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

佳作

040419
應用橢圓曲線在中文加解密之使用探討

國立馬祖高級中學

作者姓名：
高一 劉瑞軒 高二 杜安琪 高二 曹家嘉

指導老師：
胡裕仁

中華民國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：應用橢圓曲線在中文加解密之使用探討

關鍵詞：橢圓曲線、同餘運算、射影平面座標

編號：

學校名稱：

國立馬祖高中

作者姓名：

劉瑞軒、杜安琪、曹家嘉

指導老師：

胡裕仁

摘要

在此次的科展中，我們將利用高中數論所學的同餘運算，來進行加解密計算。並利用橢圓曲線逆運算不易的幾何特點[4][5]，來確保明文加密後的安全理論並設計出結合中文加密模式。我們研究結果如下：

一. 公式分析：我們先引用橢圓曲線的加解密運算式分析出它的數學原理，進而推算出其關係式以進行電腦演算。

二. 演算法內容分析：由公式分析出的結果，我們開始為每一個中文明文進行編碼，並歸納出其關係式來推論出可用的加密點。

三. 由橢圓曲線上的可加密點來進行中文注音及標點符號的編碼，並以馬致遠的「天淨沙」來實作出我們模擬的成果。

壹、研究動機

在高一上學期的數學課堂中老師教導了一個取餘數函數（模數運算）的數學觀念，例如：若 $R_7(50)=1$ 表示 $50\div 7$ 餘數為 1； $R_5(50)=0$ 表示 $50\div 5$ 餘數為 0 的數學概念[6]。

然後又在學校圖書館中發現了一本『碼書』[1]，無意中看了幾頁覺得好像跟唸國中時自己所做的一個報告『密碼鑰匙』有關。因此便向校內的老師請益，希望老師協助我將之前一份不成熟的作品加以修正並且指導自己對於科學研究的學習指導。老師建議我先把『碼書』好好研讀一遍，因為在這本書裡，將密碼學的古今歷史及相關故事詳盡敘述一遍，使我對於密碼學的了解更加深入。

而且書中提及到非對稱鑰匙的加解密系統更為當代密碼學上的顯學。『碼書』中的非對稱鑰匙的加解密系統，首推 RSA 加解密系統，由三位麻省理工學院的電腦科學研究員所研究出來的非對稱鑰匙的加解密系統。我們雖然只是幾位平凡的高中生，也不敢期望自己能研究出新的加解密系統，但是還是希望能以此成為我們學習科學研究的第一步。

貳、研究目的

在歷屆全國中小學科展中有很多作品是利用 RSA 非對稱密碼系統，因此老師建議我尋找其它加解密系統，因此便利用網際網路找出一套新的加解密系統 ECC(Elliptic Curves Cryptography，橢圓曲線密碼編碼學），它是屬於非對稱公開密鑰加解密系統演算法之一。

採用 ECC 是因為它所需要的秘密金鑰的長度相較於 RSA 加解密系統演算法而言比較小[5]，也就是代表 ECC 較 RSA 的加解密效率在相同金鑰的長度之下為高且安全，本文將採用以提高加解密的應用效率。

相較於傳統易受頻率法攻擊的代替式密碼[1]，目前以非對稱的密碼為主流（仍算是代替式密碼法的延伸）。

本節將簡要說明代替式密碼法的優劣。若在密碼傳送時攻方攔截到密文，並以可能的出現的字進行頻率分析將可進而猜測出明文。因此為增強明文編碼的安全，特別利用高一數學的同餘概念（取餘數方法），來實作出一套新的中文密碼方法。並利用公開金鑰與私密金鑰的非對稱式加密來強化密碼傳送時的安全。

參、研究設備及器材

一、可上網際網路的奔騰第四代 3.0GHz 電腦壹台。

二、可以編輯數學方程式符號的 MathType、Word 軟體及計算用 Excel 軟體各壹套。

三、繪圖軟體 Visio、GSP 各壹套。

四、一台彩色印表機。

五、一堆不要用的計算紙及三粒清楚的人腦。

肆、 研究過程及方法

橢圓曲線被應用於加解密系統最早始自西元 1985 年來自華盛頓大學 Neal Koblitz 及當時任職於 IBM 的 Victor Miller[10]。本文將借用來進行中文的密碼加解密應用。假設平行線在很遠很遠的地方相交了，即平行線相交於無窮遠點$O\infty$，如圖 1。這樣做所帶來的好處是所有的直線都相交了，且交於一點。因此定義出了一些無窮遠點的性質，以下是無窮遠點的幾個性質[8]。

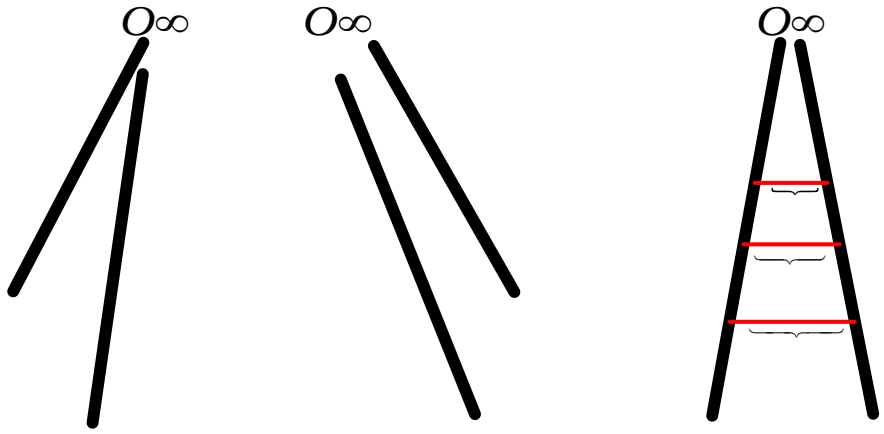


圖 1

無窮遠點的性質：

一、直線L上的無窮遠點只能有一個。

二、平面上一組相互平行的直線有公共的無窮遠點。

三、平面上任何相交的兩直線L_1，L_2有不同的無窮遠點。

四、平面上全體無窮遠點構成一條**無窮遠直線**。

五、平面上全體無窮遠點與全體平常點構成**射影平面**。

射影平面坐標系：由於普通平面直角坐標系沒有為無窮遠點設計座標，不能表示無窮遠點，為了表示無窮遠點產生了射影平面坐標系，當然射影平面坐標系同樣能很好的表示舊有的平常點。我們對普通平面直角坐標系上的點A的座標(x,y)做如下轉變：令$x=\frac{X}{Z}$，$y=\frac{Y}{Z}$（$Z\neq 0$），則A點可以表示為$(X:Y:Z)$。若實數$P\neq 0$則$(PX:PY:PZ)$與$(X:Y:Z)$表示同一個齊次座標點。因此對平面上的點建立了一個新的座標體系即射影平面座標系[4][7][8][9]。

公式 1：無窮遠點的直線座標方程式：

若一射影平面座標上的一組平行直線方程式為 $aX+bY+c_1Z=0$ 及 $aX+bY+c_2Z=0$（$c_1\neq c_2$）

則射影平面上的無窮遠點座標為（$X:Y:0$）的通式且其直線對應的方程式是 $Z=0$。

證明：

$\because \begin{cases} aX+bY+c_1Z=0 \\ aX+bY+c_2Z=0 \end{cases}$，（$c_1\neq c_2$）將方程式聯立求解，有 $c_2Z=c_1Z=-(aX+bY)$，

（$\because c_1\neq c_2 \ \therefore Z=0 \ \therefore aX+bY=0$）；所以無窮遠點就是這種形式（$X:Y:0$）表示。注意平常點 $Z\neq 0$，無窮遠點 $Z=0$，因此無窮遠點的直線對應的方程式是 $Z=0$。

定義 1：射影平面坐標系的橢圓曲線方程式：

若在射影平面坐標系上能夠滿足 Weierstrass 方程式[4]（次數為 3 的齊次方程式）

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \text{---（1-1）}$$

的所有點的集合，且曲線上的每個點都是非奇異或光滑的，則稱為射影平面坐標系的橢圓曲線方程式。

說明：

以方程式（1-1）來說，曲線上的每個點都是非奇異或光滑的，也就是說曲線上的每個點都存在該點的切線，即曲線上任意一點的偏導數 $F_x(x,y)$，$F_y(x,y)$ 不能同時為 0，圖形如下圖 2、3。

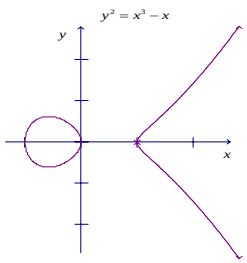


圖 2

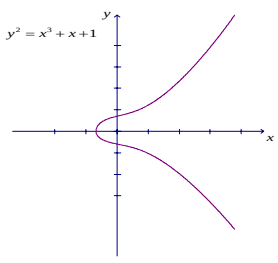


圖 3

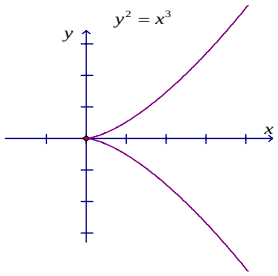


圖 4

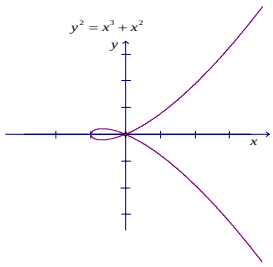


圖 5

在圖 2、3 中由於滿足方程式的偏導數 $F_x(x,y)$，$F_y(x,y)$ 不同時為 0，因此屬於橢圓曲線。而圖 4、5 中的兩張圖在射影平面座標系中的 $(0,0)$ 點的座標位置（即原點）並未能滿足方程式的偏導數不同時為 0 的條件，故在原點時切線不存在，因此不能算是橢圓曲線[4][7]。

定義 2：普通平面直角坐標系的橢圓曲線方程式：

若在普通平面坐標系上能夠滿足（1-1）方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{---（1-2）}$$

的所有點的集合，且曲線上的每個點都是非奇異或光滑的，則稱為普通平面坐標系的橢圓曲線方程式。

說明：

知道了橢圓曲線上的無窮遠點，我們就可以把橢圓曲線放到普通平面直角坐標系上了。因為普通平面直角坐標系只比射影平面坐標系少無窮遠點，因此我們在普通平面直角坐標系上，求出橢圓曲線上所有平常點組成的曲線方程式，再加上無窮遠點 $O\infty$，即構成橢圓曲線。令 $x = \frac{X}{Z}$，$y = \frac{Y}{Z}$ 代入方程式（1-1）經變數變換後得到式（1-2）。也就是說滿足普通平面直角坐標系方程式（1-2）的光滑曲線加上一個無窮遠點 $O\infty$ 組成了橢圓曲線。為了方便運算表述，本文之後論述橢圓曲線將主要使用（1-2）的形式。

進行橢圓曲線加解密的計算時，需先了解橢圓曲線上任一點的切線斜率的計算方法。

公式 2：橢圓曲線上任一點的切線斜率

若一橢圓曲線方程式為 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$，則在此橢圓曲線上的切線斜率 $m=\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}$ ---（1-3）。

證明：

由橢圓曲線的定義可以知道，橢圓曲線是光滑的，因此橢圓曲線上的平常點都有切線，可以求切線斜率 m。因為橢圓曲線方程式 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$，設一平常點 $A(x,y)$ 的切線斜率為 m。

解：令 $F(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$

求偏導數：

$$\frac{\partial F(x,y)}{\partial x}=a_1y-3x^2-2a_2x-a_4$$

$$\frac{\partial F(x,y)}{\partial y}=2y+a_1x+a_3$$

則導數為：

$$\frac{dF(x,y)}{dx}=-\frac{\frac{\partial F(x,y)}{\partial x}}{\frac{\partial F(x,y)}{\partial y}}=-\frac{a_1y-3x^2-2a_2x-a_4}{2y+a_1x+a_3}=\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}$$

所以斜率為 $m=\frac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}$。

由定義 2 及公式 2 知在密碼學中的橢圓曲線並不是全部皆可用來進行加解密，它必須定義在一組實數點 (x,y) 集合裡。常用的橢圓曲線方程式有 $y^2=x^3+ax+b$，在此（a、$b\in R$）而且 a、b 需滿足關係式 $4a^3+27b^2\neq 0$ [4][5]，由此得來的橢圓曲線方程式方可進行加解密運算 [10]。

在許多的加解密系統裡通常需要使用一些代數體（Algebraic Groups）運算，橢圓曲線也是其中之一，滿足橢圓曲線所定義的圖形上，每一個點即為體的元素，故橢

圓曲線加解密運算便是利用代數體的運算，而加解密是利用代數學中的有限體（Finite Field）來限制其範圍（利用同餘方式來定出範圍內的元素個數）[9]。在數學中體的概念是表示一些特定元素的集合，也就是說在射影平面座標系中將組成橢圓曲線的所有點，合成一個體，在此集合中我們可以任意將其中的任兩元素做加、減、乘及除等運算 [2]。

橢圓曲線運算法則：圖 6 為一橢圓曲線有參數 $a=-7$ 、 $b=0$ 且滿足判別式 $4a^3+27b^2\neq 0$，因此為可用來加解密之橢圓曲線之一，若於一橢圓曲線圖形中任取兩點 P、Q（設 $P\neq Q$，若在圖 7 中若 $P=Q$ 時，則作 P、Q 切線交橢圓曲線於 $-R$）且其座標分別為 $P(-2.35,-1.86)$、$Q(-0.1,0.836)$，然後作 P、Q 兩點的直線交橢圓曲線的另一圖形於 $-R$ 點，則 $-R$ 座標為 $-R$ $(3.89,5.62)$，再以 $-R$ 座標點作一平行 y 軸的直線交橢圓於 R，則可得到如下之結果 $P+Q=R$，其中「+」並不是實數中的一般加法，而是代數體運算中的一個加體。在橢圓曲線運算法則中，可以知道橢圓曲線無窮遠點 $O\infty$ 在垂線上與橢圓曲線上一點 P (x,y) 的連線交於 $-P$ $(x,-y)$，過 $-P$ 作 y 軸的平行線交於 P (x,y)，所以有無窮遠點 $O\infty+P=P$（兩點於同一直線的情形）。無窮遠點 $O\infty$ 的作用與普通加法中零的作用相當即 0+2=2，因此把無窮遠點 $O\infty$ 稱為**零元**。同時把 $-P$ 稱為 P 的**負元** [4][10]，如圖 7、8。

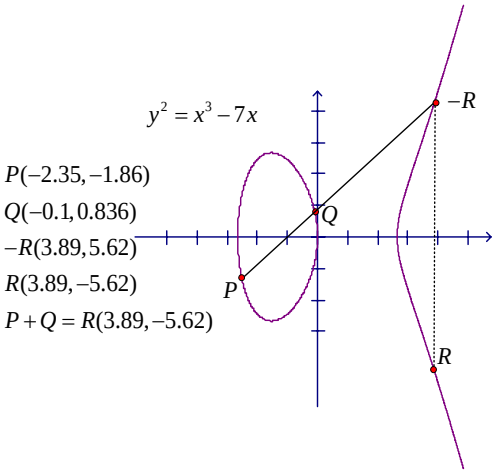


圖 6

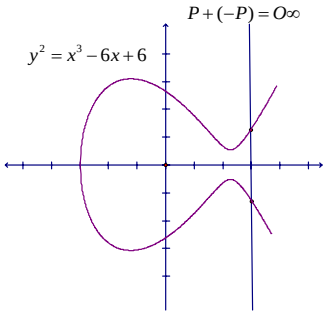


圖 7

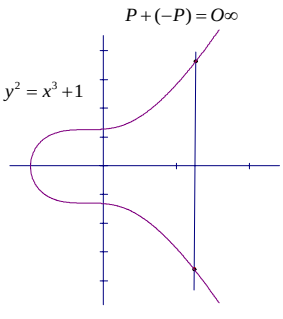


圖 8

由上列法則可知，若橢圓曲線上有三個點且橢圓曲線上的三個點 A 、 B 、 C 位於同一條直線上，那麼他們的和等於零元，即 $A+B+C=O\infty$ 。因此 k 個相同的點 P 相加，我們記作 kP ，如圖 9： $P+P+P=2P+P=3P$ 。因此下面我們利用 P 、 Q 點的座標 (x_1,y_1) ， (x_2,y_2) ，求出 $R=P+Q$ 的座標 (x_4,y_4) 。

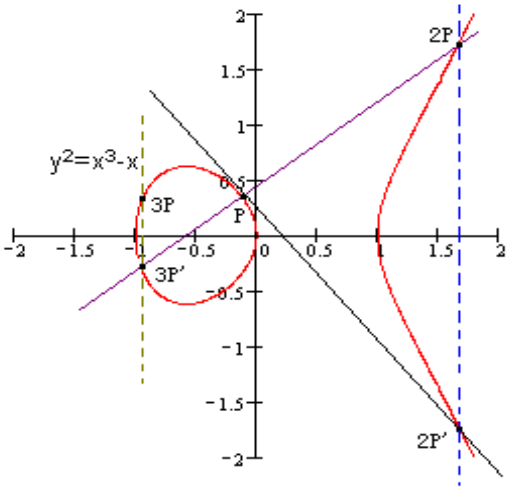


圖 9

公式 3：若已知 $P(x_1,y_1)$ ， $Q(x_2,y_2)$ 的座標為一橢圓曲線方程式 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 上的兩平常點，設兩平常點的和為 $R(x_4,y_4)$ ，則 $R(x_4,y_4)$ 的座標為（ $x_4=m^2+ma_1+a_2+x_1+x_2$ ， $y_4=m(x_1-x_4)-y_1-a_1x_4-a_3$ ）。

證明：

（1）先求點 $-R(x_3,y_3)$

因為 P 、 Q 、 $-R$ 三點共線，故設共線方程式為 $y=kx+b$ ，其中若 $P\neq Q$ （ P ， Q 兩點不重合）則直線斜率 $m=\dfrac{y_1-y_2}{x_1-x_2}$ 。若 $P=Q$ （即 P 、 Q 兩點重合）則直線為橢圓曲線的切線，故由式（4-3）可知： $m=\dfrac{3x^2+2a_2x+a_4-a_1y}{2y+a_1x+a_3}$ 因此 P 、 Q 、 $-R$ 三點的座標值就是方程組： $\begin{cases} y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6---[1] \\ y=mx+b----------[2] \end{cases}$ 的解。將 [2]，代入[1]得出 $(mx+b)^2+a_1x(mx+b)+a_3(mx+b)=x^3+a_2x^2+a_4x+a_6---[3]$

對[3]化為一般方程式，即 $x^3+(a_2-m^2-ma_1)x^2+(a_4-2mb-a_1b-ma_3)x+(a_6-b^2-a_3b)=0$ ---[4] 由三次方程式根與係數關係知（若 $(x-x_1)\cdot(x-x_3)\cdot(x-x_3)=0$ 即 $x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_2x_3+x_3x_1)x-x_1x_2x_3=0$ 因此 $-x_1x_2x_3$ 為常數項係數，$x_1x_2+x_2x_3+x_3x_1$ 為一次項係數，$-(x_1+x_2+x_3)$ 等於二次項係數。）所以 $\begin{cases}-x_1x_2x_3=a_6-b^2-a_3b\\x_1x_2+x_2x_3+x_3x_1=a_4-2mb-a_1b-ma_3\\-(x_1+x_2+x_3)=a_2-m^2-ma_1\end{cases}$，解開 $x_3=m^2+ma_1-a_2-x_1-x_2$ --（求出 $-R$ 的橫坐標）。因為 $m=\frac{y_1-y_2}{x_1-x_2}=\frac{y_1-y_3}{x_1-x_3}$ 故 $y_3=y_1-m(x_1-x_3)$---（求出點 $-R$ 的縱坐標）。

（2）利用 $-R$ 求 R

顯然有 $x_4=x_3=m^2+ma_1+a_2+x_1+x_2$------（求出點 R 的橫坐標），求 y_3、y_4 即求 $x=x_4$ 時，方程式 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 的解化為一般方程 $y^2+(a_1x+a_3)y-(x^3+a_2x^2+a_4x+a_6)=0$，由二次方程式根與係數關係得 $-(a_1x+a_3)=y_3+y_4$，所以 $y_4=-y_3-(a_1x+a_3)=m(x_1-x_4)-y_1-(a_1x_4+a_3)$----（求出點 R 的縱坐標）即：$x_4=m^2+ma_1+a_2+x_1+x_2$，$y_4=m(x_1-x_4)-y_1-a_1x_4-a_3$。

密碼學上的橢圓曲線：由於橢圓曲線是連續的，並不適合用於加密，所以必須把橢圓曲線變成離散的點。因為橢圓曲線上點座標是實數，也就是說前面的橢圓曲線是定義在實數體上的，由於實數是連續的，導致了曲線的連續。因此須把橢圓曲線定義在有限體（Finite Field）上。如此才能用來進行加解密工作。而進行加解密工作前，須定出一個有限體 F_P（利用同餘方法），滿足 F_P 中只有 P 個元素，即滿足 0、…、$P-1$ 或 1、2、…、P。

模（mod）數及同餘運算法則：在求F_P元素的運算中，我們將利用高一數論所學的取餘數方式來定出有限域F_P內部元素。令三整數a，b及$P\neq 0$，我們稱a在模P時與b同餘，若且唯若a與b的差為P的整數倍（$R_P(a)=R_P(b)\Leftrightarrow a-b=k\cdot P$，$k\in Z$）。我們以$a\equiv b \pmod P$表示$a$與$b$有同餘。所有整數在模$P$中被分成$P$個不同的餘數，即$0$、…、$P-1$或$1$、$2$、…、$P$，而此$P$個餘數所產生的集合稱為模$P$之完全剩餘集（Complete Set Of Residues），以符號Z_P表示[2]，即定義出F_P的範圍。由於並不是所有的橢圓曲線都適合加密，型如：$y^2=x^3+ax+b$正好是一種可用來加解密的橢圓曲線，也是最為簡單的一類[4]。下面就把$y^2=x^3+ax+b$這條曲線定義在F_P上：試選擇兩個滿足下列條件的（小於P，P為質數）的非負整數a、b且$4a^3+27b^2\neq 0 \pmod P$），則滿足下列方程式的所有點(x,y)，再加上無窮遠點$O\infty$，即構成一條橢圓曲線。即$y^2=x^3+ax+b \pmod P$）其中x，y屬於0到$P-1$間的整數，並將這條橢圓曲線記為$E_P(a,b)$。

定義 3：F_P的模數及同餘運算法則

法則 1：F_P中只有P（P為質數）個元素，即0、1、2、…、$P-1$。

法則 2：F_P的加法，若$(a+b) \bmod P=[(a \bmod P)+(b \bmod P)] \bmod P$。

法則 3：F_P的減法，若$(a-b) \bmod P=[(a \bmod P)-(b \bmod P)] \bmod P$。

法則 4：F_P的乘法，若$(a\cdot b) \bmod P=[(a \bmod P)\times(b \bmod P)] \bmod P$。

法則 5：F_P的除法，若$(a\div b) \bmod P=[(a \bmod P)\times(\frac{1}{b} \bmod P)] \bmod P$。

例 4-3：設求 $y^2 = x^3 + x + 1$（mod 23）或 $R_{23}(x^3 + x + 1)$，即求 $y^2 = x^3 + x + 1$ 在 F_{23} 的圖像？ 解：因為 $4(1)^3 + 27(1)^2 \neq 0$，故 $y^2 = x^3 + x + 1$ 為可用來加密之橢圓曲線。因此可得 $y^2 \bmod 23 = x^3 + x + 1 \bmod 23$，故 y 軸用 0 至 23 代入、x 軸用 0 至 23 代入，若能滿足 $y^2 \bmod 23 = x^3 + x + 1 \bmod 23$ 則可將該點座標標示於平面直角座標上，而且圖形明顯對稱於 $y = \frac{p}{2} = \frac{23}{2}$，如圖 10。由本例可知在 F_{23} 的橢圓曲線已經變成離散的點，因此可知橢圓曲線在不同的體中有不同的型態，其運算法則仍和實數域上同[4]。

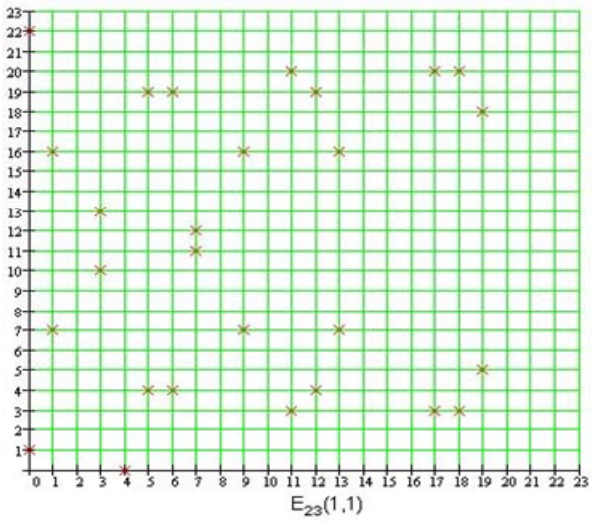


圖 10

定義 4：離散橢圓曲線運算法則

一、無窮遠點 $O\infty$ 是零元，有 $O\infty + O\infty = O\infty$， $O\infty + P = P$。

二、$P(x, y)$ 的負元是 $-P(x, -y)$，有 $P + (-P) = O\infty$。

三、$P(x_1, y_1)$，$Q(x_2, y_2)$ 的和 $R(x_3, y_3)$ 有如下關係：

$$x_3 \equiv m^2 - x_1 - x_2 \text{（mod } P\text{）} \Leftrightarrow R_P(m^2 - x_1 - x_2)$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \text{（mod } P\text{）} \Leftrightarrow R_P(m(x_1 - x_3) - y_1)$$

其中

若 $P = Q$ 則 $m = \frac{(3x^2 + a)}{2y_1}$

若 $P \neq Q$ 則 $m = \frac{(y_2 - y_1)}{(x_2 - x_1)}$

最後，講一下橢圓曲線上的點的階。如果橢圓曲線上一點 P，存在最小的正整數 n，使得 G 點乘積 $nP = O\infty(0,1,0)$，則將 n 稱為 P 的**階**，若 n 不存在，我們說 P 是無限階的。事實上，在有限體上定義的橢圓曲線上所有的點的階 n 都是存在的[4]。

伍、研究結果

橢圓曲線上的加密解密方法：橢圓曲線加密法是基於一個數學上的難題，即在有限體橢圓曲線上的加法逆運算的不易[4][5]。考慮下式：$K=kG$[其中K，G為$E_P(a,b)$上的點，k為小於n（n是點G的階）的整數]因此不難發現，給定k和G，根據加法法則，計算K很容易；但給定K和G，求k就相對困難了。這就是橢圓曲線加密演算法所採用的難題[4][7]。點G稱為基點（base point），k（$k<n$，n為基點G的階）稱為私有密鑰（Privte Key），K稱為公開密鑰（Public Key）。現在我們描述一個利用橢圓曲線進行加密通信的過程：

密文傳送演算法分析：

步驟1：用戶A及用戶B先定義出明文編碼$M(x_i,y_i)$，$0<i\le n$，$i\in N$。

步驟2：用戶A初始化橢圓曲線$E_P(a,b)$，即$R_P(y^2)=R_P(x^3+ax+b)$，並任取一$G(x_G,y_G)$點作為基點。

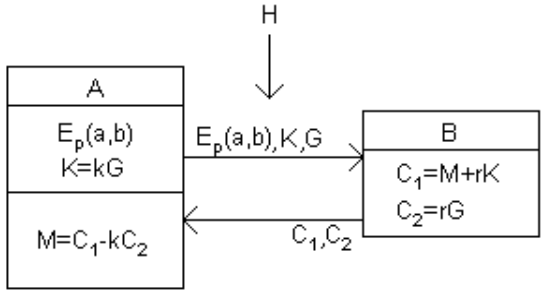
步驟3：用戶A算出公開金鑰$K=k\cdot G$、$0<k\le n, k\in N$（即$K(x_K,y_K)$點），n為橢圓曲線$E_P(a,b)$的G點個數。

步驟4：用戶A傳送公開金鑰$E_P(a,b)$、K及G給用戶B

步驟5：用戶B計算$C_1=M+r\cdot K$及$C_2=r\cdot G$並隨機取一自然數r，$0<r\le n$。

步驟6：用戶B回傳私密金鑰C_1及C_2給用戶A計算C_1-kC_2得出明文M。

因為$C_1-kC_2=M+rK-k(rG)=M+rK-r(kG)=M$。再對點$M$進行解碼就可以得到明文。在這個加密通信中，如果有一個偷窺者H，他只能看到$E_P(a,b)$、K、G、C_1、C_2而通過K、G求k或通過C_2、G求r都是相對困難的。因此H無法得到A、B間傳送的明文資訊，如流程圖1。



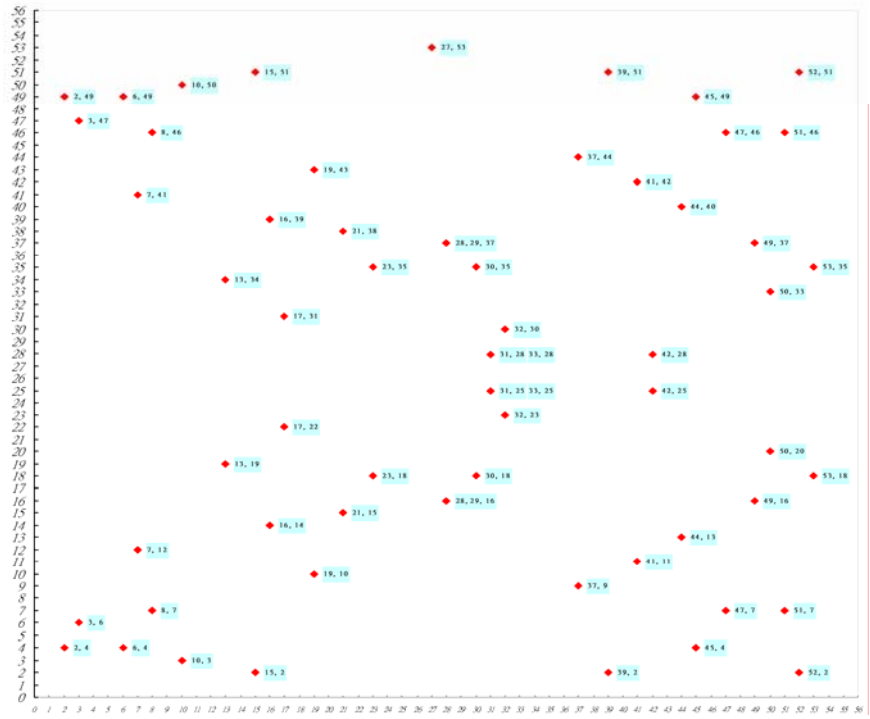
流程圖1

實驗方法：本實驗中的 ECC 公開密鑰密碼法將利用 EXCEL 軟體來模擬 $E_{53}(1,6)$（即 $R_{53}(y^2)=R_{53}(x^3+x+6)$）這條橢圓曲線，並且用來加密馬致遠的元曲「天淨沙」來作為我們的實驗結果，因此橢圓曲線為滿足 $y^2 \bmod 53 = x^3+x+6 \bmod 53$，由 EXCEL 軟體模擬出來下列的結果如 G 點對照表中的數值。在 G 點對照表中的 x_G 及 y_G 為滿足有限域 $P=53$ 的 G（基點）x 及 y 的座標數值，圖形如下。

G 點對照表

$n\cdot G$	x_G	y_G	$n\cdot G$	x_G	y_G	$n\cdot G$	x_G	y_G	$n\cdot G$	x_G	y_G	$n\cdot G$	x_G	y_G
1G	2	4	14G	13	34	27G	27	53	40G	37	9	56G	50	20
2G	2	49	15G	15	2	28G	28	16	41G	37	44	57G	50	33
3G	3	6	16G	15	51	29G	28	37	42G	39	2	58G	51	7
4G	3	47	17G	16	14	30G	29	16	43G	39	51	59G	51	46
5G	6	4	18G	16	39	31G	29	37	44G	41	11	60G	52	2
6G	6	49	19G	17	22	32G	30	18	45G	41	42	61G	52	51
7G	7	12	20G	17	31	33G	30	35	46G	42	25	62G	53	18
8G	7	41	21G	19	10	34G	31	25	47G	42	28	63G	53	35
9G	8	7	22G	19	43	35G	31	28	48G	44	13			
10G	8	46	23G	21	15	36G	32	23	52G	47	7			
11G	10	3	24G	21	38	37G	32	30	53G	47	46			
12G	10	50	25G	23	18	38G	33	25	54G	49	16			
13G	13	19	26G	23	35	39G	33	28	55G	49	37			

$E_{53}(1,6)$



加密程序：若 $P(x_1, y_1)$ ，$Q(x_2, y_2)$ 且 $P \neq -Q$ 時，則若 $P+Q=(x_3, y_3)$ ，

$$\begin{cases} x_3 = m^2 - x_1 - x_2 \bmod P \\ y_3 = m(x_1 - x_3) - y_1 \bmod P \end{cases}$$ ，$$m = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} \bmod p, (P = Q) \\ \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p, (P \neq Q) \end{cases}$$ ，nG 運算性質如下：

$1G = G$ ，$2G = G + G$ ，$3G = 2G + G$ ，…，$(n-1)G = (n-2)G + G$ ，$nG = O(0,0)$ ，$(n+1)G = G$ ，n 為階（G 點的個數）。加密之前須把明文對應到 G 點，做一對一的對應。在本實驗中一個 $P = 53$ 的 ECC 可以對應出 63 個明文，因此足夠我們進行中文注音的加解密編碼使用其明文對照表如下：

明文密碼對照表

G明文編碼	X	Y	明文	G明文編碼	X	Y	明文	G明文編碼	X	Y	明文	G明文編碼	X	Y	明文
1G	2	4	ㄅ	17G	16	14	ㄕ	33G	30	35	ㄢ	49G	44	40	
2G	2	49	ㄆ	18G	16	39	ㄖ	34G	31	25	ㄣ	50G	45	4	
3G	3	6	ㄇ	19G	17	22	ㄗ	35G	31	28	ㄤ	51G	45	49	
4G	3	47	ㄈ	20G	17	31	ㄘ	36G	32	23	ㄥ	52G	47	7	
5G	6	4	ㄉ	21G	19	10	ㄙ	37G	32	30	一聲	53G	47	46	
6G	6	49	ㄊ	22G	19	43	ㄧ	38G	33	25	二聲	54G	49	16	
7G	7	12	ㄋ	23G	21	15	ㄨ	39G	33	28	三聲	55G	49	37	
8G	7	41	ㄌ	24G	21	38	ㄩ	40G	37	9	四聲	56G	50	20	
9G	8	7	ㄍ	25G	23	18	ㄚ	41G	37	44	輕聲	57G	50	33	
10G	8	46	ㄎ	26G	23	35	ㄛ	42G	39	2	，	58G	51	7	
11G	10	3	ㄏ	27G	27	53	ㄜ	43G	39	51	。	59G	51	46	
12G	10	50	ㄐ	28G	28	16	ㄝ	44G	41	11	！	60G	52	2	
13G	13	19	ㄑ	29G	28	37	ㄞ	45G	41	42	？	61G	52	51	
14G	13	34	ㄒ	30G	29	16	ㄟ	46G	42	25	、	62G	53	18	
15G	15	2	ㄓ	31G	29	37	ㄠ	47G	42	28	；	63G	53	35	
16G	15	51	ㄔ	32G	30	18	ㄡ	48G	44	13	：				

在明文對照表中，我們利用每一個 G 點對應出一個注音或標點符號以進行加密前的編碼工作，以下將進行橢圓曲線的加解密計算工作。

計算示例：若 $P=53$，$a=1$，$b=6$，起始 G 點(19，43)，私密金鑰 k 為 7，若隨機數 $r=14$，求算公開金鑰 $K=k\cdot G$，C_1，C_2 及 M 之值？

詳解：如下表

Ep(a, b)	$E_{53}(1,6)$		
起始 G 點	(19，43)		
私密金鑰 k	7	（$0<k<n$，$k\in Z$）	
公開金鑰 $K=k\cdot G$	$7\times(19,43)=1\times(19,43)+6\times(19,43)=(19,43)+(28,16)=(15,51)$		
	明文ㄅ爲 $1\cdot G$（2, 4）	指定明文ㄅ為 ECC 圖上的 G 點(2, 4)座標	
	隨機數 $r=14$	（$0<r\leq n$，$r\in Z$）	
C_1	$M+r\cdot K$	（2, 4）+ 14x(15, 51)	(31, 28)
C_2	$r\times G$	$14\times(19,43)$	(17, 22)
$C_1-k\cdot C_2$	$(M+r\cdot K)-k\cdot(r\cdot G)$	$(M+r\cdot K\cdot G)+(-k\cdot r\cdot G)$	M (2, 4)

陸、討論

明文：天淨沙						
枯	藤	老	樹	昏	鴉	，
小	橋	流	水	人	家	，
古	道	西	風	瘦	馬	。
夕	陽	西	下	，		
斷	腸	人	在	天	涯	。

表 1

實驗探討：我們將用一完整的範例來說明中文 ECC 加解密之應用模式，並採用上列密碼表來加密明文「天淨沙」表 1 並將其分析如表 2，由此表可知明文（含空白）可分成 35 個單字且每個單位的長度皆不同。因此我們必須對每一個單字中的明文進行加解密運算。

明文：注音對照表						
ㄎㄨ　一聲	ㄊㄥˊ	ㄌㄠˇ	ㄕㄨˋ	ㄏㄨㄣ一聲	ㄧㄚ　一聲	，
ㄒㄧㄠˇ	ㄑㄧㄠˊ	ㄌㄧㄡˊ	ㄕㄨㄟˇ	ㄖㄣˊ	ㄐㄧㄚ一聲	，
ㄍㄨˇ	ㄉㄠˋ	ㄒㄧ　一聲	ㄈㄥ　一聲	ㄕㄡˋ	ㄇㄚˇ	。
ㄒㄧㄚˋ	ㄧㄤˊ	ㄒㄧ　一聲	ㄒㄧㄚˋ	，		
ㄉㄨㄢˋ	ㄔㄤˊ	ㄖㄣˊ	ㄗㄞˋ	ㄊㄧㄢ一聲	ㄧㄚˊ	。

表 2

利用明文對照表可為 35 個單字求出對應的 G 點，如表 3

對應 G 點						
10 23 37	06 36 38	08 31 39	17 23 40	11 23 34 37	22 25 37	42
14 22 31 39	13 22 31 38	08 22 32 38	17 23 30 37	18 34 38	12 22 25 37	42
09 23 39	05 31 38	14 22 37	04 36 37	17 32 40	03 25 37	43
14 22 40	22 35 38	14 22 37	14 22 25 40	42		
05 23 33 40	16 35 38	18 34 38	19 29 40	06 22 33 37	22 25 38	43

表 3

我們設定用戶 A 利用參數 $k=7$，$r=14$，$G(19,43)$，$E_{53}(1,6)$，來進行資訊編碼並傳送出 $E_{53}(1,6)$，$G(19,43)$，$K(15,51)$ 三筆參數給用戶 B 進行加密編碼。而用戶 B 將要

傳送的資訊利用 A 所提供的參數編碼來加密得出 C_1（表 4）及 $C_2(17,22)$再回傳給 A 計算 $C_1 - kC_2$，最後求出點 M 。

對應出 C_1 點						
09 19 53	27 16 34	06 62 46	20 19 26	01 19 (0,0) 53	44 41 53	33
15 44 62 46	54 44 62 34	06 44 43 34	20 19 31 53	61 (0,0) 34	32 58 51	33
57 19 46	07 62 34	15 44 53	48 16 53	20 43 26	28 41 53	08
15 44 26	44 35 34	15 44 53	15 44 41 26	33		
07 19 45 26	13 35 34	61 (0,0) 34	18 04 26	63 44 45 53	44 41 34	08

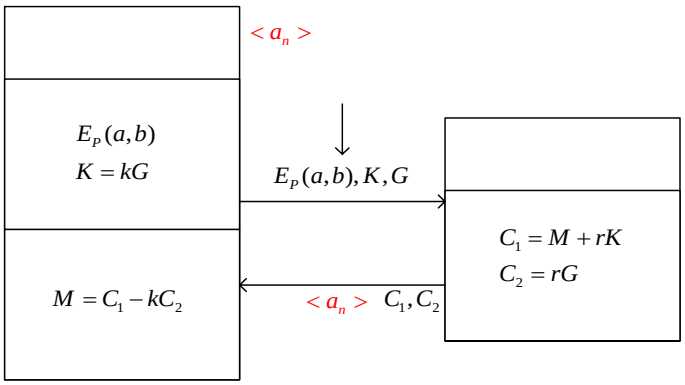
表 4

未來展望：在本實驗中雖然有留下 13 個空白 G 點未加以編碼，但就密碼本身而論空白愈多攻方要破解機會就愈小，因且在進行明文編碼時我們也可採用混合數列的方式，來進行明文編碼。

混合數列明文密碼表										
G明文編碼	X	Y	明文	G明文編碼	X	Y	明文	G明文編碼	X	Y	明文
1G	2	4	ㄅ	22G	19	43	空白 1	43G	39	51	空白 7
2G	2	49	空白 1	23G	21	15	空白 2	44G	41	11	空白 8
3G	3	6	ㄆ	24G	21	38	空白 3	45G	41	42	ㄍ
4G	3	47	空白 1	25G	23	18	空白 4	46G	42	25	空白 1
5G	6	4	空白 2	26G	23	35	空白 5	47G	42	28	空白 2
6G	6	49	ㄇ	27G	27	53	空白 6	48G	44	13	空白 3
7G	7	12	空白 1	28G	28	16	ㄋ	49G	44	40	空白 4
8G	7	41	空白 2	29G	28	37	空白 1	50G	45	4	空白 5
9G	8	7	空白 3	30G	29	16	空白 2	51G	45	49	空白 6
10G	8	46	ㄈ	31G	29	37	空白 3	52G	47	7	空白 7
11G	10	3	空白 1	32G	30	18	空白 4	53G	47	46	空白 8
12G	10	50	空白 2	33G	30	35	空白 5	54G	49	16	空白 9
13G	13	19	空白 3	34G	31	25	空白 6	55G	49	37	ㄎ
14G	13	34	空白 4	35G	31	28	空白 7	56G	50	20	
15G	15	2	ㄉ	36G	32	23	ㄌ	57G	50	33	
16G	15	51	空白 1	37G	32	30	空白 1	58G	51	7	
17G	16	14	空白 2	38G	33	25	空白 2	59G	51	46	
18G	16	39	空白 3	39G	33	28	空白 3	60G	52	2	
19G	17	22	空白 4	40G	37	9	空白 4	61G	52	51	
20G	17	31	空白 5	41G	37	44	空白 5	62G	53	18	
21G	19	10	ㄊ	42G	39	2	空白 6	63G	53	35	

表 5

例如：表 5 所示，即在每一個明文之間先留下一個事先約定好的間隔（公差 $d=1$），而 A、B 兩方在傳送金鑰時，如果再加上間隔參數將可更有效地維護資訊安全，但是它須要依賴快速的電腦來，才能效率地完成，因此所要的 G 點個數勢必增多，產生費時間的缺點，但如果找出一合適的混合數列，則可以加強密碼本身的安全及效率，如流程圖 2。



流程圖 2

A

柒、結論

在上一節我們知道橢圓曲線雖然具有高度的安全性，但是如果可以配合一些混合數列的方法相信必定可以再強化其安全性，在流程圖 2 中我們利用不同的數列方法將原來的傳送方式加以修改，並增加一組參數$<a_n>$來增加密鑰的個數希望藉由不同的組合造成不同明文排列以提昇橢圓曲線的安全性，因此我們將此點做為我們下個階段努力的具體目標，希望利用電腦模擬出一套理想的混合數列的問題，並找出如何在有限G點內組合出較複雜的數列方法，以做為我們產生的一把新的金鑰。

橢圓曲線的相關論述及參考資料目前在台灣好像不多，因此我們這一組在找相關資料時經常找不到可以參考的資料，還好目前網路發達可以協助我們尋找一些相關的資訊，但是卻找到一堆大陸簡體字及英文的參考文章，在組員的分工合作之下，我們終於將一疊有著各種文字的參考資料整理出這套比較有系統的研究報告，並且也提昇了我們幾個人對於英文資料的閱讀能力。

在此次的研究中，除了感謝學校老師的指導之外，我們也對數學的應用有著更多的認識，而且對於有關高一上數學中關於數論的同餘數計算應用也有更深刻的體會，且說明書所提的偏微分求斜率以及幾何學所提的橢圓曲線及射影平面也有一些基本的認識。

相較於本次的實驗內容，覺得自己以前國中所做的科展真是小巫見大巫，且同學彼此也對自己的專題製作能力有明顯的提昇而感到興奮，加上此次電腦模擬的經驗，更提昇了我們自己在使用電腦解決問題的能力，希望將來我們能有更好的成果貢獻出來，並且可以解決更多的數學或工程問題，例如：開發出更好的演算法等來提昇密碼的安全性等…。

捌、參考資料及其他

[1]賽門辛 Simon Singh 著，劉燕芬譯，碼書，台灣商務印書館，2000。

[2]賴溪松、韓亮、張真誠，近代密碼學及其應用，松崗，1995。

[3]黃葳理、賴宜璟、許庭瑋、趙傳真，簡單函數在密碼學之應用-三重加密法，中華民國第四十三屆中小學科展優等，2003。

[4] 張利海，ECC 加密演算法入門介紹，2005，取自，http://blog.csdn.net/mfkplus/archive/2005/01/02/237748.aspx［簡體］。

[5]吳明璋、黃珮瑩、溫志宏、陳澤雄，植基於橢圓曲線密碼系統之存取控制，第十三屆國際資訊管理學術研討會，2002。

[6]李虎雄、陳昭地、黃登源、李政貴、林礽堂、儲啟政，康熙圖書高中數學第一冊第二章，康熙圖書網路股份有限公司，2005。

[7]業餘數學天地-科普園地-橢圓曲線密碼學，取自，http://jamesjoe.51.net/refrence/ellipse.html[簡體]。

[8] 王九逵，射影平面六講，中央大學數學系「中學教師暑期數學研習營」講義，1999。

[9]吉林大學數學學院，射影解析幾何初步，幾何與代數網路版第九章，取自，http://math.jlu.edu.cn/jiaowu/doc/CAI/geometry&algebra/Chapters/Chapter11/Sec11_1/Sec11_1.html［簡體］。

[10]Certicom Securing Innovation，from，http://www.certicom.com/ index.php?action=ecc_tutorial[英文]。

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

佳作

040419

應用橢圓曲線在中文加解密之使用探討

國立馬祖高級中學

評語：

1. 橢圓曲線乃屬於研究所的課題，使有的方法超過中學生所能理解、消化。
2. 本作品包含若干目前熱門的數學方法。