高階線性遞迴數列中的餘數數列及因倍數性質之探討

臺北市立成淵高級中學　楊承恩
指導老師　林鳳美

中文摘要

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、數個不全為 0 均勻分割，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。

1　前言

1.1　研究目的

1. 探討高階線性遞迴數列中的餘數數列之週期性質。
2. 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 或數個不全為 0 均勻分割，進一步探討出區分條件。
3. 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。

1.2　名詞定義

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 $(k \geq 2)$ *個正整數* c_1、c_2、$\cdots$、c_k*，其中* $c_k \neq 0$*，滿足兩條件：*

(i) (初始條件) $a_1^{(k)} = 1$、$a_i^{(k)} = 0$*，其中* $i = 0, -1, -2, \ldots, -(k-2)$。

(ii) (遞迴關係)

$$a_n^{(k)} = c_1 a_{n-1}^{(k)} + c_2 a_{n-2}^{(k)} + c_3 a_{n-3}^{(k)} + \cdots + c_{k-1} a_{n-k+1}^{(k)} + c_k a_{n-k}^{(k)}\text{，}n \geq 2\text{。} \quad (1)$$

則稱數列 $\{a_n^{(k)}\}$ 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])**.** *費氏數列 $\{a_n^{(2)}\}$ 中每一項 $a_n^{(2)}$ 除以正整數 m 所得到的餘數數列，會有週期性質，參考資料 [7]、[8] 與表 1。稱此餘數數列為週期數列 (period sequence)，其週期記作 $\pi_2(m)$，表 1 中 $\pi_2(2) = 3$，$\pi_2(3) = 8$，$\pi_2(4) = 6$。另外表 1 中的* mod3 *循環週期列中可用 0 均勻分割，即循環週期列為 0 1 1 2 0 2 2 1 0，用 0 均勻分割的每一小段的長度，記作 $\ell_2(m)$，其段數定義為 s，即 $\pi_2(m) = s \cdot \ell_2(m)$。表 1 中的* mod3 *的情形為 $\ell_2(3) = 4$、$s = 2 \Rightarrow \pi_2(3) = 2 \cdot 4 = 8$。*

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 1：費氏數列的週期性質

本作品將上述週期性質推廣至一般 k 階線性遞迴數列的情形，稱此餘數數列為 k 階餘數數列，記作 $\{r_n^{(k)}\}$，其數列分為週期數列或前週期數列 (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 k 階的情形，會是由 $k-1$ 個 0 均勻分割及 $k-1$ 個不全為 0 (記作 x_1、$\cdots$、x_{k-1}) 均勻分割等二種。由於初始條件的緣故，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，參見表 3。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。**

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

表 2：$\{a_n^3\}: a_n = a_{n-1} + a_{n-2} + a_{n-3}$ 且 $m = 7$ ($\pi_3(7) = 3 \cdot 16 = 48$)

第一段 $r_1, r_2, \ldots, r_{12}$	1	3	14	21	3	6	3	19	10	17	11	0
第二段 $r_{13}, r_{14}, \ldots, r_{24}$	15	1	12	7	1	2	1	21	18	31	11	0
第三段 $r_{25}, r_{26}, \ldots, r_{36}$	5	15	4	17	15	8	15	7	6	19	11	0
第四段 $r_{37}, r_{38}, \ldots, r_{48}$	9	5	16	13	5	10	5	17	2	21	11	0
第五段 $r_{49}, r_{50}, \ldots, r_{60}$	3	9	20	19	9	18	9	13	8	7	11	0

表 3：$\{a_n^3\} : a_n = 3a_{n-1} + 5a_{n-2} + 8a_{n-3}$ 且 $m = 22$ ($\pi_3(22) = 5 \cdot 12 = 60$)

1.3 預備知識

預備定理 1. (二階 Cassini 恆等式，Rogers, N. [8]) *對於任意正整數 n，$a_{n-1}^{(2)} a_{n+1}^{(2)} - \left(a_n^{(2)}\right)^2 = (-1)^n c_2^{n-1}$。*

預備定理 2. (k 階 Cassini 恆等式，Rogers, N. [8]) *對於任意正整數 n，*

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

預備定理 3. (鴿籠原理，The Pigeonhole Principle，Grimaldi, Ralph P. [5]) *若有 n 個籠子與 $n \geq 1$ 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. (中國剩餘定理，Hardy, G. H. and Wright, E. M. [6]) *設 $m = m_1 m_2 \cdots m_t$，其中 m_1、m_2、$\cdots$、m_t 為兩兩互質，若 b_1、b_2、$\cdots$、$b_t \in \mathbb{Z}$，則方程組：$x \equiv b_i \pmod{m_i}$ 其中 $1 \leq i \leq t$，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 $\varphi(m)$ 為歐拉函數，表示不大於 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 $s \mid \varphi(m)$。*

設 $m > 1$，k、$d \in \mathbb{N}$，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 $\varphi(m)$ 為歐拉函數。*

2 探討 k 階餘數數列的週期性質

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

性質 1： $c_1 r_{n-1}^{(k)} + c_2 r_{n-2}^{(k)} + \cdots + c_k r_{n-k}^{(k)} \equiv r_n^{(k)} \pmod{m}$。

證明. 設 $a_n^{(k)} = qm + r_n^{(k)}$、$a_{n-1}^{(k)} = q_1 m + r_{n-1}^{(k)}$、$a_{n-2}^{(k)} = q_2 m + r_{n-2}^{(k)}$、$\cdots$、$a_{n-k}^{(k)} = q_k m + r_{n-k}^{(k)}$，其中 q、q_1、q_2、$\cdots$、$q_k \in \mathbb{N} \cup \{0\}$，因為 $a_n^{(k)} = c_1 a_{n-1}^{(k)} + c_2 a_{n-2}^{(k)} + c_3 a_{n-3}^{(k)} + \cdots + c_{k-1} a_{n-k+1}^{(k)} + c_k a_{n-k}^{(k)}$，所以

$$
\begin{aligned}
& c_1 r_{n-1}^{(k)} + c_2 r_{n-2}^{(k)} + c_3 r_{n-3}^{(k)} + \cdots + c_k r_{n-k}^{(k)} \\
&= c_1 (a_{n-1}^{(k)} - q_1 m) + c_2 (a_{n-2}^{(k)} - q_2 m) + c_3 (a_{n-3}^{(k)} - q_3 m) + \cdots + c_k (a_{n-k}^{(k)} - q_k m) \\
&= a_n^{(k)} - m(c_1 q_1 + c_2 q_2 + \cdots + c_k q_k) \quad 。
\end{aligned}
$$

因此，$c_1 r_{n-1}^{(k)} + c_2 r_{n-2}^{(k)} + \cdots + c_k r_{n-k}^{(k)} \equiv r_n^{(k)} \pmod{m}$。 □

定理 1： (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. 由於 $r_n^{(k)} \in \{0,1,2,\ldots,m-1\}$，可令 $(r_i^{(k)}, r_{i+1}^{(k)}, \ldots, r_{i+k-1}^{(k)})$ 為 k 階餘數數列中相鄰 k 個項的數對，其中 $r_i^{(k)}, r_{i+1}^{(k)}, \ldots, r_{i+k-1}^{(k)} \in \{0,1,2,\ldots,m-1\}$，則數對 $(r_i^{(k)}, r_{i+1}^{(k)}, \ldots, r_{i+k-1}^{(k)})$ 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 $m^k < j \leq m^k + k$ 使得 $r_i^{(k)} = r_j^{(k)}$，又由於是 k 階餘數數列，故數對 $(r_i^{(k)}, r_{i+1}^{(k)}, \ldots, r_{i+k-1}^{(k)}) = (r_j^{(k)}, r_{j+1}^{(k)}, \ldots, r_{j+k-1}^{(k)})$。又由性質 1 知 $c_1 r_{n-1}^{(k)} + c_2 r_{n-2}^{(k)} + \cdots + c_k r_{n-k}^{(k)} \equiv r_n^{(k)} \pmod{m}$，得到 $r_i^{(k)}$、$r_{i+1}^{(k)}$、$\ldots$、$r_{i+k-1}^{(k)} \cdots$ 與 $r_j^{(k)}$、$r_{j+1}^{(k)}$、$\ldots$、$r_{j+k-1}^{(k)}$ 完全相同，即 k 階餘數數列從第 i 項後開始出現循環數列。

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 $X_{n-1}=\begin{bmatrix} a_{n-1}^{(k)} \\ a_{n-2}^{(k)} \\ a_{n-3}^{(k)} \\ \vdots \\ a_{n-k}^{(k)} \end{bmatrix}$ 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 $a_1^{(k)}=1$，$a_i^{(k)}=0$，對於 $-(k-2)\le i\le 0$，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 $\ell\in\mathbb{N}$，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。

□

3 由 $k-1$ 個 0 均勻分割來區分循環週期列

3.1 $\gcd(c_2,m)=1$

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 $\gcd(c_k,m)=1$，則 k 階餘數數列中的每個週期循環列中會是由 $k-1$ 個 0 均勻分割。

證明. 考慮在 $(r_1^{(k)},r_{m^k+k}^{(k)})$ 中重複的相鄰 k 項為 $r_i^{(k)}=r_j^{(k)}$，$r_{i+1}^{(k)}=r_{j+1}^{(k)}$，$r_{i+2}^{(k)}=r_{j+2}^{(k)}$，$\cdots$，$r_{i+k+1}^{(k)}=r_{j+k+1}^{(k)}$。由性質 1 知 $c_1r_{j-i+k-1}^{(k)}+c_2r_{j-i+k-2}^{(k)}+\cdots+c_kr_{j-i}^{(k)}\equiv$

$r_{j-i+k}^{(k)} \pmod m$，故

$$\begin{aligned} c_k r_{j-i}^{(k)} &\equiv r_{j-i+k}^{(k)} - c_1 r_{j-i+k-1}^{(k)} - c_2 r_{j-i+k-2}^{(k)} - \cdots - c_{k-1} r_{j-i+1}^{(k)} \pmod m \\ &\equiv r_k^{(k)} - c_1 r_{k-1}^{(k)} - c_2 r_{k-2}^{(k)} - \cdots - c_{k-1} r_1^{(k)} \equiv 0 \pmod m \end{aligned} \tag{2}$$

當 $c_k = 1$ 時，(2) 式為 $r_{j-i}^{(k)} \equiv 0 \pmod m$。事實上，當 $\gcd(c_k, m) = 1$ 時，(2) 式同樣地可得到 $r_{j-i}^{(k)} \equiv 0 \pmod m$。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。

□

底下所有性質與定理中符號 $[\![x]\!]$ 是指 x 模 m 後的餘數。

性質 3： 設 $\gcd(c_k, m) = 1$，若 2 階餘數數列中的週期循環列是由 0 均勻分割且 $r_i^{(2)}$ 為第 i 次由 0 均勻分割的 0 之前一項 $(1 \le s \le s-1)$，則

(i) 當 $c_2 = 1$ 時，$r_{i+j}^{(2)} \equiv \left[\!\left[r_j^{(2)} r_{i-1}^{(2)} \right]\!\right] \pmod m$，其中 $j \in \mathbb{N}$。

(ii) 當 $c_2 \neq 1$ 時，$r_{i+j}^{(2)} \equiv \left[\!\left[c_2 r_j^{(2)} r_{i-1}^{(2)} \right]\!\right] \pmod m$，其中 $j \in \mathbb{N}$。

證明. 注意到當 $\gcd(c_2, m) = 1$ 時，有分 $c_2 = 1$ 或 $c_2 \neq 1$ 的情形。

(i) 令 $c_2 = 1$，由於 $a_{i-1}^{(2)} = mq_1 + r_{i-1}^{(2)}$，$a_i^{(2)} = mq_2$ $(q_1 \text{、} q_2 \in \mathbb{N} \cup \{0\})$，則給定一個正整數 j，

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

兩邊模 m 得到，$r_{i+j}^{(2)} = \left[\!\left[r_j^{(2)} r_{i-1}^{(2)} \right]\!\right] \pmod m$，其中 $j \in \mathbb{N}$，以 $\{a_n^{(2)}\} : a_n^{(2)} = 2a_{n-1}^{(2)} + a_{n-2}^{(2)}$ 且模 13 為例：

第 1 段	$r_j^{(2)}$	$r_1^{(2)}=1$	$r_2^{(2)}=2$	$r_3^{(2)}=5$	$r_4^{(2)}=12$	$r_5^{(2)}=3$	$r_6^{(2)}=5$	$r_7^{(2)}=0$
		↓	↓	↓	↓	↓	↓	↓
第 2 段	$\left[\!\left[r_j^{(2)}r_6^{(2)}\right]\!\right]$ mod 13	5	10	$[\![25]\!]$	8	2	12	0
第 3 段	$\left[\!\left[r_j^{(2)}(r_6^{(2)})^2\right]\!\right]$ mod 13	$[\![25]\!]$	11	8	1	10	8	0

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

(ii) 仿照 (i) 來證明，(3) 式改為

$$a_{i+j}^{(2)}=c_2a_j^{(2)}\cdot(mq_1+r_{i-1}^{(2)})+a_{j+1}^{(2)}\cdot mq_2\text{，}j\in\mathbb{N}\text{。}\tag{4}$$

兩邊模 m 得到 $r_{i+j}^{(2)}=\left[\!\left[c_2r_j^{(2)}r_{i-1}^{(2)}\right]\!\right]\pmod m$，其中 $j\in\mathbb{N}$ ，且 $\left[\!\left[c_2r_j^{(2)}r_{i-1}^{(2)}\right]\!\right]$ 為 $c_2r_j^{(2)}r_{i-1}^{(2)}$ 模 m 後的餘數且 $1\le i\le s-1$，$j\in\mathbb{N}$。以 $\{a_n^{(2)}\}$：$a_n^{(2)}=a_{n-1}^{(2)}+2a_{n-2}^{(2)}$ 且模 11 為例：

第 1 段	$r_j^{(2)}$	$r_1^{(2)}=1$	$r_2^{(2)}=1$	$r_3^{(2)}=3$	$r_4^{(2)}=5$	$r_5^{(2)}=0$
	$c_2r_j^{(2)}r_4^{(2)}$	10	10	30	50	0
第 2 段	$\left[\!\left[c_2r_j^{(2)}r_4^{(2)}\right]\!\right]$ mod 11	10	10	8	6	0

□

為了方便，定義 $r_{\alpha+1}^{(2)}$ 為 2 階餘數數列中的第 1 段週期循環列由 0 均勻分割的 0 之位置，其中 $\alpha=\ell_2(m)-1$。

定理 2： 設 $\gcd(c_2,m)=1$，則

(i) 當 $c_2\ne1$ 時，$\left[\!\left[(r_\alpha+1^{(2)})^2\right]\!\right]\equiv\left[\!\left[c_2^{\alpha-1}\right]\!\right]\pmod m$ 或 $\left[\!\left[(r_\alpha+1^{(2)})^4\right]\!\right]\equiv c_2^{2\alpha-2}\pmod m$。

(ii) 當 $c_2=1$ 時，$\left[\!\left[(r_\alpha+1^{(2)})^2\right]\!\right]\equiv1\pmod m$ 或 $\left[\!\left[(r_\alpha+1^{(2)})^4\right]\!\right]\equiv1\pmod m$。

證明. (i) 令 $\ell_2(m)=1$，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

$$1,r_2^{(2)}=\{c_1\},r_3^{(2)},r_4^{(2)},r_5^{(2)},\cdots,r_\alpha^{(2)},0\text{；}$$

第二段為

$$\left[\!\left[c_2r_1^{(2)}r_\alpha^{(2)}\right]\!\right],\left[\!\left[c_2r_2^{(2)}r_\alpha^{(2)}\right]\!\right],\left[\!\left[c_2r_3^{(2)}\right]\!\right],\cdots,\left[\!\left[c_2(r_\alpha^{(2)})^2\right]\!\right],0\text{；}$$

第三段為

$$\left[\!\left[c_2^2(r_\alpha^{(2)})^2\right]\!\right], \left[\!\left[c_2^2 r_2^{(2)}(r_\alpha^{(2)})^2\right]\!\right], \left[\!\left[c_2^2 r_3^{(2)}(r_\alpha^{(2)})^2\right]\!\right], \cdots, \left[\!\left[c_2^2(r_\alpha^{(2)})^3\right]\!\right], 0\ ;$$

以此類推得第 s 段為

$$\left[\!\left[c_2^{s-1}(r_\alpha^{(2)})^{s-1}\right]\!\right], \left[\!\left[c_2^{s-1} r_2^{(2)}(r_\alpha^{(2)})^{s-1}\right]\!\right], \cdots, \left[\!\left[c_2^{s-1}(r_\alpha^{(2)})^s\right]\!\right], 0\text{。}$$

得到

$$r_{\alpha+1}^{(2)} = 0\text{，}\ r_{s(\alpha+1)-1}^{(2)} = \left[\!\left[c_2^{s-1}(r_\alpha^{(2)})^s\right]\!\right]\text{，}\ r_{s(\alpha+1)+1}^{(2)} = \left[\!\left[c_2^{s}(r_\alpha^{(2)})^s\right]\!\right]\text{。}$$

又由二階 Cassini 恆等式知 $a_{\alpha-1}^{(2)}a_{\alpha+1}^{(2)} - (a_\alpha^{(2)})^2 = (-1)^\alpha c_2^{\alpha-1}$，兩邊模 m 可以得到 $\left[\!\left[(r_{\alpha+1}^{(2)})^2\right]\!\right] \equiv \pm\left[\!\left[c_2^{\alpha-1}\right]\!\right] \pmod m$。即

$$\left[\!\left[(r_{\alpha+1}^{(2)})^2\right]\!\right] \equiv \left[\!\left[c_2^{\alpha-1}\right]\!\right] \pmod m \text{ 或 } \left[\!\left[(r_{\alpha+1}^{(2)})^4\right]\!\right] \equiv \left[\!\left[c_2^{2\alpha-2}\right]\!\right] \pmod m\text{。} \quad (5)$$

(ii) 仿照 (i) 來證明，(5) 式改為 $\left[\!\left[(r_\alpha^{(2)})^2\right]\!\right] \equiv \pm 1 \pmod m$，因此，

$$\left[\!\left[(r_{\alpha+1}^{(2)})^2\right]\!\right] \equiv 1 \pmod m \text{ 或 } \left[\!\left[(r_{\alpha+1}^{(2)})^4\right]\!\right] \equiv 1 \pmod m\text{。} \quad (6)$$

□

定理 3： 設 $\gcd(c_2, m) = 1$，$c_2 \neq 1$，若 s 為 2 階餘數數列中的週期循環列由 0 均勻分割之段數，則 $\pi_2(m) = s \cdot \ell_2(m)$，其中 $s \mid \varphi(m)$。

證明. 由定理 2 中知每個週期循環列中每段以 0 均勻分割位置的前一項依序分別為 $r_\alpha^{(2)}$、$c_2(r_\alpha^{(2)})^2$、$c_2^2(r_\alpha^{(2)})^3$、$\cdots$、$c_2^{s-1}(r_\alpha^{(2)})^s$。因為 $\gcd(r_2, m) = 1$ 且 $\gcd(c_2, m) = 1$，由鴿籠原理與高次剩餘知 (5) 式必有解且循環，以 $\{a_n^{(2)}\} : a_n^{(2)} = 3a_{n-1}^{(2)} + 2a_{n-2}^{(2)}$ 為例參見表 4。由於要滿足 $r_\alpha^{(2)} \to c_2(r_\alpha^{(2)})^2 \to c_2^2(r_\alpha^{(2)})^3 \to \cdots \to c_2^{s-1}(r_\alpha^{(2)})^s$，又回到 $r_\alpha^{(2)}$，由高次剩餘知 $s \mid \varphi(m)$，因此，$\pi_2(m) = s \cdot \ell_2(m)$，其中 $s \mid \varphi(m)$。

m \ t	$t = 1$	$r_\alpha^{(2)} \to c_2(r_\alpha^{(2)})^2 \to c_2^2(r_\alpha^{(2)})^3 \to \cdots \to c_2^{s-1}(r_\alpha^{(2)})^s$	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

表 4：二階線性遞迴數列 $\{a_n^{(2)}\} : a_n^{(2)} = 3a_{n-1}^{(2)} + 2a_{n-2}^{(2)}$ 為例

例如 1：表 4 中 $m = 9$ ($s = 2$)，$s \mid \varphi(9) \ \Rightarrow\ s \mid 9(1 - 1/3) \ \Rightarrow\ s \mid 6$。

例如 2：表 4 中 $m = 13$ ($s = 3$)，$s \mid (m - 1) \ \Rightarrow\ s \mid 12$。

□

定理 4： 設 $\gcd(c_2, m) = 1$，$c_2 = 1$，若 s 為 2 階餘數數列中的週期循環列由 0 均勻分割之段數，則 $\pi_2(m) = s \cdot \ell_2(m)$，其中 $s = 1, 2, 4$，且

$$s = \begin{cases} 1\text{，其中 } r_\alpha^{(2)} = 1\text{；} \\ 2\text{，其中 } r_\alpha^{(2)} = m-1\text{；} \\ 4\text{，其餘 } r_\alpha^{(2)} \text{ 要滿足} (r_\alpha^{(2)})^2 \equiv -1 \pmod{m}\text{。} \end{cases}$$

證明. 由定理 3 知

$$\left[\!\left[(r_{\alpha+1}^{(2)})^2 \right]\!\right] \equiv 1 \pmod{m} \text{ 或 } \left[\!\left[(r_{\alpha+1}^{(2)})^4 \right]\!\right] \equiv 1 \pmod{m}\text{。} \tag{6}$$

又 $\left[\!\left[(r_\alpha^{(2)})^s \right]\!\right] \equiv 1 \pmod{m}$ 且 $\gcd(r_\alpha^{(2)}, m) = 1$，則由歐拉-費馬定理知 $s \mid 2$ 或 $s \mid 4$。因此，$s = 1, 2, 4$。因為 $r_\alpha^{(2)} = 0, 1, \ldots, m-1$，顯然 $r_\alpha^{(2)} = 0$ 不滿足 (6) 式，且 $r_\alpha^{(2)} = 1$ 必滿足 (6) 式，即 $s = 1$；當 $r_\alpha^{(2)} = m-1$ 時，$(m-1)^2 \equiv 1 \pmod{m}$ 滿足 (6) 式，所以 $s = 2$；當 $r_\alpha^{(2)} = i$ $(i = 2, 3, \ldots, m-2)$ 時，$i^2 \equiv -1 \pmod{m}$ 滿足 (6) 式，所以 $s = 4$。因此得證。 □

3.2 $\gcd(c_k, m) = 1$

接著將定理 3、4 中每個週期循環列性質推廣到 $\gcd(c_k, m) = 1$ 的情形。

性質 4： 設 $\gcd(c_k, m) = 1$，若 k 階餘數數列中的週期循環列是由 0 均勻分割且 $r_i^{(k)}$ 為第 i 次由 $k-1$ 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，$r_{i+j+k-2}^{(k)} \equiv \left[\!\left[r_j^{(k)} r_{i-1}^{(k)} \right]\!\right] \pmod{m}$，其中 $j \in \mathbb{N}$。

(ii) 當 $c_k \neq 1$ 時，$r_{i+j+k-2}^{(k)} \equiv \left[\!\left[c_k r_j^{(k)} r_{i-1}^{(k)} \right]\!\right] \pmod{m}$，其中 $j \in \mathbb{N}$。

證明. (i) 仿造性質 3 來證明，即將 (3) 式改為

$$\begin{aligned} a_{i+j+k-2}^{(k)} = \; & a_{j+1}^{(2)} \cdot m q_k + \sum_{\ell_1=2}^{k-1} \left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} a_{j-\ell_1+\ell_2}^{(k)} \cdot m q_{k+1-\ell_2} \right] \\ & + \sum_{\ell=1}^{k-2} a_{j-\ell}^{(k)} \cdot m q_{\ell+1} + a_j^{(k)} (m q_1 + r_{i-1}^{(k)})\text{，} \end{aligned}$$

其中 $j \in \mathbb{N}$，q_1、$\cdots$、$q_k \in \mathbb{N}$，兩邊模 m 可以得到 $r_{i+j+k-2}^{(k)} \equiv \left[\!\left[r_j^{(k)} r_{i-1}^{(k)} \right]\!\right] \pmod{m}$，其中 $\left[\!\left[r_j^{(k)} r_{i-1}^{(k)} \right]\!\right]$ 為 $r_j^{(k)} r_{i-1}^{(k)}$ 模 m 後得到的餘數且 $1 \le i \le s-1$，$j \in \mathbb{N}$。以 $\{a_n^{(3)}\}$：$a_n^{(3)} = 2a_{n-1}^{(3)} + a_{n-2}^{(3)} + a_{n-3}^{(3)}$ 模 7 為例：

第 1 段	$r_j^{(k)}$	1	2	5	6	5	0	4	6	2	0	1	4	2	2	3	3	4	0	0
	$r_j^{(k)} r_{17}^{(k)}$	4	8	20	24	20	0	16	24	8	0	4	16	8	8	12	12	16	0	0
第 2 段	$\left[\!\left[r_j^{(k)} r_{17}^{(k)} \right]\!\right]$ mod 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，即 (4) 式改為

$$\begin{aligned} a_{i+j+k-2}^{(k)} = \; & a_{j+1}^{(k)} \cdot mq_k + \sum_{\ell_1=2}^{k-1} \left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} a_{j-\ell_1+\ell+2}^{(k)} \cdot mq_{k+1-\ell_2} \right] \\ & + c_k \sum_{\ell=1}^{k-2} a_{j-\ell}^{(k)} \cdot mq_{\ell+1} + c_k a_j^{(k)} (mq_1 + r_{i-1}^{(k)}) \text{。} \end{aligned}$$

兩邊模 m 得到 $r_{i+j+k-2}^{(k)} \equiv \left[\!\left[c_k r_j^{(k)} r_{i-1}^{(k)} \right]\!\right] \pmod{m}$，其中 $j \in \mathbb{N}$。 □

為了方便，定義 $r_\alpha^{(k)}$、$r_{\alpha+1}^{(k)}$、$\cdots$、$r_{\alpha+k-1}^{(k)}$ 為 k 階餘數數列中的第 1 段週期循環列由 $k-1$ 個 0 均勻分割的 0 之位置，其中 $\alpha = \ell_k(m) - k + 1$。

定理 5： 設 $\gcd(c_k, m) = 1$，則

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

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

證明. (i) 仿照定理 2 證明。由性質 2 及定義 2 知每個週期循環列中由個分割的第一段為

$$1, r_2^{(k)}, r_3^{(k)}, r_4^{(k)}, \ldots, r_\alpha^{(k)}, \underbrace{0, 0, \ldots, 0}_{k-1 \text{ 個}} \text{，}$$

第二段為

$$\left[\!\left[c_k r_1^{(k)} r_\alpha^{(k)} \right]\!\right], \left[\!\left[c_k r_2^{(k)} r_\alpha^{(k)} \right]\!\right], \ldots, \left[\!\left[c_k (r_\alpha^{(k)})^2 \right]\!\right], \underbrace{0, 0, \ldots, 0}_{k-1 \text{ 個}} \text{，}$$

第三段為

$$\left[\!\left[c_k^2 (r_\alpha^{(k)})^2 \right]\!\right], \left[\!\left[c_k^2 r_2^{(k)} (r_\alpha^{(k)})^2 \right]\!\right], \ldots, \left[\!\left[c_k^2 (r_\alpha^{(k)})^3 \right]\!\right], \underbrace{0, 0, \ldots, 0}_{k-1 \text{ 個}} \text{，}$$

以此類推得第 s 段為

$$\left[\!\left[c_k^{s-1} (r_\alpha^{(k)})^{s-1} \right]\!\right], \left[\!\left[c_k^{s-1} r_2^{(k)} (r_\alpha^{(k)})^{s-1} \right]\!\right], \ldots, \left[\!\left[c_k^{s-1} (r_\alpha^{(k)})^s \right]\!\right], \underbrace{0, 0, \ldots, 0}_{k-1 \text{ 個}} \text{。}$$

可知 $r_\alpha^{(k)} = \left[\!\left[r_\alpha^{(k)} \right]\!\right]$，$r_\alpha + 1^{(k)} = \cdots = r_{\alpha+k-1}^{(k)} = 0$。

由 k 階 Cassini 恆等式知

$$\begin{vmatrix} a_{\alpha+k-1}^{(k)} & a_{\alpha+k-2}^{(k)} & a_{\alpha+k-3}^{(k)} & \cdots & a_\alpha^{(k)} \\ a_{\alpha+k-2}^{(k)} & a_{\alpha+k-3}^{(k)} & a_{\alpha+k-4}^{(k)} & \cdots & a_{\alpha-1}^{(k)} \\ a_{\alpha+k-3}^{(k)} & a_{\alpha+k-4}^{(k)} & a_{\alpha+k-5}^{(k)} & \ddots & a_{\alpha-2}^{(k)} \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ a_\alpha^{(k)} & a_{\alpha-1}^{(k)} & a_{\alpha-2}^{(k)} & \cdots & a_{\alpha-k+1}^{(k)} \end{vmatrix} = \begin{cases} (-1)^{[k/2]} c_k^{\alpha-1}\,, \\ \qquad \text{其中 } k \text{ 為奇數}; \\ (-1)^{\alpha+k+k/2-1} c_k^{\alpha-1}\,, \\ \qquad \text{其中 } k \text{ 為偶數}。 \end{cases}$$

兩邊模 m 得到

$$\begin{vmatrix} 0 & 0 & 0 & \cdots & r_\alpha^{(k)} \\ 0 & 0 & 0 & \cdots & r_{\alpha-1}^{(k)} \\ \vdots & \vdots & \iddots & \ddots & r_{\alpha-2}^{(k)} \\ 0 & 0 & \cdots & \ddots & \vdots \\ r_\alpha^{(k)} & r_{\alpha-1}^{(k)} & r_{\alpha-2}^{(k)} & \cdots & r_{\alpha-k+1}^{(k)} \end{vmatrix} = \begin{cases} (-1)^{[k/2]} c_k^{\alpha-1} \pmod m\,, \\ \qquad \text{其中 } k \text{ 為奇數}; \\ (-1)^{\alpha+k+k/2-1} c_k^{\alpha-1} \pmod m\,, \\ \qquad \text{其中 } k \text{ 為偶數}。 \end{cases}$$

因此，

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

(ii) 因為 $c_k = 1$，所以 (7) 式改為

$$\left[\!\left[(r_\alpha^{(k)})^k \right]\!\right] \equiv \begin{cases} 1 \pmod m\text{，其中 } k \text{ 為奇數}; \\ \pm 1 \pmod m\text{，其中 } k \text{ 為偶數}。 \end{cases} \tag{8}$$

□

定理 6： 設 $\gcd(c_k, m) = 1$，$c_k \neq 1$，若 s 為 k 階餘數數列中的週期循環列由 $k-1$ 個 0 均勻分割之段數，則 $\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \mid \varphi(m)$。

證明. 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 $r_\alpha^{(k)}$、$c_k(r_\alpha^{(k)})^2$、$c_k^2(r_\alpha^{(k)})^3$、$\cdots$、$c_k^{s-1}(r_\alpha^{(k)})^s$。因為 $\gcd(r_\alpha^{(k)}, m) = 1$ 且 $\gcd(c_k, m) = 1$，由鴿籠原理與高次剩餘知 (7) 式必有解且循環，又要滿足循環長度 $r_\alpha^{(k)} \to c_k(r_\alpha^{(k)})^2 \to c_k^2(r_\alpha^{(k)})^3 \to \cdots \to c_k^{s-1}(r_\alpha^{(k)})^s$，回到 $r_\alpha^{(k)}$，由高次剩餘知 $s \mid \varphi(m)$，因此，$\pi_k(m) = s \cdot \ell_k(m)$ 其中 $s \mid \varphi(m)$。 □

定理 7： 設 $\gcd(c_k, m) = 1$，$c_k = 1$，若 s 為 k 階餘數數列中的週期循環列由 $k-1$ 個 0 均勻分割之段數，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，(8) 式為 $\left[\!\left[(r_\alpha^{(k)})^k\right]\!\right] \equiv 1 \pmod{m}$，其中 $\gcd(r_\alpha^{(k)}, m) = 1$。顯然 $r_\alpha^{(k)} = 0$ 不滿足 $\left[\!\left[(r_\alpha^{(k)})^k\right]\!\right] \equiv 1 \pmod{m}$，$r_\alpha^{(k)}$ 可能的值為 $1、\cdots、m-1$。由歐拉-費馬定理且 $\left[\!\left[(r_\alpha^{(k)})^s\right]\!\right] \equiv 1 \pmod{m}$，得到 $s \mid k$。例如：若 $k = 9$，$s \mid 9$，則 $s = 1, 3, 9$。

(ii) 當 k 為奇數時，(8) 式為 $\left[\!\left[(r_\alpha^{(k)})^k\right]\!\right] \equiv \pm 1 \pmod{m}$，即 $\left[\!\left[(r_\alpha^{(k)})^k\right]\!\right] \equiv 1 \pmod{m}$ 或 $\left[\!\left[(r_\alpha^{(k)})^{2k}\right]\!\right] \equiv 1 \pmod{m}$。由歐拉-費馬定理知 $\gcd(r_\alpha^{(k)}, m) = 1$。顯然 $r_\alpha^{(k)} = 0$ 不滿足 $\left[\!\left[(r_\alpha^{(k)})^k\right]\!\right] \equiv 1 \pmod{m}$ 或 $\left[\!\left[(r_\alpha^{(k)})^{2k}\right]\!\right] \equiv 1 \pmod{m}$，$r_\alpha^{(k)}$ 可能的值為 $1、\cdots、m-1$。又 $\left[\!\left[(r_\alpha^{(k)})^s\right]\!\right] \equiv 1 \pmod{m}$ 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 $r_\alpha^{(k)} = 0, 1, 2, \ldots, m-1$。當 $r_\alpha^{(k)} = 0$ 不滿足 (8) 式。當 $r_\alpha^{(k)} = 1$ 必滿足 (8) 式，即 $s = 1$；當 $r_\alpha^{(k)} = m-1$ 時，$(m-1)^2 \equiv 1 \pmod{m}$ 滿足 (8) 式，所以 $s = 2$；當 $r_\alpha^{(k)} = i$ $(i = 2, \ldots, m-2)$ 時，$i^3 \equiv 1 \pmod{m}$ 滿足 (8) 式，即 $s = 3$。當 $r_\alpha^{(k)} = i$ $(i = 2, \ldots, m-2)$ 時，$i^2 \equiv -1 \pmod{m}$ 滿足 (8) 式，即 $s = 4$。當 $r_\alpha^{(k)} = i$ $(i = 2, \ldots, m-2)$ 時，$i^3 \equiv -1 \pmod{m}$ 滿足 (8) 式，即 $s = 6$。當 $r_\alpha^{(k)} = i$ $(i = 2, \ldots, m-2)$ 時，$i^6 \equiv -1 \pmod{m}$ 滿足 (8) 式，即 $s = 12$。

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

3.3 $\gcd(c_k, m) \neq 1$

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？

定理 8： 設 $\gcd(c_k, m) \neq 1$ 且 $\gcd(c_1, c_2, \ldots, c_k, m) = d$，$c_k' = c_k/d$，$m' = m/d$，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 $\gcd(c_1, c_2, \ldots, c_k, m) = d \neq 1$，$c_k' = c_k/d$，$m' = m/d$，當 $\gcd(c_k', m') = 1$，則 k 階餘數數列為前週期數列。

以 $\{a_n^{(2)}\}: a_n^{(2)} = 2a_{n-1}^{(2)} + 6a_{n-2}^{(2)}$ 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 $\gcd(c_k', m') = 1$ 且 $m' = 5$，對應 $\{a_n^{(2)}\}: a_n^{(2)} = 1a_{n-1}^{(2)} + 3a_{n-2}^{(2)}$：

$$\begin{aligned} a_n^{(2)} &= 2a_{n-1}^{(2)} + 6a_{n-2}^{(2)} &&: \boxed{1,2,0},2,4,0,4,8,0,8,6,0,6,2,0 \\ a_n^{(2)} &= 1a_{n-1}^{(2)} + 3a_{n-2}^{(2)} &&: 1,1,4,2,4,0,2,2,3,4,3,0,4,4,1,3,1,0,3,3,2,1,2,0 \end{aligned}$$

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 $a_n^{(2)} = 2a_{n-1}^{(2)} + 6a_{n-2}^{(2)}$ 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 $\gcd(c_k', m') = 1$ 且 $m' = 4$，對應新數列 $\{a_n^{(2)}\}: a_n^{(2)} = 1a_{n-1}^{(2)} + 3a_{n-2}^{(2)}$：

$$\begin{aligned} a_n^{(2)} &= 2a_{n-1}^{(2)} + 6a_{n-2}^{(2)} &&: \boxed{1,2,2,0,4},0,0,0\cdots \\ a_n^{(2)} &= 1a_{n-1}^{(2)} + 3a_{n-2}^{(2)} &&: 1,1,0,3,3,0 \end{aligned}$$

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) 式簡化為 $r_{j-1} \equiv 0 \pmod{m/c_k}$，又 $\gcd(c_1, c_2, \ldots, c_k, m) = d \Rightarrow d \mid c_k$，得到 $r_{j-1} \equiv 0 \pmod{m/d}$，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 $\{a_n^{(2)}\}: a_n^{(2)} = 2a_{n-1}^{(2)} + 4a_{n-2}^{(2)}$ 且 $m = 24$ 為例，此餘數數列為前週期數列。考慮 $c_2' = 2$，$m' = 12$ 但 $\gcd(c_k', m') = 2 \neq 1$ 且 $m' = 12$，對應新數列 $\{a_n^{(2)}\}: a_n^{(2)} = 1a_{n-1}^{(2)} + 2a_{n-2}^{(2)}$：

$$\begin{aligned} a_n^{(2)} &= 2a_{n-1}^{(2)} + 4a_{n-2}^{(2)} &&: \boxed{1,2,8,0},8,16,16,0,16,8,8,0 \\ a_n^{(2)} &= 1a_{n-1}^{(2)} + 2a_{n-2}^{(2)} &&: \boxed{1,2,8,0},8,4,4,0,4,8,8,0 \end{aligned}$$

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。 □

3.4 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：$\gcd(c_k, m) = 1$ 以及 $\gcd(c_k, m) \neq 1$，$\gcd(c_1, c_2, \ldots, c_k, m) \neq 1$。$k$ 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：$\gcd(c_k, m) \neq 1$，$\gcd(c_1, c_2, \ldots, c_k, m) \neq 1$。

定理 9： 設 $\gcd(c_k, m) \neq 1$ 且 $\gcd(c_1, \ldots, c_k) = \ell$，$m = \ell^t$ $(t \in \mathbb{N})$，則 k 階餘數數列在某項後均為 0。

證明. 令 $c_1 = \ell q_1$，$c_2 = \ell q_2$，$\cdots$，$c_k = \ell q_k$，其中 $\gcd(c_1, c_2, \ldots, c_k) = \ell$，$q_1$、$q_2$、$\cdots$、$q_k \in \mathbb{N}$，$\gcd(q_1, \ldots, q_k) = 1$，則

$$\begin{aligned}
a_n^{(k)} &= \ell(c_1' a_{n-1}^{(k)} + c_2' a_{n-2}^{(k)} + \cdots + c_k' a_{n-k}^{(k)}) \\
a_{n+k}^{(k)} &= \ell^2(c_1' a_{n+k-1}^{(k)} + c_2' a_{n+k-2}^{(k)} + \cdots + c_k' a_n^{(k)}) \\
&\vdots \\
a_{n+(t-1)k}^{(k)} &= \ell^t(c_1' a_{n+(t-1)k-1}^{(k)} + c_2' a_{n+(t-1)k-2}^{(k)} + \cdots + c_k' a_{n+(t-2)k}^{(k)})
\end{aligned}$$

其中 $c_1' = c_1/\ell$，$c_2' = c_2/\ell$，$\cdots$，$c_k' = c_k/\ell$。推知存在 $t \in \mathbb{N}$，使得 $a_{n+(t-1)k}^{(k)} \equiv 0 \pmod{m = \ell^t}$，因此，$k$ 階餘數數列在某項後均為 0。

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

$$1, 2, 0, 2, 0, 0, 4, 0, 0, \ldots, 0, 0$$，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 $\{a_n^{(2)}\}$：$a_n^{(2)} = 4a_{n-1}^{(2)} + 8a_{n-2}^{(2)}$ 且 $m = 16$ 為例：

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

□

4 由 $k-1$ 個不全為 0 均勻分割來區分循環週期列

4.1 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。觀察數列 $\{a_n^{(3)}\}$：$a_n^{(3)} = 3a_{n-1}^{(3)} + 5a_{n-2}^{(3)} + 8a_{n-3}^{(3)}$ 且 $m = 22$

中的 3 階餘數數列為

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

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

	$r_1^{(3)}$	$r_2^{(3)}$	$r_3^{(3)}$	$r_4^{(3)}$	$r_5^{(3)}$	$r_6^{(3)}$	$r_7^{(3)}$	$r_8^{(3)}$	$r_9^{(3)}$	$r_{10}^{(3)}$	$r_{11}^{(3)}$	$r_{12}^{(3)}$
$m=2$	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

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

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 5。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 $r_{11}^{(3)}$ 與 $r_{12}^{(3)}$ 的線性同餘方程組為

$$\begin{cases} r_{11}^{(3)} \equiv 1 \pmod 2 \\ r_{11}^{(3)} \equiv 0 \pmod{11} \end{cases} \quad \text{且} \quad \begin{cases} r_{12}^{(3)} \equiv 0 \pmod 2 \\ r_{12}^{(3)} \equiv 0 \pmod{11} \end{cases},$$

則由中國剩餘定理知 $r_{11}^{(3)} \equiv 11 \pmod{22}$ (餘數不為零) 及 $r_{12}^{(3)} \equiv 0 \pmod{22}$ (餘數為零)，因此，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 5 中 $s = 5$，$\ell_3(22) = 12 \Rightarrow \pi_3(22) = 5 \cdot 12 = 60$。

4.2 $\gcd(c_k, m) \neq 1$，$\gcd(c_1, c_2, \ldots, c_k, m) = 1$

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 $\gcd(c_k, m) \neq 1$，$\gcd(c_1, c_2, \ldots, c_k m) = 1$ 時，k 階餘數數列會是週期數列或前週期數列。

(a) 以 $\{a_n^{(2)}\}$：$a_n^{(2)} = 4a_{n-1}^{(2)} + 3a_{n-2}^{(2)}$ 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 $\{a_n^{(2)}\}$：$a_n^{(2)} = 4a_{n-1}^{(2)} + 3a_{n-2}^{(2)}$ 且 $m = 18$ 為例：

$$\boxed{1,4,1,16,13,10,7},4,1,16,13,10,7,$$

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 $\gcd(c_k,m)\neq 1$，則

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

(ii) 當 $\gcd(c_1,c_2,\ldots,c_k,m)=d$，$c_k'=c_k/d$，$m'=m/d$ 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 $(r_1^{(k)},r_{m^k+k}^{(k)})$ 中重複的相鄰 k 項為 $r_i^{(k)}=r_j^{(k)}$，$r_{i+1}^{(k)}=r_{j+1}^{(k)}$，$r_{i+2}^{(k)}=r_{j+2}^{(k)}$，$\ldots$，$r_{i+k-1}^{(k)}=r_{j+k-1}^{(k)}$。仿照性質 2 類推知

$$\begin{aligned} c_k r_{j-i}^{(k)} &\equiv r_{j-i+k}^{(k)}-c_1 r_{j-i+k-1}^{(k)}-c_2 r_{j-i+k-2}^{(k)}-\cdots-c_{k-1}r_{j-i+1}^{(k)} \pmod m \\ &\equiv r_k^{(k)}-c_1 r_{k-1}^{(k)}-c_2 r_{k-2}^{(k)}-\cdots-c_{k-1}r_1^{(k)}\equiv 0 \pmod m \end{aligned} \tag{2}$$

(i) 若 $\gcd(c_1,c_2,\ldots,c_k,m)=1$ 但 $\gcd(c_k,m)\neq 1$，可令 $\gcd(c_k,m)=d$，由同餘性質知 (2) 式為 $r_{j-1}^{(k)}\equiv 0 \pmod{m/c_k}$，所以 $r_{j-1}^{(k)}$ 為非負整數，但 $\{r_n^{(k)}\}$ 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 $\{a_n^{(2)}\}:a_n^{(2)}=8a_{n-1}^{(2)}+12a_{n-2}^{(2)}$ 且 $m=18$ 為例，此餘數數列為前週期數列。考慮 $c_2'=6$，$m'=9$ 但 $\gcd(c_k',m')=3\neq 1$ 且 $m'=9$，對應新數列 $\{a_n^{(2)}\}:a_n^{(2)}=4a_{n-1}^{(2)}+6a_{n-2}^{(2)}$：

$$\begin{aligned} \{a_n^{(2)}\}:a_n^{(2)}=8a_{n-1}^{(2)}+12a_{n-2}^{(2)} &: \boxed{1,8,4,2,14,16},8,4,2,10,14,16 \\ \{a_n^{(2)}\}:a_n^{(2)}=4a_{n-1}^{(2)}+6a_{n-2}^{(2)} &: \boxed{1},4,4,4,\ldots,4 \end{aligned}$$

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。

□

為了方便，將由 $k-1$ 個 0 均勻分割記作為 x_1、x_2、$\cdots$、r_{k-1}。

性質 6： 設 $\gcd(c_2,m)\neq 1$，若 2 階餘數數列中的週期循環列中由 x_i 均勻分割且 $r_i^{(2)}$ 為第 i 次由 x_1 均勻分割的 x_1 之前一項 $(1\leq i\leq s-1)$，則 $r_{i+j}^{(2)}\equiv\left[\!\left[r_{j+1}^{(2)}x_1+c_2 r_j^{(2)}r_{i-1}^{(2)}\right]\!\right] \pmod m$，其中 $j\in\mathbb{N}$。

證明. 令 $a_{i-1}^{(2)} = mq_1 + r_{i-1}^{(2)}$，$a_i^{(2)} = mq_2 + x_1$ $(q_1、q_2 \in \mathbb{N} \cup \{0\})$，則

$$
\begin{aligned}
a_{i+1}^{(2)} &= c_1(mq_2 + x_1) + c_2(mq_1 + r_{i-1}^{(2)}) = a_2^{(2)} \cdot (mq_2 + x_1) + c_2 a_1^{(2)} \cdot (mq_1 + r_{i-1}^{(2)}) \\
a_{i+2}^{(2)} &= a_3^{(2)} \cdot (mq_2 + x_1) + c_2 a_2^{(2)} \cdot (mq_1 + r_{i-1}^{(2)}) \\
a_{i+3}^{(2)} &= a_4^{(2)} \cdot (mq_2 + x_1) + c_2 a_3^{(2)} \cdot (mq_1 + r_{i-1}^{(2)}) \\
&\vdots \\
a_{i+j}^{(2)} &= a_{j+1}^{(2)} \cdot (mq_2 + x_1) + c_2 a_j^{(2)} \cdot (mq_1 + r_{i-1}^{(2)})，j \in \mathbb{N}。
\end{aligned}
$$

兩邊模 m 得到 $r_{i+j}^{(2)} \equiv \left[\!\left[r_{j+1}^{(2)} x_1 + c_2 r_j^{(2)} r_{i-1}^{(2)} \right]\!\right] \pmod{m}$，其中 $j \in \mathbb{N}$。 □

為了方便，定義 $r_\alpha + 1^{(2)}$ 為 2 階餘數數列中的第 1 段週期循環列由 x_1 均勻分割的 x_1 之位置，其中 $\alpha = \ell_2(m) - 1$。

定理 10： 設 $\gcd(c_2, m) \neq 1$，$\gcd(c_1, c_2, m) = 1$，則 $\pi_2(m) = s \cdot \ell_2(m)$，$s \mid \varphi(m)$。

證明. 仿照定理 4 與定理 5 來證明。令 $\alpha = \ell_2(m) - 1$，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

$$1, r_2^{(2)}, r_3^{(2)}, r_4^{(2)}, r_5^{(2)}, \ldots, r_\alpha^{(2)}, x_1 ;$$

第二段為

$$\left[\!\left[r_2^{(2)} x_1 + c_2 r_1^{(2)} r_\alpha^{(2)} \right]\!\right], \left[\!\left[r_3^{(2)} x_1 + c_2 r_2^{(2)} r_\alpha^{(2)} \right]\!\right], \ldots, \left[\!\left[x_1^2 + c_2 (r_\alpha^{(2)})^2 \right]\!\right], x_1 ;$$

第三段為

$$\left[\!\left[r_2^{(2)} x_1 + c_2 r_1^{(2)} x_1^2 + c_2^2 r_1^{(2)} (r_\alpha^{(2)})^2 \right]\!\right], \left[\!\left[r_3^{(2)} x_1 + c_2 r_2^{(2)} x_1^2 + c_2^2 r_2^{(2)} (r_\alpha^{(2)})^2 \right]\!\right], \ldots, \left[\!\left[x_1^2 + c_2 r_\alpha^{(2)} x_1^2 + c_2^2 (r_\alpha^{(2)})^3 \right]\!\right], x_1 ;$$

以此類推得第 s 段為

$$\left[\!\left[r_2^{(2)} x_1 + r_1^{(2)} x_1^2 \sum_{i=1}^{s-2} c_2^i (r_\alpha^{(2)})^{i-1} + c_2^{s-1} r_1^{(2)} (r_\alpha^{(2)})^{s-1} \right]\!\right], \ldots, \left[\!\left[x_1^2 + x_1^2 \sum_{i=1}^{s-2} c_2^i (r_\alpha^{(2)})^i + c_2^{s-1} (r_\alpha^{(2)})^s \right]\!\right], x_1 。$$

由二階 Cassini 恆等式知 $a_{\alpha-1}^{(2)} a_\alpha + 1^{(2)} - (a_\alpha^{(2)})^2 = (-1)^\alpha c_2^{\alpha-1}$。兩邊模 m 得

$$x_1 r_{\alpha-1} - (r_{\alpha-1}^{(2)})^2 \equiv (-1)^\alpha c_2^{\alpha-1} \pmod{m} 。 \tag{9}$$

(9) 式仿造定理 6 來證明，由鴿籠原理與高次剩餘知 (9) 式必有解且循環。

以二階線性遞迴數列 $\{a_n^{(2)}\}$：$a_n^{(2)} = 3a_{n-1}^{(2)} + 2a_{n-2}^{(2)}$ 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 $x_1 = 5$，$r_\alpha^{(2)} = r_{\alpha-1}^{(2)} = 9$ 滿足 (9) 式：$5 \cdot 9 - 9^2 \equiv (-1)^5 2^4 \pmod{10}$，所以 $36 \equiv 16 \pmod{10}$。又滿足循環長度

$$r_\alpha^{(2)} \to \left[\!\left[x_1^2 + c_2 (r_\alpha^{(2)})^2\right]\!\right] \to \cdots \to \left[\!\left[x_1^2 + x_1^2 \sum_{i=1}^{s-2} c_2^i (r_\alpha^{(2)})^i + c_2^{s-1} (r_\alpha^{(2)})^s\right]\!\right],$$

又回到 $r_\alpha^{(2)}$，得到 $s \mid \varphi(m)$，因此 $\pi_2(m) = s \cdot \ell_2(m)$，其中 $s \mid \varphi(m)$。 □

定理 11： 設 $\gcd(c_k, m) \neq 1$，若 k 階餘數數列中的週期循環列中由 $x_1 \text{、} \cdots \text{、} x_{k-1}$ 均勻分割且 $r_i^{(k)}$ 為第 i 次由 $x_1 \text{、} \cdots \text{、} x_{k-1}$ 均勻分割的 x_1 之前一項 $(1 \le i \le s-1)$，則

(i) 當 $k = 3$，$r_{i+j+1}^{(3)} \equiv \left[\!\left[r_{j+1}^{(3)} x_2 + c_2 r_j^{(3)} x_1 + c_3 (r_{j-1}^{(3)} x_1 + r_j^{(3)} r_{i-1}^{(3)})\right]\!\right] \pmod{m}$，其中 $j \in \mathbb{N}$。

(ii)
$$\begin{aligned} & r_{i+j+k+2}^{(k)} \\ \equiv & \left[\!\left[r_{j+1}^{(k)} x_{k-1} + \sum_{\ell_1=2}^{k-1} \left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} r_{j-\ell_1+\ell_2}^{(k)} x_{k-\ell_2}\right] + c_k \sum_{\ell=1}^{k-2} r_{j-\ell}^{(k)} x_\ell + c_k r_j^{(k)} r_{i-1}^{(k)}\right]\!\right] \end{aligned}$$
$\pmod{m}$，其中 $j \in \mathbb{N}$。

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

證明. (i) 令 $r_i^{(3)} \text{、} r_{i+1}^{(3)}$ 為在 $\{r_n^{(3)}\}$ 中第 i 次由 $x_1 \text{、} \cdots \text{、} x_{k-1}$ 均勻分割的 $x_1 \text{、} x_2$ 之位置 $(1 \le i \le s-1)$ 且 $a_{i-1}^{(3)} = mq_1 + r_{i-1}^{(3)}$，$a_i^{(3)} = mq_2 + x_1$，$a_{i+1}^{(3)} = mq_3 + x_2$ $(q_1 \text{、} q_2 \text{、} q_3 \in \mathbb{N} \cup \{0\})$，則

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

$j \in \mathbb{N}$。兩邊模 m 得到

$$r^{(3)}_{i+j+1} \equiv \left[\!\left[r^{(3)}_{j+1}x_2 + c_2 r^{(3)}_j x_1 + c_3(r^{(3)}_{j-1}x_1 + r^{(3)}_j r^{(3)}_{i-1}) \right]\!\right] \pmod m$$，其中 $j \in \mathbb{N}$。

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

$$\begin{aligned} r^{(4)}_{i+j+2} \equiv \Big[\!\Big[& r^{(4)}_{j+1}x_3 + c_2 r^{(4)}_j x_2 + c_3(r^{(4)}_{j-1}x_1 + r^{(4)}_{j-1}x_2) \\ & + c_4(r^{(4)}_{j-1}x_1 + r^{(4)}_j x_2) + c_4 r^{(4)}_j r^{(4)}_{i-1} \Big]\!\Big] \pmod m, \end{aligned}$$

其中 $j \in \mathbb{N}$。為了方便寫成

$$\begin{aligned} r^{(4)}_{i+j+4-2} \equiv \Bigg[\!\Bigg[& r^{(4)}_{j+1}x_3 + \sum_{\ell_1=2}^{3}\left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} r^{(4)}_{j-\ell_1+\ell_2}x_{4-\ell_2} \right] \\ & + c_4 \sum_{\ell=1}^{2} r^{(4)}_{j-\ell}x_\ell + c_4 r^{(4)}_j r^{(4)}_{i-1} \Bigg]\!\Bigg] \pmod m。 \end{aligned}$$

同理類推至 k 階餘數數列的情形，推得

$$\begin{aligned} r^{(k)}_{i+j+k-2} \equiv \Bigg[\!\Bigg[& r^{(k)}_{j+1}x_{k-1} + \sum_{\ell_1=2}^{k-1}\left[c_{\ell_1} \sum_{\ell_2=2}^{\ell_1} r^{(k)}_{j-\ell_1+\ell_2}x_{k-\ell_2} \right] \\ & + c_k \sum_{\ell=1}^{k-2} r^{(k)}_{j-\ell}x_\ell + c_k r^{(k)}_j r^{(k)}_{i-1} \Bigg]\!\Bigg] \pmod m。 \end{aligned}$$

(iii) 仿照定理 10 證明，$\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \mid \varphi(m)$。

□

4.3 退化情形：在某項後皆為不為 0 的常數

在 $\gcd(c_k, m) \neq 1$ 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：$\gcd(c_k, m) \neq 1$，$\gcd(c_1, c_2, \ldots, c_k, m) = 1$ 及 $\gcd(c_1, c_2, \ldots, c_k, m) \neq 1$，$\gcd(c'_k, m') \neq 1$。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 $\{a^{(5)}_n\}$：$a^{(5)}_n = a^{(5)}_{n-1} + 2a^{(5)}_{n-2} + 2a^{(5)}_{n-3} + 2a^{(5)}_{n-4} + 2a^{(5)}_{n-5}$ 且 $m = 2$ 為例：$1, 1, 1, 1, \ldots$ 為週期數列，及以 $\{a^{(2)}_n\}$：$a^{(2)}_n = 3a^{(2)}_{n-1} + 2a^{(2)}_{n-2}$ 且 $m = 4$ 為例：$\boxed{1}, 3, 3, 3, 3, \ldots$，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。

5 探討數列的因倍數性質

5.1 2 階數列的因倍數定理

定理 12： 設 $\{a_n^{(2)}\}$ 為二階線性遞迴數列，則

(i) 對於任意正整數 m 與 n ，當 $c_1 = 1$、$c_2 \in \mathbb{N}$ 時，則

$$a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} a_n^{(2)} \text{ 且 } a_n^{(2)} \mid a_{mn}^{(2)} \text{。}$$

(ii) 對於任意正整數 m 與 n ，當 $c_1 \in \mathbb{N}$、$c_2 = 1$ 時，則

$$a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + a_{m-1}^{(2)} a_n^{(2)} \text{ 且 } a_n^{(2)} \mid a_{mn}^{(2)} \text{。}$$

(iii) 對於任意正整數 m 與 n ，當 $c_1 \in \mathbb{N} \setminus \{1\}$、$c_2 \in \mathbb{N}$ 時，則

$$a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} a_n^{(2)} \text{ 且 } a_n^{(2)} \mid a_{mn}^{(2)} \text{。}$$

證明. (i) 由於

$$\begin{aligned} a_{m+n}^{(2)} &= a_{m+n-1}^{(2)} + c_2 a_{m+n-2}^{(2)} = a_2^{(2)} a_{m+n-1}^{(2)} + a_1^{(2)} \cdot c_2 a_{m+n-2}^{(2)} \ (\because\ a_1^{(2)} = a_2^{(2)} = 1) \\ &= (c_2 a_1^{(2)} + a_2^{(2)}) a_{m+n-2}^{(2)} + c_2 a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= a_3^{(2)} \cdot a_{m+n-2}^{(2)} + c_2 a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= \cdots = a_m^{(2)} \cdot a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} \cdot a_n^{(2)} \end{aligned}$$

所以 $a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} a_n^{(2)}$。又 $a_{mn}^{(2)} = a_{n+(m-1)n}^{(2)} = a_{(m-1)n}^{(2)} a_{n+1}^{(2)} + c_2 a_{(m-1)n-1}^{(2)} a_n^{(2)}$，推導

$$\begin{aligned} a_{mn}^{(2)} &\equiv a_{(m-1)n}^{(2)} a_{n+1}^{(2)} + c_2 a_{(m-1)n-1}^{(2)} a_n^{(2)} && \pmod{a_n^{(2)}} \\ &\equiv a_{(m-1)n}^{(2)} a_{n+1}^{(2)} && \pmod{a_n^{(2)}} \\ &\equiv a_{(m-2)n}^{(2)} (a_{n+1}^{(2)})^2 && \pmod{a_n^{(2)}} \\ &\equiv \cdots \equiv a_n^{(2)} (a_{n+1}^{(2)})^{m-1} && \pmod{a_n^{(2)}} \\ &\equiv 0 && \pmod{a_n^{(2)}} \text{。} \end{aligned}$$

因此，對於任意正整數 m 與 n，$a_n^{(2)} \mid a_{mn}^{(2)}$。

(ii) 由於

$$\begin{aligned} a_{m+n}^{(2)} &= c_1 a_{m+n-1}^{(2)} + a_{m+n-2}^{(2)} \\ &= a_2^{(2)} \cdot a_{m+n-1}^{(2)} + a_1^{(2)} a_{m+n-2}^{(2)} \ (\because\ a_1^{(2)} = 1, a_2^{(2)} = c_1) \\ &= (a_1^{(2)} + c_1 a_2^{(2)}) a_{m+n-2}^{(2)} + a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= a_3^{(2)} \cdot a_{m+n-2} + a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= \cdots = a_m^{(2)} \cdot a_{n+1}^{(2)} + a_{m-1}^{(2)} \cdot a_n^{(2)}\ , \end{aligned}$$

所以 $a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + a_{m-1}^{(2)} a_n^{(2)}$。又 $a_{mn}^{(2)} = a_{n+(m-1)n}^{(2)} = a_{(m-1)n}^{(2)} a_{n+1}^{(2)} + a_{(m-1)n-1}^{(2)} a_n^{(2)}$，同理可證，對於任意正整數 m 與 n，$a_n^{(2)} \mid a_{mn}^{(2)}$。

(iii) 由於

$$\begin{aligned} a_{m+n}^{(2)} &= c_1 a_{m+n-1}^{(2)} + c_2 a_{m+n-2}^{(2)} \\ &= a_2^{(2)} \cdot a_{m+n-1}^{(2)} + a_1^{(2)} \cdot c_2 a_{m+n-2}^{(2)} \ (\because\ a_1^{(2)} = 1, a_2^{(2)} = c_1) \\ &= c_2 a_1^{(2)} + c_1 a_2^{(2)} a_{m+n-2}^{(2)} + c_2 a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= a_3^{(2)} \cdot a_{m+n-2}^{(2)} + c_2 a_2^{(2)} \cdot a_{m+n-3}^{(2)} \\ &= \cdots = a_m^{(2)} \cdot a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} \cdot a_n^{(2)}\ , \end{aligned}$$

所以 $a_{m+n}^{(2)} = a_m^{(2)} a_{n+1}^{(2)} + c_2 a_{m-1}^{(2)} a_n^{(2)}$。又 $a_{mn}^{(2)} = a_{n+(m-1)n}^{(2)} = a_{(m-1)n}^{(2)} a_{n+1}^{(2)} + c_2 a_{(m-1)n-1}^{(2)} a_n^{(2)}$，同理可證，對於任意正整數 m 與 n，$a_n^{(2)} \mid a_{mn}^{(2)}$。

□

5.2 k 階線性遞迴數列的因倍數定理

定理 13： 設 $\{a_n^{(2)}\}$ 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 $m \mid a_{n\cdot \ell_k(m)-i}^{(k)}$ 且 $m \mid a_{n\cdot \pi_k(m)-i}^{\pi}$，其中 $i = 0, 1, 2, \ldots, k-2$。

(ii) 若 $c_k \neq 1$，$\gcd(c_k', m') \neq 1$ 但 $m \neq [\gcd(c_1, c_2, \ldots, c_k)]^u$，則存在 $i \in \{0, 1, 2, \ldots, k-2\}$ 使得 $m \nmid a_{n\cdot \ell_k(m)-i}^{(k)}$ 且 $m \nmid a_{n\cdot \pi_k(m)-i}^{\pi}$。

(iii) 若 $c_k \neq 1$，$\gcd(c_k', m') \neq 1$ 但 $m = [\gcd(c_1, c_2, \ldots, c_k)]^u$，則存在 $n' \leq n$，使得 $\left[\!\left[a_{n'+j}^{(k)}\right]\!\right] \equiv 0 \pmod{m}$，其中 $j \in \mathbb{N} \cup \{0\}$。

證明. (i) 若 $c_k = 1$ 或 $c_k \neq i$，$\gcd(c_k', m') = 1$，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 $\underbrace{0,0,\ldots,0}_{k-1個}$ 均勻分割的情形，所以對於任意正整數 n，$\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \in \mathbb{N}$，即 $m \mid a^{\pi}_{n\cdot\ell_k(m)}$，$m \mid a^{\pi}_{n\cdot\ell_k(m)-1}$，$\cdots$，$m \mid a^{\pi}_{n\cdot\ell_k(m)-k+2}$ 及 $m \mid a^{\pi}_{n\cdot\pi_k(m)}$，$m \mid a^{\pi}_{n\cdot\pi_k(m)-1}$，$\cdots$，$m \mid a^{\pi}_{n\cdot\pi_k(m)-k+2}$，因此 $m \mid a^{\pi}_{n\cdot\ell_k(m)-i}$ 且 $m \mid a^{\pi}_{n\cdot\pi_k(m)-i}$，其中 $i = 0,1,\ldots,k-2$。

(ii) 若 $c_k \neq 1$，$\gcd(c_k', m') \neq 1$ 但 $m \neq [\gcd(c_1, c_2, \ldots, c_k)]^u$，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，$\pi_k(m) = s \cdot \ell_k(m)$，其中 $s \in \mathbb{N}$，即 $a^{(k)}_{n\cdot\ell_k(m)} \equiv x_1 \pmod{m}$，$a^{(k)}_{n\cdot\ell_k(m)-1} \equiv x_2 \pmod{m}$，$\cdots$，$a^{(k)}_{n\cdot\ell_k(m)-k+2} \equiv x_{k-1} \pmod{m}$ 及 $a^{(k)}_{n\cdot\pi_k(m)} \equiv x_1 \pmod{m}$，$a^{(k)}_{n\cdot\pi_k(m)-1} \equiv x_2 \pmod{m}$，$\cdots$，$a^{(k)}_{n\cdot\pi_k(m)-k+2} \equiv x_{k-1} \pmod{m}$，因此，對於任意正整數 n，存在 $i \in \{0,1,2,\ldots,k-2\}$ 使得 $m \nmid a^{(k)}_{n\cdot\ell_k(m)-i}$ 且 $m \nmid a^{\pi}_{n\cdot\pi_k(m)-i}$。

(iii) 若 $c_k \neq 1$，$\gcd(c_k', m') \neq 1$ 但 $m = [\gcd(c_1, c_2, \ldots, c_k)]^u$，則由定理 10 知 k 階餘數數列在某項後均為 0，因此，存在正整數 $n' \leq n$，使得 $\left[\!\left[a^{(k)}_{n'+j}\right]\!\right] \equiv 0 \pmod{m}$，其中 $j \in \mathbb{N} \cup \{0\}$。

□

6 結論

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 k 階 Cassini 恆等式、歐拉-費馬定理與高次剩餘論證出 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。

參考資料 (Reference)

[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 Thesis, The University of Arizona, Tucson, USA, 2007.