Delgado L.; Vallejo R.; Mutis W. & Castillo J. 2009. La Estructura de Grupo de las Curvas Elípticas. Revista Sigma, 9 (1). Pág. 20-37
http://coes.udenar.edu.co/revistasigma/articulos/articulosIX1/3.pdf

REVISTA SIGMA
Departamento de Matemáticas y Estadística
Universidad de Nariño
Volumen IX (2009), páginas 20–37

La Estructura de Grupo de las Curvas Elípticas

Luis Miguel Delgado Ordoñez[1]
Ricardo Antonio Vallejo Villarreal[2]
Wilson Fernando Mutis Cantero[3]
John Hermes Castillo Gómez[4]

Universidad de Nariño

Abstract. In the early part of this article presents an introduction to the study of elliptic curves defined over a field K and some characteristics of these curves depend on the field which have been defined and subsequently shown that it is possible to define an operation binary between the points of an elliptic curve to give abeliano group structure. In the apendix we presents the algorithms developed in this work, implemented in the computer system algebra MuPAD.

Keywords. Finite Fields, Elliptic Curves, Point to Infinity, Discriminant, Invariant.

Resumen. En la parte inicial de este artículo se presenta una introducción al estudio de las curvas elípticas definidas sobre un campo K y algunas características de dichas curvas que dependen del campo sobre el cual se han definido; posteriormente se muestra que es posible definir una operación binaria entre los puntos de una curva elíptica proporcionándole a ésta estructura de grupo abeliano. En el apéndice se presentan algoritmos desarrollados en este trabajo, implementados en el sistema de álgebra computacional MuPAD.

Palabras Clave. Campo Finito, Curva Elíptica, Punto al Infinito, Discriminante, Invariante.

Introducción

La teoría de curvas elípticas no es nueva, hace mucho tiempo que ha sido abordada desde la teoría de números y la geometría algebraica, sin embargo su estudio a tenido un mayor auge en los últimos tiempos debido al uso que éstas tuvieron en la demostración del último teorema de Fermat y por su aplicación en la criptografía.

[1]Estudiante de Licenciatura en Matemáticas de la Universidad de Nariño, Pasto - Nariño - Colombia.
[2]Estudiante de Licenciatura en Matemáticas de la Universidad de Nariño, Pasto - Nariño - Colombia.
[3]Docente Tiempo Completo de la Universidad de Nariño, Pasto - Nariño - Colombia.
[4]Docente Tiempo Completo de la Universidad de Nariño, Pasto - Nariño - Colombia.

Dada una curva elíptica E sobre un campo finito $\mathbb{F}_q$ es posible definir un grupo abeliano finito $E(\mathbb{F}_q)$ el cual es estructuralmente rico en propiedades algebraicas que permiten elaborar algoritmos computacionales eficientes.

A pesar que las curvas elípticas se pueden definir sobre cualquier campo, las que ofrecen mayores beneficios computacionales son las que se construyen sobre un campo finito, debido a que se puede simplificar la ecuación general[5] que define las curvas elípticas, cuando la característica del campo es diferente de cero, y esto facilita el trabajo que se haga con estas curvas.

La estructura de grupo $E(\mathbb{F}_q)$ en una curva elíptica es la que permite las aplicaciones computacionales, como por ejemplo la elaboración de criptosistemas eficientes; en el grupo $E(\mathbb{F}_q)$ el elemento neutro se denomina "punto al infinito" y se denota con $\boldsymbol{O}$, en general, no es fácil visualizar este elemento motivo por el cual se hace una presentación analítica del mismo.

1 Curva Elíptica

A menos que se indique lo contrario, K es un campo cualquiera y $\bar{K}$ su cerradura algebraica.

Definición 1.1 (**Curva Elíptica**). *Sean K un campo y $a_1, a_2, a_3, a_4, a_6 \in K$. Una curva elíptica construida sobre K, denotada con $E(K)$, es el conjunto de puntos $(x, y) \in K \times K$ que cumplen la ecuación*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

junto con un elemento $\boldsymbol{O}$ que se denomina punto al infinito. Es decir,

$$E(K) = \{(x, y) \in K \times K \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\boldsymbol{O}\}.$$

A continuación se estudia la definición del punto al infinito, y se mostrará que éste pertenece a toda curva elíptica.

1.1 El Punto al Infinito

En el estudio de las curvas elípticas, el punto al infinito $\boldsymbol{O}$ es difícil de visualizar, existen varias formas de presentarlo; a continuación se expone una de ellas.

Sea $A = \mathbb{R}^3 - \{(0, 0, 0)\}$, se dice que dos puntos (X, Y, Z) y (X', Y', Z') en A están relacionados, si existe un escalar $\lambda \neq 0$ tal que $(X, Y, Z) = \lambda(X', Y', Z')$. Para denotar que los puntos (X, Y, Z) y (X', Y', Z') en A están relacionados, se escribe $(X, Y, Z) \sim (X', Y', Z')$. Se puede probar que la relación definida anteriormente es una relación de equivalencia en A, y para cada $(X, Y, Z) \in A$ su clase de equivalencia $[(X, Y, Z)]$ se denomina *punto proyectivo* y esta dada por

$$\begin{aligned}
[(X, Y, Z)] &= \{(X', Y', Z') \in A : (X, Y, Z) \sim (X', Y', Z')\} \\
&= \{(X', Y', Z') \in A : (X, Y, Z) = \lambda(X', Y', Z') \text{ para algún } \lambda \in \mathbb{R} - \{0\}\} \\
&= \left\{(X', Y', Z') \in A : (X', Y', Z') = \frac{1}{\lambda}(X, Y, Z) \text{ para algún } \lambda \in \mathbb{R} - \{0\}\right\}
\end{aligned}$$

El plano proyectivo se define como el conjunto de las clases de equivalencia:

$$P = \{[(X, Y, Z)] \ : \ (X, Y, Z) \in A\}.$$

[5] A esta ecuación se la denomina Ecuación de Weierstrass.

Este plano proyectivo se puede dividir en los conjuntos de clases de equivalencia en las cuales $Z = 0$ y $Z \neq 0$.

Sea $[(X, Y, Z)]$ un punto proyectivo. Cuando Z es diferente de cero,

$$\begin{aligned}(X, Y, Z) &= Z\left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) \\ &= Z(x, y, 1)\end{aligned}$$

donde $x = \dfrac{X}{Z}$ e $y = \dfrac{Y}{Z}$.

Así, $(X, Y, Z) \sim (x, y, 1)$ por lo tanto $(x, y, 1) \in [(X, Y, Z)]$, así el plano proyectivo puede ser visualizado como los puntos (x, y) sobre $\mathbb{R}^2$, más los puntos para los cuales Z es igual a cero, éstos últimos puntos forman la *linea al infinito*.

Sea $F(x, y) = 0$ la ecuación implícita para y como una función de x en (1.1), es decir

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

entonces toda ecuación $F(x, y) = 0$ de una curva sobre $\mathbb{R}^2$ corresponde a una ecuación $\widetilde{F}(X, Y, Z) = 0$, que se encuentra al reemplazar x por X/Z, y por Y/Z y multiplicar por una potencia de Z para eliminar los denominadores, esta ecuación se satisface por los correspondientes puntos proyectivos. Tomando la ecuación (1.1), y aplicando el anterior procedimiento se encuentra su *ecuación proyectiva*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1.2}$$

Si ésta es satisfecha por un punto proyectivo $[(X, Y, Z)]$ con $Z \neq 0$, entonces el punto (x, y) debe satisfacer la ecuación (1.2), donde $x = X/Z$ e $y = Y/Z$. Ahora, tomando los puntos de la linea al infinito o mejor los puntos proyectivos con $Z = 0$ en la ecuación proyectiva, se tiene $0 = X^3$, es decir, $X = 0$. Pero el único punto proyectivo con $X = 0$ y $Z = 0$ es $[(0, 1, 0)]$, este es el punto $\boldsymbol{O}$, el cual es la intersección del eje y con la linea al infinito.

1.2 Discriminante e Invariante

Elementos que permiten conocer características de las curvas elípticas son el discriminante Δ y el invariante j, para la ecuación (1.1) se definen de la siguiente manera:

Definición 1.2 (**Discriminante**). *Sea $E(K)$ una curva elíptica, se denota su discriminante con Δ y se define como:*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

donde

$$\begin{aligned}b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.\end{aligned}$$

Ahora se define el invariante, haciendo la aclaración de que éste sólo se puede calcular si $\Delta \neq 0$.

Definición 1.3 (**Invariante**). *Sea $E(K)$ una curva elíptica, se denota su invariante con j y se define como:*

$$j = \frac{c_4^3}{-b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6} = \frac{c_4^3}{\Delta}$$

donde b_2, b_4, b_6, b_8 como arriba y

$$c_4 = b_2^2 - 24b_4.$$

1.3 Simplificación de la Ecuación General de una Curva Elíptica

El siguiente teorema presenta las posibles simplificaciones de la ecuación (1.1), las cuales dependen de la característica del campo sobre el cual se construya la curva elíptica.

Teorema 1.4 (**Simplificación de la Ecuación General de una Curva Elíptica**). *Sea $E(K)$ una curva elíptica definida por la ecuación* (1.1)*, entonces:*

1. *Si* $\operatorname{car} K$ *es diferente de* 2 *y* 3*, entonces la ecuación* (1.1) *se puede escribir como*

$$y^2 = x^3 + a_4 x + a_6 \tag{1.3}$$

   además $\Delta = -16(4a_4^3 + 27a_6^2)$, $j = 1728\left(\dfrac{4a_4^3}{4a_4^3 + 27a_6^2}\right)$ *y* $c_4 = -48a_4$.

2. *Si* $\operatorname{car} K = 3$*, entonces la ecuación* (1.1) *se puede escribir como*

$$y^2 = x^3 + a_2 x^2 + a_6 \tag{1.4}$$

   además $\Delta = -a_2^3 a_6$, $j = \dfrac{-a_2^3}{a_6}$ *y* $c_4 = a_2^2 \neq 0$.

3. *Si* $\operatorname{car} K = 3$*, entonces la ecuación* (1.1) *se puede escribir como*

$$y^2 = x^3 + a_4 x + a_6 \tag{1.5}$$

   además $\Delta = -a_4^3$, $j = 0$ *y* $c_4 = 0$.

4. *Si* $\operatorname{car} K = 2$*, entonces la ecuación* (1.1) *se puede escribir como*

$$y^2 + xy = x^3 + a_2 x^2 + a_6 \tag{1.6}$$

   además $\Delta = a_6$, $j = \dfrac{1}{a_6}$ *y* $c_4 = 1$.

5. *Si* $\operatorname{car} K = 2$*, entonces la ecuación* (1.1) *se puede escribir como*

$$y^2 + a_3 y = x^3 + a_4 x + a_6 \tag{1.7}$$

   además $\Delta = a_3^4$, $j = 0$ *y* $c_4 = 0$.

Para una demostración del Teorema 1.4, ver [4].

Definición 1.5 (**Curvas Isomorfas**). *Sean $E(K)$ y $E'(K)$ dos curvas elípticas, se dice que $E(K)$ y $E'(K)$ son isomorfas si y sólo si las dos pueden ser representadas por la misma ecuación.*

El Teorema 1.4 permite caracterizar las curvas isomorfas dependiendo de sus invariantes; este resultado se describe en el siguiente teorema:

Teorema 1.6 (**Curvas Isomorfas**). *Sean E y E' dos curvas elípticas sobre un campo $\bar{K}$, entonces $E(\bar{K})$ y $E'(\bar{K})$ son isomorfas si y sólo si tienen el mismo invariante.*

Demostración. Si se supone que $E(\bar{K})$ y $E'(\bar{K})$ son dos curvas isomorfas, entonces se puede mostrar que tienen el mismo invariante, ya que las dos pueden ser representadas por la misma ecuación.

Se supone ahora que $E(\bar{K})$ y $E'(\bar{K})$ son dos curvas con el mismo invariante, sea la car $\bar{K}$ diferente de 2 y 3. Entonces las curvas admiten ecuaciones de la forma (1.3), así:

$$E(\bar{K}):\ y^2 = x^3 + a_4x + a_6 \qquad\qquad E'(\bar{K}):\ y'^2 = x'^3 + a'_4x' + a'_6.$$

Dado que las curvas tienen el mismo invariante, se puede escribir la siguiente igualdad

$$\frac{4a_4^3}{4a_4^3 + 27a_6^2} = \frac{4{a'_4}^3}{4{a'_4}^3 + 27{a'_6}^2}.$$

Aquí se debe distinguir tres casos:

Si $a_4 = 0$ y $a_6 \neq 0$, entonces $a'_4 = 0$ y $a'_6 \neq 0$, porque $\Delta \neq 0$ (ver Definición 1.3). Se toma ahora $u \in \bar{K}$ tal que

$$u^6 = \frac{a_6}{a'_6}$$

y entonces el cambio $x = u^2x'$, $y = u^3y'$ transforma a la curva $E(\bar{K})$ en $E'(\bar{K})$.

Si $a_6 = 0$, entonces $a'_6 = 0$, $a_4 \neq 0$ y $a'_4 \neq 0$. Se toma ahora $u \in \bar{K}$ tal que

$$u^4 = \frac{a_4}{a'_4}$$

y de nuevo el cambio $x = u^2x'$, $y = u^3y'$ hace corresponder las curvas.

Si $a_4 \neq 0$ y $a_6 \neq 0$, entonces también $a'_4 \neq 0$ y $a'_6 \neq 0$. De la igualdad de los invariantes se sigue que $a_4^3{a'_6}^2 = {a'_4}^3a_6^2$ o, equivalentemente,

$$\left(\frac{a_4}{a'_4}\right)^3 = \left(\frac{a_6}{a'_6}\right)^2.$$

Ahora se toma $u \in \bar{K}$ tal que

$$u^4 = \frac{a_4}{a'_4},$$

de manera que

$$u^{12} = \left(\frac{a_6}{a'_6}\right)^2 \quad \text{y} \quad u^6 = \pm\frac{a_6}{a'_6},$$

si el signo es negativo se multiplica u por una raíz cuarta primitiva de la unidad, con lo cual u^4 sigue siendo el mismo y u^6 cambia de signo. En definitiva se tiene que

$$u^4 = \frac{a_4}{a_4'} \quad \text{y} \quad u^6 = \frac{a_6}{a_6'}.$$

El cambio $x = u^2x'$, $y = u^3y'$ transforma una curva en otra.

Ahora se supone que la car $\bar{K} = 3$ y que el invariante $j \neq 0$. Entonces las curvas admiten ecuaciones de la forma (1.4), así:

$$E(\bar{K}):\ y^2 = x^3 + a_2x^2 + a_6 \qquad E'(\bar{K}):\ y'^2 = x'^3 + a_2'x'^2 + a_6'.$$

Como se supone la igualdad del invariante, se puede escribir la siguiente

$$\frac{-a_2^3}{a_6} = \frac{-{a_2'}^3}{a_6'}.$$

Como $j \neq 0$, entonces $a_2 \neq 0$, $a_2' \neq 0$, $a_6 \neq 0$, $a_6' \neq 0$ y $a_2^3a_6' = {a_2'}^3a_6$. Se toma ahora $u \in \bar{K}$ tal que

$$u^2 = \frac{a_2}{a_2'}.$$

El cambio $x = u^2x'$, $y = u^3y'$ transforma a la curva $E(\bar{K})$ en $E'(\bar{K})$.

En este caso se supone que la car $\bar{K} = 3$ y $j = 0$, Entonces las curvas admiten ecuaciones de la forma (1.5), así:

$$E(\bar{K}):\ y^2 = x^3 + a_4x + a_6 \qquad E'(\bar{K}):\ y'^2 = x'^3 + a_4'x' + a_6'$$

con $a_4 \neq 0$ y $a_4' \neq 0$. Esta vez se considera un cambio de coordenadas de la forma $x = u^2x' + r$, $y = u^3y'$. Basta tomar $u \in \bar{K}$ y r de modo que

$$u^4 = \frac{a_4'}{a_4}, \qquad r^3 + a_4r + a_6 - u^6a_6' = 0.$$

Así se transforma a la curva $E(\bar{K})$ en $E'(\bar{K})$.

Sea ahora la car $\bar{K} = 2$ y $j \neq 0$. Entonces las curvas admiten ecuaciones de la forma (1.6), así:

$$E(\bar{K}):\ y^2 + xy = x^3 + a_2x^2 + a_6 \qquad E'(\bar{K}):\ y'^2 + x'y' = x'^3 + a_2'x'^2 + a_6'.$$

Como se supone que las curvas tienen el mismo invariante, se puede escribir la siguiente igualdad

$$\frac{1}{a_6} = \frac{1}{a_6'}.$$

Como $j \neq 0$, entonces $a_6 = a_6'$ y $a_6 \neq 0$. Se considera el cambio $x = x'$, $y = y' + sx'$, donde s es una raíz de la ecuación $s^2+s+a_2+a_2' = 0$. Así se transforma a la curva $E(\bar{K})$ en $E'(\bar{K})$.

Finalmente, sea la car $\bar{K} = 2$ y $j = 0$, entonces las curvas admiten ecuaciones de la forma (1.7), así:

$$E(\bar{K}):\ y^2 + a_3y = x^3 + a_4x + a_6 \qquad E'(\bar{K}):\ y'^2 + a_3'y' = x'^3 + a_4'x' + a_6'$$

con $a_3 \neq 0$ y $a'_3 \neq 0$. Se considera el cambio $x = u^2x' + s^2$, $y = u^3y' + u^2sx' + t$, de modo que

$$u^3 = \frac{a_3}{a'_3}, \qquad s^4 + a_3s + a_4 - u^4a'_4 = 0 \quad \text{y} \quad t^2 + a_3t + s^6 + a_4s^2 + a_6 - u^6a'_6 = 0.$$

Así, se transforma la curva $E(\bar{K})$ en $E'(\bar{K})$. □

Si las ecuaciones (1.3), (1.4) y (1.5), obtenidas en el Teorema 1.4, se igualan a cero o mejor, si $F(x, y) = 0$ es una ecuación implícita de y como una función de x, se obtienen respectivamente $F_1(x, y) = y^2 - x^3 - a_4x - a_6$, $F_2(x, y) = y^2 - x^3 - a_2x^2 - a_6$ y $F_3(x, y) = y^2 - x^3 - a_4x - a_6$. En las primeras ecuaciones se pueden presentar raíces múltiples, ya que tienen en el termino de la izquierda y^2. Pero se puede demostrar que ecuaciones de la forma (1.3), (1.4) o (1.5) no tienen raíces múltiples, si y sólo si

$$\frac{\partial F}{\partial x}(x, y) \neq 0 \quad \text{o} \quad \frac{\partial F}{\partial y}(x, y) \neq 0 \quad \text{o si} \quad \Delta \neq 0$$

para todo $(x, y) \in E(K)$ donde $E(K)$ es una curva elíptica definida por ecuaciones de la forma (1.3), (1.4) o (1.5). Las ecuaciones con ésta característica se las denomina no singulares o curvas suaves. Este resultado lo podemos encontrar en [2].

2 Estructura de Grupo de una Curva Elíptica

Para conocer explícitamente las formulas que definen la suma de dos elementos de una curva elíptica $E(K)$, se trabaja con la ecuación (1.1).

La suma de dos puntos de una curva elíptica, se regirá según la siguiente definición:

Definición 2.1 (**Suma de Puntos de** $E(K)$)**.** *Sea $E(K)$ una curva elíptica determinada por una ecuación de la forma* (1.1) *y sean P, $Q \in E(K)$. Se denomina R al tercer punto donde la recta que pasa por P y Q corta a $E(K)$, entonces $P + Q$ es el punto donde la recta que pasa por R y $\boldsymbol{O}$ corta a $E(K)$.*

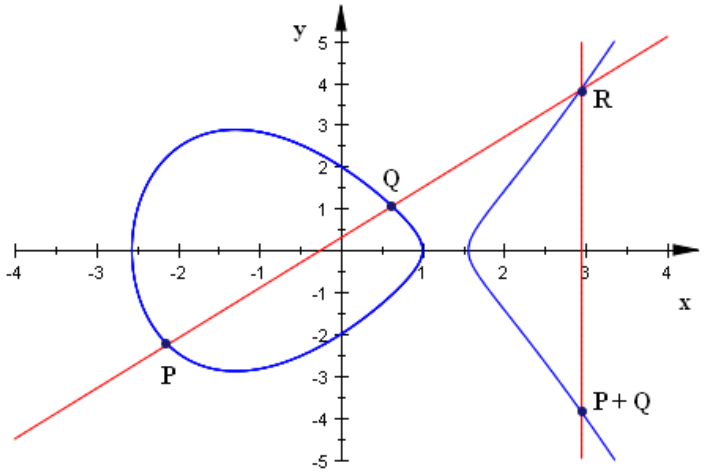
La anterior definición se puede visualizar en la Gráfica 1, donde $E(\mathbb{R}) : \ y^2 = x^3 - 5x + 4$.

Es importante aclarar con relación a lo anterior, que se puede demostrar que la recta secante que pasa por dos puntos de una curva elíptica corta a ésta en exactamente otro punto, además este tercer punto también cumple la ecuación (1.1). Tales demostraciones se pueden encontrar en [1].

2.1 Inverso

Conociendo la operación que se puede definir entre los puntos de una curva elíptica, el paso siguiente, en el estudio de la estructura que éstos forman, es la definición del inverso de todo elemento que pertenezca a ésta. Antes de definir el inverso de un punto, es necesario aclarar que se tomará como resultado de toda adición de dos puntos inversos entre si, a $\boldsymbol{O}$.

Definición 2.2 (**Inverso de un Punto**)**.** *Sea $E(K)$ una curva elíptica, y sea $P = (x_0, y_0) \in E(K)$, se define la recta l que atraviesa los puntos P y $\boldsymbol{O}$, entonces, el inverso de P, se define como el tercer y último punto de intersección entre l y la curva $E(K)$, en otras palabras la recta l es la única paralela al eje y, que pasa por el punto P.*



Gráfica 1: Suma de Puntos de una Curva Elíptica.

Para encontrar las coordenadas del inverso de un punto, que pertenezca a una curva elíptica E, se debe trabajar con la recta l de la anterior definición, la cual tiene como ecuación general $x = x_0$.

Sea el punto $P = (x_0, y_0) \in E(K)$ y sea $-P = (x_0, y_0') \in E(K)$, el tercer punto donde la recta $x = x_0$ corta a $E(K)$ (los otros dos puntos son P y $\boldsymbol{O}$).

La abscisa del punto $-P$ se conoce a partir de la Definición 2.2.

Con la ecuación (1.1), se define $F(x, y) = 0$ la ecuación implícita de y, como una función de x.

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \tag{2.1}$$

Como los únicos dos puntos con abscisa x_0 que están en $E(K)$ son P y $-P$, los cuales tienen como ordenadas a y_0 y y_0'. Se puede factorizar (2.1), así $F(x_0, y) = c(y - y_0)(y - y_0')$. Comparando los coeficientes de y^2 al desarrollar (2.1) factorizada, se tiene a $c = 1$ y al resolver $c(y - y_0)(y - y_0')$ se encuentra que los coeficientes de y son $-y_0 - y_0'$ pero deben ser igual a los coeficientes de y en (1.1), así $-y_0 - y_0' = a_1x_0 + a_3$, despejando se tiene $y_0' = -y_0 - a_1x_0 - a_3$, finalmente se concluye que

$$-P = (x_0, -y_0 - a_1x_0 - a_3).$$

Sólo falta mostrar que $-P$ es también un punto de la curva elíptica, si se conoce que P lo es.

Sea $P = (x_0, y_0)$ un punto de la curva elíptica $E(K)$, entonces se conoce que P satisface la ecuación (1.1), por lo tanto se cumple

$$y_0^2 + a_1x_0y_0 + a_3y_0 = x_0^3 + a_2x^2 + a_4x_0^2 + a_6.$$

Anteriormente se encontró que

$$-P = (x_0, -y_0 - a_1x_0 - a_3) = (x_0, Z),$$

entonces se cumple

$$Z^2 + a_1x_0Z + a_3Z = x_0^3 + a_2x^2 + a_4x_0^2 + a_6.$$

Si se reemplaza el valor de Z, y se desarrolla toda la expresión algebraica, se encuentra que se cumple la siguiente igualdad

$$y_0^2 + a_1x_0y_0 + a_3y_0 = x_0^3 + a_2x^2 + a_4x_0^2 + a_6$$

ésta igualdad se cumple ya que $P \in E$, por lo tanto se puede asegurar que $-P \in E$.

2.2 Ecuaciones Para Sumar Elementos de $E(K)$

Ahora se consideran dos puntos $P_1, P_2 \in E(K)$, tales que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$. Si $x_1 = x_2$ y $y_1 = -y_2 - a_1x_2 - a_3$, entonces por definición del inverso, $P_1 + P_2 = \boldsymbol{O}$. Descartando este caso y considerando la recta que pasa por los puntos P_1 y P_2, como la recta tangente a $E(K)$ por P_1, si $P_1 = P_2$, se va a calcular $P_1 + P_1 = 2P_1$; ahora, sea la ecuación de esta recta

$$y = \lambda x + \mu \tag{2.2}$$

Sea P_3 el tercer punto donde esta recta corta a $E(K)$. Según la Definición 2.1, $-P_3 = P_1+P_2$, ahora para calcular las coordenadas de P_3, se reemplaza $y = \lambda x + \mu$ en (2.1),

$$F(x, \lambda x + \mu) = (\lambda x + \mu)^2 + a_1x(\lambda x + \mu) + a_3(\lambda x + \mu) - x^3 - a_2x^2 - a_4x - a_6.$$

Como los puntos P_1, P_2 y P_3, son los únicos que tienen como ordenada a $\lambda x+\mu$ y pertenecen a $E(K)$. La ecuación (2.1), se puede factorizar así,

$$F(x, \lambda x + \mu) = c(x - x_1)(x - x_2)(x - x_3).$$

Igualando los coeficientes de x^3 de las ecuaciones (1.1) y (2.1) factorizada, se obtiene $c = -1$, y con los coeficientes de x^2 en estas ecuaciones, se tiene $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$, así

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2.$$

Ahora, como λ es la derivada implícita en P_1 de la ecuación (1.1), se obtiene:

$$\begin{aligned}
\frac{d}{dx}(y^2 + a_1xy + a_3y) &= \frac{d}{dx}(x^3 + a_2x^2 + a_4x + a_6) \\
2yy' + a_1xy' + a_1y + a_3y' &= 3x^2 + 2a_2x + a_4 \\
y' &= \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3} \\
\lambda &= \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}
\end{aligned} \tag{2.3}$$

ahora se reemplaza P_1 en (2.3)

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Para encontrar μ se despeja de la ecuación (2.2) y se reemplaza λ junto con P_1 o P_2. Así:

$$\begin{aligned}
\mu &= -\lambda x_1 + y_1 \\
\mu &= y_1 - \frac{(3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)x_1}{2y_1 + a_1x_1 + a_3} \\
\mu &= \frac{(2y_1^2 + a_1x_1y_1 + a_3y_1) - (3x_1^3 + 2a_2x_1^2 + a_4x_1 - a_1x_1y_1)}{2y_1 + a_1x_1 + a_3} \\
\mu &= \frac{2(y_1^2 + a_1x_1y_1 + a_3y_1) - a_1x_1y_1 - a_3y_1 - (3x_1^3 + 2a_2x_1^2 + a_4x_1 - a_1x_1y_1)}{2y_1 + a_1x_1 + a_3}.
\end{aligned}$$

Ahora se reemplaza en la igualdad anterior $y_1^2 + a_1x_1y_1 + a_3y_1$ por $x_1^3 + a_2x_1^2 + a_4x_1 + a_6$, lo cual se cumple al ser P_1 un punto de la curva $E(K)$, o mejor al ser un punto que cumple la ecuación (1.1)

$$\mu = \frac{2(x_1^3 + a_2x_1^2 + a_4x_1 + a_6) - a_1x_1y_1 - a_3y_1 - (3x_1^3 + 2a_2x_1^2 + a_4x_1 - a_1x_1y_1)}{2y_1 + a_1x_1 + a_3}$$

se obtiene finalmente

$$\mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

El caso que resta es $x_1 \neq x_2$, entonces la pendiente de la recta dada por la ecuación (2.2), se encuentra mediante las coordenadas de los puntos P_1 y P_2 los cuales pertenecen tanto a la recta como a la curva elíptica.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Para encontrar a μ, se repite el procedimiento del caso anterior, de donde

$$\mu = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}.$$

Anteriormente se encontró

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

ahora sustituyendo en la ecuación de la recta queda que $y_3 = \lambda x_3 + \mu$. Con lo cual se obtiene a P_3, pero como lo que se necesita es las coordenadas de $-P_3$, por lo tanto se aplica las anteriores coordenadas encontradas para el inverso.

Sea $-P_3 = (x_3, y_3')$, entonces $y_3' = -y_3 - a_1x_3 - a_3$, pero $y_3 = \lambda x_3 + \mu$, al reemplazar $y_3' = -(\lambda x_3 + \mu) - a_1x_3 - a_3 = -(\lambda + a_1)x_3 - \mu - a_3$.

Entonces, las coordenadas de

$$P_1 + P_2 = -P_3 = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \mu - a_3).$$

3 El Grupo $E(K)$

En esta sección se va a mostrar un pequeño acercamiento a la demostración de que $E(K)$ junto con la operación de adición que se va a definir a continuación, tiene estructura de grupo.

El siguiente teorema, muestra como encontrar las coordenadas de un punto que es la suma dos puntos de una curva elíptica, este es el resultado de la teoría expuesta en la sección anterior.

Teorema 3.1 (**Algoritmo de la Suma**). *Sea $E(K)$ una curva elíptica definida por una ecuación de la forma* (1.1). *Entonces*

1. *Si $P_0 = (x_0, y_0) \in E(K)$ es un punto finito, $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.*

2. *Si* $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ *son puntos finitos de* $E(K)$ *tales que* $x_1 = x_2$ *y* $y_1 + y_2 + a_1x_2 + a_3 = 0$, *entonces* $P_1 + P_2 = \boldsymbol{O}$. *En caso contrario, sean*

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & si\ x_1 \neq x_2, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & si\ x_1 = x_2, \end{cases}$$

y

$$\mu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}, & si\ x_1 \neq x_2, \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & si\ x_1 = x_2. \end{cases}$$

Entonces, $P_3 = P_1 + P_2$ *viene dado por*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x - 1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3.$$

Esta es una operación binaria, ya que dados P, $Q \in E(K)$, la Definición 2.1 garantiza que el tercer punto R, es decir $P + Q = R$, está también en la curva elíptica.

La propiedad asociativa es la más difícil de probar, es decir, que $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Esta puede demostrarse de por lo menos tres maneras. La primera es geométricamente, reinterpretando la ley de grupo, transfiriendo el problema a una pregunta en la geometría plana. El segundo acercamiento es usar las formulas que definen la suma para reducir la asociatividad a verificar las identidades algebraicas especificas, esto es algo tedioso de hacer a mano pero puede hacerse usando una computadora. El tercer acercamiento es desarrollar una teoría general de "los divisores en las curvas algebraicas" y así reducir la asociatividad por fuera del grupo a un corolario.

El "punto al infinito" $\boldsymbol{O}$ es el elemento identidad del grupo y debe visualizarse intuitivamente como situado infinitamente lejos del eje y. Este es el tercer punto de intersección de toda linea vertical con la curva; es decir, tal linea corta a la curva elíptica en los puntos P, $-P$ y $\boldsymbol{O}$.

Si $P = (x_0, y_0)$ satisface la ecuación (1.1), entonces $-P = (x_0, -y_0 - a_1x_0 - a_3)$ también la satisface, y además $P + (-P) = -P + P = \boldsymbol{O}$, es decir, $-P$ es el inverso de P.

Finalmente, dados P, $Q \in E(K)$ se tiene $P + Q = Q + P$, ya que $(P + Q)$, $(Q + P) \in E(K)$, están definidos por la misma recta, así el grupo $E(K)$ es abeliano.

4 Curvas Elípticas Construidas Sobre Campos Finitos

De ahora en adelante se trabajara sólo con campos finitos, es decir K es una campo finito $\mathbb{F}_q$ con q elementos, $q = p^n$ y p es primo.

Definición 4.1 (Curva Elíptica Sobre $\mathbb{F}_q$). *Sea* $\mathbb{F}_q$ *un campo finito y sean* $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$. *Una curva elíptica construida sobre* $\mathbb{F}_q$, *es el conjunto de puntos* (x, y) *que cumplen la ecuación*

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 (\text{mód } q),$$

junto con el punto al infinito. Una curva elíptica sobre $\mathbb{F}_q$, se denota con $E(\mathbb{F}_q)$ es decir:

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 (\text{mód } q)\} \cup \{\boldsymbol{O}\}$$

donde $\boldsymbol{O}$ denota el punto al infinito.

Es muy importante conocer el número de puntos que están sobre una curva elíptica construida sobre un campo finito, para dar una idea de como encontrar dicho número se trabajara con la ecuación (1.3). El máximo número de puntos que pueden tener una curva elíptica sobre $\mathbb{F}_q$ es $2q + 1$; uno es el punto al infinito, y si (x, y) satisface (1.3) entonces el punto $(x, -y)$ también satisface dicha ecuación, y dado que hay a lo más q posibles valores para x entonces existen a los más $2q$ puntos de la forma $(x, y) \in E(\mathbb{F}_q)$.

Primero se trabaja con los campos finitos $\mathbb{F}_q$ para los cuales $q = p$, con p un número primo, que se denominan campo primo, el número de puntos de una curva es igual al número de soluciones de la ecuación $y^2 = x^3 + a_4x + a_6 = u$, para todos los posibles x que pertenecen a $\mathbb{F}_q$, entonces si u es un residuo cuadrático en $\mathbb{F}_p$, es también solución de la ecuación, así las soluciones $y \in \mathbb{F}_p$, de la ecuación $y^2 = u$, es igual a $1 + \chi(u)$, donde $\chi(x) = \left(\frac{x}{p}\right)$ es el Símbolo de Legendre[6], además como entre las soluciones de 1.3 está el punto al infinito, el número de puntos de una curva elíptica es

$$1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + a_4x + a_6)) = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + a_4x + a_6).$$

El siguiente algoritmo, recoge las anteriores ideas y, determina el número de puntos de una curva elíptica definida sobre un campo primo. Esto se consigue mediante el algoritmo que se presenta a continuación.

Algoritmo 1 (**numpuntos**)**.**

Entradas: *a, b y p, donde p determina el campo primo $\mathbb{F}_p$ y $a, b \in \mathbb{F}_p$ determinan la curva elíptica $E: \ y^2 = x^3 + ax + b$.*

Salida: *$n \in \mathbb{Z}^+$, donde $n = \#E(\mathbb{F}_p)$.*

Paso 1. $n = 0$.

Paso 2. *Se calcula*

$$n = p + \sum_{x \in \mathbb{F}_p} \chi((x^3 + a_4x + a_6) \text{ mód } p).$$

El algoritmo calcula $\chi(u)$ utilizando el comando `numlib::legendre` *de MuPAD.*

Paso 3. *El algoritmo aumenta a n en uno, ya que $\boldsymbol{O}$ es un punto de la curva, determinando el entero de salida.*

---

[6]Sea a un número entero y $p > 2$ un número primo. Se define el **Símbolo de Legendre** $\left(\frac{a}{p}\right)$ igual a 0, 1 o -1, como sigue:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } p|a; \\ 1, & \text{si } a \text{ es un residuo cuadrático módulo } p; \\ -1, & \text{si } a \text{ no es un residuo cuadrático módulo } p. \end{cases}$$

A continuación se presenta un ejemplo del anterior algoritmo.

Ejemplo 1. *Si el algoritmo se aplica a la curva elíptica* $E:\ y^2 = x^3 + x + 12$ *definida sobre* $\mathbb{F}_{37}$*; se obtiene*

```
numpuntos([1,12,37])
```

```
29
```

lo que indica que $E(\mathbb{F}_{37})$ *esta conformada por* 29 *puntos.*

Un resultado de la teoría de números dice que, sólo la mitad de los elementos de ${\mathbb{F}_p}^*$ son residuos cuadráticos, por lo tanto se esperaría que el número de puntos de la curva elíptica sobre $\mathbb{F}_p$ sea la mitad de los elementos de este campo. Un resultado más aproximado es el Teorema de Hasse, el cual limita la sumatoria

$$\sum_{x \in \mathbb{F}_p} \chi(x^3 + a_4 x + a_6)$$

por $2\sqrt{p}$.

Teorema 4.2 (**Teorema de Hasse**)**.** *Sea* $E(\mathbb{F}_q)$*, con* N *el número de puntos de esta curva elíptica, entonces:*

$$|N - (q+1)| \leq 2\sqrt{q}.$$

El número de puntos de la curva elíptica $E(\mathbb{F}_p)$, es el orden del grupo que se definió anteriormente, éste se presentará con $\#E(\mathbb{F}_p)$. Además el intervalo

$$[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

es llamado el intervalo de Hasse.

Definición 4.3 (**Traza de** $E(\mathbb{F}_p)$)**.** *Sea* $E(\mathbb{F}_p)$ *una curva elíptica, con*

$$\#E(\mathbb{F}_p) = p + 1 - t,$$

donde $|t| \leq 2\sqrt{p}$*, entonces* t *se define como la traza de* E *sobre* $\mathbb{F}_p$*.*

Es útil observar que hay muchas semejanzas entre el grupo aditivo $E(\mathbb{F}_p)$ y el grupo multiplicativo $\mathbb{F}_p^*$. Ellos tienen aproximadamente el mismo número de elementos. Pero $E(\mathbb{F}_p)$ ofrece mayores ventajas (útiles en criptografía): para un solo p grande, hay muchas curvas elípticas y muchos diferentes t que se pueden escoger para obtener diferentes órdenes $\#E(\mathbb{F}_p)$. Las curvas elípticas ofrecen una rica fuente de grupos abelianos finitos.

Conocido el orden de los grupos $E(\mathbb{F}_p)$, con p un número primo, sólo hace falta determinar la forma en que se puede determinar el orden de una curva elíptica sobre un campo de extensión $\mathbb{F}_q = \mathbb{F}_{p^n}$.

Teorema 4.4 (**Orden del Grupo** $E(\mathbb{F}_{p^n})$)**.** *Sea* E *una curva elíptica definida sobre* $\mathbb{F}_p$*, y sea* $\#E(\mathbb{F}_p) = p + 1 - t$*. Entonces* $\#E(\mathbb{F}_{p^n}) = p^n + 1 - V_n$ *para todo* $n \geq 2$*, donde* $\{V_n\}$ *es la secuencia definida recursivamente por*

$$V_0 = 2, \quad V_1 = t \quad y \quad V_n = V_1 V_{n-1} - q V_{n-2} \quad para \quad n \geq 2.$$

El siguiente algoritmo encuentra, dados el número de puntos de una curva y el campo primo sobre el cual se la define, las curvas que tienen dicho número de elementos sobre $\mathbb{F}_p$.

Algoritmo 2 (**curva**).

Entradas: $n \in \mathbb{Z}^+$ *y* p *número primo, donde* $n = \#E(\mathbb{F}_p)$ *y* p *es el número de elementos de* $\mathbb{F}_p$.

Salida: *Un vector* d*, con componentes* $[a, b]$ *que determinan una curva elíptica*

$$E: \ y^2 = x^3 + ax + b.$$

Paso 1. *Se determinan todos las posibles curvas que se pueden definir sobre* $\mathbb{F}_p$.

Paso 2. *Se calcula* $c = \#E(\mathbb{F}_p)$ *para cada curva elíptica.*

Paso 3. *Se compara* n *y* c*, si son iguales se incluye la componente* $[a, b]$ *en el vector* d.

Paso 4. *Se determina el vector* d *con componentes* $[a, b]$*, éste es el vector de salida.*

Ejemplo 2. *Si el algoritmo se aplica a* $\mathbb{F}_{37}$ *y* 26 *el número de puntos deseado; se obtiene*

```
curva(26,37)
```

```
[[5,0],[6,0],[8,0],[13,0],[17,0],[19,0],[22,0],[23,0],[35,0]]
```

los cuales son todos los posibles $[a, b]$*, con* $a, b \in \mathbb{F}_{37}$*, que definen la curva elíptica* $E: \ y^2 = x^3 + ax + b$*, donde* $\#E(\mathbb{F}_{37}) = 26$.

El siguiente teorema garantiza la existencia de por lo menos una curva elíptica, para todos los posibles número de puntos que estén contenidos en el intervalo de Hasse.

Teorema 4.5 (**Ordenes Admisibles de Curvas Elípticas**). *Sea* p *un número primo y considere el campo finito* $\mathbb{F}_q$ *con* $q = p^n$*. Existe una curva elíptica* E *definida sobre* $\mathbb{F}_q$ *con* $\#E(\mathbb{F}_q) = q + 1 - t$ *si y sólo si una de las siguientes condiciones se cumple:*

1. $t \not\equiv 0 (\text{mód } p)$ *y* $t^2 \leq 4q$.
2. n *es impar y* $t = 0$.
3. n *es impar y* $t^2 = 2q$ *y* $p = 2$.
4. n *es impar y* $t^2 = 3q$ *y* $p = 3$.
5. n *es par y* $t^2 = 4q$.
6. n *es par y* $t^2 = q$ *y* $p \not\equiv 1 (\text{mód } 3)$.
7. n *es par y* $t = 0$ *y* $p \not\equiv 1 (\text{mód } 4)$.

Ejemplo 3 (**Ordenes de Curvas Elípticas Sobre** $\mathbb{F}_{41}$). *Sea* $p = 41$*. En la tabla 1, para cada entero* n *en el intervalo de Hasse*

$$[41 + 1 - 2\sqrt{41}, 41 + 1 + 2\sqrt{41}] \approx [29.2, 54.8],$$

se muestran los coeficientes (a, b) *de una curva elíptica*

$$E: \ y^2 = x^3 + ax + b$$

definida sobre $\mathbb{F}_{41}$ *con* $\#E(\mathbb{F}_{41}) = n$*. Estos coeficientes se calcularon empleando el algoritmo* **curva** *desarrollado por los autores, y que aparece en el apéndice.*

n	(a,b)	n	(a,b)	n	(a,b)	n	(a,b)	n	(a,b)
30	$(1,17)$	35	$(1,1)$	40	$(1,2)$	45	$(1,6)$	50	$(3,4)$
31	$(2,17)$	36	$(1,13)$	41	$(3,8)$	46	$(2,8)$	51	$(1,8)$
32	$(1,0)$	37	$(2,6)$	42	$(0,1)$	47	$(1,5)$	52	$(2,0)$
33	$(2,15)$	38	$(1,7)$	43	$(3,18)$	48	$(1,10)$	53	$(1,20)$
34	$(3,0)$	39	$(1,3)$	44	$(1,14)$	49	$(2,7)$	54	$(2,4)$

Tabla 1: Los ordenes admisibles $n = \#E(\mathbb{F}_{41})$ de las curvas elípticas $E:\ y^2 = x^3 + ax + b$ definidas sobre $\mathbb{F}_{41}$.

A Apéndice: Algoritmos

Los algoritmos que se presentan a continuación fueron utilizados en el desarrollo de este artículo. estos algoritmos están implementados en el sistema de álgebra computacional MuPAD.

A.1 Algoritmo numpuntos

Este algoritmo recibe tres enteros positivos a, b y p, donde a, b son los coeficientes de $E:\ y^2 = x^3 + ax + b$ y p determina el campo primo $\mathbb{F}_p$, y determina el número de puntos que conforma la curva elíptica $E(\mathbb{F}_p)$.

```
numpuntos:=proc(CE)
  begin
    n:=0;
    for i from 0 to CE[3]-1 do
      y:=(i^3+CE[1]*i+CE[2]) mod CE[3];
      n:=n+numlib::legendre(y,CE[3])+1;
    end_for;
    print(n+1);
 end_proc;
```

A.2 Algoritmo curva

Este algoritmo recibe dos enteros positivos n y p, donde n es el número de puntos que se quiere que conformen una curva elíptica y p es el número de elementos del campo primo $\mathbb{F}_p$ sobre el cual se define la curva; el algoritmo *curva* retorna un vector d con componentes de la forma $[a,b]$, las cuales definen las curvas $E:\ y^2 = x^3 + ax + b$ que se pueden construir sobre $\mathbb{F}_p$ y que tienen $\#E(\mathbb{F}_p) = n$.

```
curva:=proc(n,q)
  begin delete(c);delete(d);
    e:=0;
    for a from 0 to q-1 do
      for b from 0 to q-1 do
        c:=0;
        for i from 0 to q-1 do
          y:=(i^3+a*i+b) mod q;
          c:=c+numlib::legendre(y,q)+1;
```

```
        end_for;
        c:=c+1;
        if c=n then
          e:=e+1;
          d[e]:=[a,b];
        end_if;
      end_for;
    end_for;
    d:=[d[i]$i=1..e];
end_proc;
```

Referencias

[1] Ivorra, C. (2004). *Curvas Elípticas*. Extraído el 5 de enero de 2008 desde http://www.uv.es/ivorra/Libros/Elipticas.pdf

[2] Koblitz, Neal. A course in number theory and cryptography. Graduate Texts in Mathematics, 114. *Springer-Verlag*, *New York*, 1987. vi+208 pp. ISBN: 0-387-96576-9 MR0910297 (88i:94001).

[3] Koblitz, Neal; Menezes, Alfred; Vanstone, Scott. The state of elliptic curve cryptography. Towards a quarter-century of public key cryptography. *Des. Codes Cryptogr.* 19 (2000), no. 2-3, 173–193. MR1759616 (2001i:94065).

[4] Silverman, Joseph H. The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. *Springer-Verlag, New York*, 1992. xii+400 pp. ISBN: 0-387-96203-4 MR1329092 (95m:11054).

Departamento de Matemáticas y Estadística
Universidad de Nariño

e-mail: lumdoz@gmail.com
e-mail: ricardovallejo10@gmail.com
e-mail: wfmutis@gmail.com
e-mail: jhcastillo@gmail.com