延伸的輾轉相除法直式算則在數學算板中的實踐

林保平

臺北市立大學數學系退休副教授

壹、前言

最近在 YouTube 的教學網站上，看了一些輾轉相除法及其延伸應用的相關教學影片，覺得對輾轉相除法及其延伸的不定方程式的應用的教學說明，都不夠完整，於是就在「數學算板」上建立了幾個可以提供教師教學利用的程式，本文將就延伸的輾轉相除法直式算則及所建立的程式提出一些討論。

「數學算板」是作者退休後，將退休前在其他軟體上（主要是 GSP）建立的程式，重新以 java 語言改寫，而建立的一個完整的新程式，包含了代數算板、幾何畫板、統計與機率及龜行幾何等部分。Java 8 之前的程式實例，可參看網頁 http://mathboard.tw，這些實例，大部分只可使用 java8 開啟。較新的數學算板的程式實踐，仍在繼續當中，網頁上提供測試版，讓有興趣的讀者測試。由於 java 在網路上的執行較不方便，較新的數學算板程式，採用影片的方式呈現，可參閱 MahBoard-YouTube .

貳、輾轉相除法直式算則及其幾何意義

我們先看下面兩個問題：

長方形紙一張，長 57 單位，寬 36 單位，欲裁出正方形，紙張必須恰好用盡，

(一)若裁出的正方形大小要相同，且愈大愈好，裁出的正方形邊長是多少？可裁出多少個正方形？

(二)若裁出的正方形大小可以不相同，但大的愈多愈好，可裁出多少種不同的正方形？各種正方形各有幾個？

第一個問題很簡單，裁出的正方形的邊長一定要是 36 和 57 的公因數，否則長方形一定有一個邊會有剩餘，但我們要求的是正方形愈大愈好，因此正方形必須是 57 與 36 的最大公因數，只要求出 57 及 36 的最大公因數 3，答案就是 $\frac{57\times36}{3\times3}=228$個，這是典型求最大公因數的問題。這個問題也可以看成拼圖問題：使用相同的正方形且正方形要最大，多少個正方形可以拼出長方形？正方形的邊長是多少？圖 1 左圖展示用無法完全用盡的切割拼圖，圖 1 右圖展示的就是邊長 3 單位切割出來的 228 個正方形拼圖。圖中的 P 點是一個可以移動的點，移動此點可以展示不同大小的正方形切割，學習者可觀察切割出的正方形是否紙張用盡或正方形是否可拼出原長方形，可引導學習者觀察發現：只有邊長能同時除盡兩邊長的正方形，才是所要的正方形。

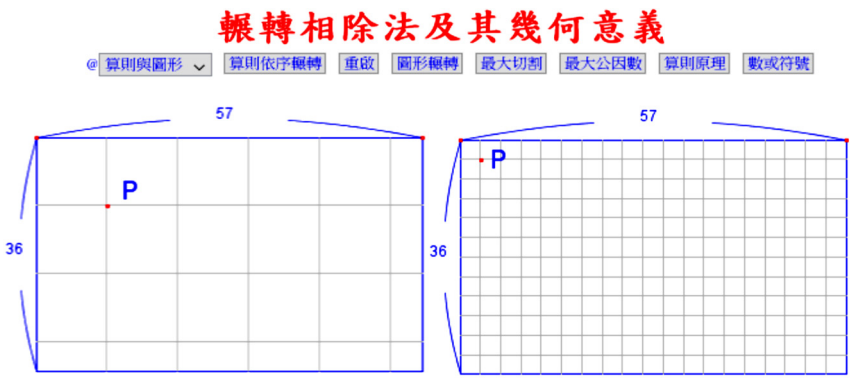
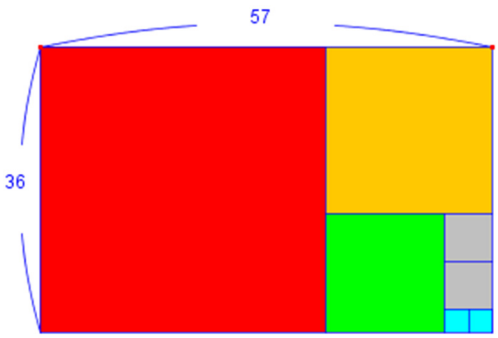


圖 1、左圖：沒有用盡紙張的正方形切割，右圖：228 個邊長 3 正方形拼出邊長 36、57 的長方形

第二個問題最大公因數就好像派不上用場了。不過我們可以透過實際操作來解決這個問題。我們先裁出邊長 36 的最大的正方形 1 個，剩下邊長為 36 及 21 的長方形，再由此長方形裁出邊長 21 的第二大正方形 1 個，剩下的就是邊長為 21 及 15 的長方形，這個活動繼續下去，我們可再裁出邊長 15 的第三正方形一個、邊長為 6 的第四正方形 2 個，及邊長為 3 的第五正方形 2 個，此時剛裁好剪完畢。圖 2 左圖展示的就是數學算板呈現的剪裁結果的拼圖。當然顏色是外加的。

前述裁剪的過程，其實就是輾轉相除的過程，每類正方形的裁剪，就是邊長的除法，商就是此類正方形的個數，除數與餘數就是新長方形的邊長。數學算板除了可展示輾轉相除的直式算則外，也有選項按鈕「算則原理」可將橫式算則與直式算則並列，方便教學時的比較。圖 2 右圖展示的是數學算板上呈現的輾轉相除的直式算則與橫式算並列的圖形。其中第一、三行是輾轉相除的兩數，第二行是商，第四行是對應的橫式算式。從圖中可以看出商行中的數 1、1、1、2、2，就是第二問題中的五類正方形的個數，而 36 及餘數 21、15、6、3（橫線下方的數，或左或右），分別就是五類正方形的邊長。第三行的最後一個數 3，就是兩數 57 與 36 的最大公因數。也有直式算則是將a,b行並列，將中間商行分成兩行，分列於a,b行左右的。



輾轉相除法原理

a	q	b	a = b q + r
57			a =57
36	1	36	b =36
21	1	21	57=36×1+21
15	1	15	36=21×1+15
6	2	12	21=15×1+6
6	2	3	15=6×2+3

圖 2、左圖：裁剪的正方形排列成原來的長方形，右圖：輾轉相除法的直式及橫式算則對照

這個幾何展示的輾轉相除的過程，也有利於解釋何以最後的餘數是兩數的最大公因數。其實整個過程就是重複下列動作：將以長方形較小邊為邊長，裁出若干個相同的最大正方形後，（1）若沒有剩餘，動作結束，（2）得到較小的新長方形，對此長方形再繼續裁。圖 3 左圖展示大長方形裁掉最大正方形後，得到小長方形，右圖展示的是：若大長方形可用最大的正方形（右圖中展式的切割小方格）拼成的話，裁掉最大正方形（紅色），剩下的小長方形也同樣可由這種同樣的小方格鋪滿，也就是說，要求大長方形兩邊長的最大公因數，只要求剩餘的小長方形兩邊長的最大公因數就可以了。用代數式來說，若 $a,b,q,r\in\mathbb{N}$且$a=bq+r,\ 0\le r<b$，則a,b（大長方形的邊長）的最大公因數就是b,r（小長方形邊長）的最大公數，記為 $(a,b)=(b,r)$。若以本文後面圖 7 右圖中，展示的輾轉相除法橫式算則來看，$(r_0,r_1)=(r_1,r_2)=\cdots=(r_{n-1},r_n)=(r_n,r_{n+1})=r_n$ 就是a,b的最大公因數，其中$r_{n+1}=0$。

數學算板中的直式的輾轉相除法程式，a,b兩數是可以自由輸入的，輸入之後，程式會自動呈現輾轉相除的表列。若有選項呈現橫式算則，則橫式算則也一樣會更新。其相應依比例展示的幾何分割圖形也會跟者修正。此外，對獨立的直式算則，有連續按鈕可以將計算的過程一步一步地展示（按鈕參看圖 1 上方），按鈕「重啟」可清除已展示的內容只呈現a,b兩數，按鈕「算則依序輾轉」可依序繼續進行下一步（按左鍵）或回復至上一步（按右鍵），按「圖形輾轉」按鈕，則可依序呈現分割矩形得到的各類正方形，「算則與圖形」選單內可選擇呈現問題、展示直式算則、展示幾何圖形、或同時呈現算則及圖形，「算則原理」在展示直式算則時，可切換只呈現直式算則實例或同時呈現橫式算則實例，「數或符號」可切換矩形邊長的展示為文字或實例中的數字。

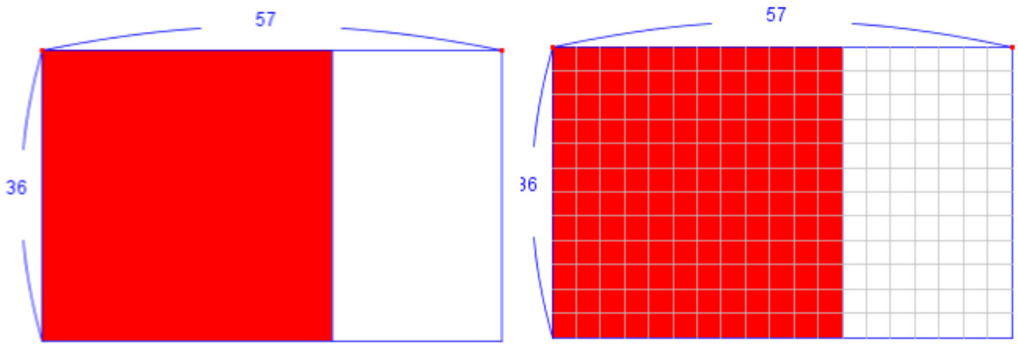


圖 3、$(a,b)=(b,r)$ 的幾何圖形解釋

參、延伸的輾轉相除法直式算則 I — 前推法

不定方程式（Indeterminate Equation）

一個二元或二元以上的方程式，其解通常未定，例如$3x-2y=7$，解會隨x或y值而改變，這類的方程式，我們稱之為不定方程式。解不定方程式時，我們常會限制解的範圍，例如求整數或正整數解。設$c_1x_1+c_2x_2+\cdots+c_nx_n=D$，其中$c_1,c_2,\cdots,c_n$為整數，$d=(c_1,c_2,\cdots,c_n)$為$c_1,c_2,\cdots,c_n$的最大公因數，若$d$不為D的因數，則此不定方程式無整數解。本文討論的方程式均為形如 $c_1x_1+c_2x_2+\cdots+c_nx_n=dr,\ r,c_i\in\mathbb{Z},i=1,2\cdots,n,\ d=(c_1,c_2,\cdots,c_n)$ 的線性不定方程式。若$c_1x_1+c_2x_2+\cdots+c_nx_n=d,\ c_i\in\mathbb{Z}$，稱此式為貝祖等式（Bézout's identity）。兩數的輾轉相除法常被推廣使用以尋找貝祖等式，亦即尋找不定方程式 $ax+by=(a,b)$ 的一組特殊整數解，被稱為延伸的輾轉相除法。

延伸的輾轉相除法基本上有兩種方法，一為前推法，一為後推法，都能有效地求出一組二元一次不定方程式的特殊解。兩者其實都可先作一次輾轉相除得到商之後，再用這些商求得延伸的結果。但前推法可以在作輾轉相除個別步驟時，同時就所得的個別商，作出延伸的個別結果。此外，前推法還可以直接算出一般解的係數。後推法，則需在作完兩數輾轉相除得到所有的商之後，再後推得到延伸的結果。

前推法 —依照輾轉相除法的計算順序，推演出一組特殊解。

這個方法基本上就是利用輾轉相除法的商，以兩個代表兩數的變數a,b，重作一次多項式的輾轉相除法。圖 4 展示的是數的輾轉相除及重作的多項式輾轉相除的直式算則對照。圖中可以看出$-5a+8b=3$亦即$(-5)57+(8)36=3$，也就是說，$x_o=-5,y_o=8$是 $57x+36y=3$的特殊解。

將圖 4 右圖做分離係數，就得到圖 5 左圖。將圖 5 左圖的a,b兩行合併為一行（只取該列與商對應的餘式），並將該行記為數對的型態，就是圖 5 右圖所展示數學算板延伸的輾轉相除法 I 中的延伸行(x_i,y_i)。

輾轉相除法直式算則

a	q	b
57		
36	1	36
21	1	21
15	1	15
6	2	12
6	2	3
0		

輾轉相除法直式算則

a	q	b
a		
b	1	b
a - b	1	a- b
-a + 2b	1	-a+2b
2a - 3b	2	4a-6b
-10a+16b	2	-5a+8b
12a-19b		

圖 4、數及多項式的輾轉相除法對照圖

輾轉相除法直式算則

a		q	b	
1	0			
0	1	1	0	1
1	-1	1	1	-1
-1	2	1	-1	2
2	-3	2	4	-6
-10	16	2	-5	8
12	-19			

延伸的輾轉相除法I

(xi , yi)	a	qi	b
(1, 0)	57		
(0, 1)	36	1	36
(1, -1)	21	1	21
(-1, 2)	15	1	15
(2, -3)	6	2	12
(-5, 8)	6	2	3
(12, -19)	0		

圖 5、多項式分離係數輾轉相除與延伸的輾轉相除法對照。

數學算板中延伸的輾轉相除法 I 的延伸行中，第 1 及第 2 列為預設列，之後的列都是前兩列與對應的商計算出來的結果。它的計算法就是：前兩列中的第 1 列減去第 2 列與對應商的積。它其實就是多項式輾轉相除餘式的係數。圖 5 右圖中延伸行與最大公因數對應的$(-5,8)$[注意：它是延伸行倒數第二列]，就是不定方程式$57x+36y=3$的一個特殊解。同樣的想法，我們也可以說$(1,-1)$，$(-1,2)$，$(2,-3)$，$(-5,8)$，$(12,-19)$分別是$57x+36y=21$，$57x+36y=15$，$57x+36y=6$，$57x+36y=3$，$57x+36y=0$的特殊解。

到目前為止我們都是用實例來分析求不定方程的特解，其實前推延伸的輾轉相除法的運算規則可以由遞迴定義的方法推導出來。圖 6 展示數學算板對任意輸入的兩數後，可呈現的原理說明畫面，這是前推法多種選項中的一種。最左行是兩數線性組合等於餘數之算式，最右行是相應的轉轉相除橫式算式，這是引導學生進入遞迴定義的步驟之一。

圖 7 展示的是圖 6 式子的一般化表示法，框框中的式子就是後面推導算則需用的式子。圖 8 展示的就是由圖 7 中左方框式子代入右方框式子推導延伸算則的過程。

圖 6、前推法原理畫面之一

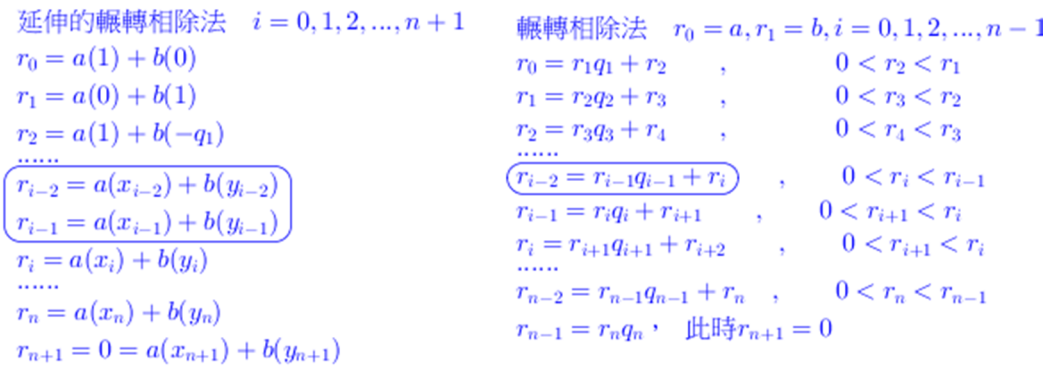


圖 7、數學算板將圖 6 最左行及最右行資料中式子以一般化的橫式表示

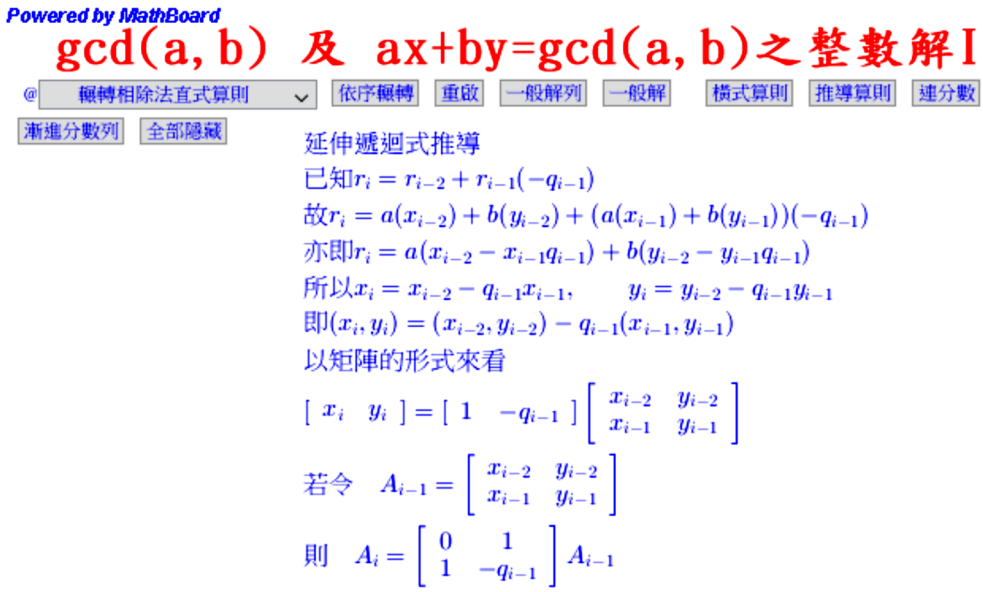


圖 8、由圖 7 兩方框內容推導出遞迴公式的過程

由這些推導，我們知道(x_i,y_i) 為不定方程式$ax+by=r_i$ 的一個整數解。又，延伸的輾轉相除法延伸行最後一列(x_{n+1},y_{n+1})，就是$ax+by=0$的解。亦即$ax_{n+1}+by_{n+1}=r_{n+1}=0$。

圖 8 中的矩陣表示法中，矩陣$\begin{bmatrix}0 & 1\\ 1 & -q_{i-1}\end{bmatrix}$ 第 1 列的作用，就是將A_{i-1}的第 2 列放到A_i第 1 列，第 2 列的作用就是將A_{i-1}的第 1 列加上第二列乘以$-q_i$，並將結果放在A_i的第 2 列，這就是這個算則能夠依序一列一列呈現，寫成直式算則的原因，因為A_i的第 1 列就是A_{i-1}第 2 列。令$A_2=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，由於 $\begin{vmatrix}0 & 1\\ 1 & -q_{i-1}\end{vmatrix}=-1$，故$|A_i|=\pm1, i=2\cdots,n+1.$。

令$\begin{cases}x=x_n+x_{n+1}\,t\\ y=y_n+y_{n+1}\,t\end{cases}$，$t\in\mathbb{Z}$，則

$$ax+by=a(x_n+x_{n+1}\,t)+b(y_n+y_{n+1}\,t)$$
$$=(ax_n+by_n)+(ax_{n+1}+by_{n+1})t$$
$$=r_n+0\times t=r_n$$

故(x,y)為$ax+by=r_n$ 的解。

反之，設(x,y)為$ax+by=r_n$ 的解。令 $\begin{cases}x=x_ns+x_{n+1}\,t\\y=y_ns+y_{n+1}\,t\end{cases}$。解此$s,t$的聯立方程式，由於$\begin{vmatrix}x_n & x_{n+1}\\y_n & y_{n+1}\end{vmatrix}=\left|{A_{n+1}}^t\right|=\pm1$，故知聯立方程式 s,t恰有一組整數解。因(x,y)為$ax+by=r_n$的解，故$ax+by=a(x_ns+x_{n+1}\,t)+b(y_ns+y_{n+1}\,t)=r_n$ ，故 $(ax_n+by_n)s+(ax_{n+1}+by_{n+1})t=r_n$，因此 $(ax_n+by_n)s=r_n$，故$s=1$。也就是說，存在$t\in\mathbb{Z}$使得 $\begin{cases}x=x_n+x_{n+1}\,t\\y=y_n+y_{n+1}\,t\end{cases}$。故知 $\begin{cases}x=x_n+x_{n+1}\,t\\y=y_n+y_{n+1}\,t\end{cases}$, $\mathrm{t}\in\mathbb{Z}$ 為$ax+by=r_n$的一般解。

綜合前述，我們可以得到下面的定理：

設 $r_i=r_{i+1}q_{i+1}+r_{i+2}$， $0<r_i<r_{i-1}$，
$i=0,1,2,\dots,n-1.$
$r_i,q_i\in\mathbb{Z}$， $r_{n+1}=0$， 其中$a=r_0,b=r_1.$
令 $x_i=x_{i-2}-x_{i-1}q_{i-1}$，
$y_i=y_{i-2}-y_{i-1}q_{i-1}$，
$i=0,1,2,\dots,n+1.$
其中$x_0=1,y_0=0,x_1=0,y_1=1$ 則

（1） r_n 就是a,b的最大公因數。

（2） (x_i,y_i) 為不定方程式$ax+by=r_i$ 的一個整數解。

（3） $\begin{cases}x=x_n+x_{n+1}\,t\\y=y_n+y_{n+1}\,t\end{cases}$， $\mathrm{t}\in\mathbb{Z}$ 為 $ax+by=r_n$ 的一般解。

圖 6 展示的輾轉相除法中，$\begin{cases}x=8-75\,t\\y=-61+572\,t\end{cases}$，$\mathrm{t}\in\mathbb{Z}$ 就是 $572x+75y=1$ 的一般解。大部分延伸輾轉相除法的討論，重點都放在求特解上，並未探討$r_{n+1}=0$這一列的延伸結果。數學算板的延伸直式算則Ⅰ(前推法)，內定並未顯示餘數為零的最後一列，但有按鈕「一般解列」可令其顯示或隱藏，可以與學生討論其內容，並得到一般解。

數學算板程式大部分都有按鈕，延伸直式算則Ⅰ的「最大公因數」按鈕可另外呈現或隱藏最大公因數;「直式算則或橫式算則」按鈕則可輪換顯示或隱藏直式算則及橫式算則;「推導算則」按鈕可展示或呈現遞迴公式的推導過程;「一般解」按鈕可呈現或隱藏一般解。「全部隱藏」按鈕可將呈現的內容全部隱藏。此外，由於展轉相除法的商，就是「連分數」的對應數字，數學算板也有按鈕，可呈現「連分數」、「連分數漸進分數」。圖 9 展示延伸輾轉相除直式算則及部分相關內容。這些內容都會隨著所取兩數a,b而變化。由於連分數不在本文的討論範圍，所以本文沒有討論連分數，有興趣的讀者可參閱(Olds,1963)。

延伸的輾轉相除法Ⅰ

(xi , yi)	a	qi	b
(1, 0)	572		
(0, 1)	525	7	75
(1, -7)	47	1	47
(-1, 8)	28	1	28
(2, -15)	19	1	19
(-3, 23)	18	2	9
(8, -61)	1	9	9
(-75, 572)			0

$572x+75y=1$的一般解為 $\begin{cases}x=8-75t\\y=-61+572t\end{cases}$，$t$整數

連分數

$$\frac{572}{75}=[7,1,1,1,2,9]$$
$$=7+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{9}}}}}$$

漸進分數列

$$\left[7,8,\frac{15}{2},\frac{23}{3},\frac{61}{8},\frac{572}{75}\right]$$

圖 9、延伸輾轉相除直式算則及可隱藏或呈現的部分相關內容

肆、延伸的輾轉相除法直式算則 II — 後推法

圖 10 展示的是直式展轉相除法算則（左圖）與延伸的輾轉相除法直式算則 II（右圖）。左圖 3 行與右圖後面 2 行對照，其實它們都是輾轉相除法直式算則，後者用於後推法。其實就是將前者a,b行合併為一行 r_i，只取餘數，省略「商與除數的積」（前面曾提到），亦即第 3 列開始，每一列都是前方第 1 列值除以第 2 列值而得到的餘數。

許多教學程式都是使用橫式的後推法來求得貝祖等式。圖 11 展示一個實例。圖中兩個方框，前者為展轉相除橫式算式，下方框展示，將前者倒推之後，得到貝祖等式$572(8)+75(-61)=1$，這個等式是圖 10 右圖延伸直式算式中，x_i,r_i行中，令第一列與第二列交叉乘積之和等於 gcd 而得的，亦即，$(8,-61)$ 為不定方程式$572x+75y=1$的一組特解。

這個後推法其實也像前推法一樣，可以推出一個遞迴的公式。圖 12 展示的是數學算板前推法遞迴公式推導的一個引導思維的展示之一。圖 12 其實是圖 11 下方的方框內容，移至圖 12 的最左行，且使用簡化的輾轉相除直式算則。圖中x_i行為延伸行，我們要找出他的遞迴公式。圖 13 將圖 12 展示實例的最左行與最右行資料以一般化的方法表示。框框中的式子就是後面推導算則需用的式子。圖 14 展示的就是推導出後推法延伸算則的過程。由這些推導，我們知道$r_0x_1+r_1x_0=r_n$ 亦即 $ax_1+bx_0=r_n$，故 (x_1,x_0) 為不定方程式 $ax+by=r_n$ 的一個整數解。

輾轉相除法直式算則

a	q	b
572		
525	7	75
47	1	47
28	1	28
19	1	19
18	2	9
1	9	9

延伸的輾轉相除法直式算則II

x_i	r_i	q_i
-61	572	
8	75	7
-5	47	1
3	28	1
-2	19	1
1	9	2
0	1	9
		=====

圖 10、簡化的輾轉相除法直式算則（對照a,b,q行與r_i，q_i行）

輾轉相除法原理

a	q	b	a = b q + r
572			a =572
525	7	75	b =75
47	1	47	572=75x7+47
28	1	28	75=47x1+28
19	1	19	47=28x1+19
18	2	9	28=19x1+9
1	9	9	19=9x2+1

$$1=19(1)+9(-2)$$
$$1=19+(28-19\times1)(-2)=28(-2)+19(3)$$
$$1=28(-2)+(47-28\times1)(3)=47(3)+28(-5)$$
$$1=47(3)+(75-47\times1)(-5)=75(-5)+47(8)$$
$$1=75(-5)+(572-75\times7)(8)=572(8)+75(-61)$$

圖 11、後推法尋找貝祖等式的實例

延伸的輾轉相除法原理II

$r_i x_{i-1} + r_{i-1} x_i = r_n$	x_i	r_i	q_i	$r_i = r_{i+1} q_{i+1} + r_{i+2}$
572(8)+75(-61)=1	-61	572		a =572
75(-5)+47(8)=1	8	75	7	b =75
47(3)+28(-5)=1	-5	47	1	572=75×7+47
28(-2)+19(3)=1	3	28	1	75=47×1+28
19(1)+9(-2)=1	-2	19	1	47=28×1+19
9(0)+1(1)=1	1	9	2	28=19×1+9
	0	1	9	19=9×2+1
			=====	

圖 12、後推法的實例與橫式算則對照

延伸的輾轉相除法II $r_0 = a, r_1 = b$

$r_n = r_0 x_1 + r_1 x_0$

$r_n = r_1 x_2 + r_2 x_1$

$r_n = r_2 x_3 + r_3 x_2$

……

$r_n = r_{i-2} x_{i-1} + r_{i-1} x_{i-2}$

$r_n = r_{i-1} x_i + r_i x_{i-1}$

$r_n = r_i x_{i+1} + r_{i+1} x_i$

……

$r_n = r_{n-2} x_{n-1} + r_{n-1} x_{n-2}$

$r_n = r_{n-1} x_n + r_n x_{n-1}$, 可令$x_n = 0, x_{n-1} = 1$

輾轉相除法 $r_0 = a, r_1 = b$

$r_0 = r_1 q_1 + r_2$, $0 < r_2 < r_1$

$r_1 = r_2 q_2 + r_3$, $0 < r_3 < r_2$

$r_2 = r_3 q_3 + r_4$, $0 < r_4 < r_3$

……

$r_{i-2} = r_{i-1} q_{i-1} + r_i$, $0 < r_i < r_{i-1}$

$r_{i-1} = r_i q_i + r_{i+1}$, $0 < r_{i+1} < r_i$

$r_i = r_{i+1} q_{i+1} + r_{i+2}$, $0 < r_{i+1} < r_i$

……

$r_{n-2} = r_{n-1} q_{n-1} + r_n$, $0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_n$， 此時$r_{n+1} = 0$

圖 13、將圖 12 的最左及最右行資料以一般化的形式表示

延伸遞迴式推導

已知$r_n = r_{i-1} x_i + r_i x_{i-1}$

將$r_i = r_{i-2} - r_{i-1} q_{i-1}$代入

得$r_n = r_{i-1} x_i + (r_{i-2} - r_{i-1} q_{i-1}) x_{i-1}$

即$r_n = r_{i-2} x_{i-1} + r_{i-1}(x_i - q_{i-1} x_{i-1})$

又因$r_n = r_{i-2} x_{i-1} + r_{i-1} x_{i-2}$

故$x_{i-2} = x_i - q_{i-1} x_{i-1}$

圖 14、 推導延伸算則的過程

圖 15 展示的就是數學算板後推法延伸直式算則 II 推導一半的過程。圖中$x_n = 0, x_{n-1} = 1$ 為預設值,由遞迴公式 $x_{i-2} = x_i - q_{i-1} x_{i-1}$,可知 $x_{n-2} = x_n - q_{n-1} x_{n-1} = 0 - 2 \times 1 = -2$、$x_{n-3} = 1 - 1 \times (-2) = 3$, $x_{n-4} = -2 - 1 \times 3 = -5, \cdots 8$ ， -61 。 因 此 $572 \times 8 + 75(-61) = 1$，亦即 $(8, -61)$ 為$572x + 75y = 1$的一組特解。數學算板倒推法的運算就是：定出 0，1，從倒數第 3 列開始，每列的計算就是將下下方列減去下方列與商的積得到的值。

數學算板使用後推法的直式算則，沒有一般解列，只能求出一個特殊解，但數

學算板使用下述定理中的（3），透過按鈕「一般解」，呈現一般解。

一般解的證明如下：

設 $\begin{cases} x = x_1 + \frac{b}{r_n}t \\ y = x_0 - \frac{a}{r_n}t \end{cases}$ ，$t \in \mathbb{Z}$，其中 (x_1, x_0) 為不定方程式 $ax + by = r_n$ 的一個整數解

則 $ax + by = a\left(x_1 + \frac{b}{r_n}t\right) + b\left(x_0 - \frac{a}{r_n}t\right)$

$= (ax_1 + bx_0) + \left(a\frac{b}{r_n} - b\frac{a}{r_n}\right)t = r_n + 0 \times t$

$= r_n$

故 (x, y) 為 $ax + by = r_n$ 的解。

反之，因 $ax_1 + bx_0 = r_n$，

故 $a(x - x_1) + b(y - x_0) = 0$

亦即 $a(x - x_1) = -b(y - x_0)$，

故 $\frac{a}{r_n}(x - x_1) = -\frac{b}{r_n}(y - x_0)$

又因 $\left(\frac{a}{r_n}, \frac{b}{r_n}\right) = 1$

所以 $\frac{a}{r_n}$ 為 $-(y - x_0)$ 的因數，故存在 $t \in \mathbb{Z}$ 使得 $y - x_0 = -\frac{a}{r_n}t$，亦即 $y = x_0 - \frac{a}{r_n}t$，且 $a(x - x_1) = b\frac{a}{r_n}t$ 故 $x - x_1 = \frac{b}{r_n}t$，亦即 $x = x_1 + \frac{b}{r_n}t$，也就是說存在 $t \in \mathbb{Z}$

使得 $\begin{cases} x = x_1 + \frac{b}{r_n}t \\ y = x_0 - \frac{a}{r_n}t \end{cases}$，

故知 $\begin{cases} x = x_1 + \frac{b}{r_n}t \\ y = x_0 - \frac{a}{r_n}t \end{cases}$，$t \in \mathbb{Z}$ 為 $ax + by = r_n$ 的一般解。

綜合前述，我們可以得到下面的定理：

設 $r_i = r_{i+1}q_{i+1} + r_{i+2}$，
$0 < r_i < r_{i-1}$，$i = 0, 1, 2, \ldots, n-1$.
$r_i, q_i \in \mathbb{Z}$，$r_n \neq 0$，$r_{n+1} = 0$，
其中 $a = r_0, b = r_1$
令 $x_{i-2} = x_i - q_{i-1}x_{i-1}$，$i = 2, \ldots, n$，
且令 $x_n = 0, x_{n-1} = 1$，則

(1) r_n 就是 a, b 的最大公因數。

(2) (x_1, x_0) 為不定方程式 $ax + by = r_n$ 的一個整數解。

(3) $\begin{cases} x = x_1 + \frac{b}{r_n}t \\ y = x_0 - \frac{a}{r_n}t \end{cases}$，$t \in \mathbb{Z}$ 為 $ax + by = r_n$ 的一般解。

Powered by MathBoard

gcd(a, b) 及 ax+by=gcd(a, b)之整數解II

@ 延伸的輾轉相除法直式算則II ⌄ | 依序輾轉 | 重啟 | 後推法實例 | 貝祖特等式 | 一般解 | 橫式算則 | 推導算則

延伸的輾轉相除法直式算則II

x_i	r_i	q_i
	572	
	75	7
	47	1
3	28	1
-2	19	1
1	9	2
0	1	9
	=====	

圖 15、後推法 x_i 行，由下方向上推導至一半的過程

伍、多重延伸的輾轉相除法

前面討論的延伸輾轉相除法，是解二元一次不定方程式的方法。其實，我們也可以延伸輾轉相除法直式算則，成為多重的輾轉相除法，並用它來解多元一次不定方程式。它基本上是使用下面這個遞迴定理的：

設 $c_1x_1+c_2x_2+\cdots+c_nx_n=d$，其中 $c_1,c_2,\cdots,c_n$ 為整數，$d=(c_1,c_2,\cdots,c_n)$ 為 $c_1,c_2,\cdots,c_n$ 的最大公因數，則 $(c_1,c_2,\cdots,c_n)=((c_1,c_2),c_3\cdots,c_n)$。

它其實就是用直式算則將不定方程前兩個係數的最大公因數求出後，再將第 3 係數與此數用直式求出新的最大公因數，這個過程一直推演下去就可以了。圖 16 展示的就是三元不定方程 $57x+36y+20z=3$ 的多重延伸輾轉相除法直式算則的一個實例。

圖中第一個輾轉相除與二元的輾轉相除完全相同。第二個輾轉相除的延伸行的第一項是 $(0,0,1)$，第二列是 $(-5,8,0)$，這是配合前面運算及元數是 3 的預設值。圖 17 展示的是以 a,b,c 為多項式重作多重延伸的輾轉相除法的實例，因 $(a,b,c)=(57,36,20)$，由多項式的係數可以清楚看出，第一輾轉相除式中，$(-5,8)$ 為 $57x+36y=3$ 的解，$(12,-19)$ 為 $57x+36y=0$ 的解；第二輾轉相除式中，倒數第二列的 $(-35,56,-1)$ 就是 $57x+36y+20z=3$ 的一個解，而 $(100,-160,3)$ 就是 $57x+36y+20z=0$ 的解。

我們以四元一次不定方程為例，描述多重的延伸輾轉相除法可得到的定理。

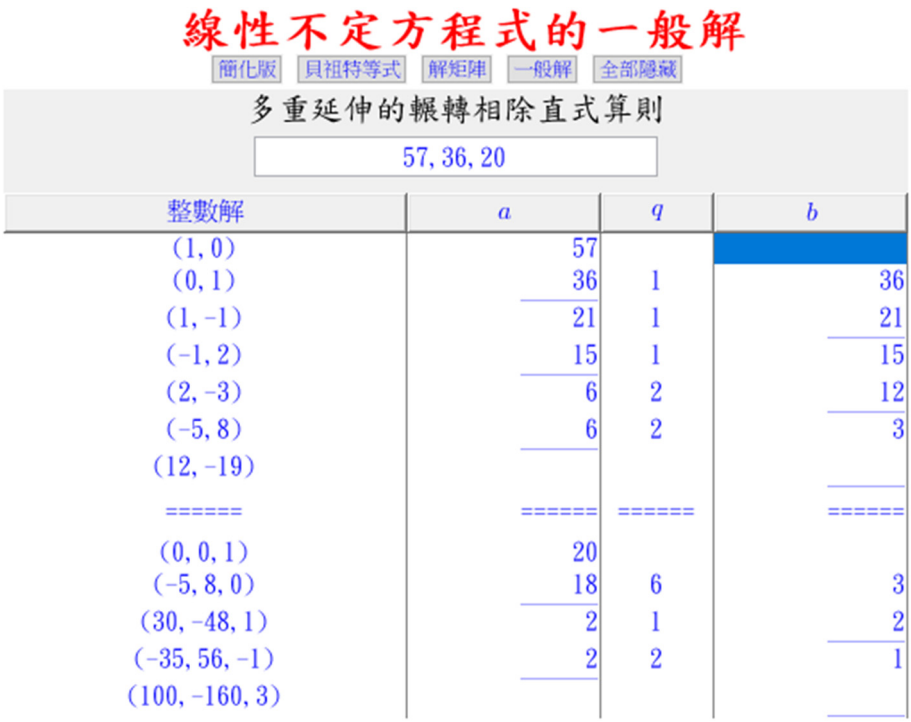


圖 16、三元不定方程式的多重直式算則實例

設$ax+by+cz+dw=e$，e為a,b,c,d的最大公因數，

若$ax_{31}+by_{31}+cz_{31}+dw_{31}=e$，
$ax_{30}+by_{30}+cz_{30}+dw_{30}=0$，
$ax_{20}+by_{20}+cz_{20}=0$，
$ax_{10}+by_{10}=0$ ，則

$$\begin{cases} x=x_{31}+x_{30}s+x_{20}t+x_{10}u \\ y=y_{31}+y_{30}s+y_{20}t+y_{10}u \\ z=z_{31}+z_{30}s+z_{20}t \\ w=w_{31}+w_{30}s \end{cases} \quad s,t,u\in\mathbb{Z}$$

為$ax+by+cz+dw=e$的一般解。

一般來說，整係數n元一次不定方程式的多重延伸輾轉相除法有$n-1$重輾轉相除算式。寫出一般解時，最後一重算式中取其延伸行的特殊解列及一般解列，其他重算式中，只取延伸行的一般解列。對於定理證明可參看 Rosser (1941)、Blankinship(1963)或 Bond (1967)，他們雖未使用多重延伸的直式算則，但對整係數n元一次不定方程式的一般解有類似的定理描述及證明。圖 19 展示的是$57x+36y+20z=1$的「一般解」及「解矩陣」按鈕呈現的內容。解矩陣就是解的係數構成的矩陣，它的行向量，就是多重延伸輾轉相除法直式算則延伸行中的向量。注意：數學算板「多重」延伸輾轉相除法程式的「一般解」按鈕，是展示更一般化的方程式解，它展示的是$c_1x_1+c_2x_2+\cdots+c_nx_n=dr$ 的一般解，其中 $d=(c_1,c_2,\cdots,c_n)$， r為任意整數，因此特殊解項上有參數r。

此外，數學算板的多重展轉相除法直式算則，可以輸入任意n個整數係數$c_1,c_2,\cdots,c_n$，作多重的輾轉相除。

多重延伸的輾轉相除直式算則

57, 36, 20

整數解	a	q	b
(1, 0)	a		
(0, 1)	b	1	b
(1, -1)	a - b	1	a - b
(-1, 2)	-a +2b	1	-a +2b
(2, -3)	2a -3b	2	4a -6b
(-5, 8)	-10a +16b	2	-5a +8b
(12, -19)	12a -19b		
======	======	======	======
(0, 0, 1)	c		
(-5, 8, 0)	-30a +48b	6	-5a +8b +0
(30, -48, 1)	30a -48b +c	1	30a -48b +c
(-35, 56, -1)	-70a +112b -2c	2	-35a +56b -c
(100, -160, 3)	100a -160b +3c		

圖 18、與圖 17 相對應多項式多重延伸的輾轉相除實例

陸、歐拉廣泛應用的線性不定方程式解法

模數除法的變數代換（以三元為例）

設$ax+by+cz=d,\ a,b,c,d\in\mathbb{Z}$

$abc\neq 0$　令$b=ab_q+b_r,\ c=ac_q+c_r$，

其中 $0\le b_r<a,\ 0\le c_r<a$

則$ax+by+cz$

$=a(x+b_qy+c_qz)+b_ry+c_rz=d$

令 $t=x+b_qy+c_qz$ 則 $at+b_ry+c_rz=d$ 這樣，由 $ax+by+cz=d$ 推得$t=x+b_qy+c_qz$ 及$at+b_ry+c_rz=d$ 的過程，我們稱之為**模數除法的變數代換**。[注意]式子中的係數 b_q,c_q 及 b_r,c_r分別是$b.c$ 分別除以a 得到的商及餘數。其實這種代換可對任一係數做類似的處理。

歐拉的線性不定方程式解法

歐拉（Euler）曾廣泛運用下述線性不定方程式的整數一般解的解法(可參看Olds,1963)。

設$21x+31y=1$，

則 $x=\frac{1-31y}{21}=-y+\frac{1-10y}{21}$，令t$=\frac{1-10y}{21}$ ，

則 $21t+10y=1$ 且 $x+y=t$

因 $y=\frac{1-21t}{10}=-2t+\frac{1-t}{10}$， 令$u=\frac{1-t}{10}$，

則 $t+10u=1$ 且 $2t+y=u$

消去t，解下列任一聯立方程式

(A) $\begin{cases}21x+31y=1\cdots\cdots(1)\\21t+10y=1\cdots\cdots(2)\\t+10u=1\cdots\cdots(3)\end{cases}$

(B) $\begin{cases}x+y=t\cdots\cdots(1)\\2t+y=u\cdots\cdots(2)\\t+10u=1\cdots\cdots(3)\end{cases}$

均可得

$y=-2+21u$ ， $x=3-31u$ 因此，

$\begin{cases}x=3-31u\\y=-2+21u\end{cases}\ u\in\mathbb{Z}$ 為$21x+31y=1$

的整數一般解。

上述解法是設定新未知數，並建立新聯立方程式(A)(B)解之而得。

其實前述解法前段四列分數相關敘述可以用下列形式呈現：

$21x+31y=1 \Rightarrow 21(x+y)+10y=1$

令$t=x+y$ 則$21t+10y=1$\

又 $21t+10y=1 \Rightarrow t+10(y+2t)=1$

令$u=y+2t$ 則 $t+10u=1$

也就是說，前面歐拉解法中的 (A)(B)兩聯立方程式，可由兩次「模數除法的變數代換」獲得。

柒、矩陣的列運算與延伸的多元輾轉相除法直式算則

矩陣的列運算

矩陣的列運算有三類：都可以用基本矩陣來表示,矩陣列運算的結果，可表示為基本矩陣與矩陣的乘積，設A為將作列運算的矩陣

$57x+36y+20z=r$的一般解為

$$\begin{cases}x=-35r+100s+12t\\y=56r-160s-19t\\z=-r+3s\end{cases},\quad r,s,t\text{整數}$$

$$\begin{bmatrix}-35&100&12\\56&-160&-19\\-1&3&0\end{bmatrix}$$

圖 19、用多重延伸的輾轉相除法直式算則按鈕得到的不定方程式一般解

(一) 令$T_{i,j}$為將單位矩陣的第 i 列與第 j 列交換的矩陣。$T_{i,j}A$ 的結果就是將A的第 i 列與第 j 列交換的矩陣。

(二) 令$L_{ij}(m)$ 為將單位矩陣的第 j 列第 i 行的 0 改為m的矩陣。$L_{ij}(m)A$就是將A的第 i 列乘以m加到第 j 列的矩陣。

(三) 令$D_i(m)$ 為將單位矩陣的第 i 列第 i 行的 1 改為m的矩陣。 $D_i(m)A$就是將A的第 i 列乘以m 的矩陣。

基本矩陣有下列性質：$\det(T_{i,j})=-1$, ${T_{i,j}}^{-1}=T_{i,j}$， $\det(L_{ij}(m))=1$。

整係數線性 n 元不定方程式的整數一般解

設 $c_1x_1+c_2x_2\ldots+c_nx_n=d$為線性 n 元不定方程式，其中$A_i$表示係數參數，$x_i$表示未知變數，對於任意已知整數係數 c_i，設d為c_i的最大公因數,我們可用下列矩陣式及其對應的增廣矩陣表示其關係

$$\begin{cases}A_1=c_1\\A_2=c_2\\\vdots\\A_n=c_n\end{cases}\Leftrightarrow\begin{bmatrix}1&0&0\cdots0\\0&1&0\cdots0\\&&\vdots\\0&0&0\cdots1\end{bmatrix}\begin{bmatrix}A_1\\A_2\\.\\.\\A_n\end{bmatrix}=\begin{bmatrix}c_1\\c_2\\\vdots\\c_n\end{bmatrix}\Leftrightarrow\left[\begin{array}{cccc|c}1&0&0\cdots0&&c_1\\0&1&0\cdots0&&c_2\\&&\vdots&&\vdots\\0&0&0\cdots1&&c_n\end{array}\right]$$

若透過矩陣第 1 及第 3 類的列運算，我們可將上述增廣矩陣變換為下列形式

$$\left[\begin{array}{cccc|c}\alpha_{11}&\alpha_{12}&\alpha_{13}\cdots\alpha_{1n}&&d\\\alpha_{21}&\alpha_{22}&\alpha_{23}\cdots\alpha_{2n}&&0\\&&\vdots&&\vdots\\\alpha_{n1}&\alpha_{n2}&\alpha_{n3}\cdots\alpha_{nn}&&0\end{array}\right]\Leftrightarrow\begin{bmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}\cdots\alpha_{1n}\\\alpha_{21}&\alpha_{22}&\alpha_{23}\cdots\alpha_{2n}\\&&\vdots\\\alpha_{n1}&\alpha_{n2}&\alpha_{n3}\cdots\alpha_{nn}\end{bmatrix}\begin{bmatrix}A_1\\A_2\\.\\.\\A_n\end{bmatrix}=\begin{bmatrix}d\\0\\\vdots\\0\end{bmatrix}$$

則 $[\alpha_{11}\ \alpha_{12}\ \alpha_{13}\cdots\alpha_{1n}]$ 為 $c_1x_1+c_2x_2+\cdots+c_nx_n=d$ 的一個解，而 $[\alpha_{i1}\ \alpha_{i2}\ \alpha_{i3}\cdots\alpha_{in}],i=2,3\cdots,n$ 為 $c_1x_1+c_2x_2+\cdots+c_nx_n=0$ 的解,亦即

$$c_1\alpha_{11}+c_2\alpha_{12}+\cdots+c_n\alpha_{1n}=d$$

及 $c_1\alpha_{i1}+c_2\alpha_{i2}+\cdots+c_n\alpha_{in}=0$,$i=2,3,\cdots,n$

亦即 $\sum_{j=1}^{j=n}c_j\alpha_{1j}=d$

及$\sum_{j=1}^{j=n}c_j\alpha_{ij}=0,i=2,3,\cdots,n$ [1]

由此我們可得到「**整係數線性 n 元不定方程式的整數一般解**」定理（參看 Rosser (1941)）：

若 $\left[\begin{array}{cccc|c}1&0&0\cdots0&&c_1\\0&1&0\cdots0&&c_2\\&&\vdots&&\vdots\\0&0&0\cdots1&&c_n\end{array}\right]$**可透過第 1、3 類的列運算化為** $\left[\begin{array}{cccc|c}\alpha_{11}&\alpha_{12}&\alpha_{13}\cdots\alpha_{1n}&&d\\\alpha_{21}&\alpha_{22}&\alpha_{23}\cdots\alpha_{2n}&&0\\&&\vdots&&\vdots\\\alpha_{n1}&\alpha_{n2}&\alpha_{n3}\cdots\alpha_{nn}&&0\end{array}\right]$,

其中 $d,c_i,\alpha_{ij}\in\mathbb{Z},i,j=1,2,\cdots,n$

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

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

$t_i\in\mathbb{Z},i=2,3,\cdots,n$ **[2]**

[證明] 由前述[1]之導引，我們由已知可推得 $\sum_{j=1}^{j=n}c_j\alpha_{1j}=d$ 及 $\sum_{j=1}^{j=n}c_j\alpha_{ij}=0,i=2,3,\cdots,n$

(1)設 $[x_1,x_2,\cdots,x_n]$ 具有**[2]** 的形式，令$r=t_1$，則

$$\begin{aligned}S&=c_1x_1+c_2x_2\ldots+c_nx_n\\&=c_1\textstyle\sum_{i=1}^{i=n}\alpha_{i1}t_i+c_2\sum_{i=1}^{i=n}\alpha_{i2}t_i+\cdots+\\&\quad c_n\textstyle\sum_{i=1}^{i=n}\alpha_{in}t_i\end{aligned}$$

對 $t_i,i=1,2,\cdots,n$ 做合併，

則 $S=\left(\sum_{j=1}^{j=n}c_j\alpha_{1j}\right)t_1+\left(\sum_{j=1}^{j=n}c_j\alpha_{2j}\right)t_2+\cdots$
$+\left(\sum_{j=1}^{j=n}c_j\alpha_{nj}\right)t_n$

亦即 $S=dt_1+0\cdot t_2+\cdots+0\cdot t_n=dr$，

故知 $[x_1,x_2,\cdots,x_n]$

為 $c_1x_1+c_2x_2\ldots+c_nx_n=dr$ 的解

反之，

(2)若$[x_1,x_2,\cdots,x_n]$

為$c_1x_1+c_2x_2\ldots+c_nx_n=dr$的解，

令

$$\begin{cases}x_1=\alpha_{11}A_1+\alpha_{21}A_2+\alpha_{31}A_3+\cdots+\alpha_{n1}A_n\\x_2=\alpha_{12}A_1+\alpha_{22}A_2+\alpha_{32}A_3+\cdots+\alpha_{n2}A_n\\\qquad\qquad\vdots\\x_n=\alpha_{1n}A_1+\alpha_{2n}A_2+\alpha_{3n}A_3+\cdots+\alpha_{nn}A_n\end{cases}$$

$A_i\in\mathbb{Z},i=2,3,\cdots,n$

設 $E=\begin{bmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}\cdots\alpha_{1n}\\\alpha_{21}&\alpha_{22}&\alpha_{23}\cdots\alpha_{2n}\\&&\vdots\\\alpha_{n1}&\alpha_{n2}&\alpha_{n3}\cdots\alpha_{nn}\end{bmatrix}$，由於 E 是單位矩陣透過 1、3 類列運算而得的結果，故 $\det(E^t)=\det(E)=\pm1$，亦即前述 A_i的聯立方程式恰有一組整數解。

故存在$A_i\in\mathbb{Z},i=2,3,\cdots,n$ 使前述聯立方程式成立。

但$[x_1,x_2,\cdots,x_n]$為

$c_1x_1+c_2x_2\ldots+c_nx_n=dr$的解，故

$c_1x_1+c_2x_2\ldots+c_nx_n$

$=c_1\sum_{i=1}^{i=n}\alpha_{i1}A_i+c_2\sum_{i=1}^{i=n}\alpha_{i2}A_i+\cdots+$
$c_n\sum_{i=1}^{i=n}\alpha_{in}A_i=dr$

分別對 $A_i,i=1,2,\cdots,n$ 做合併，

則$\left(\sum_{j=1}^{j=n}c_j\alpha_{1j}\right)A_1+\left(\sum_{j=1}^{j=n}c_j\alpha_{2j}\right)A_2+\cdots+$
$\left(\sum_{j=1}^{j=n}c_j\alpha_{nj}\right)A_n=dr$

亦即 $dA_1+0\cdot A_2+\cdots+0\cdot A_n=dr$，

故 $A_1=r$。取$\mathrm{t_i}=\mathrm{A_i},i=2,3,\cdots,n$ 亦即

對任意$c_1x_1+c_2x_2\ldots+c_nx_n=dr$的解

$[x_1,x_2,\cdots,x_n]$，存在$t_i\in\mathbb{Z},i=2,3,\cdots,n$

使得

$$\begin{cases}x_1=\alpha_{11}r+\alpha_{21}t_2+\alpha_{31}t_3+\cdots+\alpha_{n1}t_n\\x_2=\alpha_{12}r+\alpha_{22}t_2+\alpha_{32}t_3+\cdots+\alpha_{n2}t_n\\\qquad\qquad\vdots\\x_n=\alpha_{1n}r+\alpha_{2n}t_2+\alpha_{3n}t_3+\cdots+\alpha_{nn}t_n\end{cases}$$ 成立

由(1)(2)知

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

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

$t_i\in\mathbb{Z},i=2,3,\cdots,n$

對二元的情況，我們在前推法中已有說明。有關整係數n元線性不定方程式的整數一般解的討論，都可透過前述單位增廣矩陣的轉換來說明其原理。

圖 20 展示的就是列出不定方程式$2x-3y+7z=1$依前述定理作出的增廣矩陣，利用第 1、3 類矩陣列運算將其化為所求型式的結果圖示（利用代數算板作的列運算）。

故不定方程式$2x-3y+7z=1$的整數一般解為

$$\begin{cases}x=\qquad t\\y=2+7s-4t\\z=1+3s-2t\end{cases}\quad s,t\in\mathbb{Z}\qquad[3]$$

不同的 1、3 類列運算，可能得到不同形式的一般解，圖 21 展示的是另一種列運算得到的增廣矩陣。

由此我們可以得到不定方程式

$2x-3y+7z=1$的整數一般解：

$$\begin{cases}x=2-3s-14t\\y=1-2s-7t\\z=\qquad t\end{cases}\quad s,t\in\mathbb{Z}\qquad[4]$$

前述關於一般解的定理保證了[3]及[4]這兩組解的解集合是相同的，有興趣的讀者可以驗證一下。

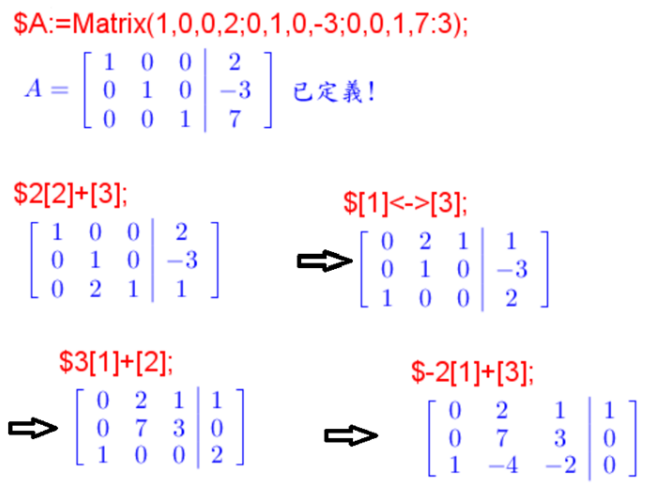


圖 20、$2x-3y+7z=1$增廣矩陣的第 1、3 類列運算

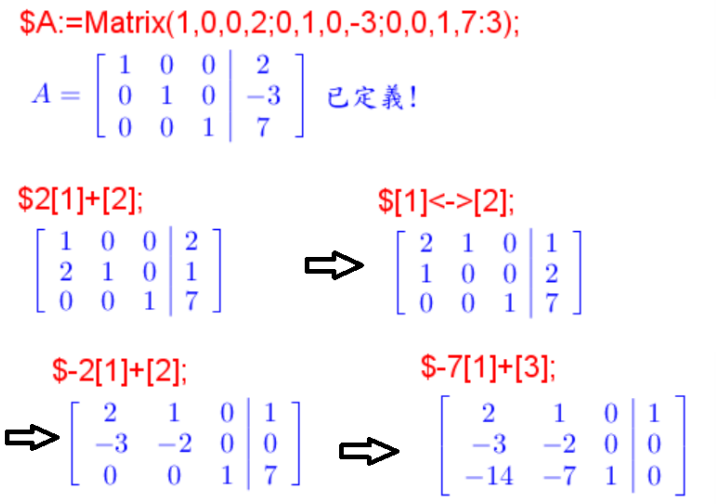


圖 21、不同於圖 20 的 1、3 類列運算得到不同的增廣矩陣

多元延伸的輾轉相除法算則

多重的延伸輾轉相除直式算則在取得特殊解時，有時數值會很大（Morito and Salkin 1979），圖 22 展示$8913x+5677y+4378z=r$的多重輾轉相除法一般解。

多重的輾轉相除法本質上仍然是兩數的相除，商行只有一行，Lehmer（1919）利用「模數除法的變數代換」的想法，提出模數「正」餘數除法的前推法多元輾轉相除法直式算則，於 1949 再提出後推法的直式算則。由於 Lehmer 這兩種多元的輾轉相除，在後續的處理中，無法在直式算則中直接獲得解矩陣（其實數學算板對這兩種方法也有建立程式及後續解法）。Morito 及 Salkin（1979）將 Lehmer（1949）後推法改為前推法得到可直接獲得解矩陣的直式算則，數學算板據此也製作了這種多元前推的一般解直式算則程式。圖 23 展示的就是這個程式的算則畫面，這是三元的實例，程式可輸入任意元的係數。

$$8913x+5677y+4378z=r, r\text{整數}\quad \text{的一般解為}$$
$$\begin{cases} x=-507r+2219646s+5677t \\ y=796r-3484888s-8913t \\ z=s \end{cases}, \quad s,t\text{整數}$$

圖 22、$8913x+5677y+4378z=r$的一般解

圖 23 中，將沒有空白的列編號為第 1 列，依序向上下編號。

a,b,c,d,q_1,q_2行計算的規則是：a_i除以b_i商為q_{1i}餘數為r_i，再將r_i除以c_i商為q_{2i}餘數為d_i，亦即 $a_i=b_i(q_{1i})+c_i(q_{2i})+d_i$，若除數是 0，則取商為 0，餘數續用。

x,y,z行計算的規則是：

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

這個規則可以用矩陣來描述，令

$$A_i=\left[\begin{array}{ccc|c} x_{i-2} & y_{i-2} & z_{i-2} & d_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} & d_{i-1} \\ x_i & y_i & z_i & d_i \end{array}\right],\ i=0,1,2,\cdots,n,$$

故 $A_0=\left[\begin{array}{ccc|c} 1&0&0&8913 \\ 0&1&0&5677 \\ 0&0&1&4378 \end{array}\right]$，其實$A_i$矩陣就是$x,y,z,d$行的第$i$列及其上方的二列構成的。令 $E_i=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -q_{1i} & -q_{2i} \end{bmatrix}$，$i=1,2,\cdots,n$，由於 $A_{i-1}=\left[\begin{array}{ccc|c} x_{i-3} & y_{i-3} & z_{i-3} & d_{i-3} \\ x_{i-2} & y_{i-2} & z_{i-2} & d_{i-2} \\ x_{i-1} & y_{i-1} & z_{i-1} & d_{i-1} \end{array}\right]$ 故知 $A_i=E_iA_{i-1}$。

E_i的第 1 列的作用，就是將A_{i-1}的第 2 列放到A_i第 1 列，第 2 列的做用就是將A_{i-1}的第 3 列放到A_i的第 2 列，第 3 列的作用就是將A_{i-1}的第 1 列加上第二列乘以$-q_{1i}$，再加上第 3 列乘以$-q_{2i}$，並將結果放在A_i的第 3 列。由於 E_i為第 1、3 類列運算組合的矩陣，$A_0\to A_{14}$的增廣矩陣推演，其實符合前面討論的「整係數線性 n 元不定方程式的整數一般解」定理的條件，因此，我

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 23、多元延伸輾轉相除直式算則，

們可以求出$8913x+5677y+4378z=r, r\in\mathbb{Z}$的一般解。最後一個矩陣$A_{14}=\left[\begin{array}{ccc|c}-19 & 36 & -8 & 1\\ -57 & 17 & 94 & 0\\ 61 & -95 & -1 & 0\end{array}\right]$，也就是說 x,y,z行的最後三列，就是圖 24 展示的解矩陣(A_{14}中不含增廣行的矩陣)。與圖 22 比較，多元輾轉相除算則得到的數值小了很多。圖 24 展示的是程式的「一般解」按鈕呈現的內容。

多元延伸的輾轉相除直式算則上，有可以展示每一列的「增廣矩陣推演」過程的按鈕，圖 25 展示的就是說明每一列相關資料的程式畫面中第 14 列的資料：第 14 增廣矩陣與獲得該矩陣的第 14 列運算矩陣及第 13 增廣矩陣。「計算進退」可改變展示不同的列資料，按左鍵前進，按右鍵後退。

圖 25（1）中，計算的規則是：a_i 除以 b_i 商為q_{1i}餘數為r_i，再將r_i除以c_i商為q_{2i}餘數為d_i，得 $a_i=b_i(q_{1i})+c_i(q_{2i})+d_i$，若除數是 0，則取商為 0，餘數續用。目前$i=14, a_i=2, b_i=1, c_i=0$，計算的規則是：2除以 1 商為2餘數為 0，再將餘數 0 除以 0，取商 0 餘數 0，亦即 $2=1(\mathbf{2})+0(\mathbf{0})+0$, 其中 $\mathbf{2},\mathbf{0}$ **分別**是兩商列上的數。

圖 25(2)中，第一列展示的是計算該列x,y,z及增廣行值的矩陣算式，得到的結果其實只是A_{14}的第三列。

圖 25(2)中，第二列中，

$E_{14}=\begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 1 & -2 & 0\end{bmatrix}$,

$A_{13}=\left[\begin{array}{ccc|c}23 & -23 & -17 & 2\\ -19 & 36 & -8 & 1\\ -57 & 17 & 94 & 0\end{array}\right]$,

$A_{14}=\left[\begin{array}{ccc|c}-19 & 36 & -8 & 1\\ -57 & 17 & 94 & 0\\ 61 & -95 & -1 & 0\end{array}\right]$

故$E_{14}A_{13}=A_{14}$。

在直式算則的推演中，E_{14}第 1 列的作用，就是將A_{13}的第 2 列放到A_{14}第 1 列，E_{14}第 2 列的做用就是將A_{13}的第 3 列放到A_{14}的第 2 列，E_{14}第 3 列的作用就是將A_{13}的第 1 列加上A_{13}第二列乘以$-q_{1i}$，再加上A_{13}第 3 列乘以$-q_{2i}$，其中$i=14$，並將結果放在A_{14}的第 3 列。

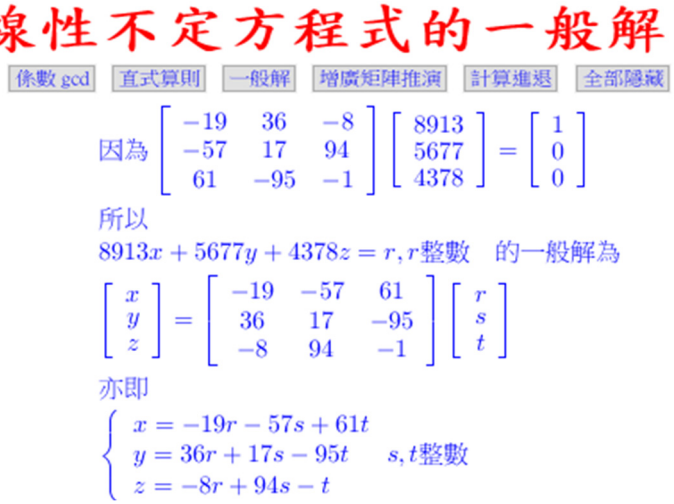


圖 24、多元延伸輾轉相除程式「一般解」按鈕呈現的畫面

矩陣方程式轉化目標

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}8913\\5677\\4378\end{bmatrix}=>\begin{bmatrix}\alpha_{11}&\alpha_{12}&\alpha_{13}\\\alpha_{21}&\alpha_{22}&\alpha_{23}\\\alpha_{31}&\alpha_{32}&\alpha_{33}\end{bmatrix}\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}$$

第 14 增廣矩陣A_{14} E_{14}為列運算矩陣 A_{13}為原增廣矩陣 $E_{14}A_{13}=A_{14}$

$(1)2=1(2)+0(0)+0$

$$(2)\begin{bmatrix}\mathbf{1}&-2&0\end{bmatrix}\left[\begin{array}{ccc|c}23&-23&-17&2\\-19&36&-8&1\\-57&17&94&0\end{array}\right]=\begin{bmatrix}61&-95&-1&0\end{bmatrix}$$

$$=>\begin{bmatrix}0&1&0\\0&0&1\\1&-2&0\end{bmatrix}\left[\begin{array}{ccc|c}23&-23&-17&2\\-19&36&-8&1\\-57&17&94&0\end{array}\right]=\left[\begin{array}{ccc|c}-19&36&-8&1\\-57&17&94&0\\61&-95&-1&0\end{array}\right]$$

第 14 矩陣方程式及方程組

$$\begin{bmatrix}-19&36&-8\\-57&17&94\\61&-95&-1\end{bmatrix}\begin{bmatrix}a\\b\\c\end{bmatrix}=\begin{bmatrix}1\\0\\0\end{bmatrix}<=>\begin{cases}-19a+36b-8c=1\\-57a+17b+94c=0\\61a-95b-c=0\end{cases}$$

圖 25、第 14 列運算相關的資料

捌、結語

本文從兩個問題出發，探求討輾轉相除法及其幾何意義，可以看出

輾轉相除法不只是一個求最大公因數的方法，它在解整係數線性不定方程式有一個重要的角色，其延伸的直式算則可以依序求出線性不定方程式的特解及一般解，對於二元的線性不定方程式，我們介紹了前推及後推兩方法的延伸直式算則及可以協助教學展示及原理說明的數學算板程式。對於多元的整係數線性不定方程式，我們也討論了本質上仍是兩數輾轉相除的多重的輾轉相除法及多個數同時參與的多元輾轉相除法直式算則，對於其相關的原理內容也有一些簡單的陳述與說明，希望本文及這些程式能對教師的教學及學生的學習有所幫助。

參考文獻

Blankinship, W. (1963). A New Version of the Euclidean Algorith. *The Ameri can Mathematical Monthly*, *70(7)*, 742-745. doi:10.2307/2312 260

Bond, J. (1967). Calculating the General Solution of a Linear Diophantine Equation. *The American Mathematical Monthly, 74(8)*, 955-957. doi:10.2307/2315274.

Lehmer, D. (1919). The General Solution of the Indeterminate Equation: Ax + By + Cz -.....= r. *Proceedinga of Nation al 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:10.2307/2302 718.

Morito,S. & Harvey M. Salkin(1979). Finding the General Solution of a Linear Diophantine Equation. *The Fibonacci Quarterly*.17-4, 361-368.

Olds, C. (1963). Continued Fractions. Mathematical Association of Ameri ca. Retrieved September 22, 2020, from http://www.jstor.org/stable/10.4169/j.ctt19b9kcr.

Rosser, B. (1941). A Note on the Linear Diophantine Equation. The Ameri can Mathematical Monthly, 48(10), 662-666. doi:10.2307/23033 05.