數學算板中多元輾轉相除法直式算則及其延伸補遺

林保平

台北市立教育大學數學系退休

壹、前言

林（民 110）曾描述多重輾轉轉相除法及多元輾轉轉相除法直式算則，「多重」是指透過 $\gcd(c_1,c_2,c_3,\dots c_n)=\gcd(\gcd(\dots(\gcd(\gcd(c_1,c_2),c_3),\dots,c_{n-1}),c_n)$ 的方式，連續作多次的兩數輾轉相除法；「多元」是指透過多個數同時參與的輾轉相除法。本文將對多元輾轉轉相除法直式算則作更近一步的改進，並討論其延伸的後推法的原理及算則，此外，我們也根據 Lehmer(1919)的討論，探討第二種解線性不定方程式整數一般解的「多元輾轉模餘推演法則」及其延伸的前推法與後推法。對於類似歐拉(Euler)透過線性不定方程式列出聯立方程組，再求其一般解的程式及原理，我們也做一些討論。

貳、多元除法及其直式算則

整數除法原理　(Boute,1992)

設$a,b\in\mathbb{Z},b\neq 0,\ \exists!\ q,r\in\mathbb{Z}\ \ni a=bq+r,\ 0\leq r<|b|$。

此除法原理被稱為歐幾里得除法（Euclid division），我們說被除數a除以除數b，得商q 餘數r。由於 $r=a\ (mod\ |b|)$，我們也稱r為模餘，此除法也稱為模餘除法。本文中所說的除法就是這個除法。本文討論除法時，常會規定除數為 0 時，商為 0，餘數為a。亦即 $a\ (mod\ 0)=a$。

多元整數除法原理

設 $c_1,c_2,c_3,\dots c_k$為整數，將c_1除以c_2得商q_1及餘數，再將餘數除以c_3得商q_2及餘數，依序做下去，最後將餘數除以c_k得商q_k餘數為r，若除數為 0 時規定商為 0，餘數續用，此時我們可得

$c_1=\ c_2q_1+c_3q_2+\cdots+c_kq_{k-1}+r,\quad 0\leq r<|c_i|$。我們稱此除法為**多元($k$元)的除法**(multiple number division)，$q_1,q_2,\dots,q_{k-1}$稱為商列，r為餘數。

由於$c_1 = c_2q_1 + c_3q_2 + \cdots + c_kq_{k-1} + r$，若 d為$c_2, c_3, \ldots c_k, r$的公因數，則d為c_1的因數，亦即d為$c_1, c_2, c_3, \ldots c_k$的公因數，反之，若$d$為$c_1, c_2, c_3, \ldots c_k$的公因數，由於$r = c_1 - c_2q_1 - c_3q_2 - \cdots - c_kq_{k-1}$，故$d$為$r$的因數，亦即 d為$c_2, c_3, \ldots c_k, r$的公因數，因此，對多元的除法類似式子，我們有下列「多元除法」的最大公因數定理：

設 $c_1, c_2, c_3, \ldots c_k$為整數，

若存在 q_i，$r \in \mathbb{Z}$ $\ni c_1 = c_2q_1 + c_3q_2 + \cdots + c_kq_{k-1} + r$

則 $\gcd(c_1, c_2, c_3, \ldots c_k) = \gcd(c_2, c_3, \ldots c_k, r)$。

設 $c_1, c_2, c_3, \ldots c_k$為正整數，令$a_{1-k} = c_1, a_{2-k} = c_2, \ldots, a_{i-k} = c_i, \ldots, a_{-1} = c_{k-1}, a_0 = c_k$亦即令$a_{j-k} = c_j$，$j = 1,2, \ldots, k$ 且

對 a 數列的前k項$a_{i-k}, a_{i-k+1}, \ldots, a_{i-2}, a_{i-1}$作多元的除法得商$q_{1i}, q_{2i}, \ldots, q_{(k-1)i}$，餘數令其為 a_i，作遞迴定義，

$a_i = a_{i-k} - a_{i-k+1}q_{1i} - \cdots - a_{i-1}q_{(k-1)i}$，其中 $0 < a_i < a_j$，$j < i$。

則存在 $n \in \mathbb{N}, \ni a_n \neq 0$，$a_{n+j} = 0$，$j = 1,2, \ldots, k-1$，

其中 $i = 1,2, \ldots n, n+1, \ldots, n+k-1$

這樣的過程，我們稱為**多元輾轉相除法**(multiple number Euclidean Algorithm)。由於

$\gcd(c_1, c_2, c_3, \ldots c_k) = \gcd(c_2, c_3, \ldots c_k, a_1) = \cdots = \gcd(a_{n-k+1}, \ldots a_{n-1}, a_n)$

$= \cdots = \gcd(a_{n-1}, a_n, 0, \ldots, 0) = \gcd(a_n, 0, \ldots, 0) = a_n$，因此我們可得到下列定理：

多元輾轉相除法原理

設 $c_1, c_2, c_3, \ldots c_k$為正整數，作多元輾轉相除法，則 $a_n = \gcd(c_1, c_2, c_3, \ldots c_k)$

圖 1 展示的就是數學算板中，8913、5677、4373 三數的三元輾轉相除法直式算則實例。

圖 1：多元輾轉相除法直式算則

圖中的a行前k個元素就是$c_1, c_2, c_3, \dots c_k$，a行輾轉相除，最後一個非零元數，就是最大公因數，圖中$q_1, q_2, \dots, q_{k-1}$等行就是商列構成的行。數學算板中，可在上方輸入兩個或兩個以上的整數，求這些數的最大公因數，並列出其商。圖中的多元除法算式行，展示的是商行中每一列的商相關的多元除法式子。數學算板可選擇呈現或隱藏算式行。圖中「重啟」按鈕可以清除所有內容只呈現輾轉相除得起始元（圖中的一二三列），「依序輾轉」按鈕可依序向下一列一列的算出及呈現每一個多元除法得商列，按右鍵，可以回到上一列。 輸入的數若只有兩個，就是兩數的輾轉相除，因此，二元的輾轉相除法直式算則是多元輾轉相除法直式算則的特例。

參、整係數線性 n 元不定方程式的整數一般解

設$c_1x_1 + c_2x_2 \dots + c_nx_n = d$為整係數線性 n 元不定方程式，設d 為$c_i$的最大公因數,由於

$A = \begin{bmatrix} \alpha_{11}\alpha_{12}\alpha_{13} \cdots \alpha_{1n} \\ \alpha_{21}\alpha_{22}\alpha_{23} \cdots \alpha_{2n} \\ \vdots \\ \alpha_{n1}\alpha_{n2}\alpha_{n3} \cdots \alpha_{nn} \end{bmatrix}$為一、三類基本矩陣(注 1)的乘積 $\Leftrightarrow \det(A) = \pm 1$

我們可將「整係數線性 n 元不定方程式的整數一般解定理」(林，民 110)，改寫為：

設 $\boldsymbol{c_1x_1 + c_2x_2 \dots + c_nx_n = dr}$，$\boldsymbol{c_i, d, r \in \mathbb{Z}}$ 為線性 n 元不定方程式，d為c_i的最大公因數，

若$\boldsymbol{A = \begin{bmatrix} \alpha_{11}\alpha_{12}\alpha_{13} \cdots \alpha_{1n} \\ \alpha_{21}\alpha_{22}\alpha_{23} \cdots \alpha_{2n} \\ \vdots \\ \alpha_{n1}\alpha_{n2}\alpha_{n3} \cdots \alpha_{nn} \end{bmatrix}}$，$\boldsymbol{\alpha_{ij} \in \mathbb{Z}}$ 且 $\boldsymbol{|det(A)| = 1}$ ， $\boldsymbol{\mathbf{A}\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix}}$

則 $\boldsymbol{c_1x_1 + c_2x_2 \dots + c_nx_n = dr, r \in \mathbb{Z}}$的一般解為

$$\begin{cases} x_1 = \alpha_{11}r + \alpha_{21}t_2 + \alpha_{31}t_3 + \cdots + \alpha_{n1}t_n \\ x_2 = \alpha_{12}r + \alpha_{22}t_2 + \alpha_{32}t_3 + \cdots + \alpha_{n2}t_n \\ \vdots \\ x_n = \alpha_{1n}r + \alpha_{2n}t_2 + \alpha_{3n}t_3 + \cdots + \alpha_{nn}t_n \end{cases} t_i \in \mathbb{Z}, i = 2, 3, \cdots, n$$ ，亦即

$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = A^t \begin{bmatrix} r \\ t_2 \\ \vdots \\ t_n \end{bmatrix}$，$A^t$稱為該不定方程式的解係數矩陣。

肆、延伸的多元輾轉相除前推法的直式算則及後推法

圖 2 是數學算板解$8913x + 5677y + 4378z = r$ 的舊直式算則前推法實例(林,民 110),圖中前四行其實只是為協助計算商列而呈現的。中間三行(d, q_1, q_2)就是我們前述的多元輾轉相除法直式算則。後面三行,其實就是「多元輾轉相除法」的延伸行(解行)。

延伸的輾轉相除直式算則III

8913, 5677, 4378

a	b	c	d	q_1	q_2	x	y	z
			8913			1	0	0
			5677			0	1	0
			4378			0	0	1
8913	5677	4378	3236	1	0	1	-1	0
5677	4378	3236	1299	1	0	0	1	-1
4378	3236	1299	1142	1	0	-1	1	1
3236	1299	1142	638	2	0	1	-3	2
1299	1142	638	157	1	0	1	0	-2
1142	638	157	33	1	3	-5	4	5
638	157	33	10	4	0	-3	-3	10
157	33	10	5	4	2	27	-10	-42
33	10	5	3	3	0	4	13	-25
10	5	3	0	2	0	-57	17	94
5	3	0	2	1	0	23	-23	-17
3	0	2	1	0	1	-19	36	-8
0	2	1	0	0	0	-57	17	94
2	1	0	0	2	0	61	-95	-1

圖 2:林(民 110)中延伸多元的輾轉相除直式算則實例

我們將圖 2 前三行省略簡化成圖 3,就是新的延伸的多元輾轉相除法直式算則。

線性不定方程式的一般解I

係數 gcd | 直式算則 | 一般解 | 增廣矩陣推演 | 重啟 | 前推法進退 | 全部隱藏

延伸的多元輾轉相除法直式算則—前推法

8913, 5677, 4378

a	q_1	q_2	x	y	z
8913			1	0	0
5677			0	1	0
4378			0	0	1
3236	1	0	1	-1	0
1299	1	0	0	1	-1
1142	1	0	-1	1	1
638	2	0	1	-3	2
157	1	0	1	0	-2
33	1	3	-5	4	5
10	4	0	-3	-3	10
5	4	2	27	-10	-42
3	3	0	4	13	-25
0	2	0	-57	17	94
2	1	0	23	-23	-17
1	0	1	-19	36	-8
0	0	0	-57	17	94
0	2	0	61	-95	-1

圖 3:簡化版延伸多元的輾轉相除法前推法直式算則

若輸入不同個數的整數時，整個延伸輾轉會重新計算展現。對延伸的N元輾轉相除，按鈕「重啟」可以將畫面資料隱藏，只留下前N列。按鈕「依序輾轉」為連續按鈕，按左鍵依序呈現下一行，按右鍵會回覆到前一行。同樣的，這個延伸多元輾轉相除法直式算則是一般化的延伸輾轉相除法。

以三元為例，要解$c_1x + c_2y + c_3z = dr, r \in \mathbb{Z}$，其中$d = \gcd(c_1, c_2, c_3)$，由林（民 110）及前多元的輾轉相除法假設，我們知道x, y, z行計算的規則是：

令 $\begin{bmatrix} x_{-2} & y_{-2} & z_{-2} \\ x_{-1} & y_{-1} & z_{-1} \\ x_0 & y_0 & z_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ，且

$$\begin{cases} x_i = x_{i-3} - x_{i-2}q_{1i} - x_{i-1}q_{2i} \\ y_i = y_{i-3} - y_{i-2}q_{1i} - y_{i-1}q_{2i} \\ z_i = z_{i-3} - z_{i-2}q_{1i} - z_{i-1}q_{2i} \end{cases}, \quad i = 1,2,\cdots,n,n+1,n+2 \quad ,$$

其中$d = a_n \neq 0$，$a_{n+1} = 0, a_{n+2} = 0$ ，以矩陣的方式來描述時就是：

$$[x_i y_i z_i] = [1 \quad -q_{1i} \quad -q_{2i}] \begin{bmatrix} x_{i-3} & y_{i-3} & z_{i-3} \\ x_{i-2} & y_{i-2} & z_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} \end{bmatrix} \qquad [1]$$

$$\begin{bmatrix} x_{i-2} & y_{i-2} & z_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} \\ x_i & y_i & z_i \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -q_{1i} & -q_{2i} \end{bmatrix} \begin{bmatrix} x_{i-3} & y_{i-3} & z_{i-3} \\ x_{i-2} & y_{i-2} & z_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} \end{bmatrix} \qquad [2]$$

其中 $E_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -q_{1i} & -q_{2i} \end{bmatrix}$,$i = 1,2,\cdots,n,n+1,n+2$為第一，三類基本列運算的合成，亦即$|\det(E_i)| = 1$,由於E_i的元素均為整數，故知 E_i^{-1}的元素也均為整數。[2]式也說明了前述直式算則可以一列一列的往下推演，而列成直式算則。再令

$$A_i = \begin{bmatrix} x_{i-2} & y_{i-2} & z_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} \\ x_i & y_i & z_i \end{bmatrix}, i = 0,1,2,\cdots,n,n+1,n+2$$，則[2]可記為

$A_i = E_i A_{i-1}, i = 1,2,\cdots,n$。 亦即 $A_n = E_n E_{n-1} \ldots E_1 A_0 = E_n E_{n-1} \ldots E_1$ 為第一，三類基本矩陣的乘積，且 $A_n \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} a_n \\ 0 \\ 0 \end{bmatrix}$。圖 2 中 $A_{14} = \begin{bmatrix} -19 & 36 & -8 \\ -57 & 17 & 94 \\ 61 & -95 & -1 \end{bmatrix}$，由整係數線性 n 元不定方程式的整數一般解定理知，$8913x + 5677y + 4378z = r$ 的一般解為

$$\begin{cases} x = -19r - 57s + 61t \\ y = \ 36r \ \ + 17s - 95t \\ z = -8r \ \ + \ 94s \ \ - t \end{cases} \quad s,t \in \mathbb{Z}$$

Lehmer（1941）曾提出後推法的算則，這個方法可以容易地透過前推法予以驗證。圖 4 展示的是數學算板的延伸多元的輾轉相除後推法的算則實例。圖 3 與圖 4 的差異只在延伸行（解行），最上方及最下方均為預設的單位矩陣構成的列，前者由上至下，後者由下至上一列一列地計算。

線性不定方程式的一般解II

係數 gcd | 直式算則 | 一般解 | 辯識矩陣推演 | 重啟後推 | 後推法進退 | 全部隱藏

延伸的多元輾轉相除直式算則—後推法

8913, 5677, 4378

a	q_1	q_2	x	y	z
8913					
5677					
4378					
3236	1	0	8913	796	3520
1299	1	0	5677	507	2242
1142	1	0	4378	391	1729
638	2	0	3236	289	1278
157	1	0	1299	116	513
33	1	3	1142	102	451
10	4	0	638	57	252
5	4	2	157	14	62
3	3	0	33	3	13
0	2	0	10	1	4
2	1	0	5	0	2
1	0	1	3	0	1
0	0	0	0	1	0
0	2	0	2	0	1
			1	0	0
			0	1	0
			0	0	1

圖 4:延伸多元的輾轉相除後推法的算則實例

仍以三元為例，要解$c_1x + c_2y + c_3z = dr, r \in \mathbb{Z}$，其中$d = \gcd(c_1, c_2, c_3)$，後推法的列計算規則是：

$$\begin{bmatrix} x_{n+3} & y_{n+3} & z_{n+3} \\ x_{n+4} & y_{n+4} & z_{n+4} \\ x_{n+5} & y_{n+5} & z_{n+5} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{且}$$

$$\begin{cases} x_i = x_{i+1}q_{1i} + x_{i+2}q_{2i} + x_{i+3} \\ y_i = y_{i+1}q_{1i} + y_{i+2}q_{2i} + y_{i+3} \\ z_i = z_{i+1}q_{1i} + z_{i+2}q_{2i} + z_{i+3} \end{cases} ,i = 1,2,\cdots,n,n+1,n+2 \quad ,$$

其中$d = a_n \neq 0$且 $a_{n+1} = 0, a_{n+2} = 0$ ，以矩陣的方式來描述時，

$$[x_i \;\; y_i \;\; z_i] = [q_{1i} \;\; q_{2i} \;\; 1] \begin{bmatrix} x_{i+1} & y_{i+1} & z_{i+1} \\ x_{i+2} & y_{i+2} & z_{i+2} \\ x_{i+3} & y_{i+3} & z_{i+3} \end{bmatrix} \quad [3]$$

$$\begin{bmatrix} x_i & y_i & z_i \\ x_{i+1} & y_{i+1} & z_{i+1} \\ x_{i+2} & y_{i+2} & z_{i+2} \end{bmatrix} = \begin{bmatrix} q_{1i} & q_{2i} & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_{i+1} & y_{i+1} & z_{i+1} \\ x_{i+2} & y_{i+2} & z_{i+2} \\ x_{i+3} & y_{i+3} & z_{i+3} \end{bmatrix} \quad [4]$$

其中$E'_i = \begin{bmatrix} q_{1i} & q_{2i} & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ ，$i = 1,2,\cdots,n,n+1,n+2$

令

$B_i = \begin{bmatrix} x_i & y_i & z_i \\ x_{i+1} & y_{i+1} & z_{i+1} \\ x_{i+2} & y_{i+2} & z_{i+2} \end{bmatrix}$ ，$i = 1,2,\ldots,n,n+1,n+2,n+31,n+2,n+3$ ，則[4]可記為

$B_i = E'_i B_{i+1}$ ，$i = 1,2,\cdots,n$，亦即 $B_1 = E'_1 E'_2 \ldots E'_n B_{n+1} = E'_1 E'_2 \ldots E'_n$，

B_1 就是我們後推法的結果矩陣。而矩陣公式[4]，也證明了在解行，我們可以一列一地由後方（下方）向前方（上方）推演。

由前推法我們知道前推法的結果矩陣 $A_n = E_n E_{n-1} \ldots E_1$ 故 $B_1 A_n = E'_1 E'_2 \ldots E'_n E_n E_{n-1} \ldots E_1$

由於$E'_i E_i = \begin{bmatrix} q_{1i} & q_{2i} & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -q_{1i} & -q_{2i} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $i = 1,2,\ldots,n$

故知$B_1 A_n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$，故 $A_n = {B_1}^{-1}$，這告訴我們，由後推法算出的解行結果矩陣的反置矩陣${B_1}^t$，其實並不是不定方程式的解係數矩陣,，$({B_1}^{-1})^{\mathrm{t}} = {A_n}^t$才是解係數矩陣。數學算板的程式，另有「一般解」按鈕，可以直接求出B_1的反矩陣，再由此求出一般解。圖 5 展示的就是圖 4 的例中，$8913x + 5677y + 4378z = r$的「一般解」按鈕列出的結果。因此延伸的多元輾轉相除法的後推法，在解線性不定方程式來看，應是略遜於前推法。

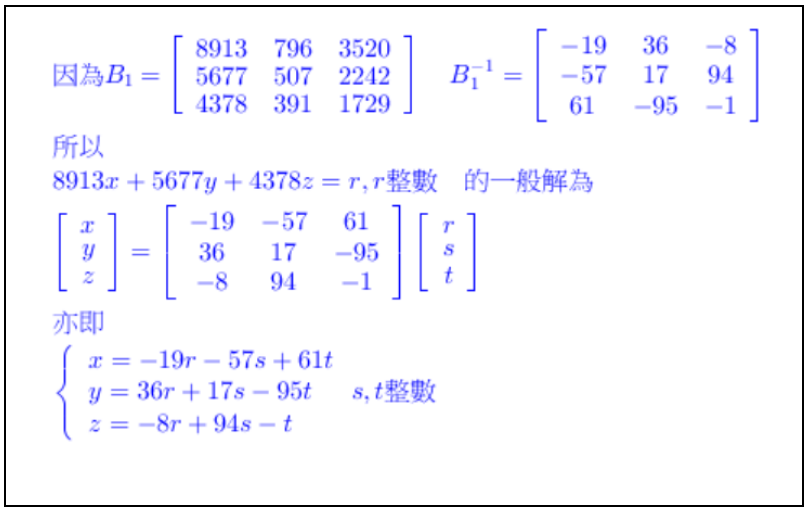

圖 5:示圖 4 例題「一般解」按鈕列出的結果

五、多元輾轉模餘推演算則及其延伸

其實除了多元輾轉相除法可以延伸求出線性不定方程的整數一般解外，「整係數線性 n 元不定方程式的整數一般解定理」其實告訴我們，只要能生成定理條件中的 A 矩陣的算則都可以求出一般解。Lehmer(1919) 就曾使用「多元輾轉正模餘推演」(取正是為了避開模數為零的狀況)於其線性不定方程式的一般解算則中。數學算板修改正模餘推演如下：

設 $c_1, c_2, c_3, \dots c_k$為整數，若

（1） $c_1 \neq 0$，將$c_2, c_3, \dots, c_k$分別除以c_1得餘數$r_1, r_2, \dots, r_{k-1}$，商列$q_1, q_2, \dots, q_{k-1}$，

其中$0 \le r_i < |c_1|,\ i = 1,2, \dots, k-1$

（2） $c_1 = 0$，取$q_i = 0,\ r_i = c_{i+1},\ i = 1,2, \dots, k-1$。

令 $r_k = c_1$。這樣，將$c_1, c_2, c_3, \dots c_k$推至$r_1, r_2, \dots, r_k$，得商列$q_1, q_2, \dots, q_{k-1}$之過程，我們特別稱之為多元模餘推演 (multiple modulo remainder deducing)。

設$a_{j1} = c_j, j = 1,2, \dots, k$, 將數列$a_{j1}$作多元模餘推演,令其結果為數列$a_{j2}, j = 1,2, \dots, k$商列$q_{11}, q_{21}, \dots, q_{(k-1)1}$ ，作遞迴定義將數列$a_{ji}, j = 1,2, \dots, k$對$i$作多元模餘推演，得餘數列$a_{j(i+1)}$，商列為$q_{1i}, q_{2i}, \dots, q_{(k-1)i}$，當$i = n-1$ （餘數列為第n列$a_{1n}, a_{2n}, \dots, a_{kn}$）且$\frac{a_{2n}}{a_{1n}}, \frac{a_{3n}}{a_{1n}}, \dots, \frac{a_{kn}}{a_{1n}}$ 均為整數時，遞迴停止。此時再取此整數列 $\frac{a_{2n}}{a_{1n}}, \frac{a_{3n}}{a_{1n}}, \dots, \frac{a_{kn}}{a_{1n}}$為第$n$列的商列,故 $0,0, \dots, a_{1n}$為餘數列(第 n+1 列)。這樣的過程稱為多元輾轉模餘推演算則。不難看出此算則有終止的時候，且$d = a_{1n} = \gcd(c_1, c_2, c_3, \dots c_k)$。在遞迴定義時，餘數有時會是零，此時就是定義（2）作用的時機，Lehmer(1919)為避開餘數為 0 之狀況，故取「正」模餘。圖 6 就是數學板中$33, 55, 79, 99$的多元輾轉模餘推演算則的一個實例。

a_1	a_2	a_3	a_4	q_1	q_2	q_3
33	55	79	99	1	2	3
22	13	0	33	0	0	1
13	0	11	22	0	0	1
0	11	9	13	0	0	0
11	9	13	0	0	1	0
9	2	0	11	0	0	1
2	0	2	9	0	1	4
0	0	1	2	0	0	0
0	1	2	0	0	0	0
1	2	0	0	2	0	0
0	0	0	1			

圖 6：多元輾轉模餘推演算則的一個實例

設$c_1x_1 + c_2x_2 \ldots + c_nx_n = dr$為線性 n 元不定方程式，其中$x_i$表示未知變數，對於任意已知整數係數$c_i$，任意整數$r$。設$d$為$c_i$的最大公因數，類似於多元輾轉相除法的前推法延伸，我們將多元輾轉模數推演算則做類似的前推延伸，令延伸行為 x_j ,$j = 1,2,\ldots,k$(若$k \le 4$以x ,y ,z ,w為行名)

$$\text{令}\quad A_0 = \begin{bmatrix} x_{1(-k+1)} & x_{2(-k+1)} & \ldots & x_{k(-k+1)} \\ x_{1(-k+2)} & x_{2(-k+2)} & \ldots & x_{k(-k+2)} \\ & \cdot & & \\ & \cdot & & \\ x_{1(-1)} & x_{2(-1)} & \ldots & x_{k(-1)} \\ x_{10} & x_{20} & \ldots & x_{k0} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ & \cdot & & \\ & \cdot & & \\ 0 & 0 & \ldots & 1 \end{bmatrix} = I_k$$

定義x_j行的第i列元素為

$$x_{ji} = \begin{bmatrix} 1 & q_{1i}q_{2i} & \ldots & q_{(k-1)i} \end{bmatrix} \begin{bmatrix} x_{j(i-k)} \\ x_{j(i-k+1)} \\ \cdot \\ \cdot \\ \cdot \\ x_{j(i-2)} \\ x_{j(i-1)} \end{bmatrix},\ j = 1,2,\ldots,k。$$

令$A_i=\begin{bmatrix} x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ x_{1(i-k+2)}x_{2(i-k+2)} & \dots & x_{k(i-k+2)} \\ & \vdots & \\ x_{1(i-1)}x_{2(i-1)} & \dots & x_{k(i-1)} \\ x_{1i}x_{2i} & \dots & x_{ki} \end{bmatrix}$

則$A_{i-1}=\begin{bmatrix} x_{1(i-k)}x_{2(i-k)} & \dots & x_{k(i-k)} \\ x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ & \vdots & \\ x_{1(i-1)}x_{2(i-1)} & \dots & x_{k(i-1)} \end{bmatrix}$，亦即

$$[x_{1i}x_{2i}\ \dots\ x_{ki}]=\begin{bmatrix}1 & q_{1i}q_{2i} & \dots & q_{(k-1)i}\end{bmatrix}\begin{bmatrix} x_{1(i-k)}x_{2(i-k)} & \dots & x_{k(i-k)} \\ x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ & \vdots & \\ x_{1(i-1)}x_{2(i-1)} & \dots & x_{k(i-1)} \end{bmatrix} \quad [5]$$

再令 $E_i=\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \vdots & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & q_{1i}q_{2i} & \dots & & q_{ki} \end{bmatrix}$ 為$(k+1)\times(k+1)$階矩陣，其中$|\det(E_i)|=1$,由於E_i

的元素均為整數，故知 E_i^{-1}的元素也均為整數。故知 $\begin{bmatrix} x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ x_{1(i-k+2)}x_{2(i-k+2)} & \dots & x_{k(i-k+2)} \\ & \vdots & \\ x_{1(i-1)}x_{2(i-1)} & \dots & x_{k(i-1)} \\ x_{1i}x_{2i} & \dots & x_{ki} \end{bmatrix}$

$$=\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \vdots & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & q_{1i}q_{2i} & \dots & & q_{ki} \end{bmatrix}\begin{bmatrix} x_{1(i-k)}x_{2(i-k)} & \dots & x_{k(i-k)} \\ x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ & \vdots & \\ x_{1(i-1)}x_{2(i-1)} & \dots & x_{k(i-1)} \end{bmatrix} \quad [6]$$

亦即 $A_i = E_i A_{i-1}$，$i = 1,2,\cdots,n-1$。因此，

$A_n = E_n A_{n-1} = E_n E_{n-1} A_{n-2} = \cdots = E_n E_{n-1} \ldots E_1 A_0 = E_n E_{n-1} \ldots E_1$

[5][6]式保證了這個前推法，可以一列一列向下推演。

圖 7 展示的就是延伸的多元輾轉模數推演直式算則前推法的四元實例。由無空白的列開始，向下為第$1,2,\ldots,n$列（配合多元輾轉模餘推演算則），向上依次為$0,-1,-2,\ldots,-k+1$列。圖 7 的前 7 行就是圖 6 下推四列的結果。

線性不定方程式的一般解

係數 gcd　直式算則　解行結果矩陣　解係數矩陣　一般解　秀藏計算　計算進退　全部隱藏

延伸的多元輾轉餘數推演算則—前推法

33, 55, 79, 99

a_1	a_2	a_3	a_4	q_1	q_2	q_3	x	y	z	w
							1	0	0	0
							0	1	0	0
							0	0	1	0
							0	0	0	1
33	55	79	99	1	2	3	1	1	2	3
22	13	0	33	0	0	1	1	2	2	3
13	0	11	22	0	0	1	1	2	3	3
0	11	9	13	0	0	0	0	0	0	1
11	9	13	0	0	1	0	2	3	5	6
9	2	0	11	0	0	1	3	5	7	9
2	0	2	9	0	1	4	15	25	36	45
0	0	1	2	0	0	0	0	0	0	1
0	1	2	0	0	0	0	2	3	5	6
1	2	0	0	2	0	0	33	55	79	99
0	0	0	1							

圖 7　延伸的輾轉模餘推演算則—前推法的四元實例

觀察圖 7 中延伸行的最後一列恰為線性不定方程式的係數33,55,79,99，對此現象（$d = 1$ 時），Lehmer(1919)指出下列定理（可由數學歸納法證明）：

當$\boldsymbol{d = (c_1, c_2, \ldots, c_k) = 1}$時，

$$\boldsymbol{a_{j1} = [a_{1i} a_{2i} a_{3i} \ \ldots \ a_{ki}] \begin{bmatrix} x_{j(i-k)} \\ x_{j(i-k+1)} \\ \cdot \\ \cdot \\ \cdot \\ x_{j(i-2)} \\ x_{j(i-1)} \end{bmatrix}}, \ \boldsymbol{j = 1, 2, \ldots, k}。$$

或 $[a_{1i}a_{2i}a_{3i} \ \dots \ a_{ki}]\begin{bmatrix} x_{1(i-k)}x_{2(i-k)} & \dots & x_{k(i-k)} \\ x_{1(i-k+1)}x_{2(i-k+1)} & \dots & x_{k(i-k+1)} \\ & \vdots & \\ x_{1(i-1)} \quad x_{2(i-1)} & \dots & x_{k(i-1)} \end{bmatrix} = [a_{11}a_{21} \dots a_{k1}]$

其中$i = 1, 2, \dots, n, n+1$。

依此定理，我們知道$[0\ 0\ \dots 1]A_n = [c_1 c_2 \dots c_k]$亦即${A_n}^t\begin{bmatrix}0\\0\\.\\.\\1\end{bmatrix} = \begin{bmatrix}c_1\\c_2\\.\\.\\c_k\end{bmatrix}$

亦即$({A_n}^t)^{-1}\begin{bmatrix}c_1\\c_2\\.\\.\\c_k\end{bmatrix} = \begin{bmatrix}0\\0\\.\\.\\1\end{bmatrix}$，將 $({A_n}^t)^{-1}$的第一列與最後一列交換後，設其為 A，則$A\begin{bmatrix}c_1\\c_2\\.\\.\\c_k\end{bmatrix} = \begin{bmatrix}1\\0\\.\\.\\0\end{bmatrix}$

因$|\det(A_n)| = 1$，故 A 合於「整係數線性 n 元不定方程式的整數一般解定理」的條件，可求出一般解，故A^t為解係數矩陣，也就是說$(A_n)^{-1}$的第一行與最後一行交換後的結果，就是解係數矩陣。由於行延伸行得出的並非最後結果，數學算板有提供「一般解」按鈕，可按鈕求出一般解。圖 8 展示的就是圖 7 例中的一般解。

因為解行結果矩陣$A_{10} = \begin{bmatrix} 15 & 25 & 36 & 45 \\ 0 & 0 & 0 & 1 \\ 2 & 3 & 5 & 6 \\ 33 & 55 & 79 & 99 \end{bmatrix}$ $A_{10}^{-1} = \begin{bmatrix} -38 & -3 & 5 & 17 \\ 7 & 0 & -3 & -3 \\ 11 & 0 & 0 & -5 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

故解係數矩陣為 $\begin{bmatrix} 17 & -3 & 5 & -38 \\ -3 & 0 & -3 & 7 \\ -5 & 0 & 0 & 11 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

所以

$33x + 55y + 79z + 99w = r, r$整數 的一般解為

$$\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 17 & -3 & 5 & -38 \\ -3 & 0 & -3 & 7 \\ -5 & 0 & 0 & 11 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} r \\ s \\ t \\ u \end{bmatrix}$$

亦即

$$\begin{cases} x = 17r - 3s + 5t - 38u \\ y = -3r - 3t + 7u \\ z = -5r + 11u \\ w = s \end{cases} \quad s, t, u\text{整數}$$

圖 8：四元線性方程式的一般解按鈕呈現的結果實例

對於圖 7 各列的計算，數學算板也有按鈕可以呈現各列的計算過程，圖 9 展示的就是第五列的計算過程，它也同時驗證 Lehmer(1919)的定理，使用者可以依序呈現每一列的計算。

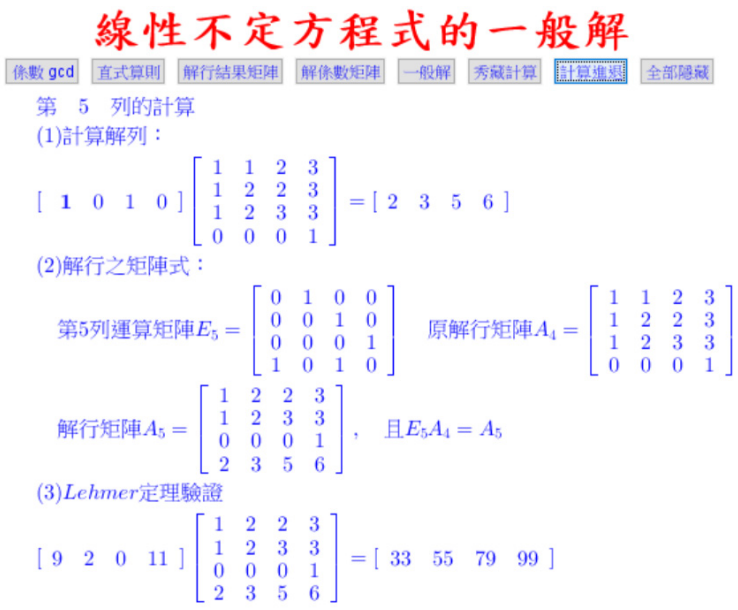

圖 9：第五列的計算及定理驗證按鈕呈現的結果

這樣看來，這個前推法的作用，好像與前述延伸的多元輾轉相除法後推法類似，結果矩陣仍需求出反矩陣才可以求出解係數矩陣。有趣的是，仿照前一節中延伸的輾轉相除—後推法的處理，我們也在數學算板上作「延伸的輾轉模餘推演—後推法」。由於前面前推法中$A_n = E_n E_{n-1} \dots E_1$，定義後推法的起始單位矩陣為

$$\begin{bmatrix} x_{1(n+1)}x_{2(n+1)} & \dots & x_{k(n+1)} \\ x_{1(n+2)}x_{2(n+2)} & \dots & x_{k(n+2)} \\ \vdots & & \\ x_{1(n+k)}x_{2(n+k)} & \dots & x_{k(n+k)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & \vdots & & \\ 0 & 0 & \dots & 1 \end{bmatrix} = I_k$$

令延伸行第i列矩陣 $B_i = \begin{bmatrix} x_{1i}x_{2i} & \dots & x_{ki} \\ x_{1(i+1)}x_{2(i+1)} & \dots & x_{k(i+1)} \\ \vdots & & \\ x_{1(i+k-1)}x_{2(i+k-1)} & \dots & x_{k(i+k-1)} \end{bmatrix}, i = 1,2,\dots,n,n+1$

再令$E'_i=\begin{bmatrix}-q_{1i} & -q_{2i} & \cdots & -q_{(k-1)i} & 1\\ 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & 0 & 0\\ & & \vdots & & \\ 0 & 0 & \cdots & 0 & 1 & 0\end{bmatrix}$，其中$i=1,2,\ldots,n$

故$B_{i+1}=\begin{bmatrix}x_{1(i+1)} & x_{2(i+1)} & \cdots & x_{k(i+1)}\\ x_{1(i+2)} & x_{2(i+2)} & \cdots & x_{k(i+2)}\\ & & \vdots & \\ x_{1(i+k)} & x_{2(i+k)} & \cdots & x_{k(i+k)}\end{bmatrix}$

令延伸行每一列的計算規則為 $[x_{1i}x_{2i} \quad \cdots \quad x_{ki}]$

$$=\begin{bmatrix}-q_{1i} & -q_{2i} & \cdots & -q_{(k-1)i} & 1\end{bmatrix}\begin{bmatrix}x_{1(i+1)} & x_{2(i+1)} & \cdots & x_{k(i+1)}\\ x_{1(i+2)} & x_{2(i+2)} & \cdots & x_{k(i+2)}\\ & & \vdots & \\ x_{1(i+k)} & x_{2(i+k)} & \cdots & x_{k(i+k)}\end{bmatrix}$$

故$\begin{bmatrix}-q_{1i} & -q_{2i} & \cdots & -q_{(k-1)i} & 1\\ 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & 0 & 0\\ & & \vdots & & \\ 0 & 0 & \cdots & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}x_{1(i+1)} & x_{2(i+1)} & \cdots & x_{k(i+1)}\\ x_{1(i+2)} & x_{2(i+2)} & \cdots & x_{k(i+2)}\\ & & \vdots & \\ x_{1(i+k)} & x_{2(i+k)} & \cdots & x_{k(i+k)}\end{bmatrix}$

$=\begin{bmatrix}x_{1i}x_{2i} & \cdots & x_{ki}\\ x_{1(i+1)}x_{2(i+1)} & \cdots & x_{k(i+1)}\\ & \vdots & \\ x_{1(i+k-1)} & x_{2(i+k-1)} & \cdots & x_{k(i+k-1)}\end{bmatrix}$，亦即 $E'_iB_{i+1}=B_i$

這保證了後推法可以由下方一列一列推至上方至第一列B_1。

且 $B_1=E'_1B_2=E'_1E'_2B_3=\cdots=E'_1E'_2\ldots E'_nB_{n+1}=E'_1E'_2\ldots E'_n$

$$\text{由於} E_i E'_i = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \cdot & & \\ & & \cdot & & \\ & & \cdot & & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & q_{1i}q_{2i} & \dots & & q_{(k-1)i} \end{bmatrix} \begin{bmatrix} -q_{1i} & -q_{2i} & \dots & -q_{(k-1)i} & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \cdot & & \\ & & \cdot & & \\ & & \cdot & & \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix} = I_k$$

因此 $A_n B_1 = E_n E_{n-1} \dots E_1 E'_1 E'_2 \dots E'_n = I_k$ 故 $B_1 = {A_n}^{-1}$

因此將後推法延伸行結果矩陣B_1的最後一行與第一行交換之後得到的矩陣就是一般解係數矩陣，圖 10 展示的就是這個後推法的一個實例。圖中延伸行的前四列構成的4×4矩陣就是B_1。圖 11 展示的是「一般解」按鈕秀出來的結果，與前推法得出的解是相同的。

a_1	a_2	a_3	a_4	q_1	q_2	q_3	x	y	z	w
33	55	79	99	1	2	3	-38	-3	5	17
22	13	0	33	0	0	1	7	0	-3	-3
13	0	11	22	0	0	1	11	0	0	-5
0	11	9	13	0	0	0	0	1	0	0
11	9	13	0	0	1	0	-9	0	2	4
9	2	0	11	0	0	1	-2	0	-1	1
2	0	2	9	0	1	4	9	0	-1	-4
0	0	1	2	0	0	0	0	1	0	0
0	1	2	0	0	0	0	0	0	1	0
1	2	0	0	2	0	0	-2	0	0	1
0	0	0	1				1	0	0	0
							0	1	0	0
							0	0	1	0
							0	0	0	1

圖 10：延伸的多元輾轉模餘推演算則—後推法之四元實例

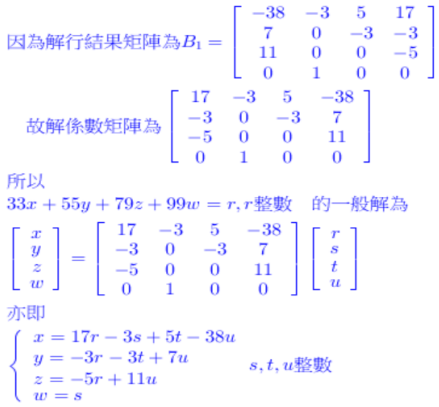

圖 11：延伸的多元輾轉模餘推演算則—後推法的「一般解」按鈕呈現的結果。

六、延伸的多元輾轉相除法與輾轉模餘推演及直式算則

比較前述兩種解線性不定方程的整數一般解的方法，我們看出延伸的「多元輾轉相除法」的前推法與延伸的「多元輾轉模餘推演法則」的後推法都可由直式算則（一列一列向前或向後）推出的延伸行矩陣直接觀察出解係數矩陣（只需轉置或交換行列），算是較方便的作法，但前者的後推法及後者的前推法的直式算則推出的解延伸行結果矩陣，都需另外再利用反矩陣以求出解係數矩陣，並未能由直式算則直接列出解係數矩陣，因此，嚴格的說並非解線性方程式整數一般解的「直式算則」。「直式算則」只是手動計算方便的法則，其實若不要求直式算則簡單計算方式的呈現，以矩陣的推演也可以直解推導出解係數矩陣。

根據「多元輾轉模餘推演」算則的遞迴算式，數列$a_{ji}, j = 1,2,\dots,k$對i 作多元模餘推演，得餘數列$a_{j(i+1)}$，商列為$q_{1i}, q_{2i}, \dots, q_{(k-1)i}$，亦即

$$\begin{bmatrix} -q_{1i} & 1 & 0 & \dots & 0 \\ -q_{2i} & 0 & 1 & \dots & 0 \\ & & \cdot & & \\ & & \cdot & & \\ -q_{(k-1)i} & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix} \begin{bmatrix} a_{1i} \\ a_{2i} \\ \cdot \\ \cdot \\ a_{(k-1)i} \\ a_{ki} \end{bmatrix} = \begin{bmatrix} a_{1(i+1)} \\ a_{2(i+1)} \\ \cdot \\ \cdot \\ a_{(k-1)(i+1)} \\ a_{k(i+1)} \end{bmatrix}, i = 1,2,\dots,n$$

令$E_i = \begin{bmatrix} -q_{1i} & 1 & 0 & \dots & 0 \\ -q_{2i} & 0 & 1 & \dots & 0 \\ & & \cdot & & \\ & & \cdot & & \\ -q_{(k-1)i} & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix}$ ，設A_0為 k 階單位矩陣 令$A_i = E_i A_{i-1}, i = 1,2,\dots,n$

故$A_n = E_n E_{n-1} \dots E_1$且$E_n E_{n-1} \dots E_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \cdot \\ \cdot \\ a_{(k-1)1} \\ a_{k1} \end{bmatrix} = \begin{bmatrix} a_{1(n+1)} \\ a_{2(n+1)} \\ \cdot \\ \cdot \\ a_{(k-1)(n+1)} \\ a_{k(n+1)} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \\ a_{1n} \end{bmatrix}$

亦即 $A_n \begin{bmatrix} c_1 \\ c_2 \\ \cdot \\ \cdot \\ \cdot \\ c_k \end{bmatrix} = A_n \begin{bmatrix} a_{11} \\ a_{21} \\ \cdot \\ \cdot \\ a_{(k-1)1} \\ a_{k1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \\ a_{1n} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \\ d \end{bmatrix}$， 令 A為A_n交換第一列及最後一列後的矩陣，

亦即 $A\begin{bmatrix}c_1\\c_2\\\cdot\\\cdot\\c_k\end{bmatrix}=\begin{bmatrix}d\\0\\\cdot\\\cdot\\0\\0\end{bmatrix}$,由於 $|\det(E_i)|=1$，故$|\det(A)|=|\det(A_n)|=1$

由線性不定方程式整數解定理知 A^t為其解係數矩陣。前述求解的過程與兩種「延伸的多元輾轉」直式算則的前推法與後推法不同的是：此處的$A_i=E_iA_{i-1}$中，E_i同時改變了A_{i-1}中至少兩列的數值，因此無法一列一列向上或向下推演（無法寫成直式算則）。但卻可以以矩陣序列的形式，展示推演的過程並直接推出解係數矩陣。

對於圖 6 展示的多元輾轉模餘推演程式中，我們也有程式按鈕，展示矩陣每一列推演的過程。圖 12 展示的是相對於圖 6「多元輾轉模餘推演」，以非直式算則的矩陣推演，求$33x+55y+79z+99w=r, r\in\mathbb{Z}$的一般解過程中，求第 1 及第 10 矩陣的過程。圖中M矩陣列為上述A矩陣列的增廣矩陣。$A=E_{10}E_9\ldots E_1$，A^t就是解係數矩陣。

第 1 矩陣的計算，列運算組合矩陣E_1　原增廣矩陣M_0　新增廣矩陣M_1

(1) 商列 1 2 3

(2) $E_1=\begin{bmatrix}-1&1&0&0\\-2&0&1&0\\-3&0&0&1\\1&0&0&0\end{bmatrix}$

(3) $M_1=E_1M_0$

$$\left[\begin{array}{cccc|c}-1&1&0&0&22\\-2&0&1&0&13\\-3&0&0&1&0\\1&0&0&0&33\end{array}\right]=\begin{bmatrix}-1&1&0&0\\-2&0&1&0\\-3&0&0&1\\1&0&0&0\end{bmatrix}\left[\begin{array}{cccc|c}1&0&0&0&33\\0&1&0&0&55\\0&0&1&0&79\\0&0&0&1&99\end{array}\right]$$

第 10 矩陣的計算，列運算組合矩陣E_{10}　原增廣矩陣M_9　新增廣矩陣M_{10}

(1) 商列 2 0 0

(2) $E_{10}=\begin{bmatrix}-2&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}$

(3) $M_{10}=E_{10}M_9$

$$\left[\begin{array}{cccc|c}-38&7&11&0&0\\-3&0&0&1&0\\5&-3&0&0&0\\17&-3&-5&0&1\end{array}\right]=\begin{bmatrix}-2&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}\left[\begin{array}{cccc|c}17&-3&-5&0&1\\-4&1&1&0&2\\-3&0&0&1&0\\5&-3&0&0&0\end{array}\right]$$

圖 12：相對於圖 6 的第 1 及 10 矩陣的推演實例，以增廣矩陣的形式呈現

圖 6 畫面中按鈕「一般解」，可以展示一般解。

七、模餘變數代換法

林(民 110)曾討論歐拉常用的解線性不定方程式的方法，並介紹模數變數代換法，說明這兩個方法其實本質上是相同的。數學算板也建立了一個「模餘變數代換法」程式，與前述輾轉多元模餘推演法則類似，只是餘數位置不同。

設 $c_1x_1 + c_2x_2 \ldots + c_kx_k = d$為線性 n 元不定方程式，$d = \gcd(c_1, c_2, c_3, \ldots c_k)$，若（1）若 $\exists j \ni c_j = 1$，則其一般解垂手可得。

（2）選取$|c_j| > 1$,類似「多元模餘推演」，將$c_1, c_2, c_3, \ldots, c_k$分別除以$c_j$得餘數 $r_1, r_2, \ldots, r_i, \ldots, \mathrm{r_k}$，商列$q_1, q_2, q_2, \ldots, q_i, \ldots \mathrm{q_k}$，使得

$c_i = c_jq_i + r_i, 0 \le r_i < |c_j|, i = 1,2, \ldots, k$，其中$q_j = 1,\ r_j = 0$，

令 $q_1x_1 + q_2x_2 + \cdots + x_j + \cdots + q_kx_k = t_j$ （指定新變數 t_j） [7]

將x_j代入原不定方程式，可得

$r_1x_1 + r_2x_2 + \cdots + r_jt_j + \cdots + r_kx_k = d$ （t_j 取代 x_j） [8]

這個過程，我們稱為模餘變數代換，這個過程繼續對新方程式作下去，由於方程式係數變小，或原變數變少，最終會停止，此時，我們會得到兩組「等價」的線性方程組，一組是設定新變數（前述[7]）而得的「商行方程組」，另一組是代入後(前述[8])得到的「模餘方程組」。解任一組，即可得到原不定方程式的一般解。圖 13 展示的就是數學算板的模餘變數代換法的內容的綜合呈現。中間是模餘係數的直式算則，左邊的是模餘方程組，右邊的是商行方程組。下方左邊及右邊分別是它們相應的增廣矩陣，變數為x, y, z, t_1, t_2, t_3，增廣矩陣最後一行為常數項，t_j變數移項至右邊。按鈕可以隱藏或呈現每一個項目。

圖 13：歐拉模餘變數代換程式的綜合呈現畫面

在數學算板中，點選任一個增廣矩陣都可透過數學算板「階梯矩陣」選項取得化簡後的簡約階梯矩陣。圖 14 就是本例化簡後的簡約階梯矩陣，最後一列描述新設變數t的關係，與主變數（x,y,z）不相關。

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 0 & -5 & -13 & 3 \\ 0 & 1 & 0 & 0 & 5 & 8 & -2 \\ 0 & 0 & 1 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 & -1 \end{array}\right]$$

圖 14：示圖 13 例中增廣矩陣化簡後的階梯矩陣

兩個增廣矩陣都會得到相同的階梯矩陣。本程式可以輸入任意線性不定方程式的整數係數，程式透過「模餘變數代換」列出係數，並可使用按鈕列出兩組聯立方程式，也可列出一般解。圖 15 展示的就是按鈕一般解列出的結果。本例中，由於增廣矩陣左方矩陣為單位矩陣，因此將將簡約階梯矩陣「增廣部分」的常數項行移到第一行，就是本例的解係數矩陣，由於t_i係數經過化簡，故重新定義變數。

模餘及商行增廣矩陣的簡約階梯矩陣去除不相關行列均為

$$\left[\begin{array}{ccc|cc} 1 & 0 & 0 & -5 & -13 & 3 \\ 0 & 1 & 0 & 5 & 8 & -2 \\ 0 & 0 & 1 & -2 & 1 & 0 \end{array}\right]$$

(注意:最後一行為常數項,移項並重定 t_i 變數)

所以 $21x+31y+25z=r$,r整數的一般解為

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 & -5 & -13 \\ -2 & 5 & 8 \\ 0 & -2 & 1 \end{bmatrix} \begin{bmatrix} r \\ s \\ t \end{bmatrix}$$

亦即

$$\begin{cases} x = 3r-5s-13t \\ y = -2r+5s+8t \quad s,t\text{整數} \\ z = -2s+t \end{cases}$$

圖 15：本例的「一般解」按鈕列出的結果

有時簡約增廣矩陣去除不相關變數列，得到的左方矩陣不是單位矩陣，此時，程式會視需要移動行並加入列，得出解係數矩陣。圖 16 展示的就是一個般解的實例。

模餘及商行增廣矩陣的簡約階梯矩陣去除不相關行列均為

$$\left[\begin{array}{cccc|cc} 1 & 2 & 0 & 3 & -24 & 11 \\ 0 & 0 & 1 & 0 & 11 & -5 \end{array}\right]$$

(注意:最後一行為常數項,移項並重定 t_i 變數)

所以 $33x+66y+72z+99w=3r$,r整數的一般解為

$$\begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 11 & -2 & -24 & -3 \\ 0 & 1 & 0 & 0 \\ -5 & 0 & 11 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} r \\ s \\ t \\ u \end{bmatrix}$$

亦即

$$\begin{cases} x = 11r-2s-24t-3u \\ y = s \\ z = -5r+11t \\ w = u \end{cases} \qquad s,t,u\text{整數}$$

圖 16：利用移動行加入列的方式得到解係數矩陣

八、結語

對於整係數線性不定方程的一般解，本文補充說明延伸多元輾轉相除法的前推法，定義數學算板所使用的整數除法、多元除法及多元輾轉相除法，並討論了 Lehmer(1919)延伸的後推法，前推法可直接由直式算則推出一般解的解係數矩陣，後後推法得出相關矩陣之後，必須另外求出它的反矩陣，才可獲得解係數矩陣。此外，我們也根據 Lehmer(1919)的多元正模餘推演法則建立了「多元模餘推演法則」，並討論其延伸的前推法及後推法，與多元輾轉相除法延伸正好相反，前推法直式算則，只能推出相關矩陣，必須另外求矩陣。但後推法則可以直接由直式算則推出一般解的解係數矩陣。「多元輾轉相除法」及「多元模餘推演法」，都強調以直式算則求解（除了求反矩陣的部分外），都是先由直式算則求出商列或餘數列，再透過延伸行求出解。其實，若不以直式算則來算，我們也介紹了直接透過矩陣運算來求一般解的算則。此外，我們也討論了「模數變數變換法」，這是與歐拉常用的解法相當的解法。透過模餘推演，列出等價的兩組線性聯立方程，解出任一組方程式，都可求出一般解。數學算板對這些方法，都有建立程式，只要輸入線性方程式的係數，電腦就可以秀出相關的流程及呈現資料，希望能夠對學生的學習及教師的教學有幫助。目前正計畫將本文相關程式，獨立出數學算板程式模組，方便對這一主題有興趣的讀者，能夠直接使用，未來會將其置於 https://mathboard.tw 上。

備註

注 1：林（民 110）pp46 中列基本矩陣的類別敘述中（2）（3）的內容應該交換

參考文獻

林保平（民 110）延伸的輾轉相除法直式算則在數學算板中的實踐，科學教育月刊，第 439 期，pp33-51。

Lehmer, D. (1919). The General Solution of the Indeterminate Equation: Ax + By + Cz - ..... = r. Proceedinga of National Academy of Science. Vol.55,1919,pp.111-114.

Lehmer, D. (1941). A Note on the Linear Diophantine Equation. The American Mathematical Monthly, 48(4), 240-246. doi:10.2307/2302718.

Raymond T. Boute（1992）. The Euclidean definition of the functions div and mod. In ACM Transactions on Programming Languages and Systems (TOPLAS), 14(2):127–144, New York, NY, USA, April 1992. ACM press.