中華民國第四十五屆中小學科學展覽會
作品說明書

高中組 數學科

040409

潘朵拉的盒子

國立馬公高級中學

作者姓名：

高二 涂珉鳳

指導老師：

顏光榮

第四十五屆中小學科學展覽會

作品說明書

科　　別：數學科

組　　別：高中組

作品名稱：潘朵拉的盒子

關 鍵 詞：密碼學，益智盒，斐波那契數列

壹：摘要

簡述益智盒的概念

↓

換成我們所找的函數模組

↓

先以某一種加密方法為例，示範一般加密的方法

↓

建構在以上的方法是利用一種新函數 $S(a,b)$ 來加碼

↓

再將轉好的碼 轉換成圖形

跳脫傳統的算法, 利用新的算法來加密解密, 並希望藉由費氏數的特性來提高密碼的安全性, 也希望能藉此和幾何連結在一起

主要的想法是，一般數字 ⟶ 費氏數 ⟶ 密碼的圖形

貳、研究動機

小時後常看會去玩些小遊戲,後來看到霍安琪的密碼學。剛好學校正在上機率統計,便突然想到不要用數論來做密碼, 用方程式來做密碼也不錯阿! 另外用圖形代替數字也很有趣。後來看到益智盒,又突然有了一些新的想法……就著手研究囉。

叁、研究目的

一、針對益智盒的概念。加上新的函數,探的其加解碼的方式。

二、將得到的明文,利用費是數列的特性把數字換成圖形。

肆、研究設備及器材

電腦與數學軟體(Mathematica)電算器，S-Plus 軟體

伍、研究過程或方法

我這次是針對尤拉步數來作為密碼的算法. 以下是對尤拉步數所做的簡單介紹, 有詳細的證明附在作品的後面

一、尤拉步數也就是輾轉相除法所需要的步數,

例如：$(12,5)\to(2,5)\to(2,1)\to(0,1)$　　所以 $E(12,5)=3$,代表之間經過 3 步。

二、這個函數 E 具有一項很重要的特性：

$E\left(F_{n+2},F_{n+1}\right)=n$,而且 $E\left(a,b\right)=n$,a,b 的 min 也是 F_{n+2} , F_{n+1} 。

例如：$\left(8,5\right)\rightarrow\left(3,5\right)\rightarrow\left(3,2\right)\rightarrow\left(1,2\right)\rightarrow\left(1,0\right)$　　$E\left(8,5\right)=4$

三、 (見下圖)從對角線開始,對於固定的 a or b, E(a 變數)是週期函數,週期爲 a。
例如：縱座標爲 2 的,從對角線開始向右算起是 121212……週期爲 2。

四、Lame 定律和另外一個：$2\log_2^n \le E\left(m,n\right)\le 5\times n$ 的位數, $m\ge n$ 。

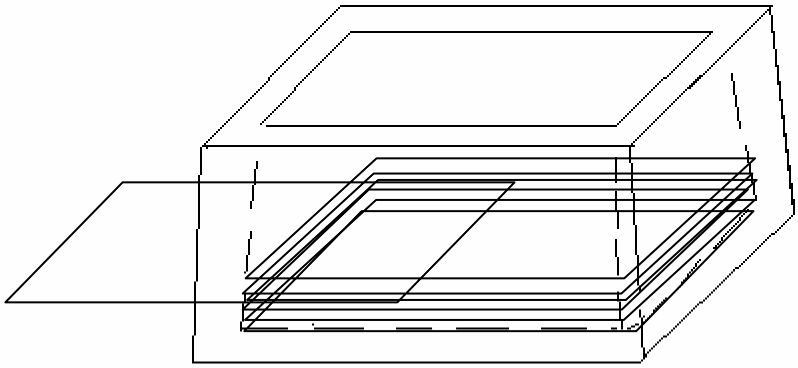
15	1	2	1	3	1	2	2	3	3	2	4	2	3	2	1
14	1	1	3	2	3	2	1	3	4	3	4	2	2	1	2
13	1	2	2	2	4	2	3	5	3	3	3	2	1	2	3
12	1	1	1	1	3	1	4	2	2	2	2	1	2	2	2
11	1	2	3	3	2	3	4	4	3	2	1	2	3	4	4
10	1	1	2	2	1	3	3	2	2	1	2	2	3	3	2
9	1	2	1	2	3	2	3	2	1	2	3	2	3	4	3
8	1	1	3	1	4	2	2	1	2	2	4	2	5	3	3
7	1	2	2	3	3	2	1	2	3	3	4	4	3	1	2
6	1	1	1	2	2	1	2	2	2	3	3	1	2	2	2
5	1	2	3	2	1	2	3	4	3	1	2	3	4	3	1
4	1	1	2	1	2	2	3	1	2	2	3	1	2	2	3
3	1	2	1	2	3	1	2	3	1	2	3	1	2	3	1
2	1	1	2	1	2	1	2	1	2	1	2	1	2	1	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

(一)PART1：(目標⇒用實物表達,理想的加密法)
在一次偶然的機會下,一位書商老闆送我的益智盒由四塊不規則形狀的積木構成。把四塊積木都拼進去時,若一個個放進去的話,是不會成功的。
解決的方法：1.乾脆抽去底板
　　　　　　2.四塊同時放進去(ie.如果只放進三塊能是沒有意義)

假設,現在有兩個人 Linda 和 Cindy, Linda 想約 Cindy 在某處見面,他做了一盒子寄給 Cindy. Cindy 收到後就裝上自己要的底板(ie.決定木塊底面 x 値的大小,在傳回給 Linda. Linda 便做一堆適合這盒子的小木塊。把這兩個分開裝寄到 Cindy. Cindy 只要將積木作他想要的調整,就可輕易的讀出 Linda 想跟他說的話了。

也或者, Cindy 和 Linda 先共同約定好要抽去底面的哪一面然後 Linda 就可以直接做了加好碼

的積木和盒子給 Cindy



如上圖，必須抽出或加入正確的板子，才可以將積木放進去，看到我們所要表達的的文字

把上述的盒子視為加密法,積木是明文。
當我要加密時,我就設定積木內部的形狀(or 底) ⇒也就是 key。這是只有我們兩個知道的 key。只要知道了就可以很容易的解出明文了

一般的加碼方式多適用數論，這裡我希望能找到一個函數,如果別人想破解必須要把整篇明文都找出來,因為就像積木一樣,一定要把所有的明文依照正確的方式加上 key,同時全部換來,才能知道這篇 code 是否正確。這樣子會增加別人家解碼的困難度也同時可以爭取到一些時間.

為了要尋找這個函數，我選擇了和費氏數列的輾轉相除法有關的步數函數，因為費氏數列具有許多的特性。 所以安排他為這次的主題,並以圖形為輔。

(二) E 函數
1.簡單的利用 E 函數加碼
首先，我們先來認識一下一般的英文加碼。就數學上來看的話,簡單的可分單表代替密碼和多表代替密碼，單表中又分加法和乘法，最簡單的加密系統就是利用同餘的概念，舉個例子來看原本是ａｂｃ‧‧現在我們把他們通通向後退一個，這樣ｂ就變成ａ，ｃ就變成ｂ了。

密	a	b	c	d	E	f	g	h	i	j	k	l	m
明	**z**	**a**	**b**	**c**	**D**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**
密	n	o	p	q	R	s	t	u	v	w	x	y	z
明	**m**	**n**	**o**	**p**	**Q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**

『例』：Happygirl = gzooxfhqk

只是這種方法只要去算某個明文上的字母頻率，就可以比較快破解。

現在我們來介紹一般的加解碼方式

加碼

(1)嘗試把英文換成數學,並用我們之前提到的函數來加碼。

再利用概念時我們介紹了一個小公式。$E\left(F_{n+2},F_{n+1}\right)=n$

原	a	b	c	d	e	f	g	h	i	j	k	l	m
密	1	2	3	4	5	6	7	8	9	10	11	12	13
原	n	o	p	q	r	s	t	u	v	w	x	y	z
密	14	15	16	17	18	19	20	21	22	23	24	25	26

像 H 的代號是 $8=E\left(F_{10},F_9\right)=5534\Rightarrow$ 這兩數連在一起,其中一個不過是另一個的下個數

或上一個數,所以我們去掉 F_9,然也可以去掉 F_{10}，只要兩個人約定好就可以了!

例如：

happy girl

= 8 1 16 15 24 6 8 17 11

= 34 1 1597 1597 121393 21 55 4181 233

= 3 4 1 1 5 9 7 1 5 9 7 1 2 1 3 9 3 2 1 5 5 4 1 8 1 2 3 3

happy girl 經由「加密」之後，變成了上式的「一大串」數字，然後我們針對每個字母所得到的數字，其中每個數字兩兩爲一組，但如果有些不能譯出英文單字的話（像３４就沒有　英文字母可以對到），我們就針對大於 25 的數字加入「0」(零)做組合，例如：

013576 這數字，可以與 0 組合成 00-13-05-07-06；0135716 解成 00-13-05-07-16。

= 0 3 0 4 1 1 0 5 0 9 0 7 1 5 0 9 0 7 1 2 1 3 0 9 0 3 2 1 0 5 0 5 0 4 1 8 1 2 0 3 0 3

明文 d e l f j h p j h m n j d o f f e s m d d

這樣最簡單的加碼就完成了!

解碼：當對方拿到的時候

明文 d e l f j h p j h m n j d o f f e s m d d

= 0 3 0 4 1 1 0 5 0 9 0 7 1 5 0 9 0 7 1 2 1 3 0 9 0 3 2 1 0 5 0 5 0 4 1 8 1 2 0 3 0 3

因爲我們都是以二個位數爲單位,所以我們就二個爲一組. 前面有 0 的話就去掉 0

= 3 4 1 1 5 9 7 1 5 9 7 1 2 1 3 9 3 2 1 5 5 4 1 8 1 2 3 3
3

接下來要換就小心一點了

$3\rightarrow F_4$　$4\rightarrow$ 沒意義　411 沒意義,………　這個時候就該知道 4 是和 3 一組的, 利用

電腦做到這樣的檢驗工作應該不難吧!

*如果說真的有一段文字，可以剛好在一小段文字內可以翻譯成不同的密文. 那麼這種例子畢竟是少數，用電腦跑一下，我們會去選擇比較合理的解釋，其實這方面並沒有很大的問題. 英文字母在換代號時, n 值我們最多用到 30,而費氏數列 F_{31}, F_{32} 只有 7 位數爲了避免如果有重覆。

如：12345678　既可以翻譯成 a_6　a_7　a_{10}　a_8　也可以解釋爲 a_{26}　a_9

換碼換成 6,7,10,8 但卻因爲他恰也可以換成 26,9,這種解釋就會出差錯。不過,如果解釋的出來是 yitzu,我想大概也沒什麼意義! 這種例子並不多. 而且,我也先檢查了! $F_1 \sim F_{32}$ 的數字發現並沒有這樣的問題,更何況費氏數列有許多特性!說不定他並不會重複!!! ⇒ 這部分可以有延伸的討論空間!

把費氏數列還原　這部分就交給電腦囉!嘗試 1~8 爲數的費氏數列,將之分類還原

=	34	1	1597	1597	121393	21	55	4181	233
=	8	1	16	15	24	6	8	17	11

Q：爲什麼只要檢查到 8 位數呢?

A：根據 Lame 的定律 $1 < E(a,b) \le 5 \times 6$ 位數 $E(a,b)$ 我們只用到 30

所以 $1 < 30 \le 5 \times 6$

⇒所以最少也要 check 到 6 位數字,不果保守起見我取 $E(a,b)$ 到 40。

$1 < 40 \le 5 \times 8$ 位數

大致上我們就是要利用這樣的模式下去變換

(2)另一種加碼方式：

=	34	1	1597	1597	121393	21	55	4181	233

在這裡就直接換成二進位，然後在數字之間加入 1111 作爲分隔以便解碼時電腦區分,

例如：34 1 就變成 0011010011110001

所以上式就變成

= 001101001111000111110001010110010111111100010101100101111111000100100001001110010011111100100001111101010101111101000001100000011111001000110011

然後可以任取多個爲一個單元(要是四的倍數喔! 這樣子在取的時候才不會有多的) 例如取八個的話，可能就會換成 18 65 24 等等的 再來就可以用一般的加密法 或者是尤拉步數再次加密也可以

不過這個方法很複雜，所以還是以第一個方法繼續討論!

2. 利用函數的週期性

第 x 排的數字，從對角線開始，就會呈現以 x 爲循環的現象。如：第二行是 2121…就是以２爲週期，不斷的重複下去。

例如：看第一個出現 3 的那一行，而也就是說：3 的週期是 $3\left(F_4\right)$，4 的週期是 $5\left(F_5\right)$

$2\Rightarrow$(就是以 2 爲週期)

$$=E\left(F_4,F_3\right)\xrightarrow{\text{按照剛剛的加碼後，但這次我們取比較大的}F_4}F_4=3$$

同理 $=E\left(5,2\right)$ 因爲 $F_4+2=5$

$$=E\left(7,2\right)\text{因爲}F_4+2\times F_3=E\left(9,2\right)\text{因爲}F_4+3\times F_3=..........$$

以此類推 $n=F_{n+2}+\alpha F_{n+1}$，這時我們用 5 來代替 3，或者是 7 來代替 3，這樣一來，這個 α 值就可以說是我們的 key。只要取任何我們想要的 α 值，就會有很多種不同的組合。

15	1	2	1	3	1	2	2	3	3	2	4	2	3	2	1
14	1	1	3	2	3	2	1	3	4	3	4	2	2	1	2
13	1	2	2	2	4	2	3	5	3	3	3	2	1	2	3
12	1	1	1	1	3	1	4	2	2	2	2	1	2	2	2
11	1	2	3	3	2	3	4	4	3	2	1	2	3	4	4
10	1	1	2	2	1	3	3	2	2	1	2	2	3	3	2
9	1	2	1	2	3	2	3	2	1	2	3	2	3	4	3
8	1	1	3	1	4	2	2	1	2	2	4	2	5	3	3
7	1	2	2	3	3	2	1	2	3	3	4	4	3	1	2
6	1	1	1	2	2	1	2	2	2	3	3	1	2	2	2
5	1	2	3	2	1	2	3	4	3	1	2	3	4	3	1
4	1	1	2	1	2	2	3	1	2	2	3	1	2	2	3
3	1	2	1	2	3	1	2	3	1	2	3	1	2	3	1
2	1	1	2	1	2	1	2	1	2	1	2	1	2	1	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

a	b	c	d	e	f	g	h	i	j	k	l	m
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
4	***7***	***11***	***18***	***29***	***47***	***76***	***123***	***144***	***322***	***521***	***843***	***1364***
n	o	p	q	r	s	t	u	v	w	x	y	z
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
2207	***3571***	***5778***	***9349***	***15127***	***24476***	***39603***	***64079***	***103682***	***167761***	***271443***	***439204***	***710647***

設定 $\alpha=2$，那麼 $\mathrm{H}\Rightarrow 8\Rightarrow F_{8+2}+2F_{8+1}=55+2\times 34=123$

我們再用 HAPPYGIRL 來看看，

H	A	P	P	Y	G	I	R	L
=8	1	16	16	25	7	9	18	12

<table>
<tr><td colspan="3">=123</td><td colspan="3">4</td><td colspan="3">5778</td><td colspan="3">5778</td><td colspan="3">439204</td><td colspan="3">76</td><td colspan="3">144</td><td colspan="3">15127</td><td colspan="3">843</td></tr>
<tr><td colspan="27">= 1 2 3 4 5 7 7 8 5 7 7 8 4 3 9 2 0 4 7 6 1 4 4 1 5 1 2 7 8 4 3</td></tr>
<tr><td>=</td><td>12</td><td>03</td><td>04</td><td>05</td><td>07</td><td>07</td><td>08</td><td>05</td><td>07</td><td>07</td><td>08</td><td>04</td><td>03</td><td>09</td><td>20</td><td>04</td><td>07</td><td>06</td><td>14</td><td>04</td><td>15</td><td>12</td><td>07</td><td>08</td><td>04</td><td>03</td></tr>
<tr><td>=</td><td>L</td><td>C</td><td>D</td><td>E</td><td>G</td><td>G</td><td>H</td><td>E</td><td>G</td><td>G</td><td>H</td><td>D</td><td>C</td><td>I</td><td>T</td><td>D</td><td>G</td><td>F</td><td>N</td><td>D</td><td>O</td><td>L</td><td>G</td><td>H</td><td>D</td><td>C</td></tr>
</table>

當對方解碼時

明文=LCDEGGHEGGHDCITDGFNDOLGHDC

=12030405070708050707080403092004070614041512070804O3(換成數字)

=1234577857784392047614415127843(去掉 0 還原成原始的碼)

再來讓電腦根據$\alpha=2$的數字表來分類

像第一個數字 1 可能是 a.h.m.r.w 但是符合第二個的只有可能是 a 和 h, 再來驗證第三個就只剩下 h 這種可能了, 像這種算法是前後彼此卡緊的. 所以會產生另一串數字的可能性不高.

=123 4 5778 5778 439204 76 144 15127 843(去掉 0 還原成原始的碼)

=h a p p y g i r l

不過, 或許他真的會有另外一對數字! 確實 當 key 取作 3 的什候, 有一段文字可以翻成 gea 又可以翻成 b p 這個時候,只要看上下文就可以決定是要用 bp 還是要用 gea 了! 所以這方面並不會造成太大的困難.

3.推廣: a.剛剛我們利用根據觀察所得到的式子$n=F_{n+2}+\alpha F_{n+1}$來做加解密的工作. 仔細看看,

這不就是一個遞迴函數的表示法嗎! 所以我們更可以繼續推廣, 把用一般的遞迴函數

的式子$A_n=\alpha A_{n-1}+\beta A_{n-2}+.....$ 這樣一來, n 值就可以用A_n,A_{n+1},A_{n+2}來表示, 例如 :

$n=\alpha A_{n+1}+\beta A_{n+2}+.....$ 來表示, 每個人可以選擇不同的遞迴式子, 然後把其中的

$\alpha\beta\gamma$ ...等值當作是 key, 因爲位數都很大,所以不用去很大的值.

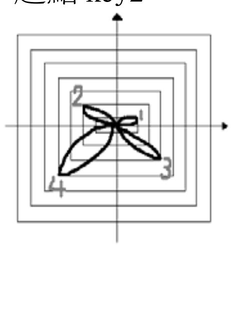
這樣一來也就等於就是能一次爲密碼上好幾層鎖.

b. 如果一段文字中出現某個數字很多遍, 那也很容易猜到那一串數字就是一組的.爲了預防這種情況發生. 我們更可以規定, 第一個 a 用$\alpha=1$的加密,第二個出現的 a 用$\alpha=2$依此類推, 不過這樣一來在解碼的時候會比較複雜. 也可以只用$\alpha=1 or 2$來當做周期交互著用. 這樣就會大大的提高了保密性.

4.圖形, 幾何: 希望能夠找到一個圖形來加密, 利用座標軸來當做 key1, 起點 key2

例如來看, 我們從第一象限開始讀 1243 也就是代表 abdc

當然還有很多方法可以表示



不過至今還是沒有找到適合的表示法, 頗爲遺憾

5.實例　這是遞迴式用 $n = F_{n+2} + 5F_{n+1}$

1542364995017306805799501865331172121056930686536472441225225532767022573642767013532
0711721299501537154215426532862255327670862767036453403733995017244165321542332255327
6702257364276709950172441803383154253306865799501653211721272441653286337724415386653
2276708640372053724412258611721213722572441154236499501736430686574037724417244186338
6995013324955372441225364403713930686536715423330676536472441225249580338322573642767
0995012255315426532653295353337244122527670653211721213922524957403780338324957139712
9990136460375372441653299501535372441225531542772441539950172441995017244080338315425
3995012495803383139653265323340375399501995019950122553995017364337995019950122553995
0173067053068656532249553403730686536472441225131542117212537403733139276705353403722
5736427670154236499501733532036433533354324037772441653240375333336532306765403722573
6427670995017244180338015
Lisa was fed up with her hair because all of her friends told her that her hairstyle was out of date. "For once,"thought Lisa,"I want to do something wild with my hair."She looked through many magazines to see the latest styles. "My goodness!"she said as she saw women with blue and green hair. Lisa decided on a toned-down hairstyle.

陸：結論

從一個小小的益智盒所啓發出來的概念，再加上費氏數列和輾轉相除法，這一切似乎毫無相關的東西，卻被密碼綁在一起。利用新函數 E，走出一條和一般不同的編碼方式。

現在的電腦的發達，要跑多少位數的數字已經不再是問題。 這次的科展中, 我並不是要像一般研究生一樣, 提升加解密的安全性. 而是要試跳脫一般的數學方法, 利用費氏數列原本就有的奇妙特性,將他和圖形做連結，並提出一個概念來詮釋我們所用的加碼方式。簡單又特別，如果真的能找到一個很美的圖形來代替這一端繁雜的文字呢！這樣聽起來不是很美好嗎？密碼不再艱深困難，讓大家能夠更了解數字的美。

染：參考資料和其他

霍安琪　　　　　　密碼學
夫蘭納里(2001 年)　數學小魔女　台北市: 天下遠見
蔡聰明　　　　　　數學發現趣談

一、步數函數 (of 費氏數列)

分析　$(2,3) \to (2,1) \to (0,1)$　　　$E(F_4, F_3) = 2$

$(3,5) \to (3,2) \to (1,2) \to (1,0)$　　　$E(F_5, F_4) = 3$

$(5,8) \to (5,3) \to (2,3) \to (1,2) \to (0,1)$　　　$E(F_6, F_5) = 4$

$(F_{n+1}, F_n) \to (F_{n-1}, F_n) \to (F_{n-1}, F_{n-2}) \ldots\ldots (1,2)$

$E（F_{n+1},F_n）=n-1$

由上很容易發現（F_{n+2}，F_{n+1}）除了第一步之外，其他的跟上一個（F_{n+1}，F_n）一模一樣，步數多一個

▲設: 費氏數列兩兩相互質 $F_{n+2}=F_{n+1}+F_n$　　$F_{n+2}>F_{n+1}>F_n$　　(n＞3)

求證：E（F_{n+2}，F_{n+1}）＝n　（$n\in N$）

證明：數列　$F_{n+2}-F_{n+1}=F_n$　，　　$F_{n+2}>F_{n+1}>F_n$　（n≧3）

$（F_{n+2}，F_{n+1}）\to（F_{n+1}，F_n）\to（F_n，F_{n-1}）\to\ldots\ldots\to（F_2,F_3）\to（F_1,F_2）$

【 $\because F_{n+1}-F_n=F_{n-1}<F_n$ 】【E（a,b）＝E（b,a）】

E（F_{n+2} ,F_{n+1}）＝n＋2－2＝n　　得証

△由以上可知，$\langle F_n\rangle$無上限　∴ E（a,b）也沒上限

在這之前已經發現，$E\left(F_{n+2},F_{n+1}\right)=n$

又從表中猜出最先出現 n 是 F_{n+2},F_{n+1}

所以我們要來分析看看這是不是對的

設 $a,b\in N\wedge b\leq a$

求證：$\because b\leq a$　　$\langle r_i\rangle$爲遞減數列　　$\exists n\in N$　　$\ni r_n=0$

$$a = b \times \left[\frac{a}{b}\right] + r_1$$

$$b = r_1 \times \left[\frac{b}{r_1}\right] + r_2$$

$$r_1 = r_2 \times \left[\frac{r_1}{r_2}\right] + r_3$$

$\therefore$ 設.

.

.

$$r_{n-2} = r_{n-1} \times \left[\frac{r_{n-2}}{r_{n-1}}\right] + r_n$$

$\because r_n = 0 \quad r_{n-2} \neq r_{n-1} \quad \therefore \left[\frac{r_{n-2}}{r_{n-1}}\right] \geq 2$ 取(min) 而 $\left[\frac{r_{n-3}}{r_{n-2}}\right] \geq 1$

$r_{n-2} = 2 \times 1 = 2 \ldots\ldots\ldots\ldots\ldots\ldots F_3$

$r_{n-3} = 2 \times 1 + 1 = 3 \ldots\ldots\ldots\ldots\ldots\ldots F_4$

$r_{n-4} = 3 \times 1 + 2 = 5 \ldots\ldots\ldots\ldots\ldots\ldots F_5$

.

令 $r_{n-1} = 1$ 則.

.

$r_1 = F_{n-1} \times 1 + F_{n-2} \ldots\ldots\ldots\ldots\ldots\ldots F_n$

$b = F_n \times 1 + F_{n-1} \ldots\ldots\ldots\ldots\ldots\ldots F_{n+1}$

$a = F_{n+1} \times 1 + F_n \ldots\ldots\ldots\ldots\ldots\ldots F_{n+2}$

所以當 $a = F_{n+1}, b = F_{n+2}$ 時爲最小値　　　　　　　Q.E.D

現在我們 已經知道步數關係　那對於任何 a,b 他的步數最少要多少呢??　我們可以從費氏數列下手

由剛剛的定理 $E\left(F_{n+1}, F_{n+2}\right) = n$，我們發現

$F_7 = 13 \geq 10$
$F_8 = 23 \geq 20$
$F_9 = 34 \geq 30$
$F_{10} = 57 \geq 50$
.
.
.
$F_n \geq n10$(n和x的關係爲一對)

而 x 的值好像費氏數列
所以

分析 $F_{n+5} = F_{n+4} + F_{n+3} = 5F_{n+1} + 3F_n = 13F_{n-1} + 8F_{n-2} = 13F_n - 5F_{n-2}$

(注： $3F_n = 3F_{n-1} + 3F_{n-2} \geq F_{n-1} + 5F_{n-2} \Rightarrow 3F_n - 5F_{n-1} \geq F_{n-1} \geq 0$)

$= 10F_n + 3F_n - 5F_{n-2} \geq 10F_n$

再將他改一下
設他共有 k 位數，k 爲自然數

則 $F_{n+5k} \geq 10^k F_n$ …………………………………………….(i)

現在令 $\langle a_n \rangle$ 爲任意一輾轉相除法的數列

由之前的定理我們知道如果 $E(a_{5k+2}, a_{5k+1}) = 5k$ ，則 $a_{5k+1} \geq F_{5k+1}$

所以利用(i)令 $n = 1$ ，則我們就知道

$a_{5k+1} \geq F_{5k+1} \geq 10^k F_1 = 10^k$ 也就是說 a_{5k+1} 要比 10^k 大

則 $E(a_{5k+2}, a_{5k+1})$ 才會等於 5k

整理一下

設 $m \geq n$ ，則 $1 \leq E(m,n) \leq 5 \times n$ 的定位，這也就是 Lame 定律

費氏數
```
> n <- 100
> A <- matrix(0, 1, n)
> A[1, 1] <- 1
> A[1, 2] <- 1
> for(i in 3:n)
```

```
        { A[1, i] <- A[1, i - 1] + A[1, i - 2] }
> A

     [,1] [,2] [,3] [,4] [,5] [,6] [,7] [,8] [,9] [,10] [,11] [,12]
[1,]    1    1    2    3    5    8   13   21   34    55    89   144
     [,13] [,14] [,15] [,16] [,17] [,18] [,19] [,20] [,21] [,22] [,23]
[1,]   233   377   610   987  1597  2584  4181  6765 10946 17711 28657
     [,24] [,25]  [,26]  [,27]  [,28]  [,29]  [,30]   [,31]   [,32]
[1,] 46368 75025 121393 196418 317811 514229 832040 1346269 2178309
```

中華民國第四十五屆中小學科學展覽會
評　　語

高中組 數學科

040409
潘朵拉的盒子

國立馬公高級中學

評語：
1. 成功的數學科展常隱藏於數學遊戲中，然而數學科展的靈魂在於遊戲的數學內涵。
2. 很難得看到作者如此感性投入於科展。