ q^2U_{n-2} + rp^{n-2}) \\ &= gcd(U_n, U_n, U_n) \\ &= U_n \end{aligned}$$

(In fact, $C_n(\alpha, \beta) = U_n(\alpha - \beta)$)

(2) $p+q+r=0$, we can simply infer that

$$U_n = \frac{(-p)^n - (-q)^n}{p-q}$$

a. $n \equiv 0\ (mod\ 2)$

$D_n = U_n$ ($\rightarrow$ See $p+q-r=0$)

b. $n \equiv 1\ (mod\ 2)$

$U_n = -qU_{n-1} + p^{n-1}$

$\Rightarrow D_n = gcd(qU_{n-1} + p^{n-1},\ U_n,\ q^2U_{n-2} + rp^{n-2})$

$= gcd(qU_{n-1} + p^{n-1}, U_n)$

$= gcd(2p^{n-1},\ U_n)$

$= 1$

(we can infer $2 \nmid U_n$ and $p \nmid U_n$
from the recurrence relation of U_n)

(3) $p+q=0$

$D_n = gcd(-pU_{n-1} + p^{n-1}, U_n, p^2U_{n-2} + rp^{n-2})$

$\because p \cdot (p^2U_{n-2} + rp^{n-2}) = p \cdot U_n + r \cdot (-pU_{n-1} + p^{n-1})$

$\because p \nmid U_n$

$\Rightarrow gcd(qU_{n-1} + p^{n-1}, U_n) \mid p^2U_{n-2} + rp^{n-2}$

$\Rightarrow\ \boldsymbol{D_n = gcd(-pU_{n-1} + p^{n-1}, U_n)}$

$= gcd(-U_{n-1} + p^{n-2}, U_n)$

$= gcd(-U_{n-1} + p^{n-2}, U_{n-2} + rk^{n-4})$

$\vdots$

$= \boldsymbol{gcd(-U_{n-k} + (-1)^k \cdot U_k \cdot p^{n-2k},}$

$\boldsymbol{-U_{n-k+1} + (-1)^{k-1} \cdot U_{k-1} \cdot p^{n-2k+2})}$

$(k \in \mathbb{N},\ n \geq 2k)$

a. $n \equiv 0 \ (mod\ 4)$, let $k = 2t \ (t \in \mathbb{N})$

$D_n = gcd(2U_{2t}, U_{2t}) = U_{n/2}$

b. $n \equiv 2 \ (mod\ 4)$, let $k = 2t + 1 \ (t \in \mathbb{N})$

$D_n = gcd(0, U_{2t+2} + U_{2t} \cdot k^2) = V_{n/2}$

c. $n \equiv 6\mathrm{t} - 3 \ (mod\ 6)$, let $k = 3t - 2 \ (t \in \mathbb{N},\ t\ is\ even)$

$$\begin{aligned} D_n &= gcd(U_{3t-1} + U_{3t-2} \cdot k, U_{3t} - U_{3t-3} \cdot k^3) \\ &= gcd(U_{3t-1} + U_{3t-2} \cdot k, U_{3t} - k(U_{3t-1} - pU_{3t-2})) \\ &= gcd(U_{3t} + (k-p)U_{3t-1}, U_{3t} - (k+p)U_{3t-1}) \\ &= gcd(k-p, 2) \end{aligned}$$

If t is odd, then the result is the same.

d. $n \equiv 6\mathrm{t} - 1 \ (mod\ 6)$, let $k = 3t - 1 (t \in \mathbb{N},\ t\ is\ even)$

$$\begin{aligned} D_n &= gcd(U_{3t} - U_{3t-1} \cdot k, U_{3t+1} + U_{3t-2} \cdot k^3) \\ &= gcd(U_{3t+1} + (k-p)U_{3t}, U_{3t+1} - (k+p)U_{3t}) \\ &= 1 \end{aligned}$$

If t is odd, then the result is the same.

e. $n \equiv 6\mathrm{t} + 1 \ (mod\ 6)$, let $k = 3t (t \in \mathbb{N},\ t\ is\ even)$

$$\begin{aligned} D_n &= gcd(U_{3t+1} + U_{3t} \cdot k, U_{3t+2} - U_{3t-1} \cdot k^3) \\ &= gcd(U_{3t+2} + (k-p)U_{3t+!}, U_{3t+2} - (k+p)U_{3t+1}) \\ &= 1 \end{aligned}$$

If t is odd, then the result is the same. ■

➢ **Value of C_n**

We are going to prove the general form of C_n:

$$C_n = \frac{|V_n - (p^n + q^n)|}{D_n}$$

Proof.

From the system of equations derived from the mathematical model:

$$\begin{cases} (qU_{n-1} + p^{n-1})\alpha - U_n\beta \equiv 0 \ (C_n(\alpha, \beta) \cdot p^{n-2}) \\ (q^2U_{n-2} + rp^{n-2})\alpha - (qU_{n-1} + p^{n-1})\beta \equiv 0 \ (C_n(\alpha, \beta) \cdot p^{n-2}) \end{cases}$$

Similar to the former operation modes, suppose $C_n(\alpha, \beta)$ has the maximal value C_n when $\alpha = \alpha_0, \ \beta = \beta_0$. By using the elimination by addition or subtraction, we can obtain:

$$C_n = \frac{|U_n(q^2U_{n-2} + rp^{n-2}) - (qU_{n-1} + p^{n-1})^2|}{D_n \cdot p^{n-2}}$$

Simplify it by the formula

$$U_n = \frac{(\frac{r + \sqrt{r^2 - 4pq}}{2})^n - (\frac{r - \sqrt{r^2 - 4pq}}{2})^n}{\sqrt{r^2 - 4pq}}$$

Finally, we can get

$$\boldsymbol{C_n = \frac{|V_n - (p^n + q^n)|}{D_n}}$$

In the meantime, the determinant of this system of equations is zero, and thus we can derive the parametric form of α_0 and β_0:

$$\begin{cases} \alpha_0 = \dfrac{(qU_{n-1} + p^{n-1}) - U_n \cdot t}{D_n \cdot p^{n-2}} \\ \beta_0 = \dfrac{(q^2U_{n-2} + rp^{n-2}) - (qU_{n-1} + p^{n-1}) \cdot t}{D_n \cdot p^{n-2}} \end{cases}$$

(Here t is an integer.) ■

Notice that a series of new sequences are discovered, and they have the form as follows:

$$S_n(p, q, r) = |V_n - (p^n + q^n)|$$

We will discuss it later.

3. Constructing all Congruence Conservation Forms:

So far, for a given operation mode and an n-gon, we can construct all *Congruence Conservation Forms* by the above results and the method we used in former operation mode.

4. Investigating the properties of the Congruence Conservation Form:

Observing the *Congruence Conservation Form*, we found they have the same properties of the former operation modes in most of situations. For exceptional cases, we will discuss it in the next part.

V. Discussions

A. New Sequences

We have derived a series of new sequences of kind $S_n(p,q,r)$ from the formula for the *Congruence Conservation Number*:

$$S_n(p,\ q,\ r) = C_n \cdot D_n$$

$$= |V_n(r,\ pq) - V_n(p+q,\ pq)|$$

in which $V_n(A,\ B)$ is the Lucas sequence which satisfies the recurrence relation:

$$\begin{cases} V_0(A,\ B) = 2 \\ V_1(A,\ B) = A \\ V_n(A,\ B) = A \cdot V_{n-1}(A,\ B) - B \cdot V_{n-2}(A,\ B)\ for\ n > 1 \end{cases}$$

We observed that $S_n(p,q,r)$ having the following identities (except for some special cases such as $p+q-r=0$):

(1) $m|n \Longrightarrow S_m(p,\ q,\ r)\big|S_n(p,\ q,\ r)$

(2) $(p+q-r)|S_n(p,\ q,\ r)$

(3) Suppose n is an odd prime, and k is the prime factor of $S_n(p,\ q,\ r)$ and $k \neq p+q-r$, then $k \equiv 1\ (mod\ n)$.

(4) Suppose n is a composite number, and k is the **primitive prime factor** of $S_n(p,\ q,\ r)$ and $k \neq p+q-r$, then either $k \equiv 1\ (mod\ n)$ or $k|D_n$.

➢ **Interpretations**

The identities (1) can be easily proved by the meaning of the *Congruence Conservation Number,* and identities (2) can be proved by Fermat's little theorem.

As for the identity (3), by similar process of proof in the "$X-Y$ Operation Mode", it can be derived that if the equation

$$x^2 \equiv r^2 - 4pq \ (mod\ S_n(p,\ q,\ r))$$

has solutions, then the identity (3) holds.

The identity (4) is a conjecture, and it can be understood by the meaning of the *Congruence Conservation Form.*

B. Special Case: $p = q$

In most of situations, the identity (3) of sequences $S_n(p, q, r)$ holds. However, we found an exceptional case where $p = q$. Suppose n is an odd prime, and then the prime factor of $S_n(p, q, r)$ (denoted by C_n') may be congruent to -1 modulo n.

➢ **Interpretation:**

We observed that when n is an odd prime, then the prime factors of C_n are the same as those of D_n. Thus when the value of n and corresponding *Congruence Conservation Number* are both prime, the two initial labels α and β (in the mathematical model) can be arbitrarily chosen. Except for the situation where $\alpha = \beta = 0$, the other possible number pairs of (α, β) will just appear once (Because a pair of (α, β) can decide a *Congruence Conservation Form*, and n is a prime, therefore, it can be inferred that a pair of (α, β) won't appear twice in a *Congruence Conservation Form*). Finally, it can be proved that

$$C_n'^2 \equiv 1 \ (mod\ n)$$

$$\Rightarrow C_n' \equiv \pm 1 \ (mod\ n)$$

VI. Conclusions

1. Develop a mathematical model to construct all Congruence Conservation Forms, and derived formula for the Congruence Conservation Number under different operation modes.

2. Discover a series of new sequences which are derived from the *Congruence Conservation Number*, and their congruence properties can be explained by the *Congruence Conservation Form*.

3. When a *Congruence Conservation Form* is achieved under the condition that $\boldsymbol{n}$ and the corresponding *Congruence Conservation Number* are both prime, the remaining labels will form a cyclic group under multiplication operation.

VII. References

1. 32nd USAMO 2003: http://mks.mff.cuni.cz/kalva/usa/usoln/usol036.html
2. G.H. Hardy & E. M. Wright, An Introduction to the Theory of Numbers, sixth edition, 2008.
3. K. Thomas, Fibonacci and Lucas Numbers with Applications, 2001.

【評語】010005

本作品由數個簡單的規則探討一離散動態系統的穩定狀態，並結合數論的同餘理論得出穩定狀態時的模式與結構，是有趣的作品，未來可再補全後續的未完成觀察，使理論面可更臻完整。