中華民國第 59 屆中小學科學展覽會

作品說明書

高級中等學校組　數學科

第三名

050407

高階線性遞迴數列中的餘數數列之探討

學校名稱：臺北市立成淵高級中學

作者：	指導老師：
高二 楊承恩	林鳳美

關鍵詞：正整係數齊次線性遞迴數列、週期、餘數數列

摘要

費氏數列中每一項除以任意正整數後所得的餘數數列具有許多有趣的性質，例如：所有餘數數列均有週期性及每個週期循環列皆是由 0 均勻分割，即數列在固定間隔某幾項後可被正整數整除，由此性質就可進一步計算週期長度。

本作品中我們嘗試將費氏數列中的餘數數列性質推廣到一般高階正整係數齊次線性遞迴數列(內文簡稱高階線性遞迴數列)的情形。我們發現除了所有餘數數列均為(前)週期數列外，每個週期循環列中的均勻分割的情形變化出二種：由數個 0 均勻分割(含某項後均為 0)、數個不全為 0 均勻分割(含某項後皆為不為 0 的常數)，進一步則探討上述二種中的區分週期循環列之條件。最後由餘數數列性質探討出其數列的因倍數定理。

壹、研究動機

高二上數學專修課時，老師提到費氏數列中每一項除以任意正整數後所得的餘數數列性質，因為好奇從而開始研究。首先探討費氏數列中的餘數數列之週期性質，推廣至一般高階線性遞迴數列的情形。在過程中我們配合高中數學課程中學過「數列與級數」、「數論中的同餘性質」、「多項式函數中因倍數定理」及「矩陣」等概念來解決問題。

貳、研究目的

一、探討高階線性遞迴數列中每一項除以任意正整數後所得餘數數列，證明餘數數列均為(前)週期數列。

二、探討高階線性遞迴數列中係數在何種條件下，其餘數數列中每個週期循環列會有數個 0 均勻分割(含在某項後皆為 0)，深入探討出區分條件。

三、探討高階線性遞迴數列中係數在何種條件下，其餘數數列中每個週期循環列會有數個不全為 0 均勻分割(含在某項後皆為不為 0 的常數)，深入探討出區分條件。

四、探討利用餘數數列性質推導出高階線性遞迴數列的因倍數性質。

參、研究設備及器材

筆、紙、電腦、Geogebra5.0 動態幾何繪圖板、電腦程式 Visual Basic。

肆、研究過程或方法

一、名詞定義與預備知識

【定義 1】(k **階正整係數齊次線性遞迴數列**，張福春、莊淨惠[1] [2])

給定一數列$\left\{a_n^k\right\}$，若存在$k\,(\geq 2)$個正整數$c_1,c_2,c_3,\cdots,c_k$，其中$c_k\neq 0$，滿足兩條件：

(i) **(初始條件)** $a_1=1,a_i=0,$ 其中 $i=0,-1,-2,\cdots,-(k-2)$

(ii) **(遞迴關係)** $a_n=c_1a_{n-1}+c_2a_{n-2}+c_3a_{n-3}+\cdots+c_{k-1}a_{n-k+1}+c_ka_{n-k},\ n\geq 2$ (1)

則稱數列$\left\{a_n^k\right\}$為k **階正整係數齊次線性遞迴數列**，內文中簡稱k **階線性遞迴數列**。

【定義 2】(k **階餘數數列的週期性質**，M. S. Renault [7]、Rogers, N. [8])

(1)式中$c_1=c_2=1$為費氏數列$\left\{a_n^2\right\}$，我們知道費氏數列中每一項a_n除以任意正整數m所得到的餘數數列，會有週期性質(Fibonacci Pisano Periods)，參考資料[7]、[8]與表 1。我們稱餘數數列為**週期數列**(Period Sequence Modulo m)，其週期記作$\pi_2(m)$，表 1 中$\pi_2(2)=3$，$\pi_2(3)=8$，$\pi_2(4)=6$。由於初始條件：$a_1=1,a_0=0$，所以表 1 中的mod 3循環週期列中可用0 **均勻分割**再細分，即循環週期列為0 1 1 2 0 2 2 1 0，每一小段的長度記作$\ell_2(m)$，其中段數記作s，即$\pi_2(m)=s\cdot\ell_2(m)$。表 1 中的mod 3的週期為$\ell_2(3)=4,s=2\Rightarrow\pi_2(3)=2\cdot 4=8$。

表 1：費氏數列的週期性質

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610
mod 2	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
mod 3	0	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1
mod 4	0	1	1	2	3	1	0	1	1	2	3	1	0	1	1	2

本作品將上述週期性質推廣至一般k階線性遞迴數列$\left\{a_n^k\right\}$的情形，稱此餘數數列為k **階餘數數列**，記作$\left\{r_n^k\right\}$，我們得到k階餘數數列為週期數列或前週期數列(**前週期數列**是指數列在

某幾項後才出現循環週期列)，其週期記作 $\pi_k(m)$。特別地，推廣至一般 k 階線性遞迴數列的情形，會是**由 $k-1$ 個 0 均勻分割(含某項後均為 0)及 $k-1$ 個不全為 0 均勻分割(含某項後均為不為 0 的常數)等二種**。由於初始條件為 $k-1$ 個 0 及 $a_1=1$，能有 $k-1$ 個 0 均勻分割是很直觀的，參見表 2，但 $k-1$ 個不全為 0 均勻分割則是需要深入探討的，正是本作品深入研究的核心之一，參見表 3。

表 2：三階線性遞迴數列 $\left\{a_n^3\right\}: a_n=a_{n-1}+a_{n-2}+a_{n-3}$ 且 $m=7$ $(\pi_3(7)=3\cdot 16=48)$

第一段 $r_1,r_2,\cdots,r_{16}$	**1**	**1**	**2**	**4**	**0**	**6**	**3**	**2**	**4**	**2**	**1**	**0**	**3**	**4**	**0**	**0**
第二段 $r_{17},r_{18},\cdots,r_{32}$	**4**	**4**	**1**	**2**	**0**	**3**	**5**	**1**	**2**	**1**	**4**	**0**	**5**	**2**	**0**	**0**
第三段 $r_{33},r_{34},\cdots,r_{48}$	**2**	**2**	**4**	**1**	**0**	**5**	**6**	**4**	**1**	**4**	**2**	**0**	**6**	**1**	**0**	**0**

表 3：三階線性遞迴數列 $\left\{a_n^3\right\}: a_n=3a_{n-1}+5a_{n-2}+8a_{n-3}$ 且 $m=22$ $(\pi_3(22)=5\cdot 12=60)$

第一段 $r_1,r_2,\cdots,r_{12}$	**1**	**3**	**14**	**21**	**3**	**6**	**3**	**19**	**10**	**17**	**11**	**0**
第二段 $r_{13},r_{14},\cdots,r_{24}$	**15**	**1**	**12**	**7**	**1**	**2**	**1**	**21**	**18**	**13**	**11**	**0**
第三段 $r_{24},r_{25},\cdots,r_{36}$	**5**	**15**	**4**	**17**	**15**	**8**	**15**	**7**	**6**	**19**	**11**	**0**
第四段 $r_{37},r_{38},\cdots,r_{48}$	**9**	**5**	**16**	**13**	**5**	**10**	**5**	**17**	**2**	**21**	**11**	**0**
第五段 $r_{49},r_{50},\cdots,r_{60}$	**3**	**9**	**20**	**19**	**9**	**18**	**9**	**13**	**8**	**7**	**11**	**0**

此外，我們也關注兩個問題：

如何區分循環週期列的條件及探究出 s 的準確值或範圍。

【預備定理 1】(二階 Cassini 恆等式，Rogers, N. [8])

設 $\left\{a_n^2\right\}$ 為二階線性遞迴數列，則對於任意正整數 n，$a_{n-1}a_{n+1}-a_n^2=(-1)^n c_2^{n-1}$。

【證明】改寫成行列式形式來證明。

$$a_{n-1}a_{n+1}-a_n^2=\begin{vmatrix} a_{n+1} & a_n \\ a_n & a_{n-1}\end{vmatrix}=\begin{vmatrix} a_{n+1}-c_1a_n & a_n \\ a_n-c_1a_{n-1} & a_{n-1}\end{vmatrix}=\begin{vmatrix} c_2a_{n-1} & a_n \\ c_2a_{n-2} & a_{n-1}\end{vmatrix}=-c_2\begin{vmatrix} a_n & a_{n-1} \\ a_{n-1} & a_{n-2}\end{vmatrix}$$

由迭代過程可得 $a_{n-1}a_{n+1}-a_n^2=-c_2(a_na_{n-2}-a_{n-1}^2)$

$$=\cdots=(-1)^{n-1}c_2^{n-1}(a_2a_0-a_1^2)=(-1)^{n-1}c_2^{n-1}(-1)=(-1)^n c_2^{n-1}$$

因此，對於任意正整數 n，$a_{n-1}a_{n+1}-a_n^2=(-1)^n c_2^{n-1}$。 ■

【預備定理 2】(k **階 Cassini 恆等式**，Rogers, N. [8])

設$\left\{a_n^k\right\}$為k階線性遞迴數列，則對於任意正整數n，

$$\begin{vmatrix} a_{n+1} & a_n & a_{n-1} & \cdots & a_{n-k+2} \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ a_{n-1} & a_{n-2} & a_{n-3} & \ddots & a_{n-k} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n-k+2} & a_{n-k+1} & a_{n-k} & \cdots & a_{n-2k+3} \end{vmatrix} = \begin{cases} (-1)^{\left\lceil \frac{k}{2} \right\rceil} c_k^{n-k+1} & ,\text{其中} k \text{ 為奇數} \\ (-1)^{n-\frac{k}{2}+1} c_k^{n-k+1} & ,\text{其中} k \text{ 為偶數} \end{cases}。$$

【證明】

$$\begin{vmatrix} a_{n+1} & a_n & a_{n-1} & \cdots & a_{n-k+2} \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ a_{n-1} & a_{n-2} & a_{n-3} & \ddots & a_{n-k} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n-k+2} & a_{n-k+1} & a_{n-k} & \cdots & a_{n-2k+3} \end{vmatrix} = \begin{vmatrix} c_k a_{n-k+1} & a_n & a_{n-1} & \cdots & a_{n-k+2} \\ c_k a_{n-k} & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ c_k a_{n-k-1} & a_{n-2} & a_{n-3} & \ddots & a_{n-k} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ c_k a_{n-2k+2} & a_{n-k+1} & a_{n-k} & \cdots & a_{n-2k+3} \end{vmatrix}$$

$$= c_k \begin{vmatrix} a_{n-k+1} & a_n & a_{n-1} & \cdots & a_{n-k+2} \\ a_{n-k} & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ a_{n-k-1} & a_{n-2} & a_{n-3} & \ddots & a_{n-k} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n-2k+2} & a_{n-k+1} & a_{n-k} & \cdots & a_{n-2k+3} \end{vmatrix}$$

$$= \begin{cases} c_k \cdot \Delta_1, \text{其中} k \text{ 為奇數} \\ -c_k \cdot \Delta_1, \text{其中} k \text{ 為偶數} \end{cases}, \Delta_1 = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_{n-k} \\ a_{n-2} & a_{n-3} & a_{n-4} & \ddots & a_{n-k-1} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n-k+1} & a_{n-k} & a_{n-k-1} & \cdots & a_{n-2k+2} \end{vmatrix}$$

$$= \cdots = \begin{cases} (c_k)^{n-k+1} \cdot \Delta_k, \text{其中} k \text{ 為奇數} \\ (-c_k)^{n-k+1} \cdot \Delta_k, \text{其中} k \text{ 為偶數} \end{cases}, \Delta_k = \begin{vmatrix} a_k & a_{k-1} & \cdots & \cdots & a_1 \\ a_{k-1} & a_{k-2} & \cdots & \iddots & 0 \\ \vdots & \vdots & \iddots & \iddots & 0 \\ a_2 & a_1 & \iddots & \iddots & \vdots \\ a_1 & 0 & 0 & \cdots & 0 \end{vmatrix} = \begin{cases} (-1)^{\left\lceil \frac{k}{2} \right\rceil}, \text{其中} k \text{ 為奇數} \\ (-1)^{\frac{k}{2}}, \text{其中} k \text{ 為偶數} \end{cases}$$

$$= \begin{cases} (-1)^{\left\lceil \frac{k}{2} \right\rceil} c_k^{n-k+1} & ,\text{其中} k \text{ 為奇數} \\ (-1)^{n-\frac{k}{2}+1} c_k^{n-k+1} & ,\text{其中} k \text{ 為偶數} \end{cases}。$$

■

【預備定理 3】(鴿籠原理(The Pigeonhole Principle)，Grimaldi, Ralph P[5])

若有 n 個籠子與 $n+1$ 隻鴿子，所有鴿子都被關在鴿籠裡，則至少有一個籠子有至少 2 隻鴿子。

【預備定理 4】(同餘性質及中國剩餘定理)，Hardy, G. H. and Wright, E. M[6])

(i)設 $\alpha,\beta,\gamma \in N$ ，若 $\gamma\alpha \equiv \gamma\beta \pmod{m}$ ，則 $\alpha \equiv \beta \left(\bmod \frac{m}{d}\right)$ ，其中 $d = \gcd(\gamma, m)$ 。

特別地，若 $\gcd(\gamma, m) = 1$ ，則 $\alpha \equiv \beta \pmod{m}$ 。

(ii)設 $m = m_1 \times m_2 \times \cdots \times m_t$ ，其中 $m_1, m_2, \cdots, m_t$ 為兩兩互質，若 $b_1, b_2, \cdots, b_t \in Z$ ，則一元線性同餘方程組： $x \equiv b_i \pmod{m_i}$ ，其中 $1 \le i \le t$ ，有共同的整數解 x_0 ，且所有共同的整數解 x 也構成一個同餘式為 $x \equiv x_0 \pmod{m_i}$ 。

【預備定理 5】(歐拉-費馬定理(Euler-Fermat Theorem))，Hardy, G. H. and Wright, E. M[6])

設 x, m 為正整數且 $\gcd(x, m) = 1$ ，則

(i) $x^{\varphi(m)} \equiv 1 \pmod{m}$ ，其中 $\varphi(m)$ 表示為不大於 m 且與 m 互質之正整數個數。

(ii)反之，若正整數 s 滿足 $x^s \equiv 1 \pmod{m}$ 且 s 是最小的一個，則 $s \mid \varphi(m)$ 。

【註 1】當 m 為質數時，(i)改為 $x^{m-1} \equiv 1 \pmod{m}$ ，稱為**費馬小定理**(Fermat's little theorem)。

【註 2】若正整數 m 的標準分解式為 $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ ，其中 $p_1, p_2, \cdots, p_t$ 為相異質數，且 $\alpha_1, \alpha_2, \cdots, \alpha_t \in N$ ，則 $\varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_t})$ 。此函數稱為**歐拉函數** (Euler's totient function)。**例如**： $\varphi(1)=1, \varphi(2)=1, \varphi(3)=2, \varphi(4)=2, \varphi(5)=4, \varphi(6)=2, \varphi(7)=6, \varphi(8)=4$ 。

設 $m > 1, k, d \in N$ ，若 $x^k \equiv d \pmod{m}$ 有解，則稱 d 為模 m 的**高次剩餘**；反之，則稱 d 為模 m 的**高次非剩餘**。

【預備定理 6】(高次剩餘，Courant, R. and Robbins, H.[4])

設 $x^k \equiv d \pmod{m}$ 有解，其中 x, m 為正整數且 $\gcd(x, m) = 1$ ，若正整數 s 滿足 $x^s \equiv d \pmod{m}$ 且 s 是最小的一個，則 $s \mid \varphi(m)$ ，其中 $\varphi(m)$ 表示為不大於 m 且與 m 互質之正整數個數。

二、探討 k 階餘數數列的週期性質

費氏數列$\{a_n^2\}$具有$a_n=a_{n-1}+a_{n-2}$的特質，因此，若令r_n為a_n模m後的餘數($m\in N$)，則很自然地，我們得到$(r_{n-1}+r_{n-2})\equiv r_n \pmod m$的性質。進一步地，這種線性關係也能推廣至$k$階線性遞迴數列，參見**性質 1**。

【性質 1】設$\{a_n^k\}$為k階線性遞迴數列，若r_n為a_n模m後的餘數($m\in N$)，則

$$(c_1r_{n-1}+c_2r_{n-2}+\cdots+c_kr_{n-k})\equiv r_n \pmod m \text{ 。}$$

【證明】設$a_n=qm+r_n, a_{n-1}=q_1m+r_{n-1}, a_{n-2}=q_2m+r_{n-2},\cdots,a_{n-k}=q_km+r_{n-k}$，其中

$q,q_1,q_2,\cdots,q_k\in N\cup\{0\}$，因為$a_n=c_1a_{n-1}+c_2a_{n-2}+c_3a_{n-3}+\cdots+c_{k-1}a_{n-k+1}+c_ka_{n-k}$，所以

$$\begin{aligned}c_1r_{n-1}+c_2r_{n-2}+\cdots+c_kr_{n-k}&=c_1(a_{n-1}-q_1m)+c_2(a_{n-2}-q_2m)+\cdots+c_k(a_{n-k}-q_km)\\&=(c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k})-m(c_1q_1+c_2q_2+\cdots+c_kq_{n-k})\\&=a_n-m(c_1q_1+c_2q_2+\cdots+c_kq_{n-k})=r_n+m(q-c_1q_1-c_2q_2-\cdots-c_kq_{n-k})\end{aligned}$$

因此，$(c_1r_{n-1}+c_2r_{n-2}+\cdots+c_kr_{n-k})\equiv r_n \pmod m$。 ■

【定理 1】設$\{a_n^k\}$為k階線性遞迴數列，若r_n為a_n模m後的餘數($m\in N$)，則(i)當$\gcd(c_k,m)=1$時，k階餘數數列為週期數列。(ii)當$\gcd(c_k,m)\neq 1$時，k階餘數數列為週期數列或前週期數列。

【證明】因為r_n為a_n模m後的餘數($m\in N$)，則$r_n\in\{0,1,2,\cdots,m-1\}$。

令$(r_i,r_{i+1},\cdots,r_{i+k-1})$為$k$階餘數數列中相鄰$k$個項的數對，其中

$r_i,r_{i+1},\cdots,r_{i+k-1}\in\{0,1,2,\cdots,m-1\}$，則數對$(r_i,r_{i+1},\cdots,r_{i+k-1})$至多可組出$m^k$種的變化。

再由**預備定理 3：鴿籠原理**知當k階餘數數列出現在m^k+k項後時，必存在

$m^k<j\le m^k+k$使得$r_i=r_j$，又由於是k階餘數數列，故數對

$$(r_i,r_{i+1},\cdots,r_{i+k-1})=(r_j,r_{j+1},\cdots,r_{j+k-1}) \text{ 。}$$

又**性質 1**知$(c_1r_{n-1}+c_2r_{n-2}+\cdots+c_kr_{n-k})\equiv r_n \pmod m$，得到$r_i,r_{i+1},\cdots,r_{i+k-1},\cdots$與

$r_j,r_{j+1},\cdots,r_{j+k-1},\cdots$完全相同，即$k$階餘數數列從第$i$項後開始出現週期循環列。

接著證明從第1項後開始出現週期循環列的條件。用矩陣來描述 k 階線性遞迴數列為

存在 k 階矩陣 $P=\begin{bmatrix} c_1 & c_2 & \cdots & \cdots & c_k \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$ 且 $X_{n-1}=\begin{bmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_{n-k} \end{bmatrix}$ 滿足 $PX_{n-1}=X_n$ 。

由於 k 階餘數數列從第 i 項後開始出現週期循環列且初始條件為

$a_1=1, a_i=0,$ 其中 $i=0,-1,-2,\cdots,-(k-2)$ ，則

(i)當 $\gcd(c_k,m)=1$ 時，$\det(P)=\begin{cases} c_k & ,\text{其中}k\text{為奇數} \\ -c_k & ,\text{其中}k\text{為偶數} \end{cases} \not\equiv 0 \pmod m$ ，推得矩陣 P 為可逆矩陣，

即存在 $\ell \in N$ ，使得 $P^{\ell}\begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix}^T=\begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix}^T$ ，此時數列從第1項後開始出現週期循環列。因此，當 $\gcd(c_k,m)=1$ 時， k 階餘數數列為週期數列。

(ii)當 $\gcd(c_k,m)\neq 1$ 時， $\det(P)\equiv 0 \pmod m$ 或 $\det(P)\not\equiv 0 \pmod m$ ，所以有些數列從第1項後開始出現週期循環列，也有從某幾項後才開始出現週期循環列，所以 k 階餘數數列可能會為週期數列或前週期數列。 ■

三、由 $k-1$ 個0均勻分割來區分循環週期列

(一) $\gcd(c_2,m)=1$

若考慮從第1項後開始出現由 $k-1$ 個0均勻分割的週期循環列，由於初始條件為 $k-1$ 個0及 $a_1=1$ ，則由**定理 1** 知滿足條件為 $\gcd(c_k,m)=1$ ，證明參見**性質 2**。

【性質 2】設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k,m)=1$ ，則每個週期循環列中會是由 $k-1$ 個0均勻分割。

【證明】由**定理 1** 可令 k 階餘數數列 $\{r_n^k\}$ $(i=1,2,\cdots,m^k+k)$ 中重複的相鄰 k 項為

$$r_i=r_j, r_{i+1}=r_{j+1}, r_{i+2}=r_{j+2}, \cdots, r_{i+k-1}=r_{j+k-1}$$ 。

注意 $a_k = c_1 a_{k-1} + c_2 a_{k-2} + \cdots + c_k a_0$ ，故 $r_k = (c_1 r_{k-1} + c_2 r_{k-2} + \cdots + c_k r_0) \pmod m$ 。

又 $(c_1 r_{j-i+k-1} + c_2 r_{j-i+k-2} + \cdots + c_k r_{j-i}) \equiv r_{j-i+k} \pmod m$ ，故

$$c_k r_{j-i} \equiv r_{j-i+k} - c_1 r_{j-i+k-1} - \cdots - c_{k-1} r_{j-i+1} \equiv r_k - c_1 r_{k-1} - c_2 r_{k-2} \cdots - c_{k-1} r_0 \equiv 0 \pmod m \qquad (2)$$

當 $c_k = 1$ 時， (2)式為 $r_{j-i} \equiv 0 \pmod m$ 。事實上，當 $\gcd(c_k, m) = 1$ 時，(2)式同樣地可得到 $r_{j-i} \equiv 0 \pmod m$ 。又 $\{r_n^k\}$ 為 k 階週期數列且循環必由 0 均勻分割，所以 0 的出現的模式為是 $k-1$ 個，因此，每個週期循環列中會是由 $k-1$ 個 0 均勻分割。 ■

接著探討段數 s 的準確值或範圍，先來觀察二階線性遞迴數列 $\{a_n^2\} : a_n = 2a_{n-1} + a_{n-2}$ 且 $m = 5$ 為例子：既然循環週期列中可用 0 來均勻分割，且分成四段，表示 0 前面兩項值 r_i, r_{i+1} 必滿足 $5 \mid (r_i + 2r_{i+1})$ ，其中 $r_i, r_{i+1} \in \{0,1,2,3,4\}$ ，簡單來說，作整數分割即得到數對 (r_i, r_{i+1}) 可能為 $(1,2),(2,4),(3,1),(4,3)$ ，在滿足 $r_0 = 0, r_1 = 1$ 下，循環週期列就僅有一種，參見表 4。那麼在**每段循環週期列是否都如上述作完全整數分割呢？事實上，是不然的。**

表 4：二階線性遞迴數列的例子

n	1	2	3	4	5	6	7	8	9	10	11	12
r_n	**1**	**2**	**0**	**2**	**4**	**0**	**4**	**3**	**0**	**3**	**1**	**0**
段	**第一段**			**第二段**			**第三段**			**第四段**		

【性質 3】設 $\{r_n^2\}$ 為二階線性遞迴數列 $\{a_n^2\}$ 中的餘數數列且 $\gcd(c_2, m) = 1$ ，若 s 為週期循環列中由 0 均勻分割的段數且 r_i 為在 $\{r_n^2\}$ 中第 i 次由 0 均勻分割的 0 之前一項 $(1 \le i \le s-1)$ ，則(i)當 $c_2 = 1$ 時， $r_{i+j} \equiv [\![r_j r_{i-1}]\!] \pmod m$ ，其中 $[\![r_j r_{i-1}]\!]$ 為 $r_j r_{i-1}$ 模 m 後的餘數且 $j \in N$ 。(ii)當 $c_2 \ne 1$ 時， $r_{i+j} \equiv [\![c_2 r_j r_{i-1}]\!] \pmod m$ ，其中 $[\![c_2 r_j r_{i-1}]\!]$ 為 $c_2 r_j r_{i-1}$ 模 m 後的餘數且 $j \in N$ 。

【證明】注意到當 $\gcd(c_2, m) = 1$ 時，有分 $c_2 = 1$ 或 $c_2 \ne 1$ 的情形：

(i)令 $c_2 = 1$ 且 r_i 為在 $\{r_n^2\}$ 中 r_i 為在 $\{r_n^2\}$ 中第 i 次由 0 均勻分割的 0 之前一項 $(1 \le i \le s-1)$ 且

$a_{i-1}=mq_1+r_{i-1}, a_i=mq_2$ $(q_1,q_2\in N\cup\{0\})$ ，則給定一個正整數 j ，

$$
\begin{aligned}
&a_{i+1}=c_1mq_2+(mq_1+r_{i-1})=a_2\cdot mq_2+a_1\cdot(mq_1+r_{i-1})\\
&a_{i+2}=c_1[c_1mq_2+(mq_1+r_{i-1})]+mq_2=c_1(mq_1+r_{i-1})+(1+c_1^2)mq_2=a_2\cdot(mq_1+r_{i-1})+a_3\cdot mq_2\\
&a_{i+3}=(1+c_1^2)(mq_1+r_{i-1})+(c_1^3+2c_1)mq_2=a_3\cdot(mq_1+r_{i-1})+a_4\cdot mq_2 \qquad (3)\\
&\quad\vdots\\
&a_{i+j}=a_j\cdot(mq_1+r_{i-1})+a_{j+1}\cdot mq_2,\quad j\in N
\end{aligned}
$$

兩邊模 m 得到 $r_{i+j}\equiv\llbracket r_jr_{i-1}\rrbracket\pmod m$ ，其中 $j\in N$ ，以 $\{a_n^2\}:a_n=2a_{n-1}+a_{n-2}$ 且模13為例：

第1段	r_j	$r_1=1$	$r_2=2$	$r_3=5$	$r_4=12$	$r_5=3$	$r_6=5$	$r_7=0$
		↓	↓	↓	↓	↓	↓	↓
第2段	$\llbracket r_jr_6\rrbracket$ mod 13	5	10	$\llbracket 25\rrbracket=12$	8	2	12	0
第3段	$\llbracket r_jr_6^2\rrbracket$ mod 13	$\llbracket 25\rrbracket=12$	11	8	1	10	8	0

故 $r_{i+j}\equiv\llbracket r_jr_{i-1}\rrbracket\pmod m$ ，其中 $\llbracket r_jr_{i-1}\rrbracket$ 為 r_jr_{i-1} 模 m 後的餘數且 $1\le i\le s-1, j\in N$ 。

(ii)仿照(i)來證明，(3)式改為 $a_{i+j}=c_2a_j\cdot(mq_1+r_{i-1})+a_{j+1}\cdot mq_2,\quad j\in N$ 。 (4)

兩邊模 m 得到 $r_{i+j}\equiv\llbracket c_2r_jr_{i-1}\rrbracket\pmod m$ ，其中 $j\in N$ 且，其中 $\llbracket c_2r_jr_{i-1}\rrbracket$ 為 $c_2r_jr_{i-1}$ 模 m 後的餘數且 $1\le i\le s-1, j\in N$ ，故 $r_{i+j}\equiv\llbracket c_2r_jr_{i-1}\rrbracket\pmod m$ ，其中 $\llbracket c_2r_jr_{i-1}\rrbracket$ 為 $c_2r_jr_{i-1}$ 模 m 後的餘數且 $1\le i\le s-1, j\in N$ 。以 $\{a_n^2\}:a_n=a_{n-1}+2a_{n-2}$ 且模11為例：

第1段	r_i	$r_1=1$	$r_2=1$	$r_3=3$	$r_4=5$	$r_5=0$
	$c_2r_jr_4$	10	10	30	50	0
第2段	$\llbracket c_2r_jr_4\rrbracket$ mod 11	10	10	8	6	0

■

【定理 2】設 $\{r_n^2\}$ 為二階線性遞迴數列 $\{a_n^2\}$ 中的餘數數列且 $\gcd(c_2,m)=1$ ，若 s 為週期循環列中由0均勻分割的段數，$r_{\alpha+1}$ 為週期循環列中第1段由0均勻分割的0之位置，其中 $\ell_2(m)-1=\alpha$ ，則(i)當 $c_2\ne1$ 時，$\llbracket r_\alpha^2\rrbracket\equiv\llbracket c_2^{\alpha-1}\rrbracket\pmod m$ 或 $\llbracket r_\alpha^4\rrbracket\equiv\llbracket c_2^{2\alpha-2}\rrbracket\pmod m$ ，其中 $\llbracket r_\alpha^2\rrbracket$ 與 $\llbracket r_\alpha^4\rrbracket$ 分別為 r_α^2 與 r_α^4 模 m 後的餘數。(ii)當 $c_2=1$ 時，$\llbracket r_\alpha^2\rrbracket\equiv1\pmod m$ 或 $\llbracket r_\alpha^4\rrbracket\equiv1\pmod m$ 。

【**證明**】(i)令 $\ell_2(m)-1=\alpha$ ，則由**性質 2** 及**定義 2** 知每個週期循環列中由 0 均勻分割的

第一段為 $1, r_2=\{c_1\}, r_3, r_4, r_5, \cdots, r_\alpha, 0$ 。

第二段為 $[\![c_2 r_1 r_\alpha]\!], [\![c_2 r_2 r_\alpha]\!], [\![c_2 r_3 r_\alpha]\!], \cdots, [\![c_2 r_\alpha^2]\!], 0$ 。

第三段為 $[\![c_2^2 r_\alpha^2]\!], [\![c_2^2 r_2 r_\alpha^2]\!], [\![c_2^2 r_3 r_\alpha^2]\!], \cdots, [\![c_2^2 r_\alpha^3]\!], 0$ 。

以此類推得由 0 分割的第 s 段為 $[\![c_2^{s-1} r_\alpha^{s-1}]\!], [\![c_2^{s-1} r_2 r_\alpha^{s-1}]\!], [\![c_2^{s-1} r_3 r_\alpha^{s-1}]\!], \cdots, [\![c_2^{s-1} r_\alpha^s]\!], 0$ 。

由上得到 $r_{\alpha+1}=0,\quad r_{s(\alpha+1)-1}=[\![c_2^{s-1} r_\alpha^s]\!], r_{s(\alpha+1)+1}=[\![c_2^s r_\alpha^s]\!]$ 。

又由**預備定理 1：二階 Cassini 恆等式**知 $a_{\alpha-1}a_{\alpha+1}-a_\alpha^2=(-1)^\alpha c_2^{\alpha-1}$ ，兩邊模 m 得到

$$r_{\alpha-1}r_{\alpha+1}-r_\alpha^2\equiv(-1)^\alpha c_2^{\alpha-1}\ (\text{mod } m)\Rightarrow r_{\alpha-1}\cdot 0-r_\alpha^2\equiv(-1)^\alpha c_2^{\alpha-1}\ (\text{mod } m)\Rightarrow [\![r_\alpha^2]\!]\equiv\pm[\![c_2^{\alpha-1}]\!]\ (\text{mod } m)$$

即 $[\![r_\alpha^2]\!]\equiv[\![c_2^{\alpha-1}]\!]\ (\text{mod } m)$ 或 $[\![r_\alpha^4]\!]\equiv[\![c_2^{2\alpha-2}]\!]\ (\text{mod } m)$ 。 (5)

(ii)仿照(i)來證明，(5)式改為 $[\![r_\alpha^2]\!]\equiv\pm1\ (\text{mod } m)$ ，因此，

$$[\![r_\alpha^2]\!]\equiv1\ (\text{mod } m)\ \text{或}\ [\![r_\alpha^4]\!]\equiv1\ (\text{mod } m) \tag{6}$$

■

【**定理 3**】設 $\{r_n^2\}$ 為二階線性遞迴數列 $\{a_n^2\}$ 中的餘數數列，若 $\gcd(c_2,m)=1, c_2\neq1$ 且 s 為週期循環列中由 0 均勻分割的段數，則 $\pi_2(m)=s\cdot\ell_2(m)$ ，其中 $s\mid\varphi(m)$ 。

【**證明**】(i)由**定理 2** 中知每個週期循環列中由 0 均勻分割的每段以 0 分割位置的前一項依序分別為 $r_\alpha, c_2 r_\alpha^2, c_2^2 r_\alpha^3, \cdots, c_2^{s-1} r_\alpha^s$ 。

因為 $\gcd(r_2,m)=1$ 且 $\gcd(c_2,m)=1$ ，由**預備定理 3**：**鴿籠原理**與**預備定理 6：高次剩餘**知(5)式必有解且循環，以 $\{a_n^2\}: a_n=3a_{n-1}+2a_{n-2}$ 為例參見表 5。

由表 5 知循環段數即是 s ，由於要滿足循環長度 $r_\alpha\to c_2 r_\alpha^2\to c_2^2 r_\alpha^3\to\cdots\to c_2^{s-1} r_\alpha^s$ 又回到 r_α ，由**預備定理 6：高次剩餘**知 $s\mid\varphi(m)$ ，因此， $\pi_2(m)=s\cdot\ell_2(m)$ ，其中 $s\mid\varphi(m)$ 。

表 5：二階線性遞迴數列$\left\{a_n^2\right\}:a_n=3a_{n-1}+2a_{n-2}$為例

m \ t	$t=1$	$r_\alpha \to c_2 r_\alpha^2 \to c_2^2 r_\alpha^3 \to \cdots \to c_2^{s-1} r_\alpha^s$	s
5($\alpha=5$)	$4^2 \equiv 2^4 \pmod 5$	$4 \to 2 \to 1 \to 3$	4
9($\alpha=5$)	$4^2 \equiv 2^4 \pmod 9$	$4 \to 5$	2
13($\alpha=3$)	$11^2 \equiv 2^2 \pmod{13}$	$11 \to 8 \to 7$	3

例如 1：表 5 中$m=9(s=2)$，$s\mid\varphi(9)\Rightarrow s\mid 9\left(1-\frac{1}{3}\right)\Rightarrow s\mid 6$。

例如 2：表 5 中$m=13(s=3)$，$s\mid(m-1)\Rightarrow s\mid 12$。 ■

【定理 4】設$\left\{r_n^2\right\}$為二階線性遞迴數列$\left\{a_n^2\right\}$中的餘數數列且$\gcd(c_2,m)=1,c_2=1$，若s為週期循環列中由0均勻分割的段數，$r_{\alpha+1}$為週期循環列中第1段由0均勻分割的0之位置，其中$\ell_2(m)-1=\alpha$，則(i)$\pi_2(m)=s\cdot\ell_2(m)$，其中$s=1,2,4$。(ii)當$r_\alpha=1$時，$s=1$；當$r_\alpha=m-1$時，$s=2$；其餘的r_α滿足$r_\alpha^2\equiv -1\pmod m$的值時，$s=4$。

【證明】(i)由**定理 3**知$\left[\!\left[r_\alpha^2\right]\!\right]\equiv 1\pmod m$或$\left[\!\left[r_\alpha^4\right]\!\right]\equiv 1\pmod m$ (6)

又$\left[\!\left[r_\alpha^s\right]\!\right]\equiv 1\pmod m$且$\gcd(r_\alpha,m)=1$，則由**預備定理 5：歐拉-費馬定理**知$s\mid 2$或$s\mid 4$。

因此，$s=1,2,4$。

(ii)因為$r_\alpha=0,1,\cdots,m-1$，顯然$r_\alpha=0$不滿足(6)式，且$r_\alpha=1$必滿足(6)式，即$s=1$。

(a) 當$r_\alpha=m-1$時，$(m-1)^2\equiv 1\pmod m$滿足(6)式，所以$s=2$。

(b) 當$r_\alpha=i\ \ (i=2,\cdots,m-2)$時，$i^2\equiv -1\pmod m$滿足(6)式，所以$s=4$。

因此，$s=\begin{cases}1, & \text{其中 } r_\alpha=1\\ 2, & \text{其中 } r_\alpha=m-1\\ 4, & \text{其餘 } r_\alpha \text{ 要滿足 } r_\alpha^2\equiv -1\pmod m\end{cases}$。以$m=10$為例，$r_\alpha$滿足$\gcd(r_\alpha,m)=1$的值為$1,3,5,7,9$。(a)當$r_\alpha=1$時，必滿足(6)式，即$s=1$。

(b)當$r_\alpha=9$時，滿足(6)式，所以$s=2$。以$\left\{a_n^2\right\}:a_n=3a_{n-1}+a_{n-2}$為例：1 3 0 3 **9 0** 9 7 0 7 1 **0**。

(c)除了 $r_\alpha = 1,9$ 外， r_α 滿足 $r_\alpha^2 \equiv -1 \pmod m$ ，僅有 $r_\alpha = 3$ 或 7 ，滿足(6)式，所以 $s = 4$ 。

以 $\left\{a_n^2\right\} : a_n = a_{n-1} + a_{n-2}$ 且 $r_\alpha = 7$ 為例：

1 1 2 3 5 8 3 1 4 5 9 4 3 **7** **0** 7 7 4 1 5 6 1 7 8 5 3 8 1 9 **0**

9 9 8 7 5 2 7 9 6 5 1 6 7 3 **0** 3 3 6 9 5 4 9 3 2 5 7 2 9 1 **0**

(d)剩下 $r_\alpha = 5$ 時，不滿足(6)式。綜合上述情形，故 $s = 1,2,4$ 。

因此， $\pi_2(m) = s \cdot \ell_2(m)$ ，其中 $s = 1,2,4$ 。 ■

(二) $\gcd(c_k, m) = 1$

接著，將**定理 3~4** 中每個週期循環列性質推廣至 $\gcd(c_k, m) = 1$ 的情形。

【性質 4】 設 $\left\{r_n^k\right\}$ 為 k 階線性遞迴數列 $\left\{a_n^k\right\}$ 中的餘數數列且 $\gcd(c_k, m) = 1$ ，若 s 為週期循環列中由 $k-1$ 個 0 均勻分割的段數且 r_i 為在 $\left\{r_n^k\right\}$ 中第 i 次由 $k-1$ 個 0 均勻分割的第一個出現 0 之前一項 $(1 \le i \le s-1)$ ，則(i)當 $c_k = 1$ 時， $r_{i+j+k-2} \equiv \left[\!\left[r_j r_{i-1} \right]\!\right] \pmod m$ ，其中 $\left[\!\left[r_j r_{i-1} \right]\!\right]$ 為 $r_j r_{i-1}$ 模 m 後的餘數且 $j \in N$ 。(ii)當 $c_k \ne 1$ 時， $r_{i+j+k-2} \equiv \left[\!\left[c_k r_j r_{i-1} \right]\!\right] \pmod m$ ，其中 $\left[\!\left[c_k r_j r_{i-1} \right]\!\right]$ 為 $c_k r_j r_{i-1}$ 模 m 後的餘數且 $j \in N$ 。

【證明】 由**性質 2** 知每個週期循環列中會由 $k-1$ 個 0 均勻分割。(i)仿照**性質 3** 來證明，若 r_i 為

在 $\left\{r_n^k\right\}$ 中第 i 次由 $k-1$ 個 0 均勻分割的第一個出現 0 之前一項 $(1 \le i \le s-1)$

將(3)式改為

$$a_{i+j+k-2} = a_{j+1} \cdot mq_k + \sum_{\ell_1=2}^{k-1} \left[\sum_{\ell_2=2}^{\ell_1} a_{j-\ell_1+\ell_2} \cdot mq_{k+1-\ell_2} \right] + \sum_{\ell=1}^{k-2} a_{j-\ell} \cdot mq_{\ell+1} + a_j (mq_1 + r_{i-1}), \quad j \in N, q_1, \cdots, q_k \in N$$

，兩邊模 m 得到

$r_{i+j+k-2} \equiv \left[\!\left[r_j r_{i-1} \right]\!\right] \pmod m$ ，其中 $\left[\!\left[r_j r_{i-1} \right]\!\right]$ 為 $r_j r_{i-1}$ 模 m 後的餘數且 $1 \le i \le s-1, j \in N$ 。

以 $\left\{a_n^3\right\} : a_n = 2a_{n-1} + a_{n-2} + a_{n-3}$ 模 7 為例：

第1段	r_j	1	2	5	6	5	0	4	6	2	0	1	4	2	2	3	3	4	0	0
	$r_j r_{17}$	4	8	20	24	20	0	16	24	8	0	4	16	8	8	12	12	16	0	0
第2段	$\left[\!\left[r_j r_{17} \right]\!\right]_{\bmod 7}$	4	1	6	3	6	0	2	3	1	0	4	2	1	1	5	5	2	0	0

(ii)仿照**性質 3**來證明，(4)式改為

$$a_{i+j+k-2} = c_k a_j \cdot (mq_1 + r_{i-1}) + a_{j+1} \cdot mq_2, \quad j \in N$$

$$a_{i+j+k-2} = a_{j+1} \cdot mq_k + \sum_{\ell_1=2}^{k-1} \left[\sum_{\ell_2=2}^{\ell_1} c_{\ell_1} a_{j-\ell_1+\ell_2} \cdot mq_{k+1-\ell_2} \right] \quad 。$$

$$+ c_k \sum_{\ell=1}^{k-2} a_{j-\ell} \cdot mq_{\ell+1} + c_k a_j (mq_1 + r_{i-1}), \quad j \in N, q_1, \cdots, q_k \in N$$

兩邊模m得到$r_{i+j+k-2} \equiv \left[\!\left[c_k r_j r_{i-1} \right]\!\right] (\bmod m)$，其中$j \in N$且$\left[\!\left[c_k r_j r_{i-1} \right]\!\right]$為$c_k r_j r_{i-1}$模$m$後的餘數且$j \in N$。以$\left\{a_n^3\right\}: a_n = a_{n-1} + 2a_{n-2} + 2a_{n-3}$且$m=5$為例：

第1段	r_i	1	1	3	2	0	0
	$c_3 r_j r_4$	4	4	12	8	0	0
第2段	$\left[\!\left[c_3 r_j r_4 \right]\!\right]_{\bmod 5}$	4	4	2	3	0	0

■

【定理 5】設$\left\{r_n^k\right\}$為k階線性遞迴數列$\left\{a_n^k\right\}$中的餘數數列且$\gcd(c_k, m) = 1$，若s為週期循環列中由$k-1$個0均勻分割的段數，$r_{\alpha+1}, r_{\alpha+2} \cdots, r_{\alpha+k-1}$為週期循環列中第1段由$k-1$個0均勻分割的0之位置，其中$\ell_k(m) - k + 1 = \alpha$，則(i)當$c_k \neq 1$時，$\left[\!\left[r_\alpha^k \right]\!\right] \equiv \begin{cases} c_k^{\alpha-1} & ,\text{其中} k \text{為奇數} \\ \pm c_k^{\alpha-1} & ,\text{其中} k \text{為偶數} \end{cases} (\bmod m)$，其中$\left[\!\left[r_\alpha^k \right]\!\right]$為$r_\alpha^k$模$m$後的餘數。(ii)當$c_k = 1$時，$\left[\!\left[r_\alpha^k \right]\!\right] \equiv \begin{cases} 1 & ,\text{其中} k \text{為奇數} \\ \pm 1 & ,\text{其中} k \text{為偶數} \end{cases} (\bmod m)$。

【證明】(i)仿照**定理 2**證明。令$\ell_k(m) - k + 1 = \alpha$，則由**性質 2**及**定義 2**知每個週期循環列中由$k-1$個0分割的第一段為$1, r_2, r_3, r_4, r_5, \cdots, r_\alpha, \underbrace{0, 0, \cdots, 0}_{k-1\text{個}}$。

第二段為$\left[\!\left[c_k r_1 r_\alpha \right]\!\right], \left[\!\left[c_k r_2 r_\alpha \right]\!\right], \cdots, \left[\!\left[c_k r_\alpha^2 \right]\!\right], \underbrace{0, 0, \cdots, 0}_{k-1\text{個}}$。

第三段為$\left[\!\left[c_k^2 r_\alpha^2 \right]\!\right], \left[\!\left[c_k^2 r_2 r_\alpha^2 \right]\!\right], \cdots, \left[\!\left[c_k^2 r_\alpha^3 \right]\!\right], \underbrace{0, 0, \cdots, 0}_{k-1\text{個}}$。

以此類推得第s段為$\left[\!\left[c_k^{s-1} r_\alpha^{s-1} \right]\!\right], \left[\!\left[c_k^{s-1} r_2 r_\alpha^{s-1} \right]\!\right], \left[\!\left[c_k^{s-1} r_3 r_\alpha^{s-1} \right]\!\right], \cdots, \left[\!\left[c_k^{s-1} r_\alpha^s \right]\!\right], \underbrace{0, 0, \cdots, 0}_{k-1\text{個}}$。

由上可知 $r_\alpha = [\![r_\alpha]\!], r_{\alpha+1} = \cdots = r_{\alpha+k-1} = 0$。由**預備定理 2：$k$ 階 Cassini 恆等式**知

$$\begin{vmatrix} a_{\alpha+k-1} & a_{\alpha+k-2} & a_{\alpha+k-3} & \cdots & a_\alpha \\ a_{\alpha+k-2} & a_{\alpha+k-3} & a_{\alpha+k-4} & \cdots & a_{\alpha-1} \\ a_{\alpha+k-3} & a_{\alpha+k-4} & a_{\alpha+k-5} & \ddots & a_{\alpha-2} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_\alpha & a_{\alpha-1} & a_{\alpha-2} & \cdots & a_{\alpha-k+1} \end{vmatrix} = \begin{cases} (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} c_k^{\alpha-1} & ,\text{其中} k \text{ 為奇數} \\ (-1)^{\alpha+k+\frac{k}{2}-1} c_k^{\alpha-1} & ,\text{其中} k \text{ 為偶數} \end{cases}$$

兩邊模 m 得到 $\begin{vmatrix} 0 & 0 & 0 & \cdots & r_\alpha \\ 0 & 0 & 0 & \cdots & r_{\alpha-1} \\ \vdots & \vdots & \iddots & \ddots & r_{\alpha-2} \\ 0 & 0 & \cdots & \ddots & \vdots \\ r_\alpha & r_{\alpha-1} & r_{\alpha-2} & \cdots & r_{\alpha-k+1} \end{vmatrix} \equiv \begin{cases} (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} c_k^{\alpha-1} & ,\text{其中} k \text{ 為奇數} \\ (-1)^{\alpha+k+\frac{k}{2}-1} c_k^{\alpha-1} & ,\text{其中} k \text{ 為偶數} \end{cases} \pmod m$

$$\Rightarrow (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} [\![r_\alpha^k]\!] \equiv \begin{cases} (-1)^{\left\lfloor \frac{k}{2} \right\rfloor} c_k^{\alpha-1} & ,\text{其中} k \text{ 為奇數} \\ (-1)^{\alpha+k+\frac{k}{2}-1} c_k^{\alpha-1} & ,\text{其中} k \text{ 為偶數} \end{cases} \pmod m \text{，因此，}$$

$$[\![r_\alpha^k]\!] \equiv \begin{cases} c_k^{\alpha-1} & ,\text{其中} k \text{ 為奇數} \\ \pm c_k^{\alpha-1} & ,\text{其中} k \text{ 為偶數} \end{cases} \pmod m \tag{7}$$

(ii)因為 $c_k = 1$，所以(7)式改為 $[\![r_\alpha^k]\!] \equiv \begin{cases} 1 & ,\text{其中} k \text{ 為奇數} \\ \pm 1 & ,\text{其中} k \text{ 為偶數} \end{cases} \pmod m$。 (8)

■

【定理 6】設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列且 $\gcd(c_k, m) = 1, c_k \neq 1$，若 s 為週期循環列中由 $k-1$ 個 0 均勻分割的段數，則 $\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \mid \varphi(m)$。

【證明】(i)仿照**定理 3** 證明。由**定理 5** 知每個週期循環列中由 $k-1$ 個 0 的每段以 0 分割位置的前一項依序分別為 $r_\alpha, c_k r_\alpha^2, c_k^2 r_\alpha^3, \cdots, c_k^{s-1} r_\alpha^s$。因為 $\gcd(r_\alpha, m) = 1$ 且 $\gcd(c_k, m) = 1$，由**預備定理 3-鴿籠原理**與**預備定理 6：高次剩餘**知(7)式必有解且循環，又循環段數即是 s，由於要滿足循環長度 $r_\alpha \to c_2 r_\alpha^2 \to c_2^2 r_\alpha^3 \to \cdots \to c_2^{s-1} r_\alpha^s$，回到 r_α，由**預備定理 6：高次剩餘**知 $s \mid \varphi(m)$，因此，$\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \mid \varphi(m)$。 ■

【定理 7】設$\left\{r_n^k\right\}$為k階線性遞迴數列$\left\{a_n^k\right\}$中的餘數數列且$\gcd(c_k,m)=1,c_k=1$，若s為週期循環列中由$k-1$個0均勻分割的段數且$r_{\alpha+1},r_{\alpha+2}\cdots,r_{\alpha+k-1)}$為週期循環列中第1段由$k-1$個0均勻分割的0之位置，其中$\ell_k(m)-k+1=\alpha$，則(i)當$k$為奇數時，$\pi_k(m)=s\cdot\ell_k(m)$，其中$s\mid k$。

(ii)當k為偶數時，$\pi_k(m)=s\cdot\ell_k(m)$，其中$s\mid 2k$。

【證明】(i) 當k為奇數時，則(8)式為$\left[\!\left[r_\alpha^k\right]\!\right]\equiv 1\pmod m$，其中$\gcd(r_\alpha,m)=1$。

顯然$r_\alpha=0$不滿足$\left[\!\left[r_\alpha^k\right]\!\right]\equiv 1\pmod m$，$r_\alpha$可能的值為$1,\cdots,m-1$。

由**預備定理 5：歐拉-費馬定理**且$\left[\!\left[r_\alpha^s\right]\!\right]\equiv 1\pmod m$得到$s\mid k$。

例如：若$k=9,s\mid 9$，則$s=1,3,9$。

(ii)若k為偶數，則(8)式為$\left[\!\left[r_\alpha^k\right]\!\right]\equiv \pm 1\pmod m$，即$\left[\!\left[r_\alpha^k\right]\!\right]\equiv 1\pmod m$或$\left[\!\left[r_\alpha^{2k}\right]\!\right]\equiv 1\pmod m$。

由**預備定理 5：歐拉-費馬定理**知$\gcd(r_\alpha,m)=1$。

顯然$r_\alpha=0$不滿足$\left[\!\left[r_\alpha^k\right]\!\right]\equiv 1\pmod m$或$\left[\!\left[r_\alpha^{2k}\right]\!\right]\equiv 1\pmod m$，$r_\alpha$可能的值為$1,\cdots,m-1$。

由**預備定理 5：歐拉-費馬定理**且$\left[\!\left[r_\alpha^s\right]\!\right]\equiv 1\pmod m$得到$s\mid k$或$s\mid 2k$。

因此，若k為偶數，$\pi_k(m)=s\cdot\ell_k(m)$，其中$s\mid 2k$。

以$k=6$為例，$s\mid 2k\Rightarrow s\mid 12$，所以$s=1,2,3,4,6,12$。又$r_\alpha=0,1,2,\cdots,m-1$。

當$r_\alpha=0$不滿足(8)式，且$r_\alpha=1$必滿足(8)式，即$s=1$。

當$r_\alpha=m-1$時，$(m-1)^2\equiv 1\pmod m$滿足(8)式，所以$s=2$。

當$r_\alpha=i\ \ (i=2,\cdots,m-2)$時，$i^2\equiv -1\pmod m$滿足(8)式，所以$s=4$。

當$r_\alpha=i\ \ (i=2,\cdots,m-2)$時，$i^3\equiv -1\pmod m$滿足(8)式，所以$s=6$。

當$r_\alpha=i\ \ (i=2,\cdots,m-2)$時，$i^6\equiv -1\pmod m$滿足(8)式，所以$s=12$。

因此，若$k=6$為偶數，$\pi_k(m)=s\cdot\ell_k(m)$，其中$s=1,2,3,4,6,12$。 ■

(三) $\gcd(c_k,m)\neq 1$

除了 $\gcd(c_k,m)=1$ 是每個週期循環列是由 $k-1$ 個 0 均勻分割的情形，係數在哪些條件下也是由 $k-1$ 個 0 均勻分割的情形呢？參見**定理 8**。

【定理 8】設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k,m)\neq 1$ 且 $\gcd(c_1,c_2,\cdots,c_k,m)=d, c_k^{'}=c_k/d, m'=m/d$ ，則(i)當 $\gcd(c_k^{'},m')=1$ 時， k 階餘數數列是前週期數列且每個週期循環列中會是由 $k-1$ 個 0 均勻分割。(ii)當 $\gcd(c_k^{'},m')\neq 1$ 時，每個週期循環列中會有由 $k-1$ 個 0 均勻分割。

【證明】(i) 由**定理 1** 知當 $\gcd(c_k,m)\neq 1$ 時， k 階餘數數列可能會為週期數列或前週期數列。

得到若 $\gcd(c_1,c_2,\cdots,c_k,m)=d\neq 1, c_k^{'}=c_k/d, m'=m/d$ ，若 $\gcd(c_k^{'},m')=1$ ，則 k 階餘數數列為前週期數列。以 $\{a_n^2\}:a_n=2a_{n-1}+6a_{n-2}$ 且 $m=10$ 為例，此餘數數列為前週期數列。

考慮 $c_2^{'}=6/2=3, m'=10/2=5$ 但 $\gcd(c_k^{'},m')=\gcd(3,5)=1$ 且 $m'=5$

對應新數列 $\{a_n^2\}:a_n=1a_{n-1}+3a_{n-2}$ 且 $m'=5$ ：

$$\{a_n^2\}:a_n=2a_{n-1}+6a_{n-2}:\boxed{1,2,0},2,4,0,4,8,0,8,6,0,6,2,0$$
$$\{a_n^2\}:a_n=1a_{n-1}+3a_{n-2}:1,1,4,2,4,0,2,2,3,4,3,0,4,4,1,3,1,0,3,3,2,1,2,0$$

由上述兩個餘數數列共同性質為保持由 0 均勻分割且 $s=4$ 是相同的。

以 $\{a_n^2\}:a_n=2a_{n-1}+6a_{n-2}$ 且 $m=8$ 為例，此餘數數列為前週期數列。

考慮 $c_2^{'}=6/2=3, m'=8/2=4$ 但 $\gcd(c_k^{'},m')=\gcd(3,4)=1$ 且 $m'=4$

對應新數列 $\{a_n^2\}:a_n=1a_{n-1}+3a_{n-2}$ 且 $m'=4$ ：

$$\{a_n^2\}:a_n=2a_{n-1}+6a_{n-2}:\boxed{1,2,2,0,4},0,0,0,\cdots$$
$$\{a_n^2\}:a_n=1a_{n-1}+3a_{n-2}:1,1,0,3,3,0$$

由上述兩個餘數數列共同性質為保持由 0 均勻分割，特別是 $m=8$ 時，由 0 均勻分割的退化情形-在某項後皆為 0。現在證明為何是由 0 均勻分割呢？

當 $\gcd(c_k,m)\neq 1$時，(2)式化簡為 $r_{j-i}\equiv 0 \left(\bmod \frac{m}{c_k}\right)$，又 $\gcd(c_1,c_2,\cdots,c_k,m)=d \Rightarrow d\mid c_k$，

由**預備定理 4** 知得到 $r_{j-i}\equiv 0 \left(\bmod \frac{m}{d}\right)$，令 $c_k^{'}=c_k/d, m'=m/d$ 且 $\gcd(c_k^{'},m')=1$，則由**性質 2** 知每個週期循環列中會是由 $k-1$ 個 0 均勻分割。

(ii)當 $\gcd(c_k^{'},m')\neq 1$時，k 階餘數數列也是前週期數列，同時每個週期循環列中會有由 $k-1$ 個 0 均勻分割。以 $\left\{a_n^2\right\}: a_n=2a_{n-1}+4a_{n-2}$ 且 $m=24$ 為例，此餘數數列為前週期數列。

考慮 $c_2^{'}=4/2=2, m'=24/2=12$ 但 $\gcd(c_k^{'},m')=\gcd(2,12)=2\neq 1$ 且 $m'=12$

對應新數列 $\left\{a_n^2\right\}: a_n=1a_{n-1}+2a_{n-2}$ 且 $m'=12$ ：

$$\left\{a_n^2\right\}: a_n=2a_{n-1}+4a_{n-2}: \boxed{1,2,8,0},8,16,16,0,16,8,8,0$$
$$\left\{a_n^2\right\}: a_n=1a_{n-1}+2a_{n-2}: \boxed{1,2,8,0},8,4,4,0,4,8,8,0$$

上述兩個餘數數列共同性質為保持由 0 均勻分割且 $s=2$ 是相同的，皆是前週期數列。■

(四)退化情形：在某項後皆為 0

在 $\gcd(c_k,m)=1$ 條件下，每個週期循環列中僅有由 $k-1$ 個 0 均勻分割，事實上，k 階餘數數列在某項後均為 0 可說是由 $k-1$ 個 0 均勻分割的**退化情形**。而區分 k 階餘數數列每個週期循環列中僅有由 $k-1$ 個 0 均勻分割的條件共有 **2** 種：

$$\gcd(c_k,m)=1 \text{ 、 } \gcd(c_k,m)\neq 1, \gcd(c_1,c_2,\cdots,c_k,m)\neq 1 \text{ 。}$$

k 階餘數數列在某項後均為 0 理當區分條件是 **2** 種，但考慮初始條件中 $a_1=1$，所以在某項後均為 0 的 k 階餘數數列必為前週期數列，故 $\gcd(c_k,m)=1$ 的情形不會發生，因此，區分條件僅有 **1** 種： $\gcd(c_k,m)\neq 1, \gcd(c_1,c_2,\cdots,c_k,m)\neq 1$ 。證明參見**定理 9**。

【定理 9】 設 $\left\{r_n^k\right\}$ 為 k 階線性遞迴數列 $\left\{a_n^k\right\}$ 中的餘數數列，若 $\gcd(c_k,m)\neq 1$ 且 $\gcd(c_1,c_2,\cdots,c_k)=\ell, m=\ell^t\ (t\in N)$，則 k 階餘數數列 $\left\{r_n^k\right\}$ 在某項後均為 **0**。

【證明】 令 $c_1=\ell q_1, c_2=\ell q_2,\cdots,c_k=\ell q_k$，其中 $\gcd(c_1,c_2,\cdots,c_k)=\ell,\ q_1,\cdots,q_k\in N, \gcd(q_1,\cdots,q_k)=1,$ ，

則 $a_n=\ell(c_1'a_{n-1}+c_2'a_{n-2}+\cdots+c_k'a_{n-k})$，其中 $c_1'=c_1/\ell, c_2'=c_2/\ell,\cdots,c_k'=c_k/\ell$ 。

$$a_{n+k}=\ell^2(c_1'a_{n+k-1}+c_2'a_{n+k-2}+\cdots+c_k'a_n)$$

$$\vdots$$

$$a_{n+(t-1)k}=\ell^t(c_1'a_{n+(t-1)k-1}+c_2'a_{n+(t-1)k-2}+\cdots+c_k'a_{n+(t-2)k})$$

推知存在 $t\in N$，使得 $a_{n+(t-1)k}\equiv 0 \pmod{m=\ell^t}$，因此，$k$ 階餘數數列 $\{r_n^k\}$ 在某項後均為 **0**。

(a) $\gcd(c_k', m')=1$：以三階線性遞迴數列 $\{a_n^3\}: a_n=2a_{n-1}+4a_{n-2}+2a_{n-3}$ 且 $m=8$ 為例：

1,2,0,2,0,0,4,0,0,$\cdots$,0,0 ， k 階餘數數列在第 8 項後均為 0。

(b) $\gcd(c_k', m')\neq 1$：以二階線性遞迴數列 $\{a_n^2\}: a_n=4a_{n-1}+8a_{n-2}$ 且 $m=16$ 為例：

1,4,8,0,0,$\cdots$,0,0，k 階餘數數列在第 4 項後均為 0。 ■

四、由 $k-1$ 個不全為 0 均勻分割來區分循環週期列

(一)由 $k-1$ 個 0 均勻分割與由 k 個不全為 0 均勻分割的關連性

我們已探討每個週期循環列中會有由 $k-1$ 個 0 均勻分割，事實上，也會有由 $k-1$ 個不全為 0 均勻分割。觀察三階線性遞迴數列 $\{a_n^3\}: a_n=3a_{n-1}+5a_{n-2}+8a_{n-3}$ 且 $m=22$ 的 3 階餘數數列為

1,3,14,21,3,6,3,19,10,17,11,0, 15,1,12,7,1,2,1,21,18,13,11,0,
5,15,4,17,15,8,15,7,6,19,11 0, 9,5,16,13,5,10,5,17,2,21,11,0, 3,9,20,19,9,18,9,13,8,7,11,0

可見 3 階餘數數列是由 2 個不全為 0 均勻分割， 2 個不全為 0 為 11,0 。

表 6：三階線性遞迴數列 $\{a_n^3\}: a_n=3a_{n-1}+5a_{n-2}+8a_{n-3}$ 為例

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}
$m=2$	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**1**	**0**
$m=11$	**1**	**3**	**3**	**10**	**3**	**6**	**3**	**8**	**10**	**6**	**0**	**0**
$m=22$	**1**	**3**	**14**	**21**	**3**	**6**	**3**	**19**	**10**	**17**	**11**	**0**

由於 $m=2\times 11$ ，所以考慮 $m=2$ 及 $m=11$ 的第 1 段的週期循環列，參見表 6。因為 $\gcd(c_2, m)=1$，則當 $m=2$ 及 $m=11$ 時，每個週期循環列中會是由 $k-1$ 個 0 均勻分割。

考慮 r_{11} 與 r_{12} 的**線性同餘方程組**為 $\begin{cases} r_{11} \equiv 0 \pmod 2 \\ r_{11} \equiv 0 \pmod{11} \end{cases}$ 且 $\begin{cases} r_{12} \equiv 1 \pmod 2 \\ r_{12} \equiv 0 \pmod{11} \end{cases}$，

則由**預備定理 4：中國剩餘定理**知

$$r_{11} \equiv 0 \pmod{22}\ (\textbf{餘數必為零}) \text{及} r_{12} \equiv 11 \pmod{22}\ (\textbf{餘數必不為零})$$

可見 $m=2$ 是三階中退化情形，是由 2 個不全為 0 均勻分割。

同樣地，定義由 $k-1$ 個不全為 0 均勻分割的週期記作 $\pi_k(m)$，其循環週期列中可由 $k-1$ 個不全為 0 均勻分割再細分，每一小段的長度記作 $\ell_k(m)$，其中段數記作 s，即 $\pi_k(m)=s\cdot\ell_k(m)$。

表 6 中 $s=5, \ell_3(22)=12 \Rightarrow \pi_3(22)=5\cdot 12=60$。

更一般的情形，只要 $m=p_1\times p_2\times\cdots\times p_{k-1}$，其中 $p_1, p_2, \cdots, p_{k-1}$ 為相異質數，且模 $p_1, p_2, \cdots, p_{k-1}$ 後的餘數數列的週期循環列中是由 $k-1$ 個 0 均勻分割均勻分割所形成的。則由**預備定理 4：中國剩餘定理**知 k 階餘數數列中的週期循環列中會有由 $k-1$ 個不全為 0 均勻分割。

(二) $\gcd(c_k, m)\neq 1, \gcd(c_1, c_2, \cdots, c_k, m)=1$

由**定理 1** 知當 $\gcd(c_k, m)\neq 1$ 時，k 階餘數數列可能會為週期數列或前週期數列。當 $\gcd(c_k, m)\neq 1, \gcd(c_1, c_2, \cdots, c_k, m)=1$ 時，k 階餘數數列會是週期數列或前週期數列。

(a)以 $\left\{a_n^2\right\}: a_n=4a_{n-1}+3a_{n-2}$ 且 $m=21$ 為例：1,4,19,4,10,10,7,16,1,10,1,13,13,7,4,16,13,16,19,19,7

此餘數數列為週期數列，是由 7 均勻分割。

(b)以 $\left\{a_n^2\right\}: a_n=4a_{n-1}+3a_{n-2}$ 且 $m=18$ 為例：1,4,1,16,13,10,7,4,1,16,13,10,7，此餘數數列為前週期數列，每個週期循環列中在第八項後是由 7 均勻分割。

【性質 5】 設 $\left\{r_n^k\right\}$ 為 k 階線性遞迴數列 $\left\{a_n^k\right\}$ 中的餘數數列，若 $\gcd(c_k, m)\neq 1$，則

(i)當 $\gcd(c_1, c_2, \cdots, c_k, m)=1$ 時，每個週期循環列中會是由 $k-1$ 個不全為 0 均勻分割。

(ii)當 $\gcd(c_1, c_2, \cdots, c_k, m)=d, c_k^{'}=c_k/d, m'=m/d$ 且 $\gcd(c_k^{'}, m')\neq 1$ 時，每個週期循環列中會有由 $k-1$ 個不全為 0 均勻分割。

【**證明**】考慮在(r_1, r_{m^k+k})中重複的相鄰k項為$r_i = r_j, r_{i+1} = r_{j+1}, r_{i+2} = r_{j+2}, \cdots, r_{i+k-1} = r_{j+k-1}$。

仿照**性質 2**類推知

$$c_k r_{j-i} \equiv r_{j-i+k} - c_1 r_{j-i+k-1} - \cdots - c_{k-1} r_{j-i+1} \equiv r_k - c_1 r_{k-1} - c_2 r_{k-2} - \cdots - c_{k-1} r_1 \equiv 0 \pmod{m} \qquad (2)$$

(i)若$\gcd(c_1, c_2, \cdots, c_k, m) = 1$但$\gcd(c_k, m) \neq 1$，可令$\gcd(c_k, m) = d$，由**預備定理 4**知(2)式為

$r_{j-i} \equiv 0 \left(\bmod \frac{m}{c_k} \right)$，所以$r_{j-i}$可為非負整數，但$\left\{ r_n^k \right\}$為$k$階週期數列，故每個週期循環列是$k-1$個不全為0的出現模式，因此，每個週期循環列中是由$k-1$個不全為0均勻分割。

(ii)當$\gcd(c_k', m') \neq 1$時，k階餘數數列必為前週期數列，同時每個週期循環列中會有由$k-1$個不全為0均勻分割。以$\left\{ a_n^2 \right\} : a_n = 8a_{n-1} + 12a_{n-2}$且$m = 18$為例，此餘數數列為前週期數列。

考慮$c_2' = 12/2 = 6, m' = 18/2 = 9$但$\gcd(c_k', m') = \gcd(6,9) = 3 \neq 1$且$m' = 9$

對應新數列$\left\{ a_n^2 \right\} : a_n = 4a_{n-1} + 6a_{n-2}$且$m' = 9$：

$$\left\{ a_n^2 \right\} : a_n = 8a_{n-1} + 12a_{n-2} : \boxed{1,8,4,2,14,16},8,4,2,10,14,16$$
$$\left\{ a_n^2 \right\} : a_n = 4a_{n-1} + 6a_{n-2} : \boxed{1},4,4,4,\cdots,4$$

上述兩個餘數數列共同性質為保持由1個不全為0均勻分割，皆是前週期數列。 ■

【**性質 6**】設$\left\{ r_n^2 \right\}$為二階線性遞迴數列$\left\{ a_n^2 \right\}$中的餘數數列，若$\gcd(c_2, m) \neq 1$且s為週期循環列中由 1 個不全為0(記作x_1)均勻分割的段數，及r_i為在$\left\{ r_n^2 \right\}$中第i次由x_1均勻分割的x_1之前一項$(1 \leq i \leq s-1)$，則$r_{i+j} \equiv \left[\!\left[r_{j+1} x_1 + c_2 r_j r_{i-1} \right]\!\right] \pmod{m}$，其中$\left[\!\left[r_{j+1} x_1 + c_2 r_j r_{i-1} \right]\!\right]$為$r_{j+1} x_1 + c_2 r_j r_{i-1}$模$m$後的餘數且$j \in N$。

【**證明**】令r_i為在$\left\{ r_n^2 \right\}$中第i次由x_1均勻分割之位置$(1 \leq i \leq s-1)$且

$a_{i-1} = mq_1 + r_{i-1}, a_i = mq_2 + x_1 \ (q_1, q_2 \in N \cup \{0\})$，則

$$a_{i+1} = c_1(mq_2 + x_1) + c_2(mq_1 + r_{i-1}) = a_2 \cdot (mq_2 + x_1) + c_2 a_1 \cdot (mq_1 + r_{i-1})$$
$$a_{i+2} = a_3 \cdot (mq_2 + x_1) + c_2 a_2 \cdot (mq_1 + r_{i-1})$$

$$a_{i+3}=a_4\cdot(mq_2+x_1)+c_2a_3\cdot(mq_1+r_{i-1})$$
$$\vdots$$
$$a_{i+j}=a_{j+1}\cdot(mq_2+x_1)+c_2a_j\cdot(mq_1+r_{i-1}),\quad j\in N$$

兩邊模 m 得到 $r_{i+j}\equiv\left[\!\left[r_{j+1}x_1+c_2r_jr_{i-1}\right]\!\right]\pmod m$，其中 $j\in N$，故 $r_{i+j}\equiv\left[\!\left[r_{j+1}x_1+c_2r_jr_{i-1}\right]\!\right]\pmod m$，

其中 $\left[\!\left[r_{j+1}x_1+c_2r_jr_{i-1}\right]\!\right]$ 為 $r_{j+1}x_1+c_2r_jr_{i-1}$ 模 m 後的餘數且 $j\in N$。 ■

【定理 10】設 $\left\{r_n^2\right\}$ 為二階線性遞迴數列 $\left\{a_n^2\right\}$ 中的餘數數列，若 $\gcd(c_2,m)\neq1,\gcd(c_1,c_2,m)=1$ 且 s 為週期循環列中由 x_1 均勻分割的段數，則 $L_2(m)=s\cdot\ell_2(m)$，其中 $s\mid\varphi(m)$。

【證明】仿照**定理 4** 與**定理 5** 來證明。令 $\ell_2(m)-1=\alpha$，則由**性質 2** 及**定義 2** 知每個週期循環列中由 x_1 均勻分割的第一段為 $r_1,r_2,r_3,r_4,r_5,\cdots,r_\alpha,x_1$。

第二段為 $\left[\!\left[r_2x_1+c_2r_1r_\alpha\right]\!\right],\left[\!\left[r_3x_1+c_2r_2r_\alpha\right]\!\right],\cdots,\left[\!\left[x_1^2+c_2r_\alpha^2\right]\!\right],x_1$。

第三段為 $\left[\!\left[r_2x_1+c_2r_1x_1^2+c_2^2r_1r_\alpha^2\right]\!\right],\left[\!\left[r_3x_1+c_2r_2x_1^2+c_2^2r_2r_\alpha^2\right]\!\right],\cdots,\left[\!\left[x_1^2+c_2r_\alpha x_1^2+c_2^2r_\alpha^3\right]\!\right],x_1$。

以此類推得第 s 段為 $\left[\!\left[r_2x_1+r_1x_1^2\sum_{i=1}^{s-2}c_2^ir_\alpha^{i-1}+c_2^{s-1}r_1r_\alpha^{s-1}\right]\!\right],\cdots,\left[\!\left[x_1^2+x_1^2\sum_{i=1}^{s-2}c_2^ir_\alpha^i+c_2^{s-1}r_\alpha^s\right]\!\right],x_1$。

令 $\ell_2(m)-1=\alpha$，則由**預備定理 1：二階 Cassini 恆等式**知 $a_{\alpha-1}a_{\alpha+1}-a_\alpha^2=(-1)^\alpha c_2^{\alpha-1}$。

兩邊模 m 得 $x_1r_{\alpha-1}-r_\alpha^2\equiv(-1)^\alpha c_2^{\alpha-1}\pmod m$。 (9)

(9)式可透過配方法可化為同餘式的最簡表示式為

$$(r_\alpha')^2\equiv(-1)^\alpha c_2^{\alpha-1}\pmod m\Rightarrow\left[\!\left[(r_\alpha')^2\right]\!\right]\equiv\pm\left[\!\left[c_2^{\alpha-1}\right]\!\right]\pmod m。$$

即 $\left[\!\left[(r_\alpha')^2\right]\!\right]\equiv\left[\!\left[c_2^{\alpha-1}\right]\!\right]\pmod m$ 或 $\left[\!\left[(r_\alpha')^2\right]\!\right]\equiv-\left[\!\left[c_2^{2\alpha-2}\right]\!\right]\pmod m$。 (10)

仿照**定理 6** 來證明，由**預備定理 3**：**鴿籠原理**與**預備定理 6**：**高次剩餘**知(10)式必有解且循環。以二階線性遞迴數列 $\left\{a_n^2\right\}:a_n=3a_{n-1}+2a_{n-2}$ 且 $m=10$ 為例：

1 3 1 9 9 **5** 3 9 3 7 7 **5** 9 7 9 1 1 **5** 7 1 7 3 3 **5**

其中 $x_1=5, r_\alpha=r_{\alpha-1}=9$ 滿足(10)式： $5\cdot 9-9^2\equiv(-1)^5 2^4 \pmod{10}\Rightarrow 36\equiv 16\pmod{10}$ 。

因為循環段數即是 s ，要滿足循環長度 $r_\alpha\to\left[\!\left[x_1^2+c_2r_\alpha^2\right]\!\right]\to\cdots\to\left[\!\left[x_1^2+x_1^2\sum_{i=1}^{s-2}c_2^i r_\alpha^i+c_2^{s-1}r_\alpha^s\right]\!\right]$

又回到 r_α ，由**預備定理 5：歐拉-費馬定理**知 $s\mid\varphi(m)$ ，因此，由表 1 知循環段數即是 s ，

因此，由**預備定理 5：歐拉-費馬定理**知 $\pi_2(m)=s\cdot\ell_2(m)$ 。 ■

【定理 11】設 $\left\{r_n^k\right\}$ 為 k 階線性遞迴數列 $\left\{a_n^k\right\}$ 中的餘數數列，若 $\gcd(c_k,m)\neq 1$ 且 s 為週期循環列中由 $k-1$ 個不全為 0 均勻分割的段數且 r_i 為在 $\left\{r_n^k\right\}$ 中第 i 次由 $k-1$ 個不全為 0 (記作 $x_1,\cdots,x_{k-1}$) 均勻分割的出現 x_1 之前一項 $(1\le i\le s-1)$ ，則

(i)當 $k=3$ 時， $r_{i+j+1}\equiv\left[\!\left[r_{j+1}x_2+c_2r_jx_1+c_3(r_{j-1}x_1+r_jr_{i-1})\right]\!\right]\pmod m$ ，其中

$\left[\!\left[r_{j+1}x_2+c_2r_jx_1+c_3(r_{j-1}x_1+r_jr_{i-1})\right]\!\right]$ 為 $r_{j+1}x_2+c_2r_jx_1+c_3(r_{j-1}x_1+r_jr_{i-1})$ 模 m 後的餘數且 $j\in N$ 。

(ii) $r_{i+j+k-2}\equiv\left[\!\left[r_{j+1}x_{k-1}+\sum_{\ell_1=2}^{k-1}\left[c_{\ell_1}\sum_{\ell_2=2}^{\ell_1}r_{j-\ell_1+\ell_2}x_{k-\ell_2}\right]+c_k\sum_{\ell=1}^{k-2}r_{j-\ell}x_\ell+c_kr_jr_{i-1}\right]\!\right]\pmod m$ ，其中

$\left[\!\left[r_{j+1}x_{k-1}+\sum_{\ell_1=2}^{k-1}\left[c_{\ell_1}\sum_{\ell_2=2}^{\ell_1}r_{j-\ell_1+\ell_2}x_{k-\ell_2}\right]+c_k\sum_{\ell=1}^{k-2}r_{j-\ell}x_\ell+c_kr_jr_{i-1}\right]\!\right]$ 為

$r_{j+1}x_{k-1}+\sum_{\ell_1=2}^{k-1}\left[c_{\ell_1}\sum_{\ell_2=2}^{\ell_1}r_{j-\ell_1+\ell_2}x_{k-\ell_2}\right]+c_k\sum_{\ell=1}^{k-2}r_{j-\ell}x_\ell+c_kr_jr_{i-1}$ 模 m 後的餘數且 $j\in N$ 。

(iii) $\pi_2(m)=s\cdot\ell_2(m)$ ，其中 $s\mid\varphi(m)$ 。

【證明】(i)令 r_i,r_{i+1} 為在 $\left\{r_n^3\right\}$ 中第 i 次由 x_1,x_2 均勻分割的 2 個不全為 0 之位置 $(1\le i\le s-1)$ 且

$a_{i-1}=mq_1+r_{i-1}, a_i=mq_2+x_1, a_{i+1}=mq_3+x_2$ $(q_1,q_2,q_3\in N\cup\{0\})$ ，則

$$
\begin{aligned}
a_{i+2}&=a_2(mq_3+x_2)+a_1[c_2(mq_2+x_1)+c_3(mq_1+r_{i-1})]\\
a_{i+3}&=a_3(mq_3+x_2)+a_2[c_2(mq_2+x_1)+c_3(mq_1+r_{i-1})]+a_1[c_3(mq_2+x_1)]\\
a_{i+4}&=a_4(mq_3+x_2)+a_3[c_2(mq_2+x_1)+c_3(mq_1+r_{i-1})]+a_2[c_3(mq_2+x_1)]\\
&\vdots\\
a_{i+j+1}&=a_{j+1}(mq_3+x_2)+a_j[c_2\cdot(mq_2+x_1)+c_3\cdot(mq_1+r_{i-1})]+a_{j-1}[c_3(mq_2+x_1)],\quad j\in N
\end{aligned}
$$

兩邊模 m 得到 $r_{i+j+1} \equiv \left[\!\left[r_{j+1}x_2 + c_2 r_j x_1 + c_3(r_{j-1}x_1 + r_j r_{i-1}) \right]\!\right] \pmod m$ ，其中

$\left[\!\left[r_{j+1}x_2 + c_2 r_j x_1 + c_3(r_{j-1}x_1 + r_j r_{i-1}) \right]\!\right]$ 為 $r_{j+1}x_2 + c_2 r_j x_1 + c_3(r_{j-1}x_1 + r_j r_{i-1})$ 模 m 後的餘數且 $j \in N$ 。

(ii)仿照(i)推得對於 $1 \le i \le s-1, j \in N$ ，當 $k=4$ 時，

$$r_{i+j+2} \equiv \left[\!\left[r_{j+1}x_3 + c_2 r_j x_2 + c_3(r_j x_1 + r_{j-1}x_2) + c_4(r_{j-1}x_1 + r_{j-2}r_2) + c_4 r_j r_{i-1} \right]\!\right] \pmod m ,$$

其中 $\left[\!\left[r_{j+1}x_3 + c_2 r_j x_2 + c_3(r_j x_1 + r_{j-1}x_2) + c_4(r_{j-1}x_1 + r_{j-2}r_2) + c_4 r_j r_{i-1} \right]\!\right]$ 為

$r_{j+1}x_3 + c_2 r_j x_2 + c_3(r_j x_1 + r_{j-1}x_2) + c_4(r_{j-1}x_1 + r_{j-2}r_2) + c_4 r_j r_{i-1}$ 模 m 後的餘數。

為了方便寫成 $r_{i+j+4-2} \equiv \left[\!\left[r_{j+1}x_3 + \sum_{\ell_1=2}^{3}\left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} r_{j-\ell_1+\ell_2} x_{4-\ell_2} \right] + c_k \sum_{\ell=1}^{2} r_{j-\ell}x_\ell + c_4 r_j r_{i-1} \right]\!\right] \pmod m$

同理類推至 k 階餘數數列的情形，推得

$$r_{i+j+k-2} \equiv \left[\!\left[r_{j+1}x_{k-1} + \sum_{\ell_1=2}^{k-1}\left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} r_{j-\ell_1+\ell_2} x_{k-\ell_2} \right] + c_k \sum_{\ell=1}^{k-2} r_{j-\ell}x_\ell + c_k r_j r_{i-1} \right]\!\right] \pmod m \text{ 。}$$

(ii)仿照**定理 5** 證明，滿足如(7)式的式子可透過配方可化為同餘式的最簡表示式為

$$\left[\!\left[(r_\alpha^{'})^k \right]\!\right] \equiv \begin{cases} c_k^{\alpha-1} & \text{,其中} k \text{ 為奇數} \\ \pm c_k^{\alpha-1} & \text{,其中} k \text{ 為偶數} \end{cases} \pmod m$$

因此，(ii)當 m 為質數時， $\pi_k(m) = s \cdot \ell_k(m)$ ，其中 $s \mid m-1$ 。

(iii)當 m 為合數時， $\pi_k(m) = s \cdot \ell_k(m)$ ，其中 $s \mid \varphi(m)$ 且 $\varphi(m)$ 表示為不大於 m 且與 m 互質之正整數個數。 ■

(三)退化情形：在某項後皆為不為 0 的常數

在 $\gcd(c_k, m) \ne 1$ 條件下，每個週期循環列中才會有由 $k-1$ 個不全為 0 均勻分割，事實上，k 階餘數數列在某項後均為不為 0 的常數可說是由 $k-1$ 個不全為 0 均勻分割的**退化情形**。而區分 k 階餘數數列每個週期循環列中僅有由 $k-1$ 個不全為 0 均勻分割的條件共有 2 種：

$$\gcd(c_k, m) \ne 1, \gcd(c_1, c_2, \cdots, c_k, m) = 1 \text{ 及 } \gcd(c_1, c_2, \cdots, c_k, m) \ne 1, \gcd(c_k^{'}, m^{'}) \ne 1 \text{ 。}$$

所以由$k-1$個不全為0均勻分割的區分條件也是2種，這是正確的。由$k-1$個不全為0均勻分割不受初始條件中$a_1=1$的影響，以五階線性遞迴數列$\{a_n^5\}:a_n=a_{n-1}+2a_{n-2}+2a_{n-3}+2a_{n-4}+2a_{n-5}$且$m=2$為例：1,1,1,1,…為週期數列，及以$a_n=3a_{n-1}+2a_{n-2}$且$m=4$為例：1,3,3,3,3,…，此$k$階餘數數列為前週期數列，因此，在某項後均為不為0的常數的k階餘數數列為週期數列或前週期數列。

五、計算k階餘數數列中的循環週期

進一步計算循環週期，若$m=p_1^{t_1}\times\cdots\times p_u^{t_u}$，其中$p_1,p_2,\cdots,p_u$為相異質數且$t_1,\cdots,t_u\in N\cup\{0\}$且$\beta_1,\beta_2,\cdots,\beta_u,\pi_k(m),\beta_1'$分別為$k$階線性遞迴數列$\{a_n^k\}$中模$p_1^{t_1},\cdots,p_u^{t_u},p_1^{t_1}\times\cdots\times p_u^{t_u},p_1$後的餘數數列的週期，則$\pi_k(m)=lcm(\beta_1,\beta_2,\cdots,\beta_u)$且$\pi_k(m)=p_1^{t_1-1}\beta_1'$，參見表 7。

表 7：以$\{a_n^2\}:a_n=a_{n-1}+3a_{n-2}$為例

m	2	4		8	16	2^{t_1}
$\pi_2(m)=p_1^{t_1-1}\beta_1'$	**3**	$6=2^{2-1}\cdot3$		$12=2^{3-1}\cdot3$	$24=2^{4-1}\cdot3$	$\pi_2(m)=2^{t_1-1}\cdot3$
m	**3**	**5**	**7**	**12**	**10**	**28**
$L_2(m)=lcm(\beta_1,\cdots,\beta_u)$	**1**	**24**	**24**	$6=lcm(6,1)$	$24=lcm(3,24)$	$24=lcm(6,24)$

(一)計算2階餘數數列的週期

【性質 7】設r_n分別為$\{a_n^2\}$中模m_1,m_2後的餘數，且其週期分別β_1,β_2，其中$c_1\in N,c_2=1$。(i)若$m_2\mid m_1$，則$\beta_2\mid\beta_1$。(ii)若$\pi_2(m)$為$\{a_n^2\}$中模m_1m_2後的餘數數列的週期，其中$\gcd(m_1,m_2)=1$，則$\pi_2(m)=lcm(\beta_1,\beta_2)$。

【證明】(i)由餘數數列可令$r_{\beta_1-1}=m_1q_1+1,r_{\beta_1}=m_1q_2$且$m_1=tm_2$，其中$q_1,q_2\in N$，則

$$r_{\beta_1-1}=m_1q_1+1=(m_2t)q_1+1,\quad r_{\beta_1}=m_1q_2=(m_2t)q_2$$

再由週期循環性質知 $\beta_2 \mid \beta_1$ 。

(ii)設 $\pi_2(m) < lcm(\beta_1, \beta_2)$ ，則由**定理 6** 及(i)知 $m_1 \mid r_{\beta_1}, m_2 \mid r_{\beta_1}$ 且 $m_1 \mid \left(r_{\beta_1-1}-1\right), m_2 \mid \left(r_{\beta_1-1}-1\right)$ 。

但 $\gcd(m_1, m_2)=1$ ，所以 $m_1 m_2 \mid r_{\beta_1}$， $m_1 m_2 \mid \left(r_{\beta_1-1}-1\right)$ ，與假設矛盾，因此 $\pi_2(m) = lcm(\beta_1, \beta_2)$ 。

■

【定理 12】設 β 為 $\left\{a_n^2\right\}$ 中模 m 後的餘數數列的週期，若 $m = p_1^{t_1} \times p_2^{t_2} \times \cdots \times p_u^{t_u}$ ，其中 $p_1, p_2, \cdots, p_u$ 為相異質數且 $t_1, t_2, \cdots, t_u \in N \cup \{0\}$ 且 $\beta_1, \beta_2, \cdots, \beta_u$ 分別為 $\left\{a_n^2\right\}$ 中模 $p_1^{t_1}, p_2^{t_2}, \cdots, p_u^{t_u}$ 後的餘數數列的週期，則 $\pi_2(m) = lcm(\beta_1, \beta_2, \cdots, \beta_u)$ 。

【證明】令 $m = p_1 \times p_2 \times \cdots \times p_u$ 且 $\beta_1', \beta_2', \cdots, \beta_u'$ 分別為 $\left\{a_n^2\right\}$ 中模 $p_1, p_2, \cdots, p_u$ 後的餘數數列的週期，則由**性質 7** 知此時 $\pi_2(m) = lcm(\beta_1', \beta_2', \cdots, \beta_u')$ 。

當 $m = p_1^{t_1}$ 時，由**性質 7** 知 $\beta_1' \mid \beta_1$ ，即 $L_2(m) = p_1^{t_1-1}\beta_1'$ ，

由上述類推得到若 $m = p_1^{t_1} \times p_2^{t_2} \times \cdots \times p_u^{t_u}$ ，則 $\pi_2(m) = lcm(\beta_1, \beta_2, \cdots, \beta_u)$ 。 ■

(二)計算 k 階餘數數列的週期

【性質 8】設 r_n 分別為 $\left\{a_n^k\right\}$ 中模 m_1, m_2 後的餘數，且其週期分別 β_1, β_2 ，其中 $c_1, c_2, \cdots, c_{k-1} \in N, c_k = 1$ 。(i)若 $m_2 \mid m_1$ ，則 $\beta_2 \mid \beta_1$ 。(ii)若 $\pi_k(m)$ 為 $\left\{a_n^k\right\}$ 中模 $m_1 m_2$ 後的餘數數列的週期，其中 $\gcd(m_1, m_2)=1$ ，則 $\pi_k(m) = lcm(\beta_1, \beta_2)$ 。

【證明】仿照**性質 7** 來證明。

(i)由餘數數列可令 $r_{\beta_1-k+1} = m_1 q_1 + 1, r_{\beta_1-k+2} = m_1 q_2, \cdots, r_{\beta_1} = m_1 q_k$ 且 $m_1 = t m_2$ ，其中 $q_1, q_2 \in N$ ，

則 $r_{\beta_1-k+1} = m_1 q_1 + 1 = (m_2 t) q_1 + 1, \quad r_{\beta_1-k+2} = m_1 q_2 = (m_2 t) q_2, \cdots, \quad r_{\beta_1} = m_1 q_k = (m_2 t) q_k$

再由週期循環性質知 $\beta_2 \mid \beta_1$ 。(ii)設 $L_k(m) < lcm(\beta_1, \beta_2)$ ，則由(i)知

$m_1 \mid r_{\beta_1}, m_2 \mid r_{\beta_1}$ 、 $m_1 \mid r_{\beta_1-1}, m_2 \mid r_{\beta_1-1}$ 、 $\cdots$ 、 $m_1 \mid r_{\beta_1-k+1}, m_2 \mid r_{\beta_1-k+1}$ 、 $m_1 \mid \left(r_{\beta_1-k}-1\right), m_2 \mid \left(r_{\beta_1-k}-1\right)$ ，

但 $\gcd(m_1,m_2)=1$，所以 $m_1m_1 \mid r_{\beta_1}$，$m_1m_2 \mid \left(r_{\beta_1-k}-1\right)$，與假設矛盾。

因此，$\pi_k(m)=lcm(\beta_1,\beta_2)$。 ■

【定理 13】設 β 為 $\left\{a_n^k\right\}$ 中模 m 後的餘數數列的週期，若 $m=p_1^{t_1}\times p_2^{t_2}\times\cdots\times p_u^{t_u}$，其中 $p_1,p_2,\cdots,p_u$ 為相異質數且 $t_1,t_2,\cdots,t_u\in N\cup\{0\}$ 且 $\beta_1,\beta_2,\cdots,\beta_u$ 分別為 $\left\{a_n^k\right\}$ 中模 $p_1^{t_1}$, $p_2^{t_2}$,$\cdots$, $p_u^{t_u}$ 後的餘數數列的週期，則 $\pi_k(m)=lcm(\beta_1,\beta_2,\cdots,\beta_u)$。

【證明】令 $m=p_1\times p_2\times\cdots\times p_u$ 且 $\beta_1',\beta_2',\cdots,\beta_u'$ 分別為 $\left\{a_n^k\right\}$ 中模 $p_1,p_2,\cdots,p_u$ 後的餘數數列的週期，則由**性質 8** 知此時 $\beta=lcm(\beta_1',\beta_2',\cdots,\beta_u')$。當 $m=p_1^{t_1}$ 時，由**性質 8** 知 $\beta_1' \mid \beta_1$，即 $\beta=p_1^{t_1-1}\beta_1'$，由上述類推得到若 $m=p_1^{t_1}\times p_2^{t_2}\times\cdots\times p_u^{t_u}$，則 $\pi_k(m)=lcm(\beta_1,\beta_2,\cdots,\beta_u)$。 ■

六、探討數列的因倍數性質

(一)2 階數列的因倍數定理

【定理 14】設 $\left\{a_k^2\right\}$ 為費氏數列，則對於任意正整數 m 與 n，$a_{m+n}=a_ma_{n+1}+a_{m-1}a_n$ 且 $a_n \mid a_{mn}$。

【證明】由於

$$a_{m+n}=a_{m+n-1}+a_{m+n-2}=a_2\cdot a_{m+n-1}+a_1\cdot a_{m+n-2}\ (\because a_1=a_2=1)=a_2\cdot(a_{m+n-2}+a_{m+n-3})+a_1\cdot a_{m+n-2}$$
$$=(a_1+a_2)a_{m+n-2}+a_2\cdot a_{m+n-3}=a_3\cdot a_{m+n-2}+a_2\cdot a_{m+n-3}=\cdots=a_m\cdot a_{n+1}+a_{m-1}\cdot a_n$$

所以 $a_{m+n}=a_ma_{n+1}+a_{m-1}a_n$。又 $a_{mn}=a_{n+(m-1)n}=a_{(m-1)n}a_{n+1}+a_{(m-1)n-1}a_n$，推導

$$a_{mn}\equiv a_{(m-1)n}a_{n+1}+a_{(m-1)n-1}a_n \pmod{a_n}\equiv a_{(m-1)n}a_{n+1} \pmod{a_n}\equiv a_{(m-2)n}a_{n+1}^2 \pmod{a_n}$$
$$\equiv\cdots\equiv a_na_{n+1}^{m-1} \pmod{a_n}\equiv 0 \pmod{a_n}$$

因此，對於任意正整數 m 與 n，$a_n \mid a_{mn}$。 ■

【**定理 15**】設$\left\{a_k^2\right\}$為二階線性遞迴數列，則

(i) 對於任意正整數m與n，當$c_1=1, c_2\in N$時，則$a_{m+n}=a_m a_{n+1}+c_2 a_{m-1}a_n$且$a_n \mid a_{mn}$。

(ii) 對於任意正整數m與n，當$c_1\in N, c_2=1$時，則$a_{m+n}=a_m a_{n+1}+a_{m-1}a_n$且$a_n \mid a_{mn}$。

(iii) 對於任意正整數m與n，當$c_1\in N\setminus\{1\}, c_2\in N$時，則$a_{m+n}=a_m a_{n+1}+c_2 a_{m-1}a_n$且$a_n \mid a_{mn}$。

【**證明**】(i)由於$a_{m+n}=a_{m+n-1}+c_2 a_{m+n-2}=a_2\cdot a_{m+n-1}+a_1\cdot c_2 a_{m+n-2}$ $(\because a_1=a_2=1)$

$$=a_2\cdot(a_{m+n-2}+c_2 a_{m+n-3})+a_1\cdot c_2 a_{m+n-2}=(c_2a_1+a_2)a_{m+n-2}+c_2a_2\cdot a_{m+n-3}$$
$$=a_3\cdot a_{m+n-2}+c_2a_2\cdot a_{m+n-3}=\cdots=a_m\cdot a_{n+1}+c_2a_{m-1}\cdot a_n$$

所以$a_{m+n}=a_m a_{n+1}+c_2 a_{m-1}a_n$。又$a_{mn}=a_{n+(m-1)n}=a_{(m-1)n}a_{n+1}+c_2a_{(m-1)n-1}a_n$，推導

$$a_{mn}\equiv a_{(m-1)n}a_{n+1}+c_2a_{(m-1)n-1}a_n \pmod{a_n}\equiv a_{(m-1)n}a_{n+1} \pmod{a_n}\equiv a_{(m-2)n}a_{n+1}^2 \pmod{a_n}$$
$$\equiv\cdots\equiv a_n a_{n+1}^{m-1} \pmod{a_n}\equiv 0 \pmod{a_n}$$

因此，對於任意正整數m與n，$a_n \mid a_{mn}$。

(ii)由於$a_{m+n}=c_1a_{m+n-1}+a_{m+n-2}=a_2\cdot a_{m+n-1}+a_1\cdot a_{m+n-2}$ $(\because a_1=1, a_2=c_1)$

$$=a_2\cdot(c_1a_{m+n-2}+a_{m+n-3})+a_1\cdot a_{m+n-2}=(a_1+c_1a_2)a_{m+n-2}+a_2\cdot a_{m+n-3}$$
$$=a_3\cdot a_{m+n-2}+a_2\cdot a_{m+n-3}=\cdots=a_m\cdot a_{n+1}+a_{m-1}\cdot a_n$$

所以$a_{m+n}=a_m a_{n+1}+a_{m-1}a_n$。又$a_{mn}=a_{n+(m-1)n}=a_{(m-1)n}a_{n+1}+a_{(m-1)n-1}a_n$，同理可證，對於任意正整數$m$與$n$，$a_n \mid a_{mn}$。

(iii)由於$a_{m+n}=c_1a_{m+n-1}+c_2a_{m+n-2}=a_2\cdot a_{m+n-1}+a_1\cdot c_2a_{m+n-2}$ $(\because a_1=1, a_2=c_1)$

$$=a_2\cdot(c_1a_{m+n-2}+c_2a_{m+n-3})+a_1\cdot c_2a_{m+n-2}=(c_2a_1+c_1a_2)a_{m+n-2}+c_2a_2\cdot a_{m+n-3}$$
$$=a_3\cdot a_{m+n-2}+c_2a_2\cdot a_{m+n-3}=\cdots=a_m\cdot a_{n+1}+c_2a_{m-1}\cdot a_n$$

所以$a_{m+n}=a_m a_{n+1}+c_2 a_{m-1}a_n$。又$a_{mn}=a_{n+(m-1)n}=a_{(m-1)n}a_{n+1}+c_2a_{(m-1)n-1}a_n$，同理可證，對於任意正整數$m$與$n$，$a_n \mid a_{mn}$。 ■

(二) k **階數列的因倍數定理**

【定理 16】設$\left\{a_n^k\right\}$為k階線性遞迴數列，對於任意正整數n，

(i)若$c_k=1$或$c_k\neq 1,\gcd(c_k^{'},m')=1$，則$m\mid a_{n\ell_k(m)-i}$且$m\mid a_{n\pi_k(m)-i}$，其中$i=0,1,\cdots,k-2$。

(ii)若$c_k\neq 1,\gcd(c_k^{'},m')\neq 1$但$m\neq[\gcd(c_1,c_2,\cdots,c_k)]^u$，則存在$i\in\{0,1,\cdots,k-2\}$使得$m\nmid a_{n\ell_k(m)-i}$且$m\nmid a_{n\pi_k(m)-i}$。(iii)若$c_k\neq 1,\gcd(c_k^{'},m')\neq 1$但$m=[\gcd(c_1,c_2,\cdots,c_k)]^u$，則存在正整數$m\leq n$，使得$\left[\!\left[a_{m+j}\right]\!\right]\equiv 0$，其中$j=0,1,\cdots,n-m$且$\left[\!\left[a_{m+j}\right]\!\right]$為$\left[\!\left[a_{m+j}\right]\!\right]$模$m$後的餘數。

【證明】(i)若$c_k=1$或$c_k\neq 1,\gcd(c_k^{'},m')=1$，則由**性質 4**知$k$階餘數數列中的每個週期循環列中會有由$\underbrace{0,0,\cdots,0}_{k-1\text{個}}$均勻分割的情形，所以對於任意正整數$n$，$L_k(m)=s\cdot\ell_k(m)$，其中$s\in N$，即$m\mid a_{n\ell_k(m)},m\mid a_{n\ell_k(m)-1},\cdots,m\mid a_{n\ell_k(m)-k+2}$及$m\mid a_{n\pi_k(m)},m\mid a_{n\pi_k(m)-1},\cdots,m\mid a_{n\pi_k(m)-k+2}$，因此，$m\mid a_{n\ell_k(m)-i}$且$m\mid a_{n\pi_k(m)-i}$，其中$i=0,1,\cdots,k-2$。

(ii)若$c_k\neq 1,\gcd(c_k^{'},m')\neq 1$但$m\neq[\gcd(c_1,c_2,\cdots,c_k)]^u$，則由**性質 5**知$k$階餘數數列中的每個週期循環列中會有由非負整數$x_1,\cdots,x_{k-1}$均勻分割，所以對於任意正整數$n$，$L_k(m)=s\cdot\ell_k(m)$，其中$s\in N$，即

$a_{n\ell_k(m)}\equiv x_1\pmod m, a_{n\ell_k(m)-1}\equiv x_2\pmod m,\cdots,a_{n\ell_k(m)-k+2}\equiv x_{k-1}\pmod m$及

$a_{n\pi_k(m)}\equiv x_1\pmod m, a_{n\pi_k(m)-1}\equiv x_2\pmod m,\cdots,a_{n\pi_k(m)-k+2}\equiv x_{k-1}\pmod m$

因此，對於任意正整數n，存在$i\in\{0,1,\cdots,k-2\}$使得$m\nmid a_{n\ell_k(m)-i}$且$m\nmid a_{n\pi_k(m)-i}$。

(iii)若$c_k\neq 1,\gcd(c_k^{'},m')\neq 1$但$m=[\gcd(c_1,c_2,\cdots,c_k)]^u$，則由**定理 10**知$k$階餘數數列$\left\{r_n^k\right\}$在某項後均為 **0**，因此，存在正整數$m\leq n$，使得$\left[\!\left[a_{m+j}\right]\!\right]\equiv 0$，其中$j=0,1,\cdots,n-m$且$\left[\!\left[a_{m+j}\right]\!\right]$為$a_{m+j}$模$m$後的餘數。 ■

伍、研究結果

(一)**區分 k 階餘數數列為週期數列或前週期數列的條件**

1.當 $\gcd(c_k, m) = 1$ 時， k 階餘數數列為週期數列。

2.當 $\gcd(c_k, m) \neq 1, \gcd(c_1, \cdots, c_k, m) = 1$ 時， k 階餘數數列為週期數列或前週期數列。

3.當 $\gcd(c_k, m) \neq 1, \gcd(c_1, \cdots, c_k, m) \neq 1$ 時， k 階餘數數列為前週期數列。

(二)**區分每個週期循環列的條件**：每個週期循環列分成二種-由 $k-1$ 個 0 均勻分割(含某項後均為 0)、 $k-1$ 個不全為 0 均勻分割(含某項後皆為不為 0 的常數)。

1.當 $\gcd(c_k, m) = 1$ 時，每個週期循環列是由 $k-1$ 個 0 均勻分割(不含某項後均為 0)。

2.當 $\gcd(c_k, m) \neq 1, \gcd(c_1, \cdots, c_k, m) = 1$ 時，每個週期循環列是由 $k-1$ 個不全為 0 均勻分割(含某項後皆為不為 0 的常數)。

3.當 $\gcd(c_k, m) \neq 1, \gcd(c_1, \cdots, c_k, m) \neq 1, \gcd(c_k', m') = 1$ 時，每個週期循環列是由 $k-1$ 個 0 均勻分割(含某項後均為 0)。

4.當 $\gcd(c_k, m) \neq 1, \gcd(c_1, \cdots, c_k, m) \neq 1, \gcd(c_k', m') \neq 1$ 時，每個週期循環列是由 $k-1$ 個 0 均勻分割(含某項後均為 0)或由 $k-1$ 個不全為 0 均勻分割(含某項後皆為不為 0 的常數)。

最後利用 k 階餘數數列的週期性質，推導出 k 階線性遞迴數列的因倍數定理。

陸、結論與未來展望

本作品將費氏數列中的餘數數列性質推廣到一般高階線性遞迴數列的情形，所得餘數數列為週期數列或前週期數列，先用 $\gcd(c_k, m) = 1$ 與 $\gcd(c_k, m) \neq 1$ 分成二類來討論，這兩類中探討出區分週期循環列的四種條件，有趣地每個週期循環列有由 $k-1$ 個 0 均勻分割或由 $k-1$ 個不全為 0 均勻分割，這是令人驚喜的結果，即週期長度 $\pi_k(m) = s \cdot \ell_k(m)$ ，其中 $\ell_k(m)$ 為每一小段均勻分割的長度且 s 為段數，其中由初始條件推論出為何是由 $k-1$ 個 0 均勻分割及用**中國**

剩餘定理推論出為何是由$k-1$個不全為 0 均勻分割。更精細計算段數s，是由**推廣 Cassini 恆等式**與**歐拉-費馬定理**論證出s的準確值或範圍。

最後將週期性質推導出k階線性遞迴數列的因倍數定理，更可見到數列遞增中的規律性。此研究的結果可應用於密碼學及大數分解上，期盼未來可被廣泛採用。

柒、參考資料

[1]張福春、莊淨惠 (2009)。線性遞迴關係之求解(上)。**數學傳播**，**33**(4)，47-62。

[2]張福春、莊淨惠 (2009)。線性遞迴關係之求解(下)。**數學傳播**，**34**(1)，35-57。

[3]Bolat, C. and Köse, H., On the Properties of k-Fibonacci Numbers, *Int J Contemp Math .Sciences*, 22: 1097-1105, 2010.

[4] Courant, R. and Robbins, H. *Quadratic Residues. 2nd ed.* Oxford, England: Oxford University Press, pp. 38-40, 1996.

[5]Grimaldi, Ralph P. *Discrete and Combinatorial Mathematics: An Applied Introduction.* Mass.:Addison-Wesley Longman. P 244–248, 1998.

[6] Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers, 5th ed.* Oxford, England: Clarendon Press, pp. 67-68, 1979.

[7] M. S. Renault, *The Fibonacci Sequence Under Various Moduli*, Master's Thesis, Wake Forest University, 1996.

[8] Rogers, N., Campbell, C.W., The Period of the Fibonacci Sequence Modulo j, Phd, The University of Arizona, Tucson, USA, 2007.

【評語】050407

此作品從探討費氏數列中的餘數數列之週期性質出發，進而推廣至一般高階線性遞迴數列的情形。由於線性遞迴有一定的遞迴關係，其(mod m)餘數數列自然有遞迴關係。又由於餘數的數字是有限個可能，因此在一定的項數後會具有週期性，應該是可預期的結果，而且這個週期性應該會由於遞迴關係的生成函數、矩陣性質有不錯的工具來進行分析。這樣的問題是有趣的題材。本文主要對於餘數數列的進行了循環週期性質的探討，對於循環週期的分割、循環週期的長度、以及遞迴數列係數等等面向都有清楚的討論。作者有觀察到分段的現象並且對於分段的性質有不少的討論與證明，整題而言，作者的掌握度佳，是一篇相當有意思的作品。

作品海報

一、前言

1.研究動機

費氏數列中每一項除以任意正整數後所得的餘數數列具有許多有趣的性質，例如：**所有餘數數列均有週期性及每個週期循環列皆是由0均勻分割**，即數列在固定間隔某幾項後可被正整數整除，由此性質就可進一步計算週期長度。

本作品中我們嘗試將費氏數列中的餘數數列性質推廣到**一般高階正整係數齊次線性遞迴數列**(內文簡稱**高階線性遞迴數列**)的情形。我們發現除了**所有餘數數列均為(前)週期數列**外，**每個週期循環列中的均勻分割的情形變化出二種**：**由數個0均勻分割(含某項後均為0)**、**數個不全為0均勻分割(含某項後皆為不為0的常數)**，進一步則探討上述二種中的**區分週期循環列之條件**。最後探討出數列的**因倍數定理**。

2.研究目的

一、探討高階線性遞迴數列中每一項除以任意正整數後所得餘數數列，證明餘數數列均為**(前)週期數列**。

二、探討高階線性遞迴數列中係數在何種條件下，其餘數數列中每個週期循環列會**有數個0均勻分割(含在某項後皆為0)，探討出區分條件。**

三、探討高階線性遞迴數列中係數在何種條件下，其餘數數列中每個週期循環列會**有數個不全為0均勻分割(含在某項後皆為不為0的常數)，深入探討出區分條件。**

四、探討利用餘數數列性質推導出**高階線性遞迴數列的因倍數性質**。

3.定義與預備定理

【定義1】(k **階正整係數齊次線性遞迴數列**，張福春、莊淨惠[1] [2])

給定一數列 $\{a_n^k\}$，若存在 $k\ (\geq 2)$ 個正整數 $c_1, c_2, \cdots, c_k$，滿足兩條件

(i) (**初始條件**) $a_1 = 1, a_i = 0,$ 其中 $-(k-2) \leq i \leq 0$。

(ii) (**遞迴關係**) $a_n = c_1 a_{n-1} + c_2 a_{n-2} + c_3 a_{n-3} + \cdots + c_{k-1} a_{n-k+1} + c_k a_{n-k},\ n \geq 2$

則滿足(i)與(ii)式的數列 $\{a_n^k\}$，稱為 k **階正整係數齊次線性遞迴數列**，內文簡稱 k **階線性遞迴數列**。

其次，稱 k 階線性遞迴數列中每一項除以正整數 m 後所得的餘數數列為 k **階餘數數列** $\{r_n^k\}$。

計算週期長度 定義 k **階餘數數列的週期長度**，記作 $\pi_k(m)$。

研究方法：每個週期循環列中會有 $\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ **或** $x_1,\cdots,x_{k-1}$ **均勻分割情形，其均勻分割長度**記作為 $\ell_k(m)$，即存在正整數 s 使得 $\pi_k(m) = s \cdot \ell_k(m)$，其中 s 為 $\pi_k(m)$ 中出現 $\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ 或 $x_1,\cdots,x_{k-1}$ 的段數。

另外，k 階餘數數列在某項後均為常數，顯然**週期長度等於1**，即 $\pi_k(m) = 1$。

【定義2】(k**階餘數數列的週期性質**，M. S. Renault [7]、Rogers, N. [8])

表 1：費氏數列的週期性質

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610
mod 2	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
mod 3	0	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1
mod 4	0	1	1	2	3	1	0	1	1	2	3	1	0	1	1	2

表 2：三階線性遞迴數列 $\{a_n^3\}: a_n = a_{n-1} + a_{n-2} + a_{n-3}, m = 7 \quad (\pi_3(7) = 3 \cdot 16 = 48)$

第一段	1	1	2	4	0	6	3	2	4	2	1	0	3	4	0	0
第二段	4	4	1	2	0	3	5	1	2	1	4	0	5	2	0	0
第三段	2	2	4	1	0	5	6	4	1	4	2	0	6	1	0	0

表 3：三階線性遞迴數列 $\{a_n^3\}: a_n = 3a_{n-1} + 5a_{n-2} + 8a_{n-3}, m = 22 \quad (\pi_3(22) = 5 \cdot 12 = 60)$

第一段	1	3	14	21	3	6	3	19	10	17	11	0
第二段	15	1	12	7	1	2	1	21	18	13	11	0
第三段	5	15	4	17	15	8	15	7	6	19	11	0
第四段	9	5	16	13	5	10	5	17	2	21	11	0
第五段	3	9	20	19	9	18	9	13	8	7	11	0

有些數列在某幾項後才出現循環週期列，稱為**前週期數列**。

$\{a_n^2\}: a_n = 2a_{n-1} + 6a_{n-2}, m = 10:$

1,2,0,2,4,0,4,8,0,8,6,0,6,2,0

退化情形

k **階餘數數列在某項後均為0**，即 $\{a_n^3\}: a_n = 2a_{n-1} + 4a_{n-2} + 2a_{n-3}, m = 8: 1,2,0,2,0,0,4,0,0,\cdots,0,0$

k **階餘數數列在某項後均為不全為0的常數**，即 $\{a_n^2\}: a_n = 4a_{n-1} + 6a_{n-2}, m = 18: 1,4,4,\cdots,4,4$

【預備定理 1~2】(k **階Cassini恆等式**， Rogers, N. [8])

$$\begin{vmatrix} a_{n+1} & a_n & a_{n-1} & \cdots & a_{n-k+2} \\ a_n & a_{n-1} & a_{n-2} & \cdots & a_{n-k+1} \\ a_{n-1} & a_{n-2} & a_{n-3} & \ddots & a_{n-k} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n-k+2} & a_{n-k+1} & a_{n-k} & \cdots & a_{n-2k+3} \end{vmatrix} = \begin{cases} (-1)^{\left[\frac{k}{2}\right]} c_k^{n-k+1} & ,\text{其中} k \text{為奇數} \\ (-1)^{n-\frac{k}{2}+1} c_k^{n-k+1} & ,\text{其中} k \text{為偶數} \end{cases}$$

【預備定理 6】

(**高次剩餘**，Courant, R. and Robbins, H.[4])

若 s 滿足 $x^s \equiv d \pmod m$ 且 s 是**最小的一個**，則 $s \mid \varphi(m)$ 。

【預備定理 5】(**歐拉-費馬定理**(Euler-Fermat Theorem)， Hardy and Wright [6])

設 x, m 為正整數且 $\gcd(x,m) = 1$，則(i) $x^{\varphi(m)} \equiv 1 (\bmod m)$，其中 $\varphi(m)$ 為歐拉函數。

(ii)反之，若正整數 s 滿足 $x^s \equiv 1 \pmod m$ 且 s 是**最小的一個**，則 $s \mid \varphi(m)$ 。

二、研究方法或過程或結果

1.探討 k 階餘數數列的週期性質

【定理 1】設 $\{a_n^k\}$ 為 k 階線性遞迴數列，若 r_n 為 a_n 模 m 後的餘數($m \in N$)，則

(i) $\gcd(c_k, m) = 1$: **週期數列**。 (ii) $\gcd(c_k, m) \neq 1$: **週期數列或前週期數列**。

2.由 $k-1$ 個0均勻分割來區分循環週期列

【性質 2】設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k, m) = 1$，

則每個週期循環列中會是由 $\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ 均勻分割。

區分週期循環列的條件

(1) $\gcd(c_k,m)=1$：每個週期循環列會是由 $\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ 均勻分割，參見性質 2。

【性質 3~4】 設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列且 $\gcd(c_k,m)=1$，則
(i)當 $c_k=1$ 時，$r_{i+j+k-2}\equiv[\![r_jr_{i-1}]\!]\pmod m$，其中 $[\![r_jr_{i-1}]\!]$ 為 r_jr_{i-1} 模 m 後的餘數。 (ii)當 $c_k\neq 1$ 時，$r_{i+j+k-2}\equiv[\![c_kr_jr_{i-1}]\!]\pmod m$。

$c_2=1$ $\{a_n^2\}:a_n=2a_{n-1}+a_{n-2},m=13$

第1段	r_j	$r_1=1$	$r_2=2$	$r_3=5$	$r_4=12$	$r_5=3$	$r_6=5$	$r_7=0$
		↓	↓	↓	↓	↓	↓	↓
第2段	$[\![r_jr_6]\!]\bmod 13$	5	10	25 $=12$	8	2	12	0
第3段	$[\![r_jr_6^2]\!]\bmod 13$	25 $=12$	11	8	1	10	8	0

$c_2\neq 1$ $\{a_n^2\}:a_n=a_{n-1}+2a_{n-2},m=11$

第1段	r_j	$r_1=1$	$r_2=1$	$r_3=3$	$r_4=5$	$r_5=0$
	$c_2r_jr_4$	10	10	30	50	0
第2段	$[\![c_2r_jr_4]\!]\bmod 11$	10	10	8	6	0

每個週期循環列中分段方式

【定理 2】 設 $\{r_n^2\}$ 為二階線性遞迴數列 $\{a_n^2\}$ 中的餘數數列且 $\gcd(c_2,m)=1$，若 s 為週期循環列中由0均勻分割的段數，
其中 $\ell_2(m)-1=\alpha$，則(i)當 $c_2\neq 1$ 時，$[\![r_\alpha^2]\!]\equiv[\![c_2^{\alpha-1}]\!]\pmod m$ 或 $[\![r_\alpha^4]\!]\equiv[\![c_2^{2\alpha-2}]\!]\pmod m$。
(ii)當 $c_2=1$ 時，$[\![r_\alpha^2]\!]\equiv 1\pmod m$ 或 $[\![r_\alpha^4]\!]\equiv 1\pmod m$。

【定理 5】 設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列且 $\gcd(c_k,m)=1$，若 s 為週期循環列中由0均勻分割的段數，

其中 $\ell_k(m)-k+1=\alpha$，則(i)當 $c_k\neq 1$ 時，$[\![r_\alpha^k]\!]\equiv\begin{cases}c_k^{\alpha-1}&,\text{其中}k\text{為奇數}\\ \pm c_k^{\alpha-1}&,\text{其中}k\text{為偶數}\end{cases}\pmod m$ (ii)當 $c_k=1$ 時，$[\![r_\alpha^k]\!]\equiv\begin{cases}1,\text{其中}k\text{為奇數}\\ \pm 1,\text{其中}k\text{為偶數}\end{cases}\pmod m$。

第一段為 $1,r_2,r_3,r_4,r_5,\cdots,r_\alpha,0$

第二段為 $c_2r_1r_\alpha$ ， $c_2r_2r_\alpha$ ，$\cdots,[\![c_2r_\alpha^2]\!],0$

$\vdots$

第 s 段為 $[\![c_2^{s-1}r_\alpha^{s-1}]\!],[\![c_2^{s-1}r_2r_\alpha^{s-1}]\!],[\![c_2^{s-1}r_3r_\alpha^{s-1}]\!],\cdots,[\![c_2^{s-1}r_\alpha^s]\!],0$

由2階Cassini恆等式知 $a_{\alpha-1}a_{\alpha+1}-a_\alpha^2=(-1)^\alpha c_2^{\alpha-1}$

第一段為 $1,r_2,r_3,r_4,r_5,\cdots,r_\alpha,\underbrace{0,0,\cdots,0}_{k-1\text{個}}$

第二段為 $c_kr_1r_\alpha$ ， $c_kr_2r_\alpha$ ，$\cdots,[\![c_kr_\alpha^2]\!],\underbrace{0,0,\cdots,0}_{k-1\text{個}}$

$\vdots$

第 s 段為 $[\![c_k^{s-1}r_\alpha^{s-1}]\!],[\![c_k^{s-1}r_2r_\alpha^{s-1}]\!],[\![c_k^{s-1}r_3r_\alpha^{s-1}]\!],\cdots,[\![c_k^{s-1}r_\alpha^s]\!],\underbrace{0,0,\cdots,0}_{k-1\text{個}}$

探討週期循環列均勻分割的段數

【定理 4】 設 $\{r_n^2\}$ 為二階線性遞迴數列 $\{a_n^2\}$ 中的餘數數列，若 $\gcd(c_2,m)=1,c_2=1$，則 $s=\begin{cases}1,&\text{其中}r_\alpha=1\\ 2,&\text{其中}r_\alpha=m-1\\ 4,&\text{其餘}r_\alpha\text{要滿足}r_\alpha^2\equiv -1\pmod m\end{cases}$

由**【定理 2】**知 $[\![r_\alpha^2]\!]\equiv 1\pmod m$ 或 $[\![r_\alpha^4]\!]\equiv 1\pmod m$，由**預備定理 5：歐拉-費馬定理且** $[\![r_\alpha^s]\!]\equiv 1\pmod m$ 知 $s=1,2,4$ 。

(a)當 $r_\alpha=1$ 時，$s=1$。 (b)當 $r_\alpha=m-1$ 時，$s=2$ 。 (c)當 $r_\alpha=i\,(i=2,\cdots,m-2)$ 時，$i^2\equiv -1\pmod m$ 所以 $s=4$。

【定理 7】 設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k,m)=1,c_k=1$，則
(i)當 k 為奇數時，$\pi_k(m)=s\cdot\ell_k(m)$，其中 $s\mid k$。(ii)當 k 為偶數時，$\pi_k(m)=s\cdot\ell_k(m)$，其中 $s\mid 2k$。

(i)當 k 為奇數時，由**定理 5**知 $[\![r_\alpha^k]\!]\equiv 1\pmod m$ 。由**預備定理 5：歐拉-費馬定理**且 $[\![r_\alpha^s]\!]\equiv 1\pmod m$ 得到 $s\mid k$ 。
例如： $k=9,s\mid 9\Rightarrow s=1,3,9$

(ii)當 k 為偶數時，由**定理 5**知 $[\![r_\alpha^k]\!]\equiv 1\pmod m$ 或 $[\![r_\alpha^{2k}]\!]\equiv 1\pmod m$。由**預備定理 5：歐拉-費馬定理**且 $[\![r_\alpha^s]\!]\equiv 1\pmod m$ 知 $s\mid 2k$
以 $k=6$ 為例，$s\mid 2k\Rightarrow s\mid 12$ ，所以 $s=1,2,3,4,6,12$

(a)當 $r_\alpha=1$ 時，$s=1$。
(b)當 $r_\alpha=m-1$ 時，$s=2$ 。
(c)當 $r_\alpha=i\,(i=2,\cdots,m-2)$ 時， $i^3\equiv 1\pmod m$ 所以 $s=3$。
(d)當 $r_\alpha=i\,(i=2,\cdots,m-2)$ 時，$i^2\equiv -1\pmod m$，所以 $s=4$。
(e)當 $r_\alpha=i\,(i=2,\cdots,m-2)$ 時， $i^3\equiv -1\pmod m$，所以 $s=6$。
(f)當 $r_\alpha=i\,(i=2,\cdots,m-2)$ 時，$i^6\equiv -1\pmod m$，所以 $s=12$。

【定理 3,6】 設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k,m)=1,c_k\neq 1$，則 $\pi_k(m)=s\cdot\ell_k(m)$，其中 $s\mid\varphi(m)$。

預備定理 6：高次剩餘知 $[\![r_\alpha^k]\!]\equiv\begin{cases}c_k^{\alpha-1}&,\text{其中}k\text{為奇數}\\ \pm c_k^{\alpha-1}&,\text{其中}k\text{為偶數}\end{cases}\pmod m$ 必有解且循環 $r_\alpha\to c_2r_\alpha^2\to c_2^2r_\alpha^3\to\cdots\to c_2^{s-1}r_\alpha^s\to r_\alpha$

(2) $\gcd(c_k,m)\neq 1$：每個週期循環列會是由 $\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ 均勻分割。

【定理 8】 設 $\{r_n^k\}$ 為 k 階線性遞迴數列 $\{a_n^k\}$ 中的餘數數列，若 $\gcd(c_k,m)\neq 1$，且 $\gcd(c_1,c_2,\cdots,c_k,m)=d,c_k'=c_k/d,m'=m/d$
則(i)當 $\gcd(c_k',m')=1$ 時，k 階餘數數列是前週期數列且每個週期循環列中會是由 $k-1$ 個0均勻分割。
(ii)當 $\gcd(c_k',m')\neq 1$ 時，k 階餘數數列是前週期數列且每個週期循環列中會有由 $k-1$ 個0均勻分割。

$\{a_n^2\}:a_n=2a_{n-1}+6a_{n-2},m=10$ 考慮 $c_2'=6/2=3,m'=10/2=5$
1,2,0,2,4,0,4,8,0,8,6,0,6,2,0 但 $\gcd(c_k',m')=\gcd(3,5)=1$ $m'=5$
對應新數列 $\{a_n^2\}:a_n=1a_{n-1}+3a_{n-2},m=5$
1,1,4,2,4,0,2,2,3,4,3,0,4,4,1,3,1,0,3,3,2,1,2,0

$\{a_n^2\}:a_n=2a_{n-1}+4a_{n-2},m=24$ 考慮 $c_2'=4/2=2,m'=24/2=12$
1,2,8,0,8,16,16,0,16,8,8,0 但 $\gcd(c_k',m')=\gcd(2,12)=2$ $m'=12$
對應新數列 $\{a_n^2\}:a_n=1a_{n-1}+2a_{n-2},m=12$
1,2,8,0,8,4,4,0,4,8,8,0

$\underbrace{0,0,\cdots,0}_{k-1\text{個}}$ 均勻分割的退化情形

【定理 9】 設 $\{r_n^k\}$ 為 k 階餘數數列，若 $\gcd(c_k,m)\neq 1$ 且 $\gcd(c_1,c_2,\cdots,c_k)=\ell,m=\ell^t\,(t\in N)$，則 **$k$ 階餘數數列 $\{r_n^k\}$ 在某項後均為0。**

(a) $\gcd(c_k',m')=1$ $\{a_n^3\}:a_n=2a_{n-1}+4a_{n-2}+2a_{n-3},m=8$ 1,2,0,2,0,0,4,0,0,$\cdots$,0,0 **k 階餘數數列在第8項後均為0**
(b) $\gcd(c_k',m')\neq 1$ $\{a_n^2\}:a_n=4a_{n-1}+8a_{n-2},m=16$ 1,4,8,0,0,$\cdots$,0,0 **k 階餘數數列在第4項後均為0**

3.由 $k-1$個不全為0均勻分割來區分循環週期列

區分週期循環列的條件

(3) $\gcd(c_k,m)\neq 1$:每個週期循環列會是由 $x_1,x_2,\cdots,x_{k-1}$ 均勻分割，參見性質 5。

$\left\{a_n^3\right\}: a_n=3a_{n-1}+5a_{n-2}+8a_{n-3}, m=22$

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}
$m=2$	1	1	0	1	1	0	1	1	0	1	1	0
$m=11$	1	3	3	10	3	6	3	8	10	6	0	0
$m=22$	1	3	14	21	3	6	3	19	10	17	11	0

考慮r_{11}與r_{12}的**線性同餘方程組**為

$$\begin{cases} r_{11}\equiv 1 \pmod 2 \\ r_{11}\equiv 0 \pmod{11} \end{cases}, \begin{cases} r_{12}\equiv 0 \pmod 2 \\ r_{12}\equiv 0 \pmod{11} \end{cases}$$

則由**中國剩餘定理**知 $r_{11}\equiv 11 \pmod{22}, r_{12}\equiv 0 \pmod{22}$

可見 $m=2$ 是三階中退化情形，是由2個不全為0均勻分割。

區分週期循環的條件

週期數列

$\gcd(c_k,m)=1$

$0,0,\cdots,0$（$k-1$個） **均勻分割**

週期數列或前週期數列

$\gcd(c_1,\cdots,c_k,m)=d\,(d>1), c_k'=c_k/d, m'=m/d$

$\gcd(c_k,m)\neq 1$

$\gcd(c_k',m')=1$

$0,0,\cdots,0$（$k-1$個） **均勻分割**

在某項後均為0

$\gcd(c_k',m')\neq 1$

$\gcd(c_1,\cdots,c_k,m)\neq 1$

$0,0,\cdots,0$（$k-1$個）或 $x_1,x_2,\cdots,x_{k-1}$ **均勻分割**

在某項後均為0或不全為0的常數

$\gcd(c_1,\cdots,c_k,m)=1$

$x_1,x_2,\cdots,x_{k-1}$ **均勻分割**

在某項後均為不全為0的常數

(a) $\gcd(c_k',m')\neq 1$ $\quad \left\{a_n^2\right\}: a_n=8a_{n-1}+12a_{n-2}, m=18$: 1,8,4,2,14,16,8,4,2,10,14,16

(b) $\gcd(c_1,\cdots,c_k,m)=1$ $\quad \left\{a_n^2\right\}: a_n=4a_{n-1}+3a_{n-2}, m=18$: 1,4,1,16,13,10,7,4,1,16,13,10,7

【性質 6】 設 $\left\{r_n^2\right\}$ 為二階線性遞迴數列 $\left\{a_n^2\right\}$ 中的餘數數列且 $\gcd(c_2,m)\neq 1$，則 $r_{i+j}\equiv\left[\!\left[r_{j+1}x_1+c_2r_jr_{i-1}\right]\!\right] \pmod m$ 。

【定理 10-11 】 設 $\left\{r_n^k\right\}$ 為 k 階餘數數列，若 $\gcd(c_k,m)\neq 1, \gcd(c_1,\cdots,c_k,m)=1$ ，則

(i) 當 $k=3$ 時，$r_{i+j+1}\equiv\left[\!\left[r_{j+1}x_2+c_2r_jx_1+c_3(r_{j-1}x_1+r_jr_{i-1})\right]\!\right] \pmod m$ 。

(ii) $r_{i+j+k-2}\equiv\left[\!\left[r_{j+1}x_{k-1}+\sum_{\ell_1=2}^{k-1}\left[c_{\ell_1}\sum_{\ell_2=2}^{\ell_1} r_{j-\ell_1+\ell_2}x_{k-\ell_2}\right]+c_k\sum_{\ell=1}^{k-2} r_{j-\ell}x_\ell+c_kr_jr_{i-1}\right]\!\right] \pmod m$。

(iii) $\pi_k(m)=s\cdot\ell_k(m)$，其中 $s\mid\varphi(m)$。

第一段 $\quad r_1,r_2,r_3,r_4,r_5,\cdots,r_\alpha,x_1$

第二段 $\quad r_2x_1+c_2r_1r_\alpha$ ， $r_3x_1+c_2r_2r_\alpha$ ，$\cdots$，$\left[\!\left[x_1^2+c_2r_\alpha^2\right]\!\right], x_1$

第三段 $\quad \left[\!\left[r_2x_1+c_2r_1x_1^2+c_2^2r_1r_\alpha^2\right]\!\right],\cdots,\left[\!\left[x_1^2+c_2r_\alpha x_1^2+c_2^2r_\alpha^3\right]\!\right], x_1$

第 s 段 $\quad \left[\!\left[r_2x_1+r_1x_1^2\sum_{i=1}^{s-2}c_2^ir_\alpha^{i-1}+c_2^{s-1}r_1r_\alpha^{s-1}\right]\!\right],\cdots,\left[\!\left[x_1^2+x_1^2\sum_{i=1}^{s-2}c_2^ir_\alpha^i+c_2^{s-1}r_\alpha^s\right]\!\right], x_1$

由**Cassini恆等式**知 $a_{\alpha-1}a_{\alpha+1}-a_\alpha^2=(-1)^\alpha c_2^{\alpha-1}$。

兩邊模m得 $x_1r_{\alpha-1}-r_\alpha^2\equiv(-1)^\alpha c_2^{\alpha-1} \pmod m$。

$\left\{a_n^2\right\}: a_n=3a_{n-1}+2a_{n-2}, m=10$

1 3 1 9 9 **5** 3 9 3 7 7 **5** 9 7 9 1 1 **5** 7 1 7 3 3 **5**

$5\cdot 9-9^2\equiv(-1)^5 2^4 \pmod{10}\Rightarrow 36\equiv 16 \pmod{10}$

退化情形

在某項後均為不為0的常數 $\gcd(c_k,m)\neq 1, \gcd(c_1,c_2,\cdots,c_k,m)=1$ 及 $\gcd(c_1,c_2,\cdots,c_k,m)\neq 1, \gcd(c_k',m')\neq 1$

$\left\{a_n^2\right\}: a_n=4a_{n-1}+6a_{n-2}, m=9$ 1,4,4,4,$\cdots$,4 $\quad \left\{a_n^5\right\}: a_n=a_{n-1}+2a_{n-2}+2a_{n-3}+2a_{n-4}+2a_{n-5}, m=2$ 1,1,1,1,$\cdots$

4.計算 k 階餘數數列中的循環週期

【定理 12~13】（k階餘數數列的週期循環性質）

設β 為 $\left\{a_n^k\right\}$ 中模m 後的餘數數列的週期，若 $m=p_1^{t_1}\times p_2^{t_2}\times\cdots\times p_u^{t_u}$，且$\beta_1,\cdots,\beta_u$ 分別為 $\left\{a_n^k\right\}$ 中模 $p_1^{t_1},\cdots,p_u^{t_u}$ 後的餘數數列的週期，則 $\pi_k(m)=lcm(\beta_1,\beta_2,\cdots,\beta_u)$。

m	2	4		8	16	2^{t_1}
$\pi_2(m)=p_1^{t_1-1}\beta_1'$	**3**	$6=2^{2-1}\cdot 3$		$12=2^{3-1}\cdot 3$	$24=2^{4-1}\cdot 3$	$\pi_2(m)=2^{t_1-1}\cdot 3$
m	**3**	**5**	**7**	**12**	**10**	**28**
$\pi_2(m)=lcm(\beta_1,\beta_2,\cdots,\beta_u)$	**1**	**24**	**24**	$6=lcm(6,1)$	$24=lcm(3,24)$	$24=lcm(6,24)$

5.探討數列的因倍數性質

【定理 14】 費氏數列: $a_{m+n}=a_ma_{n+1}+a_{m-1}a_n$ **且** $a_n\mid a_{mn}$

【定理 15】 二階線性遞迴數列

(i) 當$c_1=1, c_2\in N$ 時，則 $a_{m+n}=a_ma_{n+1}+c_2a_{m-1}a_n$ **且** $a_n\mid a_{mn}$。(ii) 當$c_1\in N, c_2=1$ 時，則 $a_{m+n}=a_ma_{n+1}+a_{m-1}a_n$ **且** $a_n\mid a_{mn}$。

(iii) 當 $c_1\in N\setminus\{1\}, c_2\in N$ 時，則 $a_{m+n}=a_ma_{n+1}+c_2a_{m-1}a_n$ **且** $a_n\mid a_{mn}$ 。

【定理 16】 k **階線性遞迴數列**

(i) 當 $c_k=1$ **或** $c_k\neq 1, \gcd(c_k',m')=1$ 時，則 $m\mid a_{n\ell_k(m)-i}$ **且** $m\mid a_{n\pi_k(m)-i}$ ，其中 $i=0,1,\cdots,k-2$。

(ii)其餘 $m\nmid a_{n\ell_k(m)-i}$ **且** $m\nmid a_{n\pi_k(m)-i}$ 或 $\left[\!\left[a_{n'+j}\right]\!\right]\equiv 0 \pmod m$, **其中** $j=0,1,\cdots$ 。

三、結論與未來展望

1.結論

本作品將費氏數列中的**餘數數列性質**推廣到高階線性遞迴數列的情形，所得餘數數列為週期數列或前週期數列。我們探討出**區分週期循環的條件**，進一步用週期循環列均勻分割方式得到均勻分割循環規律，精確計算其週期長度。 最後由週期性質推導**高階線性遞迴數列的因倍數性質** 。

2.未來展望

(i) 探討前週期數列的性質。 (ii)探討因倍數定理。期盼未來可被廣泛應用於密碼學及大數分解上。

四、參考資料

[1] 張福春、莊淨惠 (2009)。線性遞迴關係之求解(上)。**數學傳播**，**33**(4)，47-62。

[2] 張福春、莊淨惠 (2009)。線性遞迴關係之求解(下)。**數學傳播**，**34**(1)，35-57。

[3]Bolat, C. and Köse, H., On the Properties of k-Fibonacci Numbers, *Int J Contemp Math .Sciences*, 22: 1097-1105, 2010.

[4] Courant, R. and Robbins, H. *Quadratic Residues. 2nd ed.* Oxford, England: Oxford University Press, pp. 38-40, 1996.

[5]Grimaldi, Ralph P. *Discrete and Combinatorial Mathematics: An Applied Introduction.* Mass.:Addison-Wesley Longman. P 244–248, 1998.

[6] Hardy, G. H. and Wright, E. M. *An Introduction to the Theory of Numbers, 5th ed.* Oxford, England: Clarendon Press, pp. 67-68, 1979.

[7] M. S. Renault, *The Fibonacci Sequence Under Various Moduli*, Master's Thesis, Wake Forest University, 1996.

[8] Rogers, N., Campbell, C.W., The Period of the Fibonacci Sequence Modulo j, Phd, The University of Arizona, Tucson, USA, 2007.