中華民國第 58 屆中小學科學展覽會

作品說明書

高級中等學校組　數學科

佳作

050418

重整勾股—迭代互質畢氏數

學校名稱：臺中市立臺中第一高級中等學校

作者：	指導老師：
高二 賴昱維	陳光鴻

關鍵詞：互質畢氏數三元樹、歐幾里得家族、迭代路徑

摘要

研究目的是證明貝格倫、普萊斯與菲爾斯托夫三元樹中所有互質畢氏數相等。研究動機是在這三種三元樹中存在著某些相同的互質畢氏數，如費馬三元數等，我因此猜想這三種三元樹中所有互質畢氏數相等。研究方法是由歐幾里得家族的生成公式與這三種三元樹中的 3 階方陣迭代公式建立 2 階方陣迭代公式，然後由 2 階方陣迭代公式與歐幾里得家族的生成公式探討歐幾里得家族中任一互質畢氏數在這三種三元樹中的迭代路徑。研究結果是由 2 階方陣迭代公式與歐幾里得家族的生成公式證明了這三種三元樹中所有互質畢氏數相等，建立歐幾里得家族中任一互質畢氏數在這三種三元樹中的迭代路徑碼，改良了普萊斯的建立方法，我未來展望是想將迭代路徑碼運用於密碼學。

壹、 研究動機

畢氏數（Pythagorean triples），又名勾股數，是符合畢氏定理（$a^2+b^2=c^2$）的正整數解(a,b,c)，而互質畢氏數（primitive Pythagorean triples）是(a,b,c)的最大公因數等於1。由同一生成公式產生的$\{(a_n,b_n,c_n)\}$稱為互質畢氏數家族（容士毅〔2〕，Price〔4〕）。當互質畢氏數符合a_n與c_n為奇數且b_n為偶數時，稱之為歐幾里得家族（Euclid family）：

$$\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}=\begin{bmatrix}{u_n}^2-{v_n}^2\\2u_nv_n\\{u_n}^2+{v_n}^2\end{bmatrix}，\ n,u_n,v_n\in N，\ u_n>v_n，\ (u_n,v_n)=1，\ u_n,v_n$$為一奇一偶（容士毅〔2〕）。

由於參加科展活動接觸互質畢氏數三元樹（a ternary tree of primitive Pythagorean triples）。由(a_1,b_1,c_1)為$(3,4,5)$開始，以三個相異的迭代公式（iteration formulas）可建構成互質畢氏數三元樹。凱文賴德（Kevin Ryde）認為互質畢氏數三元樹只存在三種，即貝格倫三元樹（Berggrens' tree）、普萊斯三元樹（Price's tree）與菲爾斯托夫三元樹（Ferstov's tree）：

㈠貝格倫（B. Berggrens）以$(3,4,5)$當作(a_1,b_1,c_1)，再由迭代公式(A)、(B)和(C)迭代產生(a_2,b_2,c_2)為$(5,12,13),(15,8,17),(21,20,29)$。再以$(a_2,b_2,c_2)$產生$(a_3,b_3,c_3)$，以此類推產生$(a_4,b_4,c_4),\cdots,(a_n,b_n,c_n),(a_{n+1},b_{n+1},c_{n+1})$，並建立貝格倫三元樹 (圖1）（Price〔4〕）。

(A) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}1&-2&2\\2&-1&2\\2&-2&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (B) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}-1&2&2\\-2&1&2\\-2&2&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (C) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}1&2&2\\2&1&2\\2&2&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$

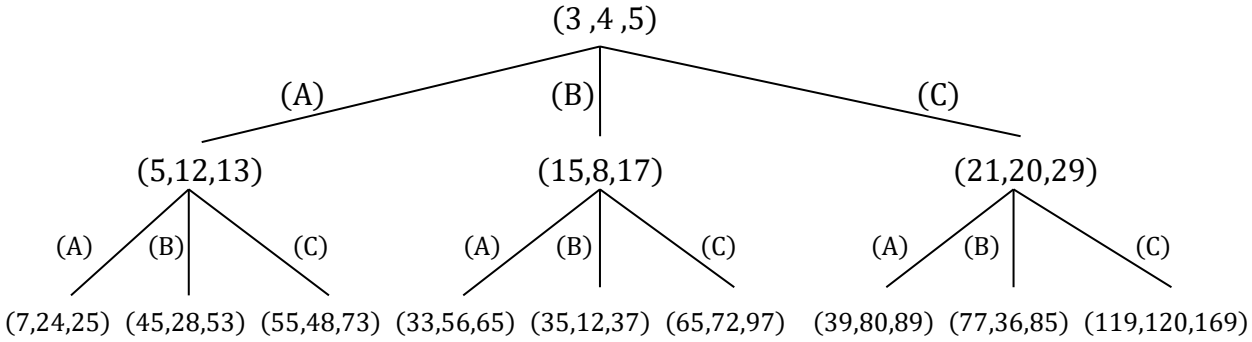


圖 1

㈡普萊斯(H. Lee Price)以$(3\ ,4\ ,5)$當作(a_1,b_1,c_1)，由迭代公式(D)、(E)和(F)產生(a_2,b_2,c_2)為$(5,12,13),(15,8,17),(7,24,25)$。同理，再以$(a_2,b_2,c_2)$產生$(a_3,b_3,c_3)$，以此方式類推產生$(a_4,b_4,c_4),\cdots,(a_n,b_n,c_n),(a_{n+1},b_{n+1},c_{n+1})$，並建立普萊斯三元樹 (圖 2) （Price〔4〕）。

(D) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&-1\\-2&2&2\\-2&1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (E) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&1\\2&-2&2\\2&-1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (F) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&-1&1\\2&2&2\\2&1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$

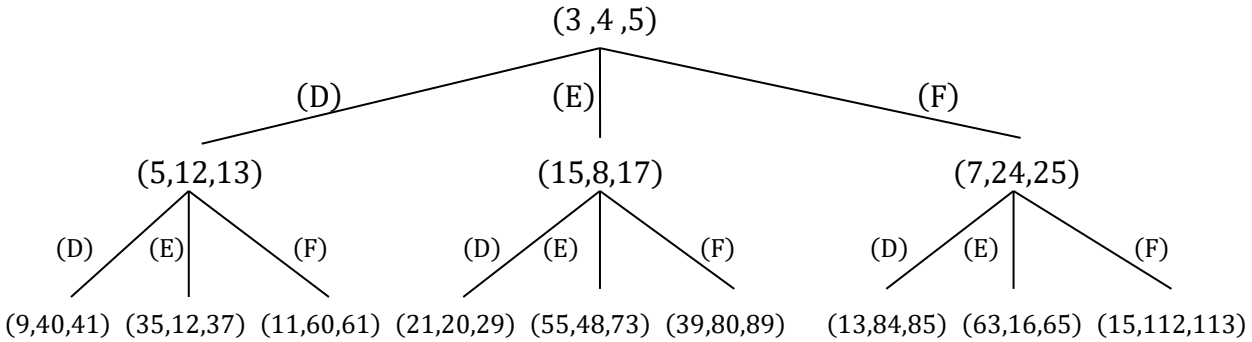


圖 2

㈢菲爾斯托夫 (V. E. Ferstov)以$(3\ ,4\ ,5)$當作(a_1,b_1,c_1)，由迭代公式(A)、(E)和(G)產生(a_2,b_2,c_2)為$(5,12,13),(15,8,17),(21,20,29)$。同理以$(a_2,b_2,c_2)$產生$(a_3,b_3,c_3)$，類推產生$(a_4,b_4,c_4),\cdots,(a_n,b_n,c_n),(a_{n+1},b_{n+1},c_{n+1})$，建立菲爾斯托夫三元樹 (圖 3) （Kevin〔3〕，Ferstov〔5〕）。

(A) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}1&-2&2\\2&-1&2\\2&-2&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (E) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&1\\2&-2&2\\2&-1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$; (G) $\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}-2&3&3\\-6&2&6\\-6&3&7\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$

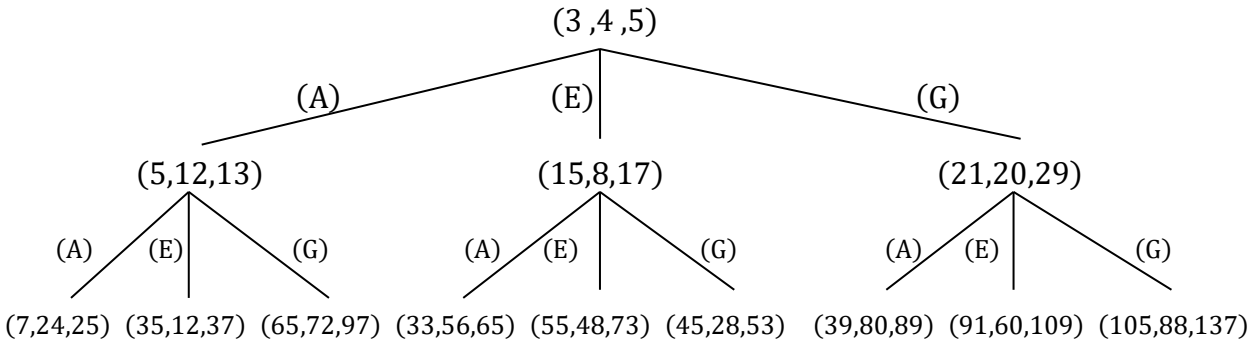


圖 3

費馬（Fermat）在 1643 年寫給梅森（Mersenne）信中提到費馬三元數（Fermat's triple），$(a,b,c)=(4565486027761,1061652293520,4687298610289)$，為符合兩股和與弦皆為完全平方數之條件的最小互質畢氏數，即$a+b=(2372159)^2$ 且$c=(2165017)^2$。普萊斯為了探討費馬三元數在貝格倫與普萊斯三元樹的迭代過程，則由(a_1,b_1,c_1)為(3 ,4 ,5)開始，透過貝格倫與普萊斯三元樹的迭代公式，得到了貝格倫三元樹的迭代路徑碼為 CAAACBBBBBB BBBABBCAAAAAAAAAAAAAAAACAACBBB，以及普萊斯三元樹的迭代路徑碼為 DDED DEDFDEDFDEDDDEDEDEDDDDDDEDDD（Price〔4〕）。其產生的過程卻是相當繁瑣。

我由歐幾里得家族的生成公式與貝格倫三元樹的迭代公式得到最簡真分數數列$\left\{\left(\frac{v_n}{u_n}\right)\right\}$的遞迴關係式，分別為 $\frac{v_{n+1}}{u_{n+1}}=\frac{1}{2-\frac{v_n}{u_n}}$，$\frac{v_{n+1}}{u_{n+1}}=\frac{1}{2+\frac{1}{\frac{v_n}{u_n}}}$，以及$\frac{v_{n+1}}{u_{n+1}}=\frac{1}{2+\frac{v_n}{u_n}}$，由此證明貝格倫三元樹產生歐幾里得家族中所有的互質畢氏數。我於是將發現的結果寫成「互質畢氏數三元樹」的文章，並且投稿中研院數研所數學傳播季刊。我之前已經在數學傳播季刊上發表了四篇有關互質畢氏數的文章，目前這一篇「互質畢氏數三元樹」為題的文章也已經獲得接受。

除了費馬三元數之外，我發現還有更多的互質畢氏數同時出現在貝格倫、普萊斯與菲爾斯托夫三元樹，例如(3 ,4 ,5)，(5 ,12 ,13)，(7,24,25)，(15 ,8 ,17)， (21,20,29) ，(35,12,37)，(39,80,89) 、(55,48,73)、…等。因此，我猜想這三種三元樹中所有的畢氏數皆相等。因為歐幾里得家族的生成公式是由二元數(u_n,v_n)產生互質畢氏數(a_n,b_n,c_n)，所以我想由歐幾里得家族的生成公式與這三種三元樹中的 3 階方陣迭代公式建立 2 階方陣迭代公式，然後由 2 階方陣迭代公式與歐幾里得家族的生成公式證明我的猜想，並且由此建立歐幾里得家族中任一互質畢氏數在這三種三元樹中的迭代路徑碼，希望由此改良普萊斯建立迭代路徑碼的方法。

貳、 研究目的

令歐幾里得家族為集合P_{Eucl}，且貝格倫、普萊斯與菲爾斯托夫三元樹集合P_{Berg}、P_{Pric}與P_{Fers}，則$P_{Eucl} = \{(a_n, b_n, c_n) \mid (a_n, b_n, c_n)$為歐幾里得家族中之數，$n \geqq 2$，$(a_1, b_1, c_1) = (3,4,5)\}$、

$P_{Berg} = \{(a_n, b_n, c_n) \mid (a_n, b_n, c_n)$為貝格倫三元樹中之數，$n \geqq 2$，$(a_1, b_1, c_1) = (3,4,5)\}$、

$P_{Pric} = \{(a_n, b_n, c_n) \mid (a_n, b_n, c_n)$為普萊斯三元樹中之數，$n \geqq 2$，$(a_1, b_1, c_1) = (3,4,5)\}$ 與

$P_{Fers} = \{(a_n, b_n, c_n) \mid (a_n, b_n, c_n)$為菲爾斯托夫三元樹中之數，$n \geqq 2$，$(a_1, b_1, c_1) = (3,4,5)\}$。

本研究的目的有三項，分別為㈠證明 $P_{Berg} = P_{Eucl}$，並建立P_{Eucl}中任一互質畢氏數在P_{Berg}的迭代路徑；㈡證明 $P_{Pric} = P_{Eucl}$，並建立P_{Eucl}中任一互質畢氏數在P_{Pric}的迭代路徑；㈢證明 $P_{Fers} = P_{Eucl}$，並建立P_{Eucl}中任一互質畢氏數在P_{Fers}的迭代路徑。

參、 研究設備及器材

筆、紙、電腦、電子計算機與excel 試算表。

肆、 研究方法與過程

一、 貝格倫三元樹與歐幾里得家族

(一) 貝格倫迭代公式與 2 階方陣的迭代公式

1. 因為歐幾里得家族生成公式由(u_n, v_n)產生 (a_n, b_n, c_n)，且貝格倫迭代公式具有3階方陣的形式，所以由貝格倫迭代公式與歐幾里得家族生成公式建立 2 階方陣的迭代公式，因此令(u_n, v_n)的迭代公式為$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} p_{11} & p_{21} \\ p_{12} & p_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$：

(1) 首先$(a_1, b_1, c_1) = (3\ ,4\ ,5)$由迭代公式(A)產生$(a_2, b_2, c_2) = (5,12,13)$，再產生$(a_3, b_3, c_3) = (7,24,25)$，再由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、

$(u_2, v_2) = (3,2)$及$(u_3, v_3) = (4,3)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} p_{11} & p_{21} \\ p_{12} & p_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(A′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

(2) 首先$(a_1, b_1, c_1) = (3,4,5)$由迭代公式(B)產生$(a_2, b_2, c_2) = (15,8,17)$，再產生$(a_3, b_3, c_3) = (35,12,37)$，再由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、$(u_2, v_2) = (4,1)$及$(u_3, v_3) = (6,1)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} p_{11} & p_{21} \\ p_{12} & p_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(B′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

(3) 首先$(a_1, b_1, c_1) = (3,4,5)$由迭代公式(C)產生$(a_2, b_2, c_2) = (21,20,29)$，再產生$(a_3, b_3, c_3) = (119,120,169)$，由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、$(u_2, v_2) = (5,2)$及$(u_3, v_3) = (12,5)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} p_{11} & p_{21} \\ p_{12} & p_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(C′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

2. 由迭代公式(A′)與歐幾里得家族的生成公式取代迭代公式(A)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(A′)與歐幾里得家族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(A′)可得$v_{n+1} = u_n$，$u_{n+1} = 2u_n - v_n$。因為$2u_n - v_n, u_n \in N$，$u_n < 2u_n - v_n$，$(2u_n - v_n, u_n) = 1$，$2u_n - v_n, u_n$為一奇一偶，所以$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}, v_{n+1}為一奇一偶。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為互質畢氏數。

(2) 由迭代公式(A′)可得到 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$。

證明：由歐幾里得家族的生成公式可得 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(A′)可得$v_{n+1} = u_n$，$u_{n+1} = 2u_n - v_n$。

因為 $\frac{u_{n+1}}{2}=u_n-\frac{v_n}{2}<u_n=v_{n+1}$，所以$\frac{u_{n+1}}{2}<v_{n+1}<u_{n+1}$。

(3) 由迭代公式(A′)可得到 $u_{n+1}+v_{n+1}>\ u_n+v_n$.

證明：由歐幾里得家族的生成公式可得$u_n,v_n\in N$， $v_n<u_n$， $(u_n,v_n)=1$，u_n,v_n為一奇一偶，由迭代公式(A′)可得 $v_{n+1}=u_n$， $u_{n+1}=2u_n-v_n$。因此 $u_{n+1}+v_{n+1}=2u_n-v_n+u_n=3u_n-v_n>\ u_n+v_n$。

(4) 無法由迭代公式(A′)得到$(u_{n+1},v_{n+1})=(2,1)$.

證明：令$(u_{n+1},v_{n+1})=(2,1)$，則由迭代公式(A′)可得$1=v_{n+1}=u_n$，$2=u_{n+1}=2u_n-v_n$。因此 $2=2u_n-v_n=2-v_n$，即$v_n=0$，不合。

(5) 若 $u_{n+1},v_{n+1}\in N$， $\frac{u_{n+1}}{2}<v_{n+1}<u_{n+1}$， $(u_{n+1},v_{n+1})=1$，u_{n+1},v_{n+1}為一奇一偶，則由迭代公式(A′)與歐幾里得家族生成公式所得到的(a_n,b_n,c_n) 為互質畢氏數。

證明：當$u_{n+1},v_{n+1}\in N$，$\frac{u_{n+1}}{2}<v_{n+1}<u_{n+1}$，$(u_{n+1},v_{n+1})=1$，$u_{n+1},v_{n+1}$為一奇一偶時，由迭代公式(A′)得到$v_n=-u_{n+1}+2v_{n+1}$，$u_n=v_{n+1}$。因為 $v_{n+1},-u_{n+1}+2v_{n+1}\in N$，$-u_{n+1}+2v_{n+1}<v_{n+1}$，$(v_{n+1},-u_{n+1}+2v_{n+1})=1$，$v_{n+1},-u_{n+1}+2v_{n+1}$為一奇一偶，所以$u_n,v_n\in N$，$v_n<u_n$，$(u_n,v_n)=1$，$u_n,v_n$為一奇一偶。因此，由迭代公式(A′)與歐幾里得家族的生成公式所得到的(a_n,b_n,c_n) 為互質畢氏數。

3. 由迭代公式(B′)與歐幾里得家族的生成公式取代迭代公式(B)。

(1) 若(a_n,b_n,c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(B′)與歐幾里得家族的生成公式所得到的$(a_{n+1},b_{n+1},c_{n+1})$ 為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n,v_n\in N$，$v_n<u_n$，$(u_n,v_n)=1$，u_n,v_n為一奇一偶，因此由迭代公式(B′)可得$v_{n+1}=v_n$，$u_{n+1}=u_n+2v_n$。因為$u_n+2v_n,v_n\in N$，$v_n<u_n+2v_n$，$(u_n+2v_n,v_n)=1$，u_n+2v_n,v_n為一奇一偶，所以$u_{n+1},v_{n+1}\in N$，$v_{n+1}<u_{n+1}$，$(u_{n+1},v_{n+1})=1$，u_{n+1},v_{n+1}為一奇一偶。

因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為互質畢氏數。

(2) 由迭代公式(B′)可得到 $0 < v_{n+1} < \frac{u_{n+1}}{3}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此，由迭代公式(B′)可得$v_{n+1} = v_n$，$u_{n+1} = u_n + 2v_n$。因為 $\frac{u_{n+1}}{3} = \frac{u_n}{3} + \frac{2v_n}{3} > v_n = v_{n+1} > 0$，所以 $0 < v_{n+1} < \frac{u_{n+1}}{3}$。

(3) 由迭代公式(B′)可得到 $u_{n+1} + v_{n+1} > u_n + v_n$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，由迭代公式(B′)可得$v_{n+1} = v_n$，$u_{n+1} = u_n + 2v_n$。因此 $u_{n+1} + v_{n+1} = u_n + 2v_n + v_n = u_n + 3v_n > u_n + v_n$。

(4) 無法由迭代公式(B′)得到$(u_{n+1}, v_{n+1}) = (2,1)$。

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，則由迭代公式(B′)可得$1 = v_{n+1} = v_n$，$2 = u_{n+1} = u_n + 2v_n$。因此，$2 = u_n + 2v_n = u_n + 2$，即$u_n = 0$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$，$0 < v_{n+1} < \frac{u_{n+1}}{3}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶，則由迭代公式(B′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n)為互質畢氏數。

證明：當 $u_{n+1}, v_{n+1} \in N$，$0 < v_{n+1} < \frac{u_{n+1}}{3}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶時，則由迭代公式(B′)得$u_n = u_{n+1} - 2v_{n+1}$，$v_n = v_{n+1}$。因為$u_{n+1} - 2v_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1} - 2v_{n+1}$，$(u_{n+1} - 2v_{n+1}, v_{n+1}) = 1$，$u_{n+1} - 2v_{n+1}, v_{n+1}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(B′)與歐幾里得家族的生成公式所得到的(a_n, b_n, c_n)為互質畢氏數。

4. 由迭代公式(C′)與歐幾里得家族的生成公式取代迭代公式(C)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(C′)與歐幾里得家

族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(C')可得$v_{n+1} = u_n$，$u_{n+1} = 2u_n + v_n$。因為$2u_n + v_n, u_n \in N$，$u_n < 2u_n + v_n$，$(2u_n + v_n, u_n) = 1$，$2u_n + v_n, u_n$為一奇一偶，所以$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}, v_{n+1}為一奇一偶。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為互質畢氏數。

(2) 由迭代公式(C')可得到 $\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(C')可得$v_{n+1} = u_n$，$u_{n+1} = 2u_n + v_n$。因為 $\frac{u_{n+1}}{2} = u_n + \frac{v_n}{2} > u_n = v_{n+1}$，而且$\frac{u_{n+1}}{3} = \frac{2u_n}{3} + \frac{v_n}{3} < u_n = v_{n+1}$，所以可得 $\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$。

(3) 由迭代公式(C')可得到 $u_{n+1} + v_{n+1} > u_n + v_n$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(C')可得$v_{n+1} = u_n$，$u_{n+1} = 2u_n + v_n$，所以 $u_{n+1} + v_{n+1} = 2u_n + v_n + u_n = 3u_n + v_n > u_n + v_n$。

(4) 無法由迭代公式(C')得到$(u_{n+1}, v_{n+1}) = (2,1)$。

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，由迭代公式$(C')$可得$1 = v_{n+1} = u_n$，$2 = u_{n+1} = 2u_n + v_n$。因此，$2 = 2u_n + v_n = 2 + v_n$，即$v_n = 0$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$，$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶，則由迭代公式$(C')$與歐幾里得家族生成公式所得到的$(a_n, b_n, c_n)$為互質畢氏數。

證明：當 $u_{n+1}, v_{n+1} \in N$，$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$

為一奇一偶時，則由迭代公式(C′)得$v_n = u_{n+1} - 2v_{n+1}$，$u_n = v_{n+1}$。因為$v_{n+1}, u_{n+1} - 2v_{n+1} \in N$，$u_{n+1} - 2v_{n+1} < v_{n+1}$，$(v_{n+1}, u_{n+1} - 2v_{n+1}) = 1$，$v_{n+1}, u_{n+1} - 2v_{n+1}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(C′)與歐幾里得家族的生成公式所得到的(a_n, b_n, c_n)為互質畢氏數。

(二) 貝格倫三元樹與歐幾里得家族的所有互質畢氏數相等

1. $\mathrm{P}_{\mathrm{Eucl}} \sqsubseteq \mathrm{P}_{\mathrm{Berg}}$，證明如下：

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P}_{\mathrm{Eucl}}$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且$u_{n+1}, v_{n+1}$為一奇一偶。因此，$u_{n+1}$與$v_{n+1}$的大小關係可分成$\frac{u_{n+1}}{2} = v_{n+1}$，$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$ 以及$0 < v_{n+1} < \frac{u_{n+1}}{3}$。

(2) 當 $\frac{u_{n+1}}{2} = v_{n+1}$ 時，則$(u_{n+1}, v_{n+1}) = (2,1)$；當 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$ 時，選擇迭代公式(A′)並且迭代產生(u_n, v_n)；當$0 < v_{n+1} < \frac{u_{n+1}}{3}$時，選擇迭代公式(B′)並且迭代產生$(u_n, v_n)$；當 $\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$ 時，選擇迭代公式(C′)並且迭代產生(u_n, v_n)。因此由貝格倫三元樹可得到圖 4。

(3) 按照u_{n+1}與v_{n+1}的關係選擇迭代公式(A′)、(B′)或(C′)產生(u_n, v_n)，由第 7 至 10 頁之論證可證得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此$(a_n, b_n, c_n) \in \mathrm{P}_{\mathrm{Eucl}}$。

(4) 同理，(a_n, b_n, c_n)可產生$(a_{n-1}, b_{n-1}, c_{n-1})$，且可證得$(a_{n-1}, b_{n-1}, c_{n-1}) \in \mathrm{P}_{\mathrm{Eucl}}$。

(5) 由於$(u_{n+1} + v_{n+1}) > (u_n + v_n)$，因此$(u_{n+1}, v_{n+1})$依此回推至$(u_1, v_1) = (2,1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依此回推至$(a_1, b_1, c_1) = (3,4,5)$，同樣無法再回推。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P}_{\mathrm{Berg}}$，即$\mathrm{P}_{\mathrm{Eucl}} \sqsubseteq \mathrm{P}_{\mathrm{Berg}}$。

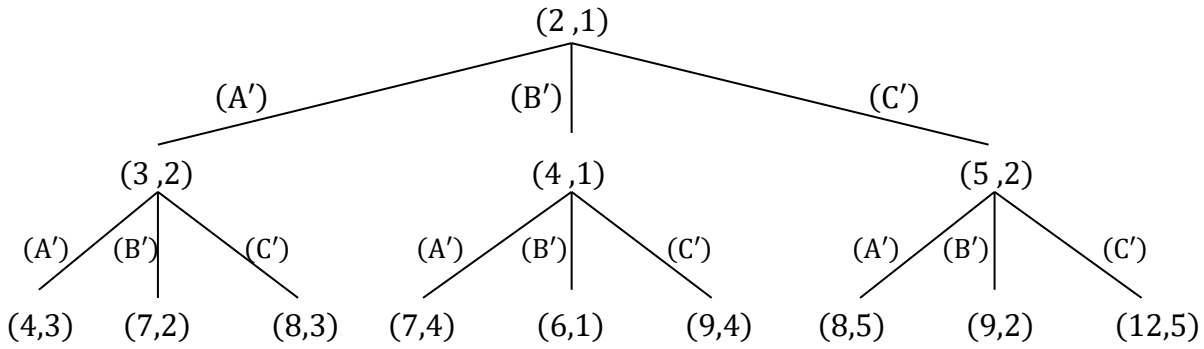


圖 4

2. $\mathrm{P_{Berg}} \sqsubseteq \mathrm{P_{Eucl}}$。證明如下：

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Berg}}$而言，存在一個長度為$n$的貝格倫路徑碼，為敘述方便起見，不失一般性，假設$\overbrace{\mathrm{AABBBCCCC\cdots ABC}}^{n}$使得$(a_1, b_1, c_1) = (3,4,5)$經過迭代公式(A)(A)(B)(B)(B)(C)(C)(C)(C)…(A)(B)(C)產生$(a_{n+1}, b_{n+1}, c_{n+1})$。

(2) 因為迭代公式(A)唯一決定迭代公式(A′)，迭代公式(B)唯一決定迭代公式(B′)，迭代公式(C)唯一決定迭代公式(C′)，所以路徑碼$\overbrace{\mathrm{AABBBCCCC\cdots ABC}}^{n}$唯一決定路徑碼$\overbrace{\mathrm{A'A'B'B'B'C'C'C'C'\cdots A'B'C'}}^{n}$。

(3) $(u_1, v_1) = (2,1)$由路徑碼$\overbrace{\mathrm{A'A'B'B'B'C'C'C'C'\cdots A'B'C'}}^{n}$迭代產生$(u_{n+1}, v_{n+1})$，由第 7 至 10 頁之論證可證得$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且$u_{n+1}, v_{n+1}$為一奇一偶。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Eucl}}$且$(a_1, b_1, c_1) \in \mathrm{P_{Eucl}}$，即$\mathrm{P_{Berg}} \sqsubseteq \mathrm{P_{Eucl}}$。

(三) 歐幾里得家族中任一互質畢氏數在貝格倫三元樹的迭代路徑

1. 由 2 階方陣的迭代公式迭代產生歐幾里得家族的互質畢氏數

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，且不等於$(3,4,5)$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$。$(u_{n+1}, v_{n+1})$依照表 1 中$u_{n+1}$與$v_{n+1}$的關係選擇迭代公式(A′)、(B′)或(C′)，並且得到(u_n, v_n)。

表 1

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
(A')	$0 < v_n < u_n$， u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$， u_{n+1}, v_{n+1}為一奇一偶
(B')	$0 < v_n < u_n$， u_n, v_n為一奇一偶	$0 < v_{n+1} < \frac{u_{n+1}}{3}$， u_{n+1}, v_{n+1}為一奇一偶
(C')	$0 < v_n < u_n$， u_n, v_n為一奇一偶	$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$， u_{n+1}, v_{n+1}為一奇一偶

(2) 同理，由u_n與v_n的關係選擇迭代公式(A')、(B')或(C')，得到u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(A')、(B')或(C')，得到(u_{n-2}, v_{n-2})。然後以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A')、(B')以及(C')的迭代路徑。再由迭代公式(A')、(B')以及(C')的迭代路徑得到迭代公式(A)、(B)以及(C)的迭代路徑。

2. 由 excel 試算表的公式迭代產生費馬三元數

(1) 因為費馬三元數$(a_{n+1}, b_{n+1}, c_{n+1})$的$(u_{n+1}, v_{n+1})$為$(2150905,246792)$，貝格倫三元樹產生費馬三元數的方法可由$(u_{n+1}, v_{n+1}) = (2150905,246792)$產生$(u_1, v_1) = (2,1)$，依照依照表 1 的規則設計 excel 試算表的公式（表 2）。

表 2

	A	B	C
6	2150905	1657321	1163737
7	246792	246792	246792
8			
9	2	2	2

(2) 迭代u_n的 excel 公式

①. A6 = u_{n+1} = 2150905

②. B6 = u_n =IF(A6=2,2,IF(2*A7>A6,A7,IF(3*A7<A6,A6-2*A7,A7)))= 1657321

③. C6=u_{n-1}=IF(B6=2,2,IF(2*B7>B6,B7,IF(3*B7<B6,B6-2*B7,B7)))= 1163737

(3) 迭代v_n的 excel 公式

①. A7 = v_{n+1} = 246792

②. B7 = v_n=IF(A6=2,1,IF(2*A7>A6,2*A7-A6,IF(3*A7<A6,A7,A6-2*A7)))= 246792

③. C7=v_{n-1}=IF(B6=2,1,IF(2*B7>B6,2*B7-B6,IF(3*B7<B6,B7,B6-2*B7)))= 246792

(4) 迭代公式的 excel 公式

①. 表格 A9、B9 與 C9 中 1 =迭代公式 A'；2 =迭代公式 B'；3 =迭代公式 C'。

②. A9 = IF(A6=2,0,IF(2*A7>A6,1,IF(3*A7<A6,2,3)))=2= 迭代公式 B'

③. B9 =IF(B6=2,0,IF(2*B7>B6,1,IF(3*B7<B6,2,3)))=2 =迭代公式 B'

④. C9 =IF(C6=2,0,IF(2*C7>C6,1,IF(3*C7<C6,2,3)))=2= 迭代公式 B'

(5) 因此由$(u_{n+1}, v_{n+1}) = (2150905,246792)$產生$(u_1, v_1) = (2,1)$，迭代公式的順序為 B'B'B'C'A'A'C'A'A'A'A'A'A'A'A'A'A'A'A'A'A'C'B'B'A'B'B'B'B' B'B'B'B'B' C'A'A'A'C'。

(6) 因此由$(a_1, b_1, c_1) = (3,4,5)$產生費馬三元數，迭代公式依序為 CAAACBBB BBBBBBABBCAAAAAAAAAAAAAAACAACBBB。

二、 普萊斯三元樹與歐幾里得家族

(一) 普萊斯的迭代公式與 2 階方陣的迭代公式

1. 因為歐幾里得家族生成公式由(u_n, v_n)產生 (a_n, b_n, c_n)，且普萊斯迭代公式具有3階方陣的形式，所以由普萊斯迭代公式與歐幾里得家族生成公式建立 2 階方陣的迭代公式，因此令(u_n, v_n)的迭代公式為$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} q_{11} & q_{21} \\ q_{12} & q_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$：

(1) $(a_1, b_1, c_1) = (3\ ,4\ ,5)$由迭代公式(D)產生$(a_2, b_2, c_2) = (5,12,13)$，再產生$(a_3, b_3, c_3) = (9,40,41)$，再由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、$(u_2, v_2) = (3,2)$及$(u_3, v_3) = (5,4)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} q_{11} & q_{21} \\ q_{12} & q_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(D′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

(2) $(a_1, b_1, c_1) = (3\ ,4\ ,5)$由迭代公式(E)產生$(a_2, b_2, c_2) = (15,8,17)$，再產生$(a_3, b_3, c_3) = (55,48,73)$，再由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、

$(u_2, v_2) = (4,1)$及$(u_3, v_3) = (8,3)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} q_{11} & q_{21} \\ q_{12} & q_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(E′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

(3) $(a_1, b_1, c_1) = (3\ ,4\ ,5)$由迭代公式(F)產生$(a_2, b_2, c_2) = (7,24,25)$，再產生$(a_3, b_3, c_3) = (15,112,113)$，由歐幾里得家族生成公式得$(u_1, v_1) = (2,1)$、$(u_2, v_2) = (4,3)$及$(u_3, v_3) = (8,7)$，代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} q_{11} & q_{21} \\ q_{12} & q_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$求得迭代公式(F′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

2. 由迭代公式(D′)與歐幾里得家族的生成公式取代迭代公式(D)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(D′)與歐幾里得家族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(D′)可得$u_{n+1} = u_n + v_n$，$v_{n+1} = 2v_n$。因為$u_n + v_n, 2v_n \in N$，$2v_n < u_n + v_n$，$(u_n + v_n, 2v_n) = 1$，$u_n + v_n$為奇數，$2v_n$為偶數，所以$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為奇數，v_{n+1}為偶數。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$為互質畢氏數。

(2) 由迭代公式(D′)可得到 $0 < v_{n+1} < u_{n+1}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此，由迭代公式(D′)可得$u_{n+1} = u_n + v_n$，$v_{n+1} = 2v_n$。因為$0 < v_{n+1} = 2v_n < u_n + v_n = u_{n+1}$，所以 $0 < v_{n+1} < u_{n+1}$。

(3) 由迭代公式(D′)可得到 $u_{n+1} + v_{n+1} > u_n + v_n$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，由迭代公式(D′)可得$u_{n+1} = u_n + v_n$，$v_{n+1} = 2v_n$。

因此，$u_{n+1} + v_{n+1} = u_n + v_n + 2v_n = u_n + 3v_n > u_n + v_n$。

(4) 無法由迭代公式(D′)得到$(u_{n+1}, v_{n+1}) = (2,1)$。

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，由迭代公式(D′)可得$1 = v_{n+1} = 2v_n$，

$2 = u_{n+1} = u_n + v_n$，所以$v_n = \frac{1}{2}$，$u_n = \frac{3}{2}$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$，$0 < v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為奇數，v_{n+1}為偶數，則由迭代公式(D′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

證明：當$0 < v_{n+1} < u_{n+1}$，u_{n+1}為奇數，v_{n+1}為偶數時，則由迭代公式(D′)得到$v_n = u_{n+1} - \frac{1}{2}v_{n+1}$，$u_n = \frac{v_{n+1}}{2}$。因為$\frac{v_{n+1}}{2}, u_{n+1} - \frac{1}{2}v_{n+1} \in N$，$u_{n+1} - \frac{1}{2}v_{n+1} < \frac{v_{n+1}}{2}$，$\left(\frac{v_{n+1}}{2}, u_{n+1} - \frac{1}{2}v_{n+1}\right) = 1$，$\frac{v_{n+1}}{2}, u_{n+1} - \frac{1}{2}v_{n+1}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(D′)與歐幾里得家族的生成公式所得到的(a_n, b_n, c_n) 為歐幾里得家族的互質畢氏數。

3. 由迭代公式(E′)與歐幾里得家族的生成公式取代迭代公式(E)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(E′)與歐幾里得家族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(E′)可得$u_{n+1} = 2u_n$，$v_{n+1} = u_n - v_n$。因為$2u_n, u_n - v_n \in N$，$u_n - v_n < 2u_n$，$(2u_n, u_n - v_n) = 1$，$2u_n$為偶數，$u_n - v_n$為奇數，所以$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為偶數，v_{n+1}為奇數。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為互質畢氏數。

(2) 由迭代公式(E′)可得到 $0 < v_{n+1} < \frac{u_{n+1}}{2}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，

u_n, v_n為一奇一偶。因此，由迭代公式(E′)可得$u_{n+1} = 2u_n$，$v_{n+1} = u_n - v_n$。

因為 $0 < v_{n+1} = \frac{u_{n+1}}{2} - v_n < \frac{u_{n+1}}{2}$，以 $0 < v_{n+1} < \frac{u_{n+1}}{2}$。

(3) 由迭代公式(E′)可得到 $u_{n+1} + v_{n+1} > u_n + v_n$.

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，由迭代公式(E′)可得$u_{n+1} = 2u_n$，$v_{n+1} = u_n - v_n$。

因此，$(u_{n+1} + v_{n+1}) = 2u_n + u_n - v_n = 3u_n - v_n > u_n + v_n$。

(4) 無法由迭代公式(E′)得到$(u_{n+1}, v_{n+1}) = (2,1)$.

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，由迭代公式(E′)可得$1 = v_{n+1} = u_n - v_n$，$2 = u_{n+1} = 2u_n$。因此，$u_n = 1$，$v_n = 0$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$，$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}$為偶數，$v_{n+1}$為奇數，則由迭代公式(E′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

證明：$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，則由迭代公式(F′)得$u_n = \frac{u_{n+1}}{2}$，$v_n = \frac{u_{n+1}}{2} - v_{n+1}$。因為$\frac{u_{n+1}}{2}, \frac{u_{n+1}}{2} - v_{n+1} \in N$，$\frac{u_{n+1}}{2} - v_{n+1} < \frac{u_{n+1}}{2}$，$\left(\frac{u_{n+1}}{2}, \frac{u_{n+1}}{2} - v_{n+1}\right) = 1$，$\frac{u_{n+1}}{2}, \frac{u_{n+1}}{2} - v_{n+1}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(F′)與歐幾里得家族的生成公式所得到的(a_n, b_n, c_n) 為歐幾里得家族的互質畢氏數。

4. 由迭代公式(F′)與歐幾里得家族的生成公式取代迭代公式(F)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(F′)與歐幾里得家族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為歐幾里得家族的互質畢氏數。

證明：歐幾里得家族的生成公式中 $u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶，因此由迭代公式(F′)可得$u_{n+1} = 2u_n$， $v_{n+1} = u_n + v_n$。因為$2u_n, u_n + v_n \in N$，$u_n + v_n < 2u_n$，$(2u_n, u_n + v_n) = 1$，$2u_n$為偶數，$u_n + v_n$

為奇數，所以$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為偶數，v_{n+1}為奇數。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為互質畢氏數。

(2) 由迭代公式(F′)可得到 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$， $v_n < u_n$， $(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此，由迭代公式(F′)可得$u_{n+1} = 2u_n$， $v_{n+1} = u_n + v_n$。因為 $\frac{u_{n+1}}{2} < v_{n+1} = \frac{u_{n+1}}{2} + v_n < u_{n+1}$，所以 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$。

(3) 由迭代公式(F′)可得到 $u_{n+1} + v_{n+1} > u_n + v_n$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$， $v_n < u_n$， $(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此，由迭代公式(F′)可得 $u_{n+1} = 2u_n$, $v_{n+1} = u_n + v_n$。所以 $u_{n+1} + v_{n+1} = 2u_n + v_n + u_n = 3u_n + v_n > u_n + v_n$。

(4) 無法由迭代公式(F′)得到$(u_{n+1}, v_{n+1}) = (2,1)$。

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，由迭代公式(F′)可得$1 = v_{n+1} = u_n + v_n$，$2 = u_{n+1} = 2u_n$，所以$u_n = 1$， $v_n = 0$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$, $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$, $(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為偶數，v_{n+1}為奇數，則由迭代公式(F′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

證明：$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，則由迭代公式(F′)得 $u_n = \frac{u_{n+1}}{2}$，$v_n = -\frac{u_{n+1}}{2} + v_{n+1}$。因為$\frac{u_{n+1}}{2}, -\frac{u_{n+1}}{2} + v_{n+1} \in N$，$-\frac{u_{n+1}}{2} + v_{n+1} < \frac{u_{n+1}}{2}$，$\left(\frac{u_{n+1}}{2}, -\frac{u_{n+1}}{2} + v_{n+1}\right) = 1$，$\frac{u_{n+1}}{2}, -\frac{u_{n+1}}{2} + v_{n+1}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(F′)與歐幾里得家族的生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

(二) 普萊斯三元樹與歐幾里得家族

1. $\mathrm{P_{Eucl}} \sqsubseteq \mathrm{P_{Pric}}$。證明如下：

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Eucl}}$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且$u_{n+1}, v_{n+1}$為一奇一偶。因此，$u_{n+1}$與$v_{n+1}$的大小關係可分成$\frac{u_{n+1}}{2} = v_{n+1}$；$0 < v_{n+1} < u_{n+1}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數；$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數；$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數。

(2) 當$\frac{u_{n+1}}{2} = v_{n+1}$時，則$(u_{n+1}, v_{n+1}) = (2,1)$；當$0 < v_{n+1} < u_{n+1}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數時，選擇迭代公式$(\mathrm{D}')$並且迭代產生$(u_n, v_n)$；當$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式$(\mathrm{E}')$並且迭代產生$(u_n, v_n)$；當$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式$(\mathrm{F}')$並且迭代產生$(u_n, v_n)$。因此，由普萊斯三元樹可得到圖 5。

(3) 按照u_{n+1}與v_{n+1}的關係選擇迭代公式(D')、(E')或(F')產生(u_n, v_n)，由第 14 至 18 頁之論證可證得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此$(a_n, b_n, c_n) \in \mathrm{P_{Eucl}}$。

(4) 同理，(a_n, b_n, c_n)可產生$(a_{n-1}, b_{n-1}, c_{n-1})$，且可證得$(a_{n-1}, b_{n-1}, c_{n-1}) \in \mathrm{P_{Eucl}}$。

(5) 由於$(u_{n+1} + v_{n+1}) > (u_n + v_n)$，因此$(u_{n+1}, v_{n+1})$依此回推至$(u_1, v_1) = (2,1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依此回推至$(a_1, b_1, c_1) = (3,4,5)$，同樣無法再回推。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Pric}}$，即$\mathrm{P_{Eucl}} \sqsubseteq \mathrm{P_{Pric}}$。

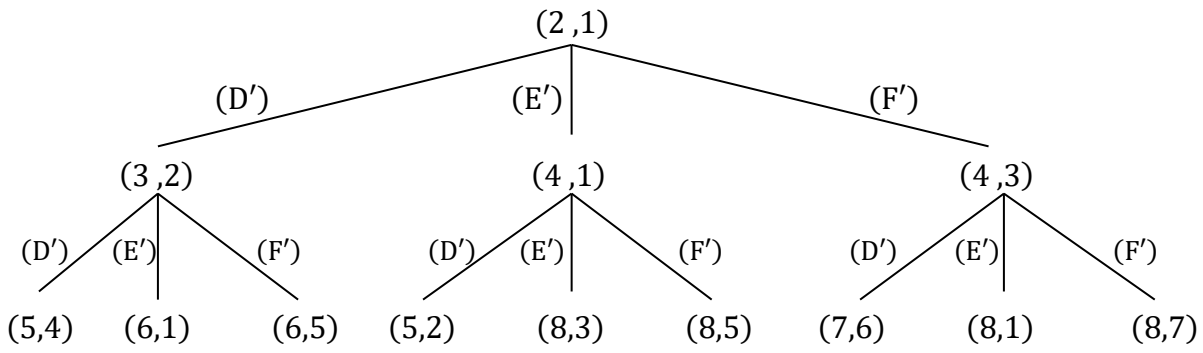


圖 5

2. $\mathrm{P_{Pric}} \sqsubseteq \mathrm{P_{Eucl}}$。證明如下：

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Pric}}$而言，存在一個長度為$n$的普萊斯路徑碼，為敘述方便起見，不失一般性，假設$\overbrace{\mathrm{DDEEEFFFF\cdots DEF}}^{n}$使得$(a_1, b_1, c_1) = (3,4,5)$經過迭代公式(D)(D)(E)(E)(E)(F)(F)(F)(F)⋯(D)(E)(F)產生$(a_{n+1}, b_{n+1}, c_{n+1})$。

(2) 因為迭代公式(D)唯一決定迭代公式(D′)，迭代公式(E)唯一決定迭代公式(E′)，迭代公式(F)唯一決定迭代公式(F′)，所以路徑碼$\overbrace{\mathrm{DDEEEFFFF\cdots DEF}}^{n}$唯一決定路徑碼$\overbrace{\mathrm{D'D'E'E'E'F'F'F'F'\cdots D'E'F'}}^{n}$。

(3) $(u_1, v_1) = (2,1)$由路徑碼$\overbrace{\mathrm{D'D'E'E'E'F'F'F'F'\cdots D'E'F'}}^{n}$迭代產生$(u_{n+1}, v_{n+1})$，由第 14 至 18 頁之論證可證得$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且$u_{n+1}, v_{n+1}$為一奇一偶。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Eucl}}$且$(a_1, b_1, c_1) \in \mathrm{P_{Eucl}}$，即$\mathrm{P_{Pric}} \sqsubseteq \mathrm{P_{Eucl}}$。

(三) 歐幾里得家族中任一互質畢氏數在普萊斯三元樹中的迭代路徑

1. 由 2 階方陣的迭代公式迭代產生歐幾里得家族中所有的互質畢氏數。

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，且不等於$(3,4,5)$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$，$(u_{n+1}, v_{n+1})$依照表 3 中$u_{n+1}$與$v_{n+1}$的關係選擇迭代公式(D′)、(E′)或(F′)，並且得到(u_n, v_n)。

表 3

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
(D′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$0 < v_{n+1} < u_{n+1}$，u_{n+1}為奇數，v_{n+1}為偶數
(E′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數
(F′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數

(2) 同理，由u_n與v_n的關係選擇迭代公式(D′)、(E′)或(F′)，得到u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(D′)、(E′)或(F′)，得到(u_{n-2}, v_{n-2})。然後以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(D′)、(E′)以及(F′)的迭代路徑。再由迭代公式(D′)、(E′)以及(F′)的迭代路徑得到迭代公式(D)、(E)以及(F)的迭代路徑。

2. 由 excel 試算表的公式迭代產生費馬三元數

(1) 因為費馬三元數$(a_{n+1}, b_{n+1}, c_{n+1})$的$(u_{n+1}, v_{n+1})$為$(2150905,246792)$，普萊斯三元樹產生費馬三元數的方法可由$(u_{n+1}, v_{n+1}) = (2150905,246792)$產生$(u_1, v_1) = (2,1)$，依照依照表 3 中的規則設計 excel 試算表的公式（表 4）。

表 4

	A	B	C
12	2150905	2027509	1965811
13	246792	123396	61698
14			
15	1	1	1

(2) 迭代u_n的 excel 公式

①. A12 = u_{n+1} = 2150905

②. B12=u_n=IF(EVEN(A13)-A13=0,A12-A13/2,IF(A12/2>A13,A12/2,IF(A12/2<A13,A12/2,2)))= 2027509

③. C12=u_{n-1}=IF(EVEN(B13)-B13=0,B12-B13/2,IF(B12/2>B13,B12/2,IF(B12/2<B13,B12/2,2)))=1965811

(3) 迭代v_n的 excel 公式

①. A13 = v_{n+1} = 246792

②. B13 =v_n=IF(EVEN(A13)-A13=0,A13/2,IF(A12/2>A13,A12/2-A13,IF(A12/2<A13,A13-A12/2,1)))= 123396

③. C13=v_{n-1}=IF(EVEN(B13)-B13=0,B13/2,IF(B12/2>B13,B12/2-B13,IF(B12/2<B13,B13-B12/2,1)))=61698

(4) 選擇迭代公式的 excel 公式

①. 表格 A15、B15 與 C15 中 1=迭代公式 D'；2=迭代公式 E'；3=迭代公式 F'。

②. A15 = IF(EVEN(A13)-A13=0,1,IF(A12/2>A13,2,IF(A12/2<A13,3,0)))=1=迭代公式 D'

③. B15 = IF(EVEN(B13)-B13=0,1,IF(B12/2>B13,2,IF(B12/2<B13,3,0)))=1=迭代公式 D'

④. C15 = IF(EVEN(C13)-C13=0,1,IF(C12/2>C13,2,IF(C12/2<C13,3,0)))=1=迭代公式 D'

(5) 因此由$(u_{n+1}, v_{n+1}) = (2150905, 246792)$產生$(u_1, v_1) = (2,1)$，迭代公式的順序為 D'D'D'E'D'D'D'F'F'E'D'F'E'F'D'D'F'D'F'F'E'F'D'E'D'。

(6) 因此由$(a_1, b_1, c_1) = (3,4,5)$產生費馬三元數，迭代公式依序為 DEDFEFFD FDDFEFDEFFDDDEDDD。

三、 菲爾斯托夫三元樹與歐幾里得家族

(一) 菲爾斯托夫的迭代公式與 2 階方陣的迭代公式

1. 由菲爾斯托夫的迭代公式(G)與歐幾里得家族的生成公式建立 2 階方陣的迭代公式。令(u_n, v_n)的迭代公式為$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} r_{11} & r_{21} \\ r_{12} & r_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，由$(a_1, b_1, c_1) = (3\ ,4\ ,5)$開始，由迭代公式(G)迭代產生$(a_2, b_2, c_2) = (21,20,29)$及$(a_3, b_3, c_3) = (105,88,137)$，然後再由歐幾里得家族的生成公式得 $(u_1, v_1) = (2,1)$、$(u_2, v_2) = (5,2)$及 $(u_3, v_3) = (11,4)$，此時再代入$\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} r_{11} & r_{21} \\ r_{12} & r_{22} \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，所以求得

(G′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$。

2. 由迭代公式(G′)與歐幾里得家族的生成公式取代迭代公式(G)。

(1) 若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由迭代公式(G′)與歐幾里得家族的生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為歐幾里得家族的互質畢氏數。

證明：若(a_n, b_n, c_n)為歐幾里得家族的互質畢氏數，則由歐幾里得家族的生成公式可得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。此時，由迭代公式(G′)可得$u_{n+1} = u_n + 3v_n$，$v_{n+1} = 2v_n$。因此$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為奇數，v_{n+1}為偶數，所以由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為互質畢氏數。因為$u_n + 3v_n, 2v_n \in N$，$2v_n < u_n + 3v_n$，$(u_n + 3v_n, 2v_n) = 1$，$u_n + 3v_n$為奇數，$2v_n$為偶數，所以

$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為奇數，v_{n+1}為偶數。因此，由歐幾里得家族生成公式所得到的$(a_{n+1}, b_{n+1}, c_{n+1})$ 為互質畢氏數。

(2) 由迭代公式(G′)可得到 $0 < v_{n+1} < \frac{u_{n+1}}{2}$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$， $v_n < u_n$， $(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此，由迭代公式(G′)可得$v_{n+1} = 2v_n$，$u_{n+1} = u_n + 3v_n$。因為 $\frac{u_{n+1}}{2} = \frac{u_n}{2} + \frac{3v_n}{2} = v_n + \frac{u_n + v_n}{2} > 2v_n > v_{n+1}$，所以 $0 < v_{n+1} < \frac{u_{n+1}}{2}$。

(3) 由迭代公式(G′)可得到 $u_{n+1} + v_{n+1} > u_n + v_n$。

證明：由歐幾里得家族的生成公式可得$u_n, v_n \in N$， $v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。此時，由迭代公式(G′)可得$v_{n+1} = 2v_n$，$u_{n+1} = u_n + 3v_n$。因此 $u_{n+1} + v_{n+1} = u_n + 3v_n + 2v_n = u_n + 5v_n > u_n + v_n$。

(4) 無法由迭代公式(G′)得到$(u_{n+1}, v_{n+1}) = (2,1)$.

證明：令$(u_{n+1}, v_{n+1}) = (2,1)$，則由迭代公式(G′)可得$1 = v_{n+1} = 2v_n$，$2 = u_{n+1} = u_n + 3v_n$。 所以 $u_n = \frac{1}{2}$， $v_n = \frac{1}{2}$，不合。

(5) 若 $u_{n+1}, v_{n+1} \in N$， $0 < v_{n+1} < \frac{u_{n+1}}{2}$， $(u_{n+1}, v_{n+1}) = 1$，u_{n+1}為奇數，v_{n+1}為偶數，則由迭代公式(G′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

證明：若$u_{n+1}, v_{n+1} \in N$，$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}$為奇數，$v_{n+1}$為偶數，則由迭代公式(G′)得$u_n = u_{n+1} - \frac{3v_{n+1}}{2}$， $v_n = \frac{v_{n+1}}{2}$。因為$u_{n+1} - \frac{3v_{n+1}}{2}$，$\frac{v_{n+1}}{2} \in N$，$\frac{v_{n+1}}{2} < u_{n+1} - \frac{3v_{n+1}}{2}$，$\left(u_{n+1} - \frac{3v_{n+1}}{2}, \frac{v_{n+1}}{2}\right) = 1$，$u_{n+1} - \frac{3v_{n+1}}{2}, \frac{v_{n+1}}{2}$為一奇一偶，所以$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，$u_n, v_n$為一奇一偶。因此，由迭代公式(G′)與歐幾里得家族生成公式所得到的(a_n, b_n, c_n) 為互質畢氏數。

(二) 菲爾斯托夫三元樹與歐幾里得家族中所有的互質畢氏數相等

1. $\mathrm{P_{Eucl}} \sqsubseteq \mathrm{P_{Fers}}$。證明如下：

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Eucl}}$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且$u_{n+1}, v_{n+1}$為一奇一偶。因此，$u_{n+1}$與$v_{n+1}$的大小關係可分成$\frac{u_{n+1}}{2} = v_{n+1}$；$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶；$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數；$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數。

(2) 當$\frac{u_{n+1}}{2} = v_{n+1}$時，則$(u_{n+1}, v_{n+1}) = (2,1)$；當$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶時，選擇迭代公式$(\mathrm{A}')$並且迭代產生$(u_n, v_n)$；當$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式$(\mathrm{E}')$並且迭代產生$(u_n, v_n)$；當$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數時，選擇迭代公式$(\mathrm{G}')$並且迭代產生$(u_n, v_n)$。因此，菲爾斯托夫三元樹可得到圖 6。

(3) 按照u_{n+1}與v_{n+1}的關係選擇迭代公式(A')、(E')或(G')產生(u_n, v_n)，由第 7 至 8 頁、第 15 至 17 頁以及第 22 至 23 頁之論證可證得$u_n, v_n \in N$，$v_n < u_n$，$(u_n, v_n) = 1$，u_n, v_n為一奇一偶。因此$(a_n, b_n, c_n) \in \mathrm{P_{Eucl}}$。

(4) 同理，(a_n, b_n, c_n)可產生$(a_{n-1}, b_{n-1}, c_{n-1})$，且可證得$(a_{n-1}, b_{n-1}, c_{n-1}) \in \mathrm{P_{Eucl}}$。

(5) 由於$(u_{n+1} + v_{n+1}) > (u_n + v_n)$，因此$(u_{n+1}, v_{n+1})$依此回推至$(u_1, v_1) = (2,1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依此回推至$(a_1, b_1, c_1) = (3,4,5)$，同樣無法再回推。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Fers}}$，即$\mathrm{P_{Eucl}} \sqsubseteq \mathrm{P_{Fers}}$。

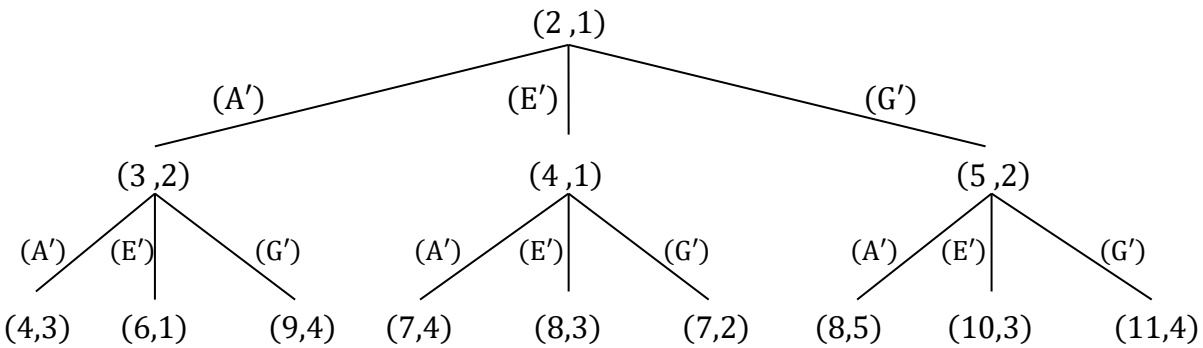


圖 6

2. $\mathrm{P_{Fers}} \sqsubseteq \mathrm{P_{Eucl}}$。證明如下：

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Fers}}$而言，存在一個長度為$n$的普萊斯路徑碼，為敘述方便起見，不失一般性，假設$\overbrace{\mathrm{AAEEEGGGG\cdots DEF}}^{n}$使得$(a_1, b_1, c_1) = (3,4,5)$經過迭代公式$\mathrm{(A)(A)(E)(E)(E)(G)(G)(G)(G)\cdots(A)(E)(G)}$產生$(a_{n+1}, b_{n+1}, c_{n+1})$。

(2) 因為迭代公式$\mathrm{(A)}$唯一決定迭代公式$\mathrm{(A')}$，迭代公式$\mathrm{(E)}$唯一決定迭代公式$\mathrm{(E')}$，迭代公式$\mathrm{(G)}$唯一決定迭代公式$\mathrm{(G')}$，所以路徑碼$\overbrace{\mathrm{AAEEEGGGG\cdots AEG}}^{n}$唯一決定路徑碼$\overbrace{\mathrm{A'A'E'E'E'G'G'G'G'\cdots A'E'G'}}^{n}$。

(3) $(u_1, v_1) = (2,1)$由路徑碼$\overbrace{\mathrm{A'A'E'E'E'G'G'G'G'\cdots A'E'G'}}^{n}$迭代產生$(u_{n+1}, v_{n+1})$，由第 7 至 8 頁、第 15 至 17 頁以及第 22 至 23 頁之論證可證得$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$且u_{n+1}, v_{n+1}為一奇一偶。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in \mathrm{P_{Eucl}}$且$(a_1, b_1, c_1) \in \mathrm{P_{Eucl}}$，即$\mathrm{P_{Fers}} \sqsubseteq \mathrm{P_{Eucl}}$。

(三) 歐幾里得家族中任一互質畢氏數在菲爾斯托夫三元樹中的迭代路徑

1. 由 2 階方陣的迭代公式迭代產生歐幾里得家族中所有的互質畢氏數

(1) 令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，且不等於$(3,4,5)$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1}, v_{n+1}$為一奇一偶，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$，$(u_{n+1}, v_{n+1})$依照表 5 中$u_{n+1}$與$v_{n+1}$的關係選擇迭代公式$\mathrm{(A')}$、$\mathrm{(E')}$或$\mathrm{(G')}$，並且得到$(u_n, v_n)$。

表 5

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
$\mathrm{(A')}$	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶
$\mathrm{(E')}$	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數
$\mathrm{(G')}$	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數

(2) 同理，由u_n與v_n的關係選擇迭代公式(A′)、(E′)或(G′)，得到u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(A′)、(E′)或(G′)，得到(u_{n-2}, v_{n-2})。然後以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A′)、(E′)以及(G′)的迭代路徑。再由迭代公式(A′)、(E′)以及(G′)的迭代路徑得到迭代公式(A)、(E)以及(G)的迭代路徑。

2. 由 excel 試算表的公式迭代產生費馬三元數

(1) 因為費馬三元數$(a_{n+1}, b_{n+1}, c_{n+1})$的$(u_{n+1}, v_{n+1})$為(2150905,246792)，菲爾斯托夫三元樹產生費馬三元數的方法可由$(u_{n+1}, v_{n+1}) = (2150905,246792)$產生$(u_1, v_1) = (2,1)$，我依照表 5 中的規則設計 excel 試算表的公式（表 6）。

表 6

	A	B	C
18	2150905	1780717	1595623
19	246792	123396	61698
20	3	3	3

(2) 迭代u_n的 excel 公式

①. A18 = u_{n+1} = 2150905

②. B18 =u_n= IF(A18=2,2,IF(2*A19>A18,A19,IF(EVEN(A19)-A19=1,A18/2,A18-A19*3/2))) = 1780717

③. C18 =u_{n-1}=IF(B18=2,2,IF(2*B19>B18,B19,IF(EVEN(B19)-B19=1,B18/2,B18-B19*3/2)))=1595623

(3) 迭代v_n的 excel 公式

①. A19 = v_{n+1} = 246792

②. B19 =v_n= IF(A18=2,1,IF(2*A19>A18,A19*2-A18,IF(EVEN(A19)-A19=1,A18/2-A19,A19/2)))= 123396

③. C19=v_{n-1}= IF(B18=2,1,IF(2*B19>B18,B19*2-B18,IF(EVEN(B19)-B19=1,B18/2-B19,B19/2)))=61698

(4) 選擇迭代公式的 excel 公式

①. 表格 A20、B20 與 C20 中 1=迭代公式 A'；2=迭代公式 E'；3=迭代公式 G'。

②. A20 = IF(A18=2,0,IF(2*A19>A18,1,IF(EVEN(A19)-A19=1,2,3)))=3=迭代公式 G'

③. B20 = IF(B18=2,0,IF(2*B19>B18,1,IF(EVEN(B19)-B19=1,2,3)))=3 =迭代公式 G'

④. C20 = IF(C18=2,0,IF(2*C19>C18,1,IF(EVEN(C19)-C19=1,2,3)))=3= 迭代公式 G'

(5) 因此由$(u_{n+1}, v_{n+1}) = (2150905,246792)$產生$(u_1, v_1) = (2,1)$，迭代公式的順序為 G'G'G'E'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'G'E'A'G'G'G'G'G'G'E'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'A'E'G'E'A'A'A'A'A'A'A'。

(6) 因此由$(a_1, b_1, c_1) = (3,4,5)$產生費馬三元數，迭代公式依序為 AAAAAAAEGEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEGGGGGGAEGAAAAAAAAAAAAAAAAAAAAAAAEGGG。

伍、 研究結果

一、 貝格倫三元樹與歐幾里得家族

(一) 由貝格倫的迭代公式與歐幾里得家族生成公式建立迭代公式(A')，(B')以及(C')。

(A') $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，$(B')$ $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，$(C')$ $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

(二) 由迭代公式(A')，(B')以及(C')證明貝格倫三元樹包含歐幾里得家族中所有的互質畢氏數，且歐幾里得家族包含貝格倫三元樹中所有的互質畢氏數，因此貝格倫三元樹中所有的互質畢氏數等於歐幾里得家族中所有的互質畢氏數。

(三) 互質畢氏數在貝格倫三元樹的迭代路徑之方法為：令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則 $u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，u_{n+1}, v_{n+1}為一奇一偶，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$。①當$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$時，選擇迭代公式$(A')$。②當 $0 < v_{n+1} < \frac{u_{n+1}}{3}$時，選擇迭代公式$(B')$。③當$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$時，選擇迭代公式$(C')$。因此$u_{n+1}$與$v_{n+1}$以迭代公式$(A')$、$(B')$以及$(C')$得到$u_n$與$v_n$。同理，由$u_n$與$v_n$的關係選擇迭代公式$(A')$、$(B')$以及$(C')$，得到

u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(A′)、(B′)以及(C′)，得到(u_{n-2}, v_{n-2})。然後以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A′)、(B′)以及(C′)的迭代路徑。再由迭代公式(A′)、(B′)以及(C′)的迭代路徑得到迭代公式(A)、(B)以及(C)的迭代路徑，即為歐幾里得家族中任一互質畢氏數在貝格倫三元樹的迭代路徑。

二、 普萊斯三元樹與歐幾里得家族

(一) 由普萊斯的迭代公式與歐幾里得家族的生成公式建立迭代公式(D′)，(E′)以及(F′)。

(D′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(E′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(F′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

(二) 由迭代公式(D′)，(E′)以及(F′)證明普萊斯三元樹包含歐幾里得家族中所有的互質畢氏數，且歐幾里得家族包含普萊斯三元樹中所有的互質畢氏數，因此普萊斯三元樹中所有的互質畢氏數等於歐幾里得家族中所有的互質畢氏數。

(三) 互質畢氏數在普萊斯三元樹的迭代路徑之方法為：令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則 $u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$。①當 $0 < v_{n+1} < u_{n+1}$，u_{n+1}為奇數，v_{n+1}為偶數時，選擇迭代公式(D′)。②當 $0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式(E′)。③當 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式(F′)。因此$u_{n+1}$與$v_{n+1}$以迭代公式(D′)、(E′)或(F′)得到$u_n$與$v_n$。同理，由$u_n$與$v_n$的關係選擇迭代公式(D′)、(E′)或(F′)，得到u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(D′)、(E′)或(F′)，得到(u_{n-2}, v_{n-2})。以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(D′)、(E′)以及(F′)的迭代路徑。再由迭代公式(D′)、(E′)以及(F′)的迭代路徑得到迭代公式(D)、(E)以及(F)的迭代路徑，即為歐幾里得家族中任一互質畢氏數在普萊斯三元樹的迭代路徑。

三、 菲爾斯托夫三元樹與歐幾里得家族

(一) 由菲爾斯托夫的迭代公式與歐幾里得家族的生成公式建立迭代公式(G′)。

(G′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

(二) 由迭代公式(A′)，(E′)以及(G′)證明菲爾斯托夫三元樹包含歐幾里得家族中所有的互質畢氏數，且歐幾里得家族包含菲爾斯托夫三元樹中所有的互質畢氏數，因此菲爾斯托夫三元樹中所有的互質畢氏數等於歐幾里得家族中所有的互質畢氏數。

(三) 互質畢氏數在菲爾斯托夫三元樹的迭代路徑之方法：令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則$u_{n+1}, v_{n+1} \in N$，$v_{n+1} < u_{n+1}$，$(u_{n+1}, v_{n+1}) = 1$，$u_{n+1} \neq 2$且$v_{n+1} \neq 1$。①當 $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶時，選擇迭代公式(A′)。②當 $0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，選擇迭代公式(E′)。③當$0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數時，選擇迭代公式(G′)。因此$u_{n+1}$與$v_{n+1}$以迭代公式(A′)、(E′)或(G′)得到$u_n$與$v_n$。同理，由$u_n$與$v_n$的關係選擇迭代公式(A′)、(E′)或(G′)，得到u_{n-1}與v_{n-1}。再由u_{n-1}與v_{n-1}的關係選擇迭代公式(A′)、(E′)或(G′)，得到(u_{n-2}, v_{n-2})。以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A′)、(E′)以及(G′)的迭代路徑。再由迭代公式(A′)、(E′)以及(G′)的迭代路徑得到迭代公式(A)、(E)以及(G)的迭代路徑，即為歐幾里得家族中任一互質畢氏數在菲爾斯托夫三元樹的迭代路徑。

陸、 討論

一、 本研究發現費馬三元數在普萊斯三元樹只需 25 次迭代，即可由$(a_1, b_1, c_1) = (3, 4, 5)$迭代產生費馬三元數，並不是普萊斯所提出的 32 次迭代。由於費馬三元數為 13 位數，是相當大的數字。若由$(a_1, b_1, c_1) = (3, 4, 5)$開始，不管是選擇貝格倫迭代公式或是普萊斯迭代公式，依序產生各種互質畢氏數，只能大海撈針地產生費馬三元樹。若由費馬三元樹開始，以貝格倫迭代公式與普萊斯迭代公式回推前一個互質畢氏數，由此產生路徑碼，雖然較可行，但是過程還是相當繁瑣。但是 2 階方陣的迭代公式卻可以改善貝格倫迭代公式與普萊斯迭代公式所遇到問題，由此改良普萊斯的方法。

二、 由$(u_1, v_1) = (2,1)$開始，按照路徑碼中的字母，選擇所代表的 2 階方陣的迭代公式，按照字母的順序連續迭代產生(u_{n+1}, v_{n+1})。因此，由(u_1, v_1)連續迭代產生(u_{n+1}, v_{n+1})的路徑碼有 n 個字母。當$(u_1, v_1) = (2,1)$與路徑碼為已知，即可求得(u_{n+1}, v_{n+1})。或者當$(u_1, v_1) = (2,1)$與(u_{n+1}, v_{n+1})為已知，只要按照u_{n+1}與v_{n+1}的關係，即可求得路徑碼。密碼學上給定的條件是$(u_1, v_1) = (2,1)$與路徑碼，需求得的答案是 (u_{n+1}, v_{n+1})，或者給定的條件是 $(u_1, v_1) = (2,1)$與(u_{n+1}, v_{n+1})，需求得的答案是路徑碼。甚至可考慮$1 < m < n + 1$，$m, n \in N$的情形，當(u_m, v_m)與路徑碼為已知，可求得(u_{n+1}, v_{n+1})。或者當(u_m, v_m)與(u_{n+1}, v_{n+1})為已知，按照u_{n+1}與v_{n+1}，即可求得路徑碼。或者按照u_m與v_m的關係，也可求得路徑碼。

三、 當$(a_1, b_1, c_1) = (3, 4, 5)$與$(a_{n+1}, b_{n+1}, c_{n+1})$為已知，由歐幾里得家族的生成公式求得$(u_1, v_1) = (2,1)$與$(u_{n+1}, v_{n+1})$，再按照$u_{n+1}$與$v_{n+1}$的關係，即可求得路徑碼。因此當$(u_{n+1}, v_{n+1})$與$(a_{n+1}, b_{n+1}, c_{n+1})$由歐幾里得家族的生成公式互相轉換時，此時設定的方式顯得更靈活。當$(u_1, v_1) = (2,1)$與路徑碼為已知，可先求得(u_{n+1}, v_{n+1})，再由歐幾里得家族的生成公式求得$(a_{n+1}, b_{n+1}, c_{n+1})$。在密碼學上給定的條件是$(a_1, b_1, c_1)$與$(a_{n+1}, b_{n+1}, c_{n+1})$，需求得的答案是路徑碼。或者給定的條件是$(a_1, b_1, c_1)$與路徑碼，需求得的答案是 $(a_{n+1}, b_{n+1}, c_{n+1})$。甚至可考慮當$1 < m < n + 1$，$m, n \in N$的情形，

當(u_m, v_m)與路徑碼為已知，求得(u_{n+1}, v_{n+1})，再由歐幾里得家族的生成公式求得$(a_{n+1}, b_{n+1}, c_{n+1})$。當$(a_m, b_m, c_m)$與$(a_{n+1}, b_{n+1}, c_{n+1})$為已知，由歐幾里得家族的生成公式求得$(u_m, v_m)$與$(u_{n+1}, v_{n+1})$，再按照$u_{n+1}$與$v_{n+1}$的關係，即可求得路徑碼。

柒、 結論

本研究由歐幾里得家族的生成公式、貝格倫、普萊斯與菲爾斯托夫迭代公式得到 2 階方陣的迭代公式，由 2 階方陣的迭代公式與歐幾里得家族的生成公式取代貝格倫、普萊斯與菲爾斯托夫迭代公式，由此證明貝格倫、普萊斯與菲爾斯托夫三元樹中所有的互質畢氏數相等，並且建立了歐幾里得家族中任一互質畢氏數在貝格倫、普萊斯與菲爾斯托夫三元樹的迭代路徑，改良了普萊斯建立迭代路徑碼的方法。因此，我未來想將互質畢氏數的迭代路徑碼運用於密碼學。

捌、 參考資料

一、高中數學課本第四冊（2017）。第三章：矩陣。南一書局。

二、容士毅（譯）（2010）。數學是什麼？台北縣：左岸文化。

三、Kevin Ryde (2008). "Trees of Primitive Pythagorean Triples ".from: https://download.tuxfamily.org/user42/triples/triples.pdf

四、Price, H. Lee (2008). "The Pythagorean Tree: A New Species". arXiv:0809.4324[math.HO], from: http://arxiv.org/pdf/0809.4324.pdf

五、V. E. Firstov. "A Special Matrix Transformation Semigroup of Primitive Pairs and the Genealogy of Pythagorean Triples". Mathematical Notes, volume 84, number 2, August 2008, pages 263-279.

【評語】050418

1. 本研究是利用 2 階方陣迭代公式與歐幾里得家族的生成公式證明了三種三元樹中所有互質畢氏數相等，建立歐幾里得家族中任一互質畢氏數在這三種三元樹中的迭代路徑碼，改近了普萊斯的建立方法，各種數學工具表徵，處理手法純熟，論述清晰，過程完整。
2. 與目前已知的結果及處理手法之間的差異性，創新度不足。
3. 研究結果應用於密碼學的關鍵在於二階變換方陣，這些樹之間的二階變換方陣之間是否存在某些關係，值得探討。

作品海報

壹、摘要

由於貝格倫、普萊斯與菲爾斯托夫三元樹中存在著某些相同的互質畢氏數，因此我猜想這三種三元樹中所有互質畢氏數相等。我由 2 階方陣的迭代公式證明這三種三元樹中所有互質畢氏數相等，並且建立歐幾里得家族中任一互質畢氏數在這三種三元樹中的迭代路徑。

貳、研究動機

除了費馬三元數(4565486027761,1061652293520,4687298610289)，還有更多的互質畢氏數同時出現在貝格倫、普萊斯與菲爾斯托夫三元樹，因此我猜想這三種三元樹中所有互質畢氏數相等。本研究將證明這個猜想，並建立互質畢氏數在這三種三元樹中的迭代路徑。

參、研究目的

一、證明貝格倫三元樹中所有的互質畢氏數(P_{Berg})與歐幾里得家族中所有的互質畢氏數(P_{Eucl})相等，建立歐幾里得家族中任一互質畢氏數在貝格倫三元樹中的迭代路徑。

二、證明普萊斯三元樹中所有的互質畢氏數(P_{Pric})與歐幾里得家族中所有的互質畢氏數(P_{Eucl})相等，建立歐幾里得家族中任一互質畢氏數在普萊斯三元樹中的迭代路徑。

三、證明菲爾斯托夫三元樹中所有的互質畢氏數(P_{Fers})與歐幾里得家族中所有的互質畢氏數(P_{Eucl})相等，建立歐幾里得家族中任一互質畢氏數在菲爾斯托夫三元樹中的迭代路徑。

肆、研究設備及器材

筆、紙、電腦、電子計算機及 excel 試算表。

伍、研究過程與方法

一、貝格倫三元樹與歐幾里得家族

(一) 貝格倫迭代公式與 2 階方陣的迭代公式

1. 公式(A)、(B)及(C)產生公式(A′)、(B′)及(C′)。
2. 公式(A′)、(B′)及(C′)取代公式(A)、(B)及(C)。

(二) 證明 $P_{Berg} = P_{Eucl}$。

1. 證明 $P_{Eucl} \sqsubseteq P_{Berg}$。

(1) 由迭代公式(A′)、(B′)及(C′)得到
$u_{n+1} + v_{n+1} > u_n + v_n$。

(2) 無法由迭代公式(A′)、(B′)及(C′)得到
$(u_{n+1}, v_{n+1}) = (2, 1)$。

(3) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，則$(u_{n+1}, v_{n+1})$依此回推至$(u_1, v_1) = (2, 1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依照①至④的規則回推至$(a_1, b_1, c_1) = (3, 4, 5)$，無法再回推。因此$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Berg}$，即$P_{Eucl} \sqsubseteq P_{Berg}$。

① $\frac{u_{n+1}}{2} = v_{n+1}$時，$(u_{n+1}, v_{n+1}) = (2, 1)$。

② $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶時，由迭代公式(A′)迭代產生$(u_n, v_n)$。

③ $0 < v_{n+1} < \frac{u_{n+1}}{3}$，$u_{n+1}, v_{n+1}$為一奇一偶時，由迭代公式(B′)迭代產生$(u_n, v_n)$。

④ $\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}, v_{n+1}$為一奇一偶時，由迭代公式(C′)迭代產生$(u_n, v_n)$。

2. 證明 $P_{Berg} \sqsubseteq P_{Eucl}$。

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Berg}$而言，存在唯一的貝格倫路徑碼。

(2) 迭代公式(A)、(B)及(C)分別唯一決定迭代公式(A′)、(B′)及(C′)。

(3) 因為$(u_1, v_1) = (2, 1)$由貝格倫路徑碼產生(u_{n+1}, v_{n+1})，所以$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，即$P_{Berg} \sqsubseteq P_{Eucl}$。

(三) P_{Eucl}中任一互質畢氏數在P_{Berg}的迭代路徑

1. 由 2 階方陣的迭代公式產生迭代路徑。
2. 由 excel 試算表的公式產生迭代路徑。

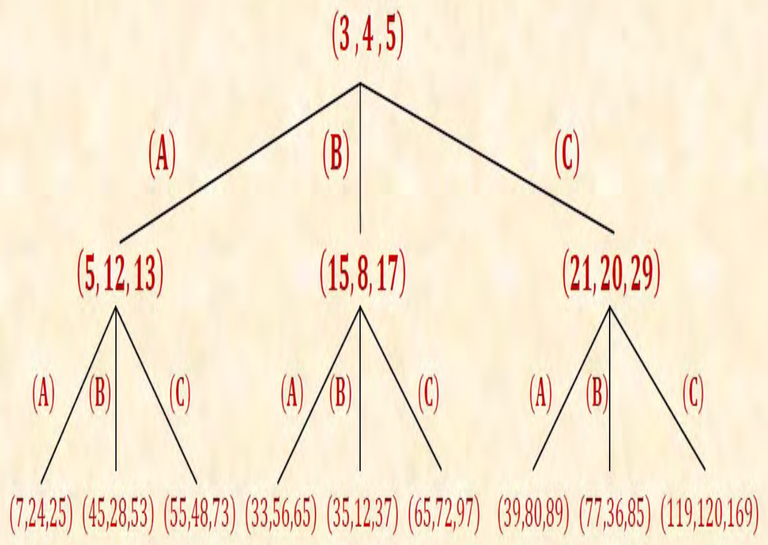
歐幾里得家族的生成公式

$$\begin{cases} a_n = u_n^2 - v_n^2 \\ b_n = 2u_n v_n \\ c_n = u_n^2 + v_n^2 \end{cases}, \quad n, u_n, v_n \in N,\ v_n < u_n,\ (u_n, v_n) = 1,\ u_n, v_n \text{為一奇一偶。}$$

貝格倫迭代公式

$$(A)\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}\begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix};(B)\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}\begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix};(C)\begin{bmatrix} a_{n+1} \\ b_{n+1} \\ c_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}\begin{bmatrix} a_n \\ b_n \\ c_n \end{bmatrix}$$

貝格倫三元樹(a_n, b_n, c_n)



2 階方陣的迭代公式

$$(A')\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} u_n \\ v_n \end{bmatrix};(B')\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} u_n \\ v_n \end{bmatrix};(C')\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} u_n \\ v_n \end{bmatrix}$$

貝格倫三元樹(u_n, v_n)

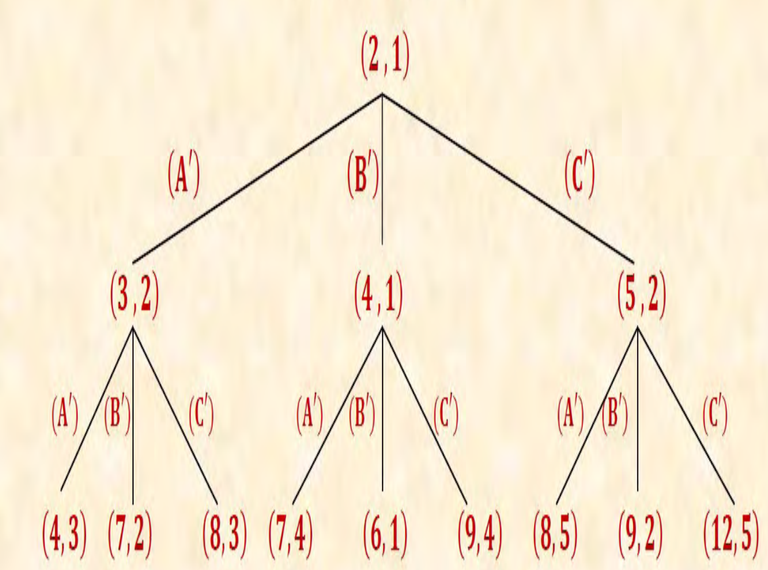


表1

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
(A′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶
(B′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$0 < v_{n+1} < \frac{u_{n+1}}{3}$，$u_{n+1}, v_{n+1}$為一奇一偶
(C′)	$0 < v_n < u_n$，u_n, v_n為一奇一偶	$\frac{u_{n+1}}{3} < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}, v_{n+1}$為一奇一偶

二、 普萊斯三元樹與歐幾里得家族

(一) 普萊斯迭代公式與2階方陣的迭代公式

1. 公式(D)、(E)及(F)產生公式(D′)、(E′)及(F′)。
2. 公式(D′)、(E′)及(F′)取代公式(D)、(E)及(F)。

(二) 證明 $P_{Pric} = P_{Eucl}$。

1. 證明 $P_{Eucl} \sqsubseteq P_{Pric}$。

(1) 由迭代公式(D′)、(E′)及(F′)得到$u_{n+1} + v_{n+1} > u_n + v_n$。

(2) 無法由迭代公式(D′)、(E′)及(F′)得到$(u_{n+1}, v_{n+1}) = (2,1)$。

(3) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，則$(u_{n+1}, v_{n+1})$依照①至④的規則回推至$(u_1, v_1) = (2,1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依此回推至$(a_1, b_1, c_1) = (3,4,5)$，無法再回推。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Pric}$，即$P_{Eucl} \sqsubseteq P_{Pric}$。

① $\frac{u_{n+1}}{2} = v_{n+1}$時，$(u_{n+1}, v_{n+1}) = (2,1)$。

② $0 < v_{n+1} < u_{n+1}$，u_{n+1}為奇數，v_{n+1}為偶數時，

由迭代公式(D′)迭代產生(u_n, v_n)。

③ $0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，

由迭代公式(E′)迭代產生(u_n, v_n)。

④ $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，

由迭代公式(F′)迭代產生(u_n, v_n)。

2. 證明 $P_{Pric} \sqsubseteq P_{Eucl}$。

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Pric}$而言，存在唯一普萊斯路徑碼。

(2) 公式(D)、(E)及(F)分別唯一決定公式(D′)、(E′)及(F′)。

(3) 因為$(u_1, v_1) = (2,1)$由普萊斯路徑碼產生(u_{n+1}, v_{n+1})，所以$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，即$P_{Pric} \sqsubseteq P_{Eucl}$。

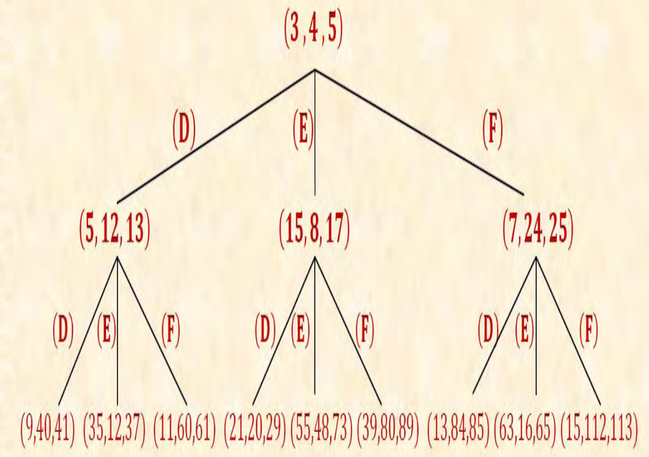
(三) P_{Eucl}中任一互質畢氏數在P_{Pric}的迭代路徑

1. 由2階方陣的迭代公式產生迭代路徑。
2. 由 excel 試算表的公式產生迭代路徑。

普萊斯迭代公式

$$(D)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&-1\\-2&2&2\\-2&1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix};(E)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&1\\2&-2&2\\2&-1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix};(F)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&-1&1\\2&2&2\\2&1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$$

普萊斯三元樹(a_n, b_n, c_n)



2階方陣的迭代公式

$$(D')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}1&1\\0&2\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix};(E')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}2&0\\1&-1\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix};(F')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}2&0\\1&1\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix}$$

普萊斯三元樹(u_n, v_n)

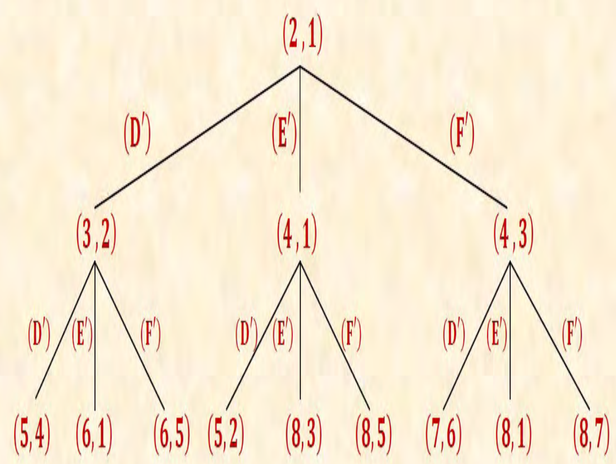


表2

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
(D′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$0<v_{n+1}<u_{n+1}$, u_{n+1}為奇數, v_{n+1}為偶數
(E′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$0<v_{n+1}<\frac{u_{n+1}}{2}$, u_{n+1}為偶數, v_{n+1}為奇數
(F′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2}<v_{n+1}<u_{n+1}$, u_{n+1}為偶數, v_{n+1}為奇數

三、 菲爾斯托夫三元樹與歐幾里得家族

(一) 菲爾斯托夫迭代公式與2階方陣的迭代公式

1. 公式(A)、(E)及(G)產生公式(A′)、(E′)及(G′)。
2. 公式(A′)、(E′)及(G′)取代公式(A)、(E)及(G)。

(二) 證明 $P_{Fers} = P_{Eucl}$。

1. 證明 $P_{Eucl} \sqsubseteq P_{Fers}$。

(1) 由迭代公式(A′)、(E′)及(G′)得到$u_{n+1} + v_{n+1} > u_n + v_n$。

(2) 無法由迭代公式(A′)、(E′)及(G′)得到$(u_{n+1}, v_{n+1}) = (2,1)$。

(3) 令$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，則$(u_{n+1}, v_{n+1})$依照①至④的規則回推至$(u_1, v_1) = (2,1)$，便無法再回推，所以$(a_{n+1}, b_{n+1}, c_{n+1})$依此回推至$(a_1, b_1, c_1) = (3,4,5)$，無法再回推。因此，$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Fers}$，即$P_{Eucl} \sqsubseteq P_{Fers}$。

① $\frac{u_{n+1}}{2} = v_{n+1}$時，$(u_{n+1}, v_{n+1}) = (2,1)$。

② $\frac{u_{n+1}}{2} < v_{n+1} < u_{n+1}$，$u_{n+1}, v_{n+1}$為一奇一偶時，

由迭代公式(A′)迭代產生(u_n, v_n)。

③ $0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為偶數，$v_{n+1}$為奇數時，

由迭代公式(E′)迭代產生(u_n, v_n)。

④ $0 < v_{n+1} < \frac{u_{n+1}}{2}$，$u_{n+1}$為奇數，$v_{n+1}$為偶數時，

由迭代公式(G′)迭代產生(u_n, v_n)。

2. 證明 $P_{Fers} \sqsubseteq P_{Eucl}$。

(1) 對任一$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Fers}$而言，存在唯一菲爾斯托夫路徑碼。

(2) 公式(A)、(E)及(G)分別唯一決定公式(A′)、(E′)及(G′)。

(3) 因為$(u_1, v_1) = (2,1)$由菲爾斯托夫路徑碼產生(u_{n+1}, v_{n+1})，所以$(a_{n+1}, b_{n+1}, c_{n+1}) \in P_{Eucl}$，即$P_{Fers} \sqsubseteq P_{Eucl}$。

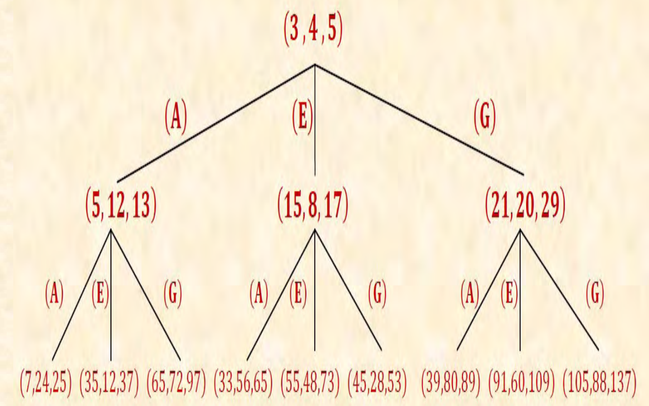
(三) P_{Eucl}中任一互質畢氏數在P_{Fers}的迭代路徑

1. 由2階方陣的迭代公式產生迭代路徑。
2. 由 excel 試算表的公式產生迭代路徑。

菲爾斯托夫迭代公式

$$(A)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}1&-2&2\\2&-1&2\\2&-2&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix};(E)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}2&1&1\\2&-2&2\\2&-1&3\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix};(G)\begin{bmatrix}a_{n+1}\\b_{n+1}\\c_{n+1}\end{bmatrix}=\begin{bmatrix}-2&3&3\\-6&2&6\\-6&3&7\end{bmatrix}\begin{bmatrix}a_n\\b_n\\c_n\end{bmatrix}$$

菲爾斯托夫三元樹(a_n, b_n, c_n)



2階方陣的迭代公式

$$(A')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}2&-1\\1&0\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix};(E')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}2&0\\1&-1\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix};(G')\begin{bmatrix}u_{n+1}\\v_{n+1}\end{bmatrix}=\begin{bmatrix}1&3\\0&2\end{bmatrix}\begin{bmatrix}u_n\\v_n\end{bmatrix}$$

菲爾斯托夫三元樹(u_n, v_n)

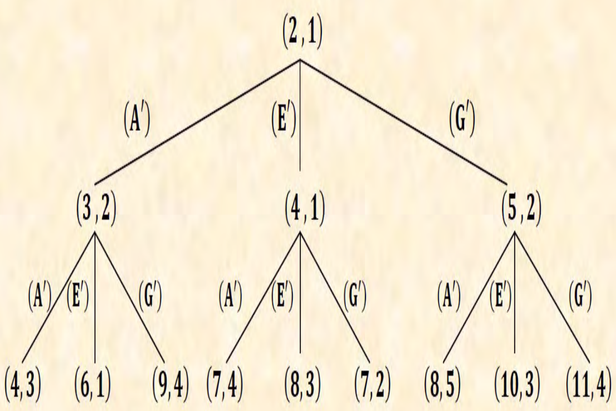


表3

公式	u_n, v_n的性質	u_{n+1}, v_{n+1}的性質
(A′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$\frac{u_{n+1}}{2}<v_{n+1}<u_{n+1}$, u_{n+1}, v_{n+1}為一奇一偶
(E′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$0<v_{n+1}<\frac{u_{n+1}}{2}$, u_{n+1}為偶數, v_{n+1}為奇數
(G′)	$0<v_n<u_n$, u_n, v_n為一奇一偶	$0<v_{n+1}<\frac{u_{n+1}}{2}$, u_{n+1}為奇數, v_{n+1}為偶數

陸、研究結果

一、貝格倫三元樹與歐幾里得家族

（一）由貝格倫迭代公式與歐幾里得家族生成公式產生迭代公式(A′)，(B′)以及(C′)。

(A′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(B′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(C′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

（二）由迭代公式(A′)，(B′)以及(C′)證明$P_{Eucl} \sqsubseteq P_{Berg}$ 且$P_{Berg} \sqsubseteq P_{Eucl}$，因此$P_{Berg} = P_{Eucl}$。

（三）令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則在貝格倫三元樹的迭代路徑之方法為：依照表 1 中u_{n+1}與v_{n+1}的關係選擇迭代公式(A′)、(B′)以及(C′)，以迭代公式(A′)、(B′)以及(C′)得到u_n與v_n。同理，得到u_{n-1}與v_{n-1}，以及u_{n-2}與v_{n-2}，以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A′)、(B′)以及(C′)的迭代路徑，再得到迭代公式(A)、(B)以及(C)的迭代路徑。

二、普萊斯三元樹與歐幾里得家族

（一）由普萊斯迭代公式與歐幾里得家族生成公式產生迭代公式(D′)，(E′)以及(F′)。

(D′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(E′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$，(F′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

（二）由迭代公式(D′)，(E′)以及(F′)證明$P_{Eucl} \sqsubseteq P_{Pric}$ 且$P_{Pric} \sqsubseteq P_{Eucl}$，因此$P_{Pric} = P_{Eucl}$。

（三）令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則在貝格倫三元樹的迭代路徑之方法為：依照表 2 中u_{n+1}與v_{n+1}的關係選擇迭代公式(D′)、(E′)以及(F′)，以迭代公式(D′)、(E′)以及(F′)得到u_n與v_n。同理，得到u_{n-1}與v_{n-1}，以及u_{n-2}與v_{n-2}，以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(D′)、(E′)以及(F′)的迭代路徑，再得到迭代公式(D)、(E)以及(F)的迭代路徑。

三、菲爾斯托夫三元樹與歐幾里得家族

（一）由菲爾斯托夫迭代公式與歐幾里得家族生成公式產生迭代公式(G′)。

(G′) $\begin{bmatrix} u_{n+1} \\ v_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} u_n \\ v_n \end{bmatrix}$

（二）由迭代公式(A′)，(E′)以及(G′)證明$P_{Eucl} \sqsubseteq P_{Fers}$ 且$P_{Fers} \sqsubseteq P_{Eucl}$，因此$P_{Fers} = P_{Eucl}$。

（三）令$(a_{n+1}, b_{n+1}, c_{n+1})$為歐幾里得家族的互質畢氏數，$(a_{n+1}, b_{n+1}, c_{n+1}) \neq (3,4,5)$，則在貝格倫三元樹的迭代路徑之方法為：依照表 3 中u_{n+1}與v_{n+1}的關係選擇迭代公式(A′)，(E′)以及(G′)，以迭代公式(A′)，(E′)以及(G′)得到u_n與v_n。同理，得到u_{n-1}與v_{n-1}，以及 u_{n-2}與v_{n-2}，以此類推最後皆產生$(u_1, v_1) = (2,1)$。由此建立迭代公式(A′)，(E′)以及(G′)的迭代路徑，再得到迭代公式(A)、(E)以及(G)的迭代路徑。

柒、討論

一、在普萊斯三元樹中由$(a_1, b_1, c_1) = (3, 4, 5)$迭代產生費馬三元數，本研究發現只需 25 次迭代，並不是普萊斯所提出的 32 次迭代。由於費馬三元數為 13 位數，不管是選擇貝格倫，普萊斯或是菲爾斯托夫迭代公式，只能大海撈針地產生費馬三元數。但是 2 階方陣的迭代公式卻具有一定的規則（表 1，2 及 3），可以按照這些規則產生費馬三元數。

二、由$(u_1, v_1) = (2,1)$開始，按照路徑碼中的字母，選擇所代表的 2 階方陣的迭代公式，按照字母的順序連續迭代產生(u_{n+1}, v_{n+1})。

（一）由$(u_1, v_1) = (2,1)$與路徑碼求得(u_{n+1}, v_{n+1})。

（二）由$(u_1, v_1) = (2,1)$與(u_{n+1}, v_{n+1})求得路徑碼。

（三）已知(u_m, v_m)與路徑碼，$1 < m < n+1$，$m, n \in N$，求得(u_{n+1}, v_{n+1})。

三、當已知$(a_1, b_1, c_1) = (3, 4, 5)$與$(a_{n+1}, b_{n+1}, c_{n+1})$，由歐幾里得家族的生成公式求得$(u_1, v_1) = (2,1)$與$(u_{n+1}, v_{n+1})$，再求得路徑碼。因此由歐幾里得家族的生成公式轉換$(u_{n+1}, v_{n+1})$與$(a_{n+1}, b_{n+1}, c_{n+1})$時，則顯得更加靈活。

（一）由(a_1, b_1, c_1)與$(a_{n+1}, b_{n+1}, c_{n+1})$求得路徑碼。

（二）由(a_1, b_1, c_1)與路徑碼時，求得$(a_{n+1}, b_{n+1}, c_{n+1})$。

（三）若$1 < m < n+1$，$m, n \in N$，則由(a_m, b_m, c_m) 與路徑碼求得$(a_{n+1}, b_{n+1}, c_{n+1})$，或由$(a_m, b_m, c_m)$ 與 $(a_{n+1}, b_{n+1}, c_{n+1})$求得路徑碼。

捌、結論

本研究由 2 階方陣的迭代公式與歐幾里得家族的生成公式取代貝格倫、普萊斯與菲爾斯托夫迭代公式，證明貝格倫、普萊斯與菲爾斯托夫三元樹中所有的互質畢氏數相等，並建立互質畢氏數在這三種三元樹的迭代路徑。我未來想將互質畢氏數的路徑碼運用於密碼學。

玖、參考資料及其他

一、高中數學課本第四冊（2017）。第三章：矩陣。南一書局。

二、容士毅（譯）（2010）。數學是什麼？台北縣：左岸文化。

三、Kevin Ryde (2008). "Trees of Primitive Pythagorean Triples ",from: https://download.tuxfamily.org/user42/triples/triples.pdf

四、H. Lee Price (2008). "The Pythagorean Tree: A New Species".arXiv: 0809.4324 [math.HO], from: http://arxiv.org/pdf/0809.4324.pdf

五、V. E. Firstov. "A Special Matrix Transformation Semigroup of Primitive Pairs and the Genealogy of Pythagorean Triples". Mathematical Notes, volume 84, number 2, August 2008, pages 263-279.