Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00183
Matrícula: 2153805980

CRIPTOSISTEMA CON AUTENTICACIÓN UTILIZANDO CURVAS ELÍPTICAS.

FLAVIA REYES PEREZ
ALUMNA

REVISÓ

DR. JOSE ANTONIO DE LOS REYES HEREDIA
SECRETARIO GENERAL

En la Ciudad de México, se presentaron a las 11:00 horas del día 3 del mes de diciembre del año 2018 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. HORACIO TAPIA RECILLAS
DR. JUAN CARLOS KU CAUICH
DR. JOSE NOE GUTIERREZ HERRERA

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRA EN CIENCIAS (MATEMÁTICAS APLICADAS E INDUSTRIALES)

DE: FLAVIA REYES PEREZ

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

Aprobar

Acto continuo, el presidente del jurado comunicó a la interesada el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

DR. HORACIO TAPIA RECILLAS

VOCAL

DR. JUAN CARLOS KU CAUICH

SECRETARIO

DR. JOSE NOE GUTIERREZ HERRERA

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA
UNIDAD IZTAPALAPA
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

"Criptosistema con autenticación utilizando curvas elípticas"

Tesis que presenta
Flavia Reyes Pérez
Para obtener el grado de
Maestro en Ciencias
(Matemáticas Aplicadas e Industriales)

Asesor
Dr. José Noé Gutiérrez Herrera

Jurado calificador

Presidente: Dr. Horacio Tapia Recillas

Secretario: Dr. José Noé Gutiérrez Herrera

Vocal: Dr. Juan Carlos Ku Cauich

Ciudad de México, México, Diciembre de 2018

Agradecimientos

Agradezco a mis padres y hermanos por haberme motivado y apoyado en la continuación de mi formación académica. A Nabor Eduardo Guzmán Vazquez por todo el apoyo brindado para la realización del posgrado y durante el desarrollo de este trabajo. A mis amigos quienes sin duda alguna me brindaron su apoyo y palabras de aliento en momentos que fueron necesarios.

A mi asesor de tesis Dr. José Noé Gutiérrez Herrera por compartirme sus conocimientos, por su asesoría y orientación, por su paciencia y apoyo brindado durante el posgrado y el desarrollo de este trabajo de tesis. Al Dr. Horacio Tapia Recillas y al Dr. Juan Carlos Ku Cauich por aceptar formar parte del jurado calificador, por el tiempo dedicado a la revisión detallada de este trabajo de tesis; quienes con sus sugerencias y observaciones hicieron de éste un mejor trabajo. También quiero agradecer al Dr. Mario Medina Valdez por todas sus palabras de ánimo durante mi estancia en la UAM-I.

Agradezco a la Universidad Autónoma Metropolitana y a la MCMAI por permitirme continuar con mi formación académica. A los profesores del Departamento de Matemáticas quienes nos compartieron sus conocimientos a lo largo del prosgrado. Al Laboratorio de Códigos y Criptografía por darme el espacio de realizar este trabajo de tesis

A la M.C. Iseo González Christen por su apoyo en el proceso administrativo ya que con su asesoría me facilitó realizar el papeleo necesario tanto en el ingreso al posgrado como en la culminación del mismo.

Al Consejo Nacional de Ciencia y Tecnología por los apoyos otorgados, ya que gracias a ello fue posible realizar mis estudios de posgrado como la culminación de este trabajo.

Flavia Reyes Pérez, diciembre de 2018

Índice general

Índice de figuras

Índice de tablas

Introducción

A lo largo de la historia el ser humano se ha visto en la necesidad de transmitir información de forma secreta. Para ello, ha diseñado métodos para disfrazar dicha información, tales que estos puedan viajar de manera segura en un canal no seguro, esto es, si un tercero no autorizado intercepta el mensaje con tal información no tenga conocimiento del mensaje original a partir del disfrazado. La criptografía es el área que se encarga de estudiar técnicas matemáticas para brindar servicios relacionados a la seguridad de la información tales como confidencialidad o privacidad, integridad, autenticidad y no-repudio; cuyo principal objetivo es permitir la comunicación de dos partes o entidades, la cuales llamaremos *emisor* y *receptor*, disfrazando (cifrando) un mensaje de tal manera que éste sólo sea legible o entendible para el receptor (ver [25], [42], [23], [30]). La *confidencialidad* garantiza que sólo los usuarios autorizados tengan conocimiento del mensaje que va dirigido a ellos. La *integridad* hace posible verificar que el mensaje no ha sido modificado, es decir, que se verifique que el mensaje no ha sido alterado ya sea mediante la inserción, eliminación o sustitución de datos. La *autenticación* es un servicio relacionado a la identificación, esto es, donde el emisor como el receptor agregan alguna información que los identifica, de esta manera cada uno de ellos puede estar seguro de dónde o de quién provino dicho mensaje. *No-repudio* previene que alguna entidad niegue alguna acción realizada.

De acuerdo con la historia la criptografía se divide en *clásica* y *moderna*. A los sistemas anteriores a la segunda guerra mundial o anteriores al nacimiento de las computadoras se les conoce como *criptografía clásica*.

Los primeros en utilizar la criptografía fueron los espartanos quienes usaron el sistema escítala que consistía en dos varas del mismo grosor que poseían los integrantes de la comunicación, para enviar un mensaje se enrrollaba una cinta en espiral a uno de los bastones y se escribía el mensaje en forma longitudinal de tal manera que en cada vuelta de la cinta se apreciara una letra a la vez. Una vez escrito el mensaje se desenrollaba la cinta y se enviaba, el receptor tenía que enrollar la cinta en otro bastón del mismo grosor para leer el mensaje. Otro ejemplo es lo que se conoce como cifrado de César cuyo nombre es en honor a Julio César quien utilizó este sistema para comunicarse con sus generales,

el cual consistía en reemplazar una letra del mensaje original por otra que se encuentra a un número fijo de posiciones más adelante en el alfabeto (ver [27]). Estos ejemplos son algunos que se pueden realizar utilizando papel y lápiz pero que se pueden descifrar de manera rápida con ayuda de una computadora. La *criptografía moderna* nace debido a las computadoras, los sistemas en esta caso basan su seguridad en algoritmos matemáticos que se consideran computacionalmente difíciles de resolver.

Dentro de la criptografía moderna se tienen sistemas simétricos como asimétricos, en los cuales se hacen uso de llaves para disfrazar (cifrar) y para quitar el disfraz (descifrar). En los sistemas simétricos o de llave privada, las llaves que se utilizan para cifrar como para descifrar coinciden (ver [42], [40]). Por tanto, parte de su seguridad se basa en mantener en secreto dicha llave por lo que ambas partes deben acordarla antes de que se aparten o por medio de un canal seguro donde no se contaba con esto último hasta antes de 1976. Así, si se tienen varios usuarios se enfrentan problemas de generación y administración de llaves, entre otros. Algunos ejemplos de este tipo de sistemas son AES, DES y varios más (ver [30], [23], [42]).

Por otro lado, para resolver los problemas que presentan los sistemas simétricos, en 1976 W. Diffie y M. Hellman inventaron la criptografía de llave pública, presentando además un sistema de intercambio de llaves que lleva sus nombres. A diferencia de los sistemas simétricos, los asimétricos o de llave pública, utilizan llaves distintas para cifrar y para descifrar, a estas llaves se les conoce como *pública* y *privada*, respectivamente, son tales que la llave privada como el mensaje original no se pueden obtener a partir de la llave pública y del proceso de cifrado. Algunos ejemplos de sistemas asimétricos son el sistema *RSA, ElGamal, NTRU*, entre otros (ver [23], [42], [30], [3]).

Lo que resulta inconveniente de los sistemas asimétricos es el uso de llaves de tamaño demasiado grande, por ejemplo en el sistema RSA se usan llaves de al menos 1024 bits (ver [30]). Una solución a este problema es el uso del grupo formado por los puntos racionales de una curva elíptica definida sobre un campo finito, los cuales fueron propuestas en 1985 de manera independiente por Neal Koblitz [15] y Victor S. Miller [26] . Además de usar llaves de longitud menores también proporcionan soluciones en cuanto a limitaciones de espacio y poder de cómputo, entre otros (ver [18]).

Una *curva elíptica* definida sobre un campo $\mathbb{K}$ es el conjunto de *puntos racionales* que satisfacen la ecuación de *Weierstrass* dada por $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, con cada a_i en $\mathbb{K}$, junto con un punto conocido como *punto al infinito*.
A partir de esta ecuación y dependiendo de la característica del campo en que se trabaje, mediante una transformación lineal se pueden obtener las respectivas expresiones para las

curvas elípticas. En particular, para campos de característica dos se obtiene que una curva elíptica sobre el campo finito $\mathbb{F}_{2^m}$ con 2^m elementos es el conjunto de puntos racionales (x, y), con x, $y \in \mathbb{F}_{2^m}$ que satisfacen una de las siguientes ecuaciones

$$y^2 + xy = x^3 + ax^2 + b, \quad \text{o} \quad y^2 + ay = x^3 + bx + c.$$

Y sobre un campo finito $\mathbb{F}_{p^m}$ con p^m elementos, p un primo impar, una curva elíptica es el conjunto de puntos racionales que satisfacen $y^2 = x^3 + ax + b$. El conjunto de puntos racionales de una curva elíptica junto con una operación suma definida en éste mismo forman un grupo abeliano, donde el punto al infinito juega el papel de neutro aditivo.

Por otro lado, se tienen aspectos matemáticos y computacionales que hacen seguro los sistemas de cifrado que se conocen actualmente, por ejemplo el sistema RSA basa su seguridad en el *problema de factorización de enteros*, que consiste en que dado un número entero grande (de al menos 1024 bits) n, hallar sus factores primos; otro ejemplo es el sistema ElGamal cuya seguridad se basa en lo que se conoce como *el problema de logaritmo discreto*, el cual se puede definir para cualquier grupo cíclico finito, en particular para los puntos racionales de una curva elíptica, que consiste en hallar n dados P y Q dos puntos racionales de una curva elíptica tal que $Q = nP$, esto es, la suma de P consigo mismo n veces.
La ventaja principal que tienen los sistemas con curvas elípticas respecto a los basados en grupos multiplicativos de un campo finito es que no se conocen algoritmos eficientes que puedan calcular logaritmos discretos (ver [18]).

El objetivo del presente trabajo es proporcionar autenticación a un sistema de cifrado que utiliza curvas elípticas, de tal manera que cada receptor estará seguro del origen del mensaje, es decir, estará seguro de quién provino el mensaje, esto es, con *autenticación*; por lo que está estructurado de la siguiente manera. En el primer capítulo describimos a los sistemas simétricos y cómo a partir de esto surge la criptografía de llave pública. En este capítulo también describimos a las funciones unidireccionales, y cómo se utilizan en los sistemas de cifrado, un ejemplo de los mismos es el sistema ElGamal, que se basa en el problema de logaritmo discreto.
En el segundo capítulo damos una introducción respecto a curvas elípticas, describiendo la forma en que se definen, las leyes y estructuras de grupo que satisfacen, como también las expresiones para dichas curvas en campos de característica dos y en característica distintas de dos y tres.

Las curvas de Koblitz han tomado importancia en la criptografía, las cuales son un caso particular de las curvas elípticas definidas en campos de característica dos. En el capítulo tres, las definimos y presentamos las propiedades matemáticas que poseen dichas curvas. En el cuarto capítulo describimos el sistema ElGamal con curvas elípticas, además presentamos lo que conocemos como sistema ElGamal con autenticación, dado que en este caso, el receptor puede estar seguro de quién provino dicho mensaje cifrado. Como último capítulo se escriben algunas conclusiones que se obtuvieron a partir de este trabajo de tesis.
También se anexan cuatro apéndices, en el primero de ellos se tienen algunas definiciones y resultados de álgebra; en el segundo se tienen pruebas de las propiedades de grupo que satisface el conjunto de puntos racionales de una curva elíptica definida sobre un campo junto con la operación suma definida; ejemplo del sistema con autenticación que se presenta cifrando un fragmento de la obra *"El principito"* de Antoine de Saint-Exupéry; y en el último se tienen los códigos de los algoritmos que se presentan durante el desarrollo de este trabajo implementados en el software *SAGE*, los cuales se utilizaron para dar ejemplos de los mismos.

Cabe mencionar que este trabajo fue realizado parcialmente en el Laboratorio de Códigos y Criptografía del Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa.

Capítulo 1

Introducción a la criptografía de llave pública

Como es usual, supongamos que A y B son dos partes o entidades que desean comunicarse por medio de mensajes de manera secreta, esto es, disfrazando dicho mensaje y a través de un medio o canal de comunicación no seguro, por ejemplo el mensaje puede ser observado por un tercero, digamos C. De esta manera, aunque C intercepte el mensaje no tendrá conocimiento del contenido del mismo.

El mensaje que se desea enviar lo llamaremos *texto en claro* y al mensaje disfrazado lo llamaremos *texto cifrado*, los cuales están escritos en algún alfabeto con cierta cantidad de caracteres. Por otro lado, al proceso de cifrar un texto se le conoce como *cifrado o encriptación* y al proceso inverso se le conoce como *descifrado o desencriptación*. Estos elementos definen un sistema criptográfico, como se describe a continuación.

Un *sistema criptográfico* es una quíntupla $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ donde $\mathcal{M}$ es un conjunto finito de posibles textos en claro, $\mathcal{C}$ es un conjunto finito de posibles textos cifrados, $\mathcal{K}$ es el conjunto de posibles llaves; $\mathcal{E} = \{e_k : k \in \mathcal{K}\}$ y $\mathcal{D} = \{d_k : k \in \mathcal{K}\}$ son familias de funciones, donde $e_k : \mathcal{M} \longrightarrow \mathcal{C}$, $d_k : \mathcal{C} \longrightarrow \mathcal{M}$ son conocidos como *funciones de encriptación* y *de desencriptación*, respectivamente y son tales que para cada $k \in \mathcal{K}$ existe una función de encriptación $e_k \in \mathcal{E}$ y una correspondiente función de desencriptación $d_k \in \mathcal{D}$ que satisfacen $d_k(e_k(m)) = m$, para cada texto en claro $m \in \mathcal{M}$ (ver [23], [42]).

En la criptografía se tienen criptosistemas simétricos o de llave privada y criptosistemas asimétricos o de llave pública. En lo que sigue hablaremos de manera breve del primer tipo de criptosistema, el resto del escrito estará dedicado al segundo y en particular, a un caso especial de este tipo de cifrados.

1.1. Criptografía de llave privada

En los sistemas simétricos también conocidos como sistemas de llave privada, para cifrar o descifrar mensajes los usuarios A y B utilizan una misma llave para realizar dichas tareas. Por ejemplo, en el caso del sistema de cifrado por sustitución que utilizó Julio César la llave es el número tres puesto que para cifrar los mensajes cada letra del alfabeto se tiene que sustituir por otra que se encuentra a tres posiciones más adelante y para descifrarla cada letra del texto cifrado se tiene que sustituir por otra que se encuentra tres posiciones atrás. Esto es, para cifrar la letra C se hace sustituyéndola por E y viceversa para descifrarla.

Como su nombre lo indica, en este tipo de criptosistemas la llave se debe mantener en secreto entre los usuarios autorizados. De donde surge una de las desventajas que presentan estos criptosistemas, puesto que los usuarios A y B deben acordar el uso de una llave secreta antes de iniciar una comunicación en un canal inseguro (ver [42], [40], [30]). En otras palabras, supongamos que $\mathcal{M}$ es el conjunto de todos los posibles textos en claro, $\mathcal{C}$ el conjunto de todos los posibles textos cifrados y $\mathcal{K}$ el conjunto de todas las posibles llaves. Un *criptosistema de llave privada* consiste de una familia de pares de funciones

$$e_k : \mathcal{M} \to \mathcal{C}, \quad d_k : \mathcal{C} \to \mathcal{M}, \quad k \in \mathcal{K},$$

tales que $d_k(e_k(m)) = m, \ \forall m \in \mathcal{M}$. Si después A desea enviarle un mensaje $m \in \mathcal{M}$ al usuario B, lo enviará como $c = e_k(m)$. Una vez recibido el texto cifrado c, B recupera el mensaje aplicando la función de desencripción d_k. Como podemos notar se utiliza la misma llave k para realizar los procesos de encriptación y desencriptación. Por ello, para que los usuarios A y B puedan utilizar sistemas de llave privada inicialmente deben acordar una llave que mantendrán en secreto, mediante un encuentro personal o utilizando un medio seguro dónde esto último no existía hasta antes de 1976.

Un ejemplo de un sistema de cifrado que tiene seguridad perfecta, esto es, que no se puede romper incluso si no se tienen limitaciones computacionales, es el conocido como *libreta de un sólo uso (o del inglés One-Time Pad)* el cual consiste en sumar vectores de bits, la llave se utiliza una única vez y es generada de manera aleatoria. En otras palabras, la llave $s_0, s_1, s_2, \ldots$ es generada de manera realmente aleatoria, no sólo pseudoaleatoria y cada vector $(s_0, s_1, s_2, \ldots, s_n)$ es usado sólo una vez. Aquí n es la longitud del mensaje que se desea cifrar. Este sistema posee secreto perfecto. En efecto, para cada bit del texto cifrado y del texto en claro $y_0, y_1, y_2, \ldots$ y $x_0, x_1, x_2, \ldots$ respectivamente, obtenemos ecuaciones de la forma $y_0 = x_0 + s_0$ mód 2, $y_1 = x_1 + s_1$ mód 2, $\ldots$ Cada una de las relaciones es una ecuación lineal módulo 2 con dos incógnitas, los cuales son imposibles de resolver. Si el

atacante conoce el valor de y_0 que puede ser 0 o 1 no puede determinar el valor de x_0. De hecho las soluciones $x_0 = 0$ o $x_0 = 1$ son igual de probables si s_0 proviene de una fuente verdaderamente aleatoria y hay un 50 % de posibilidades de que tome el valor 0 y 1. Algo similar sucede con el resto de las ecuaciones. La situación cambia cuando los valores s_i no son realmente aleatorios, en ese caso en las ecuaciones previas existe una relación de dependencia. De esta manera, aunque fuera difícil de resolver el problema el sistema ya no sería completamente seguro. Como se puede observar la libreta de un sólo uso es seguro, pero no se tiene una forma de intercambiar llaves en la práctica. Muchos sistemas de cifrado hacen uso de la técnica de cifrado de la libreta de un sólo uso, pero generando una sucesión pseudoaleatoria $s_1, s_2, \ldots$. Al combinar esta idea con otras adecuadas al sistema de cifrado que se esté desarrollando, se han logrado crear criptosistemas muy robustos, como DES, IDEA, AES y muchos más (ver [42], [30]).

A los criptosistemas de llave privada se les pide que cumplan ciertas propiedades, como las que se describen a continuación:

- Las funciones e_k y d_k deben ser fáciles de aplicar.
- Un tercero no autorizado que observa $c = e_k(m)$, no pueda determinar ya sea el mensaje m o la llave k a partir de éste.
- Que un tercero sólo pueda utilizar (acceder a) la información pública del criptosistema.

Por otro lado, supongamos que se tiene una cierta cantidad n de usuarios que desean estar comunicados unos con otros, esto implica que se deben tener $n(n-1)/2$ llaves distintas y cada usuario necesita conocer $(n-1)$ llaves. Además, como parte de su seguridad depende de mantener en secreto la llave, si algún usuario desea abandonar o unirse al grupo se tienen que generar nuevas llaves. De aquí surge otro problema al que se enfrenta el criptosistema simétrico, que es la administración de llaves, puesto que si n es suficientemente grande, el número de llaves resulta díficil de manejar (ver [23], [11]).

Por tanto, aunque la criptografía de llave privada es adecuada para muchas aplicaciones tiene las siguientes desventajas las cuales la hacen inadecuada para usarla en ciertas aplicaciones, por ejemplo las llaves se deben cambiar cada que se desee enviar un mensaje.

i) **Problema de distribución de llaves:** Los dos usuarios tienen que seleccionar una llave secreta antes de que puedan iniciar una comunicación en un canal inseguro. No se encuentra disponible un canal seguro para elegir una llave secreta.

ii) **Problema de administración de llaves:** En una red de n usuarios, cada par de ellos necesita compartir llaves de manera secreta, por lo que son necesarios un total de $n(n-1)/2$ llaves. Si n es suficientemente grande, el número de llaves resulta complicado de manejar.

Para resolver las desventajas que presentan los criptosistemas de llave privada Diffie y Hellman presentaron el protocolo que se conoce como *intercambio de llaves Diffie-Hellman*, el cual se describe en la siguiente sección.

Entre los criptosistemas de llave privada más comunes están el DES, AES, entre otros, los cuales se pueden consultar en las referencias [42], [30], [27], [40], [25].

1.2. Intercambio de llaves Diffie-Hellman

Como se ha mencionado previamente, los criptosistemas de llave privada presentan ciertos problemas, por los que en 1976 Whitfield Diffie y Martin Hellman propusieron la criptografía de llave pública describiendo un protocolo para que dos usuarios A y B pudieran enviar y recibir una pieza en común de una información secreta en un canal de comunicación inseguro (ver [6], [30], [23], [3]). Como consecuencia, los usuarios podrían utilizarla como su llave en un criptosistema simétrico.

A continuación se describe este protocolo conocido como el *Intercambio de llaves Diffie-Hellman* en términos de un grupo arbitrario.

i) Los usuarios A y B eligen un grupo multiplicativo finito, cíclico y abeliano $\mathbb{G}$ y un elemento primitivo $\alpha \in \mathbb{G}$. Se hacen públicos el grupo G y el elemento α.

ii) A genera un entero a aleatorio, después calcula α^a y transmite α^a a B.

iii) De manera similar, B genera un entero b, calcula y transmite α^b.

iv) A recibe α^b y calcula $(\alpha^b)^a$.

v) Similarmente, B recibe α^a y calcula $(\alpha^a)^b$.

De esta manera A y B obtienen un elemento de grupo en común, α^{ab}. Cabe mencionar que esto es un intercambio de llaves no autenticado, es decir, este intercambio no involucra la información privada de los usuarios; de esta manera cualquier tercero, digamos C, puede hacerse pasar por A o por B, antes de que ellos acuerden la llave a utilizar; esto se conoce como el *ataque del hombre de en medio*.

Por otro lado, si un interceptor no autorizado desea reconstruir α^{ab} a partir del conocimiento de G, α, α^a y α^b se le conoce como *el problema de Diffie-Hellman*. Mientras que el problema de calcular a dados G, α y α^a es conocido como *problema de logaritmo discreto*.

Los autores de este protocolo conjeturaron que romper el proceso de intercambio de llaves es equivalente a la dificultad de resolver el problema de logaritmo discreto. Por ello, se dice que la seguridad de intercambio de llaves está basado en la dificultad del problema de logaritmo discreto (ver [6], [23], [30]). En general no se ha probado matemáticamente tal equivalencia, pero en las referencias [5] y [20] se pueden ver las pruebas de que son equivalentes bajo ciertas condiciones.

1.3. Criptografía de llave pública

El criptosistema asimétrico o de llave pública es otro tipo de criptosistemas que se tienen en la criptografía. En este caso se consideran dos llaves, las cuales se conocen como *llave pública* y *llave privada*. La llave pública, como su nombre lo dice, se encuentra disponible para cualquier emisor y es la que se utiliza en el proceso de cifrado, mientras que la llave privada es conocida únicamente por el receptor y se utiliza para descifrar mensajes.

Nuevamente, si el usuario B le desea enviar un mensaje a A, B ocupa la llave pública de A que se encuentra, digamos, en un directorio; y una vez que A recibe el mensaje cifrado, lo descifra utilizando su llave privada, esto es, la llave que solamente A conoce. De esta manera, A y B pueden estar en comunicación (intercambiando mensajes) sin antes haberse reunido para acordar una llave común. Esto se ilustra en el siguiente diagrama.

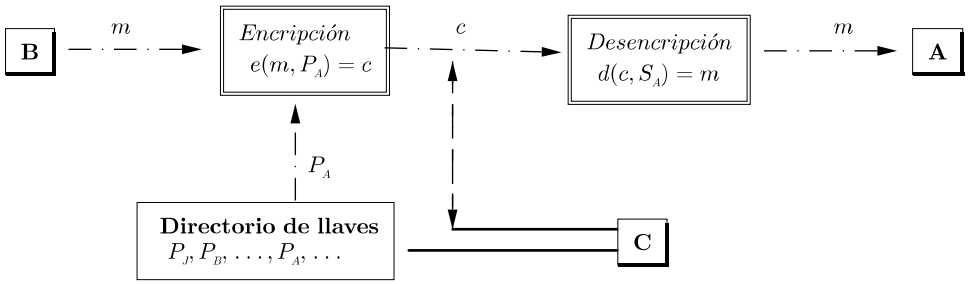

Figura 1.1: Diagrama de un criptosistema de llave pública, donde A y B son los usuarios, y C un tercero no autorizado; m y c son los textos en claro y cifrado, respectivamente; e y d son las funciones de encriptación y desencriptación; P_A y S_A son las respectivas llaves pública y privada del usuario A.

Parte de la seguridad de este tipo de criptosistemas se basa en el algoritmo de cifrado y en generar dos llaves relacionadas de tal manera que un tercero digamos C no autorizado, como se muestra en la Figura 1.1, no pueda recuperar el mensaje original y tampoco hallar la llave privada a partir de la llave pública y del algoritmo de cifrado (ver [30], [27], [23]). Una de las formas para lograr esto es haciendo uso de las funciones conocidas como *funciones unidireccionales con puerta trasera*, las cuales se describen brevemente en la siguiente sección.

1.4. Funciones unidireccionales

Como se ha mencionado previamente, se desean generar dos llaves relacionadas, la pública y la privada, para ello, a continuación describimos brevemente a las funciones unidireccionales.

Como antes, $\mathcal{M}$ y $\mathcal{C}$ son el conjunto de posibles textos en claro y cifrado, respectivamente. Una *función unidireccional o una función de un sólo sentido* $f : \mathcal{M} \to \mathcal{C}$ es una función invertible con la característica de que para cada $m \in \mathcal{M}$ es fácil de calcular $f(m)$, mientras que para la mayor parte de $c \in \mathcal{C}$ es difícil de calcular $f^{-1}(c)$. En este caso *fácil* significará que se pueda calcular en tiempo polinomial y *difícil* significará que se requiere tiempo exponencial para su cálculo. En la práctica, difícil significará que es computacionalmente imposible, esto es, que es imposible utilizando los mejores algoritmos conocidos (ver [23]).

Por otra parte, una función unidireccional $f : \mathcal{M} \to \mathcal{C}$ es llamada de *un sólo sentido con puerta trasera* (abreviado como TOF por su sigla en inglés trapdoor one-way function) si existe una información extra con la cual se puede calcular la inversa de manera eficiente. A tal información extra se le conoce como *puerta trasera*.

En la referencia [23], se explica cómo construir un criptosistema haciendo uso de las funciones de un sólo sentido con puerta trasera. De donde se tiene que para construir un criptosistema es necesaria una familia de funciones con puerta trasera $f_k : \mathcal{M} \to \mathcal{C}$, $k \in \mathcal{K}$, con la propiedad de que para cada $k \in \mathcal{K}$ la puerta trasera, que escribimos como $t(k)$, es fácil de obtener. Además, para cada $k \in \mathcal{K}$ debe ser posible escribir un algoritmo eficiente para calcular f_k, tal que a partir de esta descripción sea difícil obtener k y por tanto $t(k)$. De aquí que, dada la familia de funciones con puerta trasera, cada usuario elige de manera aleatoria $a \in \mathcal{K}$ y hace público el algoritmo E_a para calcular f_a. En este caso, el algoritmo E_a es la llave pública de cada usuario A, mientras que $t(a)$ es la llave privada. Por tanto, para que el usuario B le pueda enviar un mensaje $m \in \mathcal{M}$ a A, busca la llave pública de A y le envía $f_a(m)$. Así, solamente A puede invertir f_a y recuperar el mensaje m.

Podemos observar que ya no existe la necesidad de intercambiar llaves previo a una comunicación. Además, sólo hay un par de llaves asociado a cada usuario. De esta manera, los criptosistemas de llave pública resuelven los problemas de distribución y administración de llaves que derivan de los de llave privada.

Dentro de las informaciones que se pueden utilizar como puerta trasera se tienen el orden de un grupo y la exponenciación. Las formas de considerarlos se describen en lo que sigue.

1.5. Funciones TOF basadas en grupos

Como se ha mencionado previamente, el uso de las funciones unidireccionales con puerta trasera son de gran utilidad. En este apartado describimos las formas en que se pueden usar las características que tiene un grupo como parte de una información extra, la puerta trasera. Para ello, consideremos G un grupo abeliano, multiplicativo y finito de orden n. Además, supongamos que la operación definida en G es fácil de calcular, es decir, se conoce un algoritmo eficiente (en otras palabras, el algoritmo corre en tiempo polinomial) para calcular $\alpha \cdot \beta$, con $\alpha, \beta \in G$; y que la exponenciación en G se puede realizar mediante el método de multiplicación y elevación al cuadrado repetido como sigue.

Entrada: $\alpha \in G$, $\ell \in \mathbb{Z}$
Salida: α^{ℓ}
Sea $\ell = \sum_{i=0}^{t} b_i 2^i$, $b_i \in \{0, 1\}$, $b_t = 1$, la representación binaria de ℓ
$\beta \leftarrow \alpha$
Para i de $t-1$ a 0 hacer
    $\beta \leftarrow \beta \cdot \beta$
    Si $b_i = 1$
        $\beta = \beta \cdot \alpha$
Imprimir β

Algoritmo 1: Potencia de un elemento en un grupo.

En lo que sigue, en la primera parte describimos la forma en que se puede usar el orden de grupo como puerta trasera. Mientras que en la segunda parte se tiene la exponenciación.

1.5.1. Orden de un grupo como una TOF

Sea G un grupo y supongamos que en G se puede describir un algoritmo eficiente para obtener el producto de elementos de dicho grupo, pero de tal manera que hallar sus órdenes a partir de éste es difícil sin una pieza adicional de información, la *puerta trasera*.

Este tipo de grupos se puede utilizar para construir criptosistemas de llave pública como sigue:

Cada usuario A elige un grupo G de orden n tal que satisface la propiedad previa y tal que solamente A conoce n. Luego, A selecciona de manera aleatoria un número entero e, con $1 \leq e \leq n-1$, tal que el máximo común divisor de e y n es 1. Después calcula, utilizando el algoritmo extendido de Euclides, un entero d, $1 \leq d \leq n-1$ tal que $ed \equiv 1 \pmod{n}$.
La llave pública de A consiste en el grupo G y el entero e. Los espacios de texto en claro y texto cifrado son $\mathcal{M} = G$ y $\mathcal{C} = G$, respectivamente.
Si B desea enviar un mensaje $m \in G$ a A, entonces B simplemente envía el elemento de grupo $c = m^e$. Y A recupera m a partir de d y calculando $c^d = (m^e)^d = m$. En efecto, como $ed \equiv 1 \pmod{n}$ entonces $c^d = (m^e)^d = m^{ed} = m^{1+kn}$ para algún k entero. Como G es de orden n se tiene que $c^d = (m^e)^d = m^{ed} = m^{1+kn} = m^1 = m$, obteniendo de esta manera el mensaje original. Cabe mencionar que la puerta trasera es el orden del grupo que en este caso lo denotamos como n, puesto que conociendo n es fácil calcular el exponente de descifrado d.

Existen dos clases conocidas de grupos que satisfacen las propiedades mencionadas. La primera clase forma la base del criptosistema RSA y la segunda clase son curvas elípticas sobre campos finitos. La primera se describe a continuación, mientras que la segunda se describirá en el siguiente capítulo.

Criptosistema RSA

El criptosistema RSA fue inventado en 1977 por Rivest, Shamir y Adleman y fue el primer modelo abstracto que utilizó las ideas de Diffie y Hellman para la criptografía de llave pública (ver [33], [23], [30], [42], [46], [27]). En este criptosistema se eligen dos primos grandes (con al menos 1024 bits) p y q distintos y se calcula $n = pq$. En este caso, el grupo a usar es el grupo multiplicativo de unidades en los enteros módulo n, $G = \mathbb{Z}_n^*$. Se sabe que el orden de G es $\phi(n) = (p-1)(q-1)$, con ϕ la función de Euler. La llave pública es el par (n, e), con $e \in \{1, \ldots, n-1\}$ tal que n y e son primos relativos y la llave privada es d que satisface la congruencia $ed \equiv 1 \pmod{n}$. Las correspondientes funciones de encripción y de desencripción son: $m^e \bmod n$ y $c^d \bmod n$ con $m \in G$ mensaje en claro y c mensaje cifrado. Esto funciona, dado que $ed \equiv 1 \bmod n$ entonces $c^d \bmod n = (m^e)^d \bmod n = m \bmod n$.

Notemos que en el caso anterior calcular $\phi(n)$ dado únicamente n es computacionalmente equivalente al problema de factorizar n. Además, no se conoce un algoritmo eficiente para hallar raíces e-ésimas en $\mathbb{Z}_n^*$ sin conocer p y q, por tanto, romper el criptosistema RSA es equivalente a factorizar n. Por ello, decimos que la seguridad de RSA está basada

en el problema de factorización de enteros. De donde se tiene que la información extra o puerta trasera es el conocimiento de la factorización del orden de G, que es $n = pq$ (ver [23], [42]).

En la siguiente sección tenemos otro ejemplo en donde la exponenciación se utiliza como información extra o puerta trasera.

1.6. Criptosistema ElGamal

En 1985 Taher ElGamal propuso el siguiente sistema de llave pública basado en exponenciación discreta o bien basado en el problema de logaritmo discreto (ver [7], [23], [30], [42]). Para describirlo consideremos G un grupo multiplicativo conmutativo y finito de orden n; y supongamos que el problema de logaritmo discreto en G es difícil. En este caso, supongamos que A y B son dos usuarios que desean utilizar este sistema. Además, pensemos que B desea enviarle un mensaje m a A. Se eligen y se hacen públicos el grupo G y un elemento $\alpha \in G$.

i) El usuario A elige un entero aleatorio a y hace público α^a, en este caso, a y α^a, son las llaves privada y pública de A, respectivamente.

ii) El usuario B genera un entero k aleatorio y calcula $c_1 = \alpha^k$.

iii) Después B busca la llave pública del usuario A, α^a. Calcula $(\alpha^a)^k$ y para cifrar el mensaje $m \in G$ realiza $c_2 = m\alpha^{ak}$.

iv) B le envía a A el par de elementos de grupo (c_1, c_2).

v) Por último, A calcula c_1^a y lo utiliza para recuperar el mensaje m realizando el cálculo $m = c_2 c_1^{-a}$. Esto funciona puesto que $c_2 c_1^{-a} = (m\alpha^{ak})(\alpha^k)^{-a} = m$.

Lo anterior se ilustra en el siguiente diagrama, considerando el grupo multiplicativo del campo finito $\mathbb{Z}_p$, con p primo.

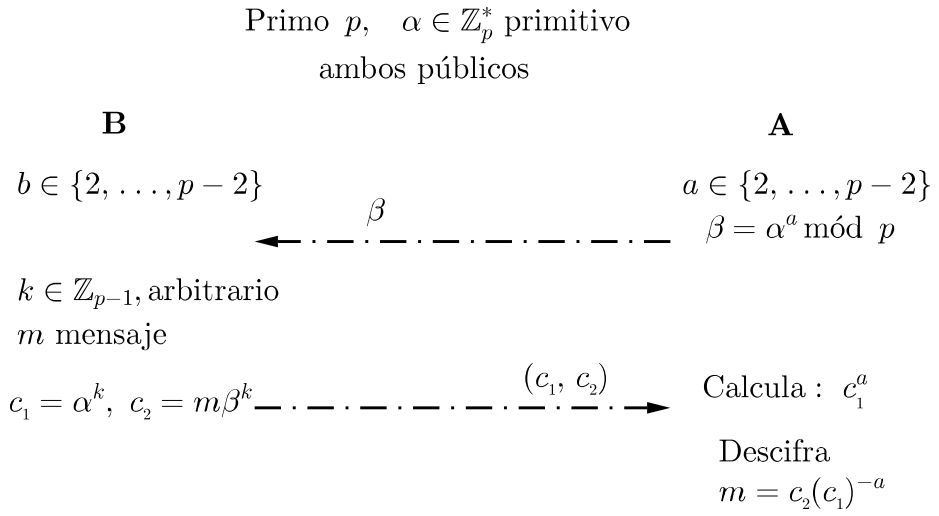

Figura 1.2: Diagrama del sistema ElGamal en el grupo multiplicativo $\mathbb{Z}_p^*$ con p un primo, A y B dos usuarios de este sistema, a y b sus respectivas llaves privadas, β la llave pública de A, m el mensaje en claro y (c_1, c_2) el correspondiente mensaje cifrado. Además, suponemos que el usuario B le desea enviar un mensaje m a A.

Como ya se mencionó en la Sección 1.2 la seguridad del intercambio de llaves que propusieron Diffie y Hellman está basada en la dificultad de resolver el problema de logaritmo discreto y dado que el criptosistema ElGamal se puede ver como una extensión de dicho intercambio de llaves, la seguridad de este sistema también está basada en la dificultad del logaritmo discreto (ver [30]). Para una implementación segura y eficiente de este criptosistema el grupo G y $\alpha \in G$ se deben elegir tales que satisfagan las siguientes condiciones.

- Para la eficiencia, la operación de grupo en G debe ser fácil de aplicar.
- Para la seguridad, el problema de logaritmo discreto en $\langle\alpha\rangle$ debe ser difícil en el sentido definido en la Sección 1.4. Donde $\langle\alpha\rangle$ es el grupo cíclico generado por α.

Se pueden considerar otros grupos entre ellos se tienen los grupos multiplicativos de los campos finitos $\mathbb{F}_{2^k}$ y $\mathbb{F}_{p^k}$ (ver Sección A.4 del Apéndice A), con p primo impar, el grupo de puntos racionales de una curva elíptica definida sobre un campo finito, el grupo de matrices no-singulares sobre un campo finito, entre otros (ver [23], [30], [42]).
Dado que se pueden trabajar otros grupos en particular podemos considerar el grupo de puntos racionales de una curva elíptica en característica dos. Por ello, en el siguiente capítulo hablamos acerca de estas curvas.

Capítulo 2

Introducción a curvas elípticas

En este capítulo introducimos algunas nociones de curvas elípticas, describimos al espacio proyectivo, esto para entender mejor la existencia de lo que se conoce como punto al infinito en dichas curvas. Además, describimos algunas características de éstas, una operación y la estructura de grupo que posee. También se utilizan algunos conceptos de álgebra que son recordados brevemente en el Apéndice A.

2.1. Curva elíptica

En algunas referencias como [46], [17], [14], se menciona que recientemente en temas de teoría de números y geometría algebraica en lo que refiere a curvas elípticas sobre campos finitos, se ha encontrado aplicación en criptografía. En esta sección definimos lo que entenderemos cuando nos referimos a una curva elíptica, en cualquier campo y en particular en campos finitos.

Por otro lado, a diferencia de la geometría euclidiana hablando de rectas paralelas en la geometría proyectiva estas rectas se intersecan en el infinito (ver [46]). Enseguida tratamos a cerca del espacio proyectivo y los puntos que lo forman, para esto, procedemos a definir el espacio proyectivo bidimensional.

Consideremos un campo $\mathbb{K}$ y el conjunto $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$. Diremos que (x_1, y_1, z_1) y $(x_2, y_2, z_2) \in \mathbb{K}^3 \setminus \{(0, 0, 0)\}$ están relacionadas, y para hacer referencia a ello escribiremos $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, si $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$, para un escalar $\lambda \in \mathbb{K}$ distinto de cero, o bien,

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \text{ si y sólo si } (x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2), \quad \lambda \neq 0. \tag{2.1}$$

Se puede verificar que la relación dada en (2.1) es de equivalencia. De donde se tiene una partición del conjunto $\mathbb{K}^3 \setminus \{(0,0,0)\}$, de aquí tenemos la siguiente definición.

Definición. El *espacio proyectivo bidimensional sobre* $\mathbb{K}$ el cual denotamos como $\mathbb{P}^2_{\mathbb{K}}$, está definido como el conjunto de clases de equivalencia de tripletas (X,Y,Z), con X,Y,Z elementos de $\mathbb{K}$, donde al menos uno de ellos es distinto de cero, dada por la relación en (2.1).

Notemos que las clases de equivalencia sólo dependen de las proporciones de X, Y y Z, es por ello que las clases de equivalencia los escribimos como $(X:Y:Z)$ y las cuales llamaremos *punto proyectivo*. En otras palabras, el espacio proyectivo bidimensional sobre el campo $\mathbb{K}$ es el conjunto,

$$\mathbb{P}^2_{\mathbb{K}} = \left\{(X:Y:Z) : (X,Y,Z) \in \mathbb{K}^3 \setminus \{(0,0,0)\}\right\}. \tag{2.2}$$

A continuación definimos lo que tomaremos como una ecuación de Weierstrass.

Definición. Una *ecuación de Weierstrass* es una ecuación homogénea de grado tres[1] de la forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.3}$$

con $a_1, a_2, a_3, a_4, a_6 \in \overline{\mathbb{K}}$, donde $\bar{\mathbb{K}}$ es la cerradura algebraica del campo $\mathbb{K}$. .
La ecuación de Weierstrass se le llama *suave* o *no-singular* si para todo punto proyectivo $P = (X:Y:Z) \in \mathbb{P}^2_{\mathbb{K}}$ que satisface

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0, \tag{2.4}$$

al menos una de las derivadas parciales $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ y $\frac{\partial F}{\partial Z}$ es distinta de cero en P, lo que equivale a decir que en la curva determinada por la ecuación de Weierstrass hay una recta tangente en el punto P. En caso contrario, esto es, si cada una de las derivadas parciales $\frac{\partial F}{\partial X}$, $\frac{\partial F}{\partial Y}$ y $\frac{\partial F}{\partial Z}$ se anulan en P tanto el punto P como la ecuación se les llama *singulares*. Cabe mencionar que como la ecuación (2.4) es homogénea entonces no depende del representante de la clase del punto proyectivo.

Si consideramos un punto proyectivo $(X:Y:Z)$ con $Z \neq 0$, entonces tenemos que $(X:Y:Z) = (X/Z : Y/Z : 1)$; a estos puntos se les conoce como *puntos "finitos" en* $\mathbb{P}^2_{\mathbb{K}}$. Sin embargo, si $Z = 0$, entonces dividiendo entre Z se podría pensar que resulta ∞ en

[1] Un *polinomio es homogéneo de grado n* si es una suma de términos de la forma $ax^iy^jz^k$, $a \in \mathbb{K}$ con $i+j+k = n$

las dos primeras entradas, X y Y. Así, los puntos de la forma $(X : Y : 0)$ son llamados *"puntos al infinito" en* $\mathbb{P}^2_{\mathbb{K}}$.

Analicemos cuáles de estos puntos al infinito pertenece a la curva elíptica. Si hacemos $Z = 0$ en la ecuación (2.3) se obtiene $X = 0$. Así, los puntos al infinito que pertenecen a la curva elíptica tienen la forma $(0 : Y : 0)$ con Y distinto de cero. De ahí que $(0 : 1 : 0)$ sea el único punto al infinito en la curva. Escribiremos $\mathcal{O}$ para hacer referencia a este punto.

Una manera de identificar los puntos del plano afín con los puntos proyectivos finitos es de la siguiente forma, consideremos el plano afín bidimensional definido como

$$\mathbb{A}^2_{\mathbb{K}} := \mathbb{K} \times \mathbb{K}.$$

Tenemos una función inclusión $i : \mathbb{A}^2_{\mathbb{K}} \hookrightarrow \mathbb{P}^2_{\mathbb{K}}$ definida por $(x, y) \longmapsto (x : y : 1)$. Así podemos ver los puntos del plano proyectivo como la unión de puntos del plano afín con los puntos al infinito. Cabe mencionar que el espacio proyectivo también se puede ver como

$$\begin{aligned}
\mathbb{P}^2_{\mathbb{K}} &= \{(x : y : 1) : (x, y) \in \mathbb{K}\} \cup \{(x : y : 0) : (x, y) \in \mathbb{K}\}, \\
&= \{(x : 1 : y) : (x, y) \in \mathbb{K}\} \cup \{(x : 0 : y) : (x, y) \in \mathbb{K}\}, \\
&= \{(1 : x : y) : (x, y) \in \mathbb{K}\} \cup \{(0 : x : y) : (x, y) \in \mathbb{K}\}.
\end{aligned}$$

De esta manera se pueden tomar cualesquiera de estas representaciones, por comodidad trabajaremos con representaciones de la forma $(x : y : 1)$.

Ahora podemos ver lo que significa la intersección en el punto al infinito de dos rectas paralelas en el espacio afín. Para ello, consideremos dos rectas no verticales con ecuaciones

$$y = mx + b_1 \quad \text{y} \quad y = mx + b_2 \quad \text{con} \quad b_1 \neq b_2,$$

donde sus ecuaciones homogéneas están dadas por $y = mx + b_1 z$, y $y = mx + b_2 z$, respectivamente. Resolviendo simultáneamente las ecuaciones obtenemos que $z = 0$ y $y = mx$.
Dado que no todas las entradas pueden ser cero entonces $x \neq 0$. Por tanto, resulta que el punto de intersección es de la forma

$$(x : mx : 0) = (1 : m : 0).$$

De manera similar cuando se tiene dos rectas verticales, esto es, $x = c_1$ y $x = c_2$, con $c_1 \neq c_2$. Observemos que y puede tomar cualquier valor, en particular, tomemos $y = b_1 z$ y

$y = b_2 z$, con $b_1 \neq b_2$. A partir de esto último obtenemos que $z = 0$, de donde se tienen los puntos $(c_1, y, 0)$ y $(c_2, y, 0)$. Como buscamos puntos de intersección entonces los puntos previos deben estar relacionados, esto es, $(c_1, y, 0) \sim (c_2, y, 0)$, lo cual implica que $c_1 = c_2$, esto contradice el hecho que c_1 y c_2 son distintos. Por tanto $c_1 = c_2 = 0$. Así, el punto de intersección es $(0 : 1 : 0)$.
Como se puede observar, en ambos casos se obtienen un punto al infinito.

Definición. Una *curva elíptica* E es el conjunto de todas las soluciones en $\mathbb{P}^2_{\mathbb{K}}$ de una ecuación de Weierstrass suave.

Usando coordenadas no homogéneas (afines) $x = X/Z$, $y = Y/Z$, la ecuación (2.3) se puede escribir como la siguiente

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.5}$$

Así, podemos redefinir una curva elíptica de la siguiente manera con $\bar{\mathbb{K}}$ es la cerradura algebraica del campo $\mathbb{K}$.

Definición. Una *curva elíptica* E es el conjunto de soluciones de la ecuación (2.5) en el plano afín $\mathbb{A}^2(\overline{\mathbb{K}}) = \overline{\mathbb{K}} \times \overline{\mathbb{K}}$ junto con un punto al infinito $\mathcal{O}$. Si $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ entonces se dice que E está definida sobre $\mathbb{K}$ y escribimos esto como $E/\mathbb{K}$.

Por otro lado, si E está definida sobre $\mathbb{K}$ el conjunto de $\mathbb{K}$-*puntos racionales de* E, que escribimos como $E(\mathbb{K})$, es el conjunto de todos los puntos cuyas entradas están en $\mathbb{K}$ junto con el punto $\mathcal{O}$. A menos que se indique lo contrario cuando se mencione a los puntos de una curva elíptica nos referiremos a los $\mathbb{K}$-puntos racionales de la curva elíptica en el plano afín y el punto al infinito $\mathcal{O}$.

A continuación mostramos algunos ejemplos de curvas elípticas considerando distintos campos.

Ejemplo 2.1. Considerando el campo de los números reales $\mathbb{R}$ y una curva elíptica con ecuación $y^2 = x^3 - 2x + 2$, donde $a_1 = a_2 = a_3 = 0$, $a_4 = -2$ y $a_6 = 2$. La gráfica de esta curva con x en el intervalo $[-2, 3]$ se ve como en la siguiente figura. Cabe mencionar que como el punto al infinito no se puede representar en coordenadas de la forma (x, y) no se puede representar en la gráfica. En este caso se puede pensar que dicho punto se encuentra en donde termina el eje y.

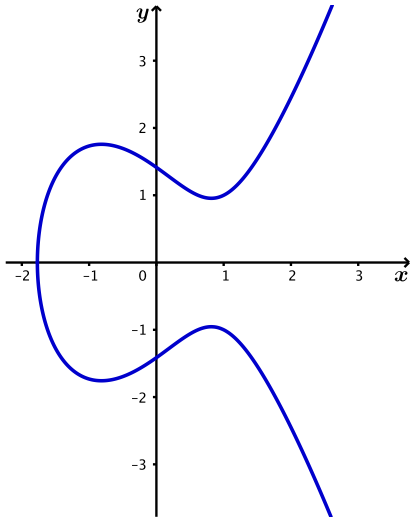

Figura 2.1: Gráfica de una curva elíptica definida en el campo de los números reales dada por la ecuación $y^2 = x^3 - 2x + 2$ con x en el intervalo $[-2, 3]$.

Ejemplo 2.2. Ahora consideremos el campo $\mathbb{Z}_{19}$ y una curva con ecuación $y^2 = x^3+11x+9$. Los $\mathbb{Z}_{19}$-puntos racionales son los siguientes cuya gráfica se muestra en la Figura 2.2.

$\mathcal{O}$,	$(0, 3)$,	$(0, 16)$,	$(2, 1)$,	$(2, 18)$,	$(6, 5)$,	$(6, 14)$,	$(7, 7)$,	$(7, 12)$,
$(8, 1)$,	$(8, 18)$,	$(9, 1)$,	$(9, 18)$,	$(10, 6)$,	$(10, 13)$,	$(11, 6)$,	$(11, 13)$,	$(12, 8)$,
$(12, 11)$,	$(14, 0)$,	$(16, 5)$,	$(16, 14)$,	$(17, 6)$,	$(17, 13)$,	$(18, 4)$,	$(18, 15)$.	

Tabla 2.1: Puntos racionales de la curva dada por la ecuación $y^2 = x^3 + 11x + 9$ definida en el campo $\mathbb{Z}_{19}$.

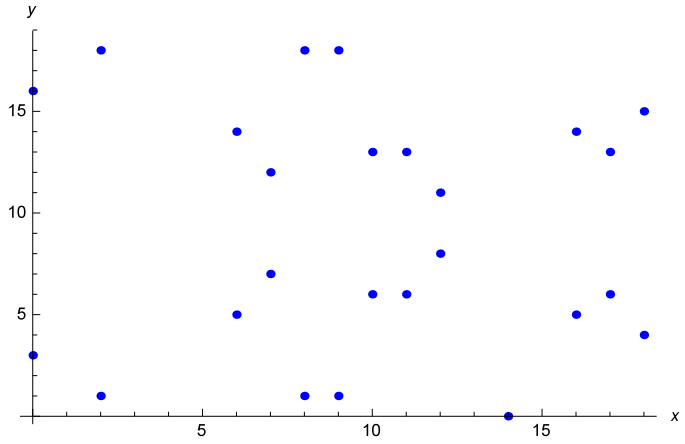

Figura 2.2: Gráfica de los puntos racionales de la curva elíptica definida sobre el campo $\mathbb{Z}_{19}$ dada por la ecuación $y^2 = x^3 + 11x + 9$.

A continuación damos la definición de isomorfismo de dos curvas elípticas y también se tienen algunos resultados que se enuncian sin demostración en [23], los cuales relacionan

dos curvas elípticas mediante isomorfismos, esto es, determinan cuándo dos curvas son isomorfas.

Definición. Dos curvas elípticas $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$ dadas por las ecuaciones

$$\begin{aligned} E_1: &\quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ E_2: &\quad y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}, \end{aligned}$$

son isomorfas sobre $\mathbb{K}$, denotada por $E_1/\mathbb{K} \cong E_2/\mathbb{K}$ si y sólo si existen $u, r, s, t \in \mathbb{K}$, $u \neq 0$ tales que el cambio de variables

$$(x, y) \longmapsto (u^2x + r, u^3y + u^2sx + t) \tag{2.6}$$

transforma la curva E_1 en E_2. La relación de isomorfismo es una relación de equivalencia.

Dado que (2.6) transforma E_1 en E_2 tenemos que el cambio de variable

$$\phi : (x, y) \longmapsto (u^{-2}(x - r), u^{-3}(y - sx - t + rs)) \tag{2.7}$$

también transforma la curva E_1 en E_2. Por otro lado, el cambio de variable

$$\varphi : (x, y) \longmapsto (u^2x + r, u^3y + u^2sx + t) \tag{2.8}$$

transforma E_2 en la curva E_1. Considerando el cambio de variable (2.8) y la curva E_1, mediante manipulación algebraica se obtienen las siguientes relaciones.

$$\begin{aligned} u\overline{a_1} &= a_1 + 2s, \\ u^2\overline{a_2} &= a_2 + 3r - a_1s - s^2, \\ u^3\overline{a_3} &= a_3 + a_1r + 2t, \\ u^4\overline{a_4} &= a_4 + 2a_2r + 3r^2 - a_3s - (rs + t)a_1 - 2st, \\ u^6\overline{a_6} &= a_6 + a_4r - a_3t + a_2r^2 - a_1rt + r^3 - t^2. \end{aligned} \tag{2.9}$$

De estas relaciones se obtiene el siguiente teorema.

Teorema 2.1. *Dos curvas elípticas $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$, con ecuaciones como en la definición inmediata anterior, son isomorfas sobre $\mathbb{K}$ si y sólo existen $u, r, s, t \in \mathbb{K}$ con $u \neq 0$ que satisfacen (2.9).*

2.1.1. Operación de grupo

Dado que tenemos un conjunto de puntos racionales que forman una curva elíptica se puede definir en dicho conjunto una operación suma como se describe a continuación.

Sean P y Q puntos racionales de una curva elíptica E sobre un campo $\mathbb{K}$ dada por la ecuación (2.5). La suma de P y Q, $P+Q$ se define como sigue,

i) Si $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$ y $Q \neq -P$, entonces sea R un tercer punto de intersección de la recta $\overline{PQ}$ con la curva elíptica si $P \neq Q$ (ver Figura 2.3) o la recta tangente a la curva en P, si $P = Q$, (ver Figura 2.4). Entonces $P+Q$ se define como el simétrico del punto R, es decir, $P+Q = -R$.

ii) $\mathcal{O} + P = P$, $P + \mathcal{O} = P$ (elemento identidad).

iii) Si $P = (x_1, y_1) \neq \mathcal{O}$, entonces $-P = (x_1, -y_1 - a_1x_1 - a_3)$
En efecto, supongamos que $-P = (x_1, y_2)$. Luego P y $-P$ satisfacen la ecuación (2.5). Esto es, $y_1^2+a_1x_1y_1+a_3y_1 = x_1^3+a_2x_1^2+a_4x+a_6$ y $y_2^2+a_1x_1y_2+a_3y_2 = x_1^3+a_2x_1^2+a_4x+a_6$. Por consiguiente se tiene una ecuación cuadrática en la variable y_2 de la siguiente forma $y_2^2 + (a_1x_1 + a_3)y_2 - (y_1^2 + (a_1x_1 + a_3)y_1) = 0$, cuyas dos raíces son y_1 y y_2. De esta manera se obtiene que $y_1 + y_2 = -(a_1x_1 + a_3)$ o bien $y_2 = -(a_1x_1 + a_3) - y_1$. De aquí que P y $-P$ son los únicos puntos con primera entrada iguales.

iv) Si $Q = -P$, entonces $P + Q = \mathcal{O}$.

v) Si S es otro punto racional de E, se cumple $(P + Q) + S = P + (Q + S)$.

vi) $P + Q = Q + P$.

Podemos notar que las propiedades del inciso i) al v) son las que se le piden a un conjunto en el cual se define una operación para que sea un grupo. Más aún, el inciso vi) nos dice que el grupo es abeliano. Esta afirmación se tiene en el siguiente teorema.

Teorema 2.2. *El par* $(E(\mathbb{K}), +)$ *es un grupo abeliano.*

Demostración. Dada una curva elíptica, de los incisos previos tenemos la cerradura de la suma, la existencia del elemento neutro e inversos aditivos. Una prueba de que la suma es asociativa se presenta en el Apéndice B.También se pueden consultar las referencias [46], [32] para dicha prueba. Con esto tenemos que el par dado es un grupo abeliano. □

Se pueden obtener expresiones algebraicas para esta operación utilizando un método que se conoce como el método de la recta secante y la recta tangente como se muestra a continuación.

Sean P y Q dos puntos racionales de una curva elíptica E sobre un campo $\mathbb{K}$ dada por la ecuación de Weierstrass (2.5). Consideremos la recta L que pasa por los dos puntos racionales y definimos la suma de estos dos como el punto que se obtiene al reflejar respecto al eje x al tercer punto de intersección de L con la curva E. Se tienen dos caso, el primero de ellos es cuando P y Q son puntos racionales distintos y el segundo es cuando son iguales.

Primero, consideremos $P = (x_1, y_1)$, $Q = (x_2, y_2)$ puntos distintos de una curva elíptica. Para ilustrar el proceso a realizar y considerando el campo de los números reales, la siguiente figura (Figura 2.3) ilustra la forma en que se realiza la suma de dos puntos distintos. Donde la ecuación de la curva es $y^2 = x^3 - 2x + 2$.

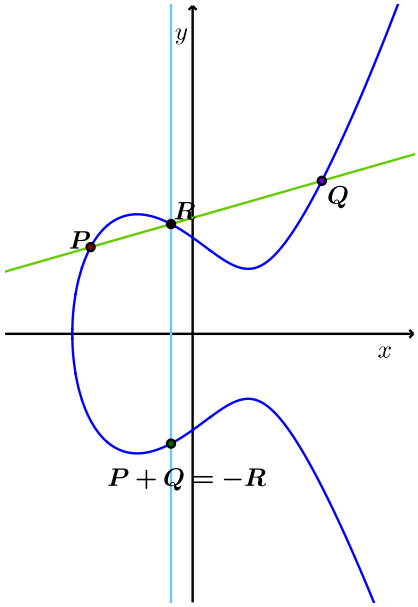

Figura 2.3: Suma de dos puntos diferentes de una curva elíptica.

Consideremos la ecuación de la recta que pasa por P y Q con $Q \neq P$ y $Q \neq -P$ dada por $y - y_1 = m(x - x_1)$, donde m es la pendiente de dicha recta dada por $m = \frac{y_2 - y_1}{x_2 - x_1}$. Por lo tanto, se tiene que $y = m(x - x_1) + y_1$. Ahora la sustituimos en la ecuación implícita de (2.5),

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0, \tag{2.10}$$

para hallar el tercer punto de intersección $R = (x_3, y_3)$ de la recta con la curva elíptica, obteniendo

$$-(m(x-x_1)+y_1)^2 - a_1x(m(x-x_1)+y_1) - a_3(m(x-x_1)+y_1) + x^3 + a_2x^2 + a_4x + a_6 = 0. \tag{2.11}$$

Dado que P, Q y R son tres puntos de intersección entonces son tres raíces de (2.11). Por

tanto, x_1, x_2 y x_3 son tales que $x_1 + x_2 + x_3 = -(a_2 - m^2 - a_1 m)$. De donde se tiene que $x_3 = m^2 + a_1 m - a_2 - x_1 - x_2$ y $y_3 = m(x_3 - x_1) + y_1$.

Por otro lado, supongamos que $P = Q$, en este caso la recta que se considera es la tangente a la curva en el punto racional P. La siguiente figura ilustra el proceso a realizar.

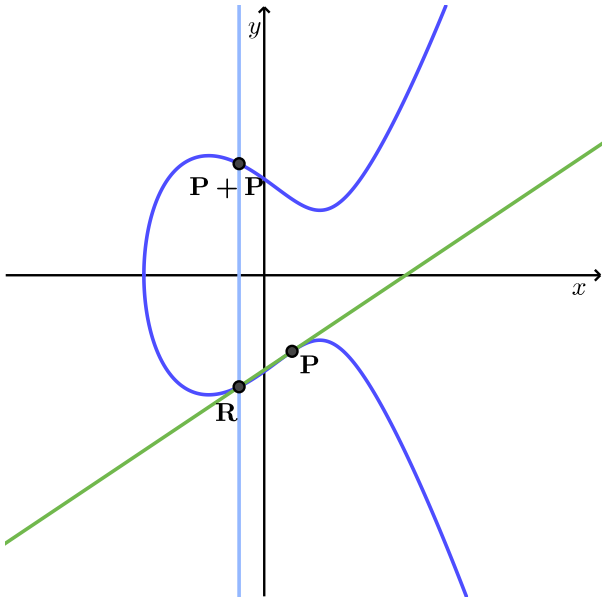

Figura 2.4: Suma de un punto racional de una curva elíptica consigo mismo.

Consideremos la ecuación implícita (2.10), derivando implícitamente e igualando a cero obtenemos que la pendiente de la recta tangente a la curva en el punto $P = (x_1, y_1)$ está dada por $m = (3x_1^2 + 2a_2x_1 - a_1y_1 + a_4)/(2y_1 + a_1x_1 + a_3)$. Las entradas del tercer punto de intersección, R, se obtienen de manera similar al caso previo.

Por lo tanto, las entradas de la suma de $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ puntos racionales de $E(\mathbb{K})$, $P + Q$, están dadas por

$$x = m^2 + a_1 m - a_2 - x_1 - x_2, \qquad y = -(m + a_1)x - b - a_3, \tag{2.12}$$

donde m está dada como

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{si } P \neq Q; \\ (3x_1^2 + 2a_2x_1 - a_1y_1 + a_4)/(2y_1 + a_1x_1 + a_3), & \text{si } P = Q. \end{cases} \tag{2.13}$$

Podemos observar que en la operación suma definida sólo se realizan operaciones váli-

das en un campo. Por tanto, se puede realizar dicha suma.

A continuación mostramos un ejemplo donde se ilustran los $\mathbb{Z}_p$-puntos racionales de una curva elíptica definida sobre un campo finito de característica $p = 71$. Además, se ejemplifica la operación definida mostrando la suma de algunos puntos racionales (ver Tabla 2.3).

Ejemplo 2.3. Sea $p = 71$ y consideremos la ecuación $y^2 = x^3 + 6x + 1$ de una curva elíptica sobre el campo $\mathbb{Z}_p$. Así, $E(\mathbb{Z}_p)$ consta de 77 puntos los cuales son los siguientes y cuya gráfica se muestra en la siguiente figura.

$\mathcal{O}$,	$(0,1)$,	$(0,70)$,	$(1,24)$,	$(1,47)$,	$(4,35)$,	$(4,36)$,	$(6,18)$,
$(6,53)$,	$(8,8)$,	$(8,63)$,	$(9,28)$,	$(9,43)$,	$(11,7)$,	$(11,64)$,	$(13,2)$,
$(13,69)$,	$(14,29)$,	$(14,42)$,	$(15,22)$,	$(15,49)$,	$(16,2)$,	$(16,69)$,	$(18,30)$,
$(18,41)$,	$(19,4)$,	$(19,67)$,	$(20,13)$,	$(20,58)$,	$(21,4)$,	$(21,67)$,	$(22,29)$,
$(22,42)$,	$(26,14)$,	$(26,57)$,	$(27,26)$,	$(27,45)$,	$(28,18)$,	$(28,53)$,	$(31,4)$,
$(31,67)$,	$(35,29)$,	$(35,42)$,	$(37,18)$,	$(37,53)$,	$(38,17)$,	$(38,54)$,	$(40,25)$,
$(40,46)$,	$(42,2)$,	$(42,69)$,	$(44,6)$,	$(44,65)$,	$(45,27)$,	$(45,44)$,	$(47,34)$,
$(47,37)$,	$(48,11)$,	$(48,60)$,	$(50,25)$,	$(50,46)$,	$(52,25)$,	$(52,46)$,	$(53,5)$,
$(53,66)$,	$(54,13)$,	$(54,58)$,	$(56,21)$,	$(56,50)$,	$(60,33)$,	$(60,38)$,	$(61,19)$,
$(61,52)$,	$(63,3)$,	$(63,68)$,	$(68,13)$,	$(68,58)$.			

Tabla 2.2: Puntos racionales de la curva $E(\mathbb{Z}_{71})$ dada por la ecuación $y^2 = x^3 + 6x + 1$, obtenidas utilizando *SAGE*.

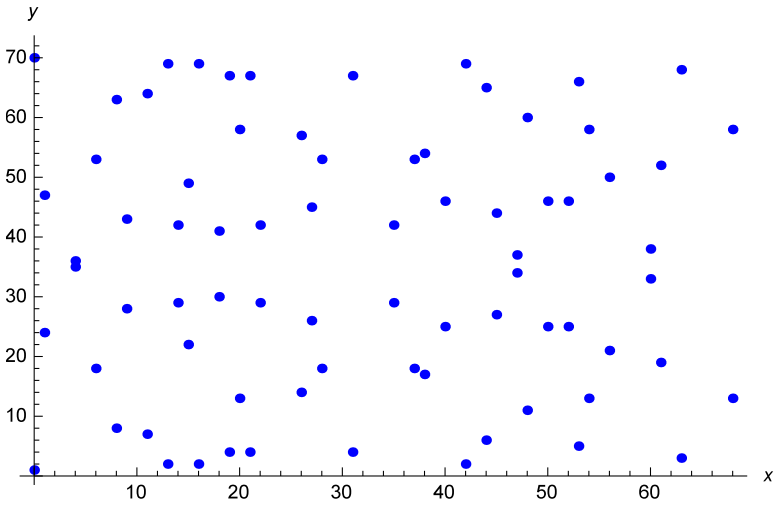

Figura 2.5: Gráfica de los puntos racionales que forman la curva elíptica definida sobre $\mathbb{Z}_{71}$ dada por la ecuación $y^2 = x^3 + 6x + 1$.

P	Q	P+Q
$(28, 18)$	$(28, 18)$	$(63, 68)$
$(28, 18)$	$(63, 68)$	$(40, 46)$
$(63, 68)$	$(63, 68)$	$(40, 25)$
$(40, 25)$	$(40, 46)$	$\mathcal{O}$
$(60, 38)$	$\mathcal{O}$	$(60, 38)$
$\mathcal{O}$	$(35, 42)$	$(35, 42)$

Tabla 2.3: Ejemplos de operación suma definida en una curva elíptica, considerando los puntos racionales de la curva elíptica del Ejemplo 2.3.

En la siguiente sección se describen el discriminante y el j-invariante de una curva elíptica, este último nos da una forma de saber cuándo dos curvas son isomorfas, por lo que mencionamos algo acerca del isomorfismo de estas curvas.

2.1.2. El discriminante y el j-invariante

Sea E una curva elíptica sobre un campo $\mathbb{K}$ definida por la ecuación no homogénea de *Weierstrass* dada por (2.5). Definimos las siguientes cantidades (ver [23]),

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= 2a_4 + a_1a_3, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= d_2^2 - 24d_4, \\ \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \qquad (2.14) \\ j(E) &= c_4^3/\Delta. \qquad (2.15) \end{aligned}$$

A la cantidad Δ se le conoce como *discriminante de la ecuación de Weierstrass* y a $j(E)$ se le conoce como el *j-invariante de E*, si $\Delta \neq 0$.
A continuación tenemos algunos resultados que caracterizan una curva elíptica utilizando el discriminante y el j-invariante de la ecuación de Weierstrass, los cuales se pueden consultar en la referencia [23].

Teorema 2.3. *La ecuación de Weierstrass es no singular si y sólo si $\Delta \neq 0$.*

Cabe mencionar que el discriminante de la curva elíptica del Ejemplo 2.3 es $\Delta = 15 \neq 0$. Otro de los resultados que se obtiene a partir de conocer el j-invariante de las curvas elípticas es el siguiente, que proporciona información acerca de cuándo estas curvas son isomorfas.

Teorema 2.4. *Si dos curvas elípticas $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$ son curvas isomorfas sobre $\mathbb{K}$, entonces $j(E_1) = j(E_2)$. El inverso es verdadero también si $\mathbb{K}$ es un campo algebraicamente cerrado.*

Por otra parte, cabe mencionar que de la ecuación (2.5) se pueden obtener expresiones de curvas elípticas sobre campos de distintas características mediante transformaciones lineales, como se resume en la siguiente tabla y las cuales se describen en las siguientes secciones.

Característica de campo $\mathbb{K}$	$j(E)$	Ecuación de la curva elíptica E
2	$j(E) \neq 0$	$y^2 + xy = x^3 + a_2x^2 + a_6$
	$j(E) = 0$	$y^2 + a_3y = x^3 + a_4x + a_6$
3	$j(E) \neq 0$	$y^2 = x^3 + a_2x^2 + a_6$
	$j(E) = 0$	$y^2 = x^3 + a_4x + a_6$
mayor que 3	$j(E) \neq 0$ $j(E) = 0$	$y^2 = x^3 + a_4x + a_6$

Tabla 2.4: Ecuaciones de curvas elípticas sobre campos de distintas características.

2.2. Curvas sobre campos de característica distinta de 2 y 3

En esta sección describimos las transformaciones que se consideran para obtener una expresión de una curva elíptica sobre un campo de característica distinta de dos y de tres.

Supongamos que E es una curva elíptica dada por la ecuación (2.5) sobre el campo $\mathbb{K}$ de característica distinta de 2. Consideremos el siguiente cambio de variables

$$(x, y) \longmapsto \left(x, y - \frac{a_1}{2}x - \frac{a_3}{2}\right),$$

sustituyendo en la ecuación (2.5) obtenemos una de la forma $y^2 = x^3 + b_2x^2 + b_4x + b_6$. Ahora, supongamos que la característica de $\mathbb{K}$ es distinta de 2 y de 3. Considerando el siguiente cambio de variables

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36},\ \frac{y}{216}\right)$$

y sustituyendo en la ecuación previa obtenemos la ecuación de *Weierstrass* simplificada

$$y^2 = x^3 + ax + b \tag{2.16}$$

Realizando los cambios correspondientes se tiene que el discriminante y el $j-invariante$ están dados como $\Delta = -16(4a^3 - 27b^2)$ y $j(E) = 1728(4a)^3/\Delta$, respectivamente. Dado que se requiere que las curvas sean no singulares entonces $\Delta \neq 0$.

De manera similar al caso general se obtienen las fórmulas de la suma definida, tomando en cuenta las características de los campos, puesto que en caso contrario se podría tener una división entre cero. Por otro lado, de las relaciones (2.9) se obtiene que

$$u^4\overline{a}_4 = a_4 = a, \quad u^6\overline{a}_6 = a_6 = b.$$

Para estas curvas elípticas tenemos el siguiente teorema, que se puede consultar también en la referencia [23].

Teorema 2.5. *Las curvas elípticas* $E_1/\mathbb{K} : y^2 = x^3 + ax + b$ *y* $E_2/\mathbb{K} : y^2 = x^3 + \overline{a}x + \overline{b}$ *son isomorfas sobre* $\mathbb{K}$ *si y sólo si existe* $u \in \mathbb{K}^*$ *tal que* $u^4\overline{a} = a$ *y* $u^6\overline{b} = b$. *Si* $E_1 \cong E_2$ *sobre* $\mathbb{K}$ *entonces el isomorfismo está dado por* $\phi : E_1 \longrightarrow E_2,\ \phi(x, y) \longmapsto (u^{-2}x, u^{-3}y)$ *o equivalentemente* $\phi : E_2 \longrightarrow E_1,\ \varphi(x, y) \longmapsto (u^2x, u^3y)$.

Con los teoremas previos tenemos una forma de saber cuándo dos curvas son isomorfas.

2.3. Curvas sobre campos de característica 2

Dado que estamos interesados principalmente en curvas elípticas sobre campos de característica dos, en la presente sección se deducen las fórmulas para sumar puntos de tales curvas. Más adelante se darán otras propiedades, en particular la manera de hacer aritmética eficiente en los grupos que determinan la familia de curvas mencionada.

Sea $\mathbb{K}$ un campo de característica 2 y consideremos una curva elíptica $E/\mathbb{K}$ dada por la ecuación de *Weierstrass* $E : y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6$. De la igualdad dada en (2.15) se tiene que $j(E) = \overline{a}_1^{12}/\Delta$. Consideremos dos casos para $j(E)$, cuando es igual a 0 y cuando es distinto de 0.
Primero supongamos que $j(E) \neq 0$ esto implica que $\overline{a}_1 \neq 0$. Con el siguiente cambio de variables

$$(x, y) \longrightarrow \left(\overline{a}_1^2x + \frac{\overline{a}_3}{\overline{a}_1},\ \overline{a}_1^3y + \frac{\overline{a}_1^2\overline{a}_4\overline{a}_3^2}{\overline{a}_1^3}\right),$$

la curva E se transforma a la curva cuya ecuación es:

$$E_1/\mathbb{K} : y^2 + xy = x^3 + a_2x^2 + a_6, \tag{2.17}$$

de donde obtenemos que $\Delta = a_6$ y $j(E_1) = 1/a_6$.
Ahora, veamos las fórmulas de la operación suma para este caso, para ello consideremos $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E_1(\mathbb{K})$. De la expresión general para el negativo de un punto racional y dado que estamos en un campo de característica dos tenemos que $-P = (x_1, y_1 + x_1)$. Suponiendo que $Q \neq -P$ y realizando un procedimiento similar al caso general, obtenemos que la pendiente de la recta que pasa por los puntos P y Q está dada por $m = (y_2 - y_1)/(x_2 - x_1) = (y_2 + y_1)/(x_2 + x_1)$. Por otro lado, la pendiente de la recta tangente a la curva en P está dada por $m = x_1 + \frac{y_1}{x_1}$. De aquí que las fórmulas para la suma son las siguientes

- caso $P \neq Q$:

$$x_3 = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + \left(\frac{y_2 + y_1}{x_2 + x_1}\right) + x_1 + x_2 + a_2, \quad y_3 = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + x_3 + y_1.$$

- caso $P = Q$:

$$x_3 = x_1^2 + \frac{a_6}{x_1^2}, \quad y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3.$$

Consideremos el caso $j(E_1) = 0$, esto es $a_1 = 0$. Tomando en cuenta el cambio de variable $(x, y) \longrightarrow (x + \overline{a}_2, y)$, la curva E se transforma a la dada por

$$E_2/\mathbb{K} : y^2 + a_3y = x^3 + a_4x + a_6. \tag{2.18}$$

Por tanto, para $E_2(\mathbb{K})$, tenemos que $\Delta = a_3^4$ y $j(E_2) = 0$.
Para obtener las fórmulas de la operación suma consideremos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ en E_2. Luego, nuevamente de la expresión general del negativo de un punto racional y considerando la característica del campo tenemos que $-P = (x_1, y_1 + a_3)$. Si $Q \neq -P$ y realizando un procedimiento similar al caso previo obtenemos que las pendientes de la recta que pasa por P y Q y la recta tangente a la curva en P, están dadas por

$$m = \frac{y_2 + y_1}{x_2 + x_1} \quad \text{y} \quad m = \frac{x_1^2 + a_4}{a_3},$$

respectivamente. De donde obtenemos que las fórmulas de la suma están dadas por:

- caso $P \neq Q$:

$$x_3 = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + x_1 + x_2, \quad y_3 = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)(x_1 + x_3) + y_1 + a_3,$$

- caso $P = Q$:

$$x_3 = \frac{x_1^4 + a_4^2}{a_3^2}, \quad y_3 = \left(\frac{x_1^2 + a_4}{a_3}\right)(x_1 + x_3) + y_1 + a_3.$$

Una curva que satisface la ecuación (2.17) se conoce como curva *no-supersingular* y su discriminante es $\Delta = a_6$; y una que satisface (2.18) se conoce como *supersingular* y su discriminante es $\Delta = a_3^4$.
Además, pedimos que los discriminantes sean distintos de cero para garantizar la suavidad de la curva, esto es, para garantizar la existencia de una única tangente para cada punto sobre la curva, esto para poder definir la suma de un punto consigo mismo o también conocido como doblado de puntos.

Dado que tenemos un conjunto formado por los puntos racionales de una curva elíptica y una operación definida que satisface las propiedades que se mencionaron en la sección 2.1.1, en la siguiente se enuncian algunas propiedades de grupo que éstos poseen y que serán importantes en el desarrollo del presente trabajo.

2.4. Estructura de grupo

En este apartado se tienen algunos resultados de la estructura de grupo que posee el conjunto de puntos racionales que forma una curva elíptica.

Sea E una curva elíptica definida sobre el campo con q elementos $\mathbb{F}_q$, con $q = p^m$, p primo y la característica de $\mathbb{F}_q$. Escribiremos $\#E(\mathbb{F}_q)$ para hacer referencia al número de puntos racionales de $E(\mathbb{F}_q)$. Si E es una curva dada por la ecuación de *Weierstrass* (ver 2.5) entonces para cada $x \in \mathbb{F}_q$ esta ecuación tiene a los más dos soluciones y tomando en cuenta el punto al infinito resulta que $\#E(\mathbb{F}_q) \leq 2q + 1$.
Tenemos el siguiente par de resultados que se pueden consultar en las referencias [23], [46], [30] con los cuales podemos tener una idea de la cantidad de puntos $\mathbb{F}_q$-racionales que tendrá una curva elíptica.

Teorema 2.6. (Teorema de Hasse) *Dada una curva elíptica E en $\mathbb{F}_q$, el número de puntos racionales $\#E(\mathbb{F}_q)$ está acotado por $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$.*

Lema 2.1. *Existe una curva elíptica $E/\mathbb{F}_q$ tal que $E(\mathbb{F}_q)$ tiene orden $q+1-t$ sobre $\mathbb{F}_q$ si y sólo si se cumple una de las siguientes condiciones.*

i) $t \not\equiv 0 \pmod{p}$ *y* $t^2 \leq 4q$.

ii) m *es impar y una de las siguientes condiciones se cumple*

1) $t = 0$;

2) $t^2 = 2q$ *y* $p = 2$;

3) $t^2 = 3q$ *y* $p = 3$.

iii) m *es par y una de las siguientes condiciones se cumple*

1) $t^2 = 4q$;

2) $t^2 = q$ *y* $p \not\equiv 1 \pmod{3}$;

3) $t = 0$ *y* $p \not\equiv 1 \pmod{4}$.

Notemos que si $q = p$ es un primo entonces existe al menos una curva elíptica E, definida sobre $\mathbb{F}_p$ con $\#E(\mathbb{F}_p) = p + 1 - t$, para cada t que satisface $\mid t \mid \leq 2\sqrt{p}$. En efecto, cuando E varía sobre todas las curvas elípticas definidas en $\mathbb{F}_p$, los valores $\#E(\mathbb{F}_p)$ están distribuidos casi uniformemente en el intervalo de longitud $\sqrt{p}$ centrado en $p+1$. Esta afirmación se precisa en el siguiente teorema la cual fue clave en el algoritmo de factorización de enteros basado en curvas elípticas de *Lenstra* (ver [23]).

Teorema 2.7. *Existen constantes c_1 y c_2 que se pueden calcular de manera eficiente, tales que para cada primo $p > 5$ y para cada subconjunto S de enteros en el intervalo $[p+1-\sqrt{p},\ p+1+\sqrt{p}]$, la probabilidad r_S de que un par aleatorio $(a,b) \in \mathbb{F}_p \times \mathbb{F}_p$ defina una curva elíptica $E : y^2 = x^3 + ax + b$ con $\#E(\mathbb{F}_q) \in S$, está acotada de la siguiente manera,*

$$\frac{\#S - 2}{2\lfloor\sqrt{p}\rfloor + 1} c_1 (\log p)^{-1} \leq r_S \leq \frac{\#S}{2\lfloor\sqrt{p}\rfloor + 1} c_2 (\log p)(\log\log p)^2.$$

Ahora utilizando la cardinalidad del conjunto de puntos racionales de una curva elíptica sobre un campo finito tenemos la siguiente caracterización (ver [23]).
La curva elíptica E es supersingular si p divide a t, donde p es un número primo y $\#E(\mathbb{F}_q) = q + 1 - t$. En caso contrario, es llamada no supersingular.

También tenemos el siguiente resultado referente a las curvas elípticas supersingulares sobre campos de característica 2 o 3.

Si $p = 2$ o $p = 3$, entonces la curva elíptica E es supersingular si y sólo si $j(E) = 0$ (ver [23]).
Por otro lado, del Lema 2.1 se deduce el siguiente corolario.

Corolario 2.7.1. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$ con $q = p^m$ y p número primo. Entonces E es supersingular si y sólo si $t^2 = 0, q, 2q, 3q$ o $4q$.*

Como es común, con $\mathbb{Z}_n$ haremos referencia al grupo cíclico con n elementos. Primero, recordamos un resultado de grupos abelianos, que se puede encontrar en cualquier texto sobre el tema, por ejemplo en [8], [13].
Todo grupo abeliano finito G se descompone como una suma directa de grupos cíclicos, como sigue

$$G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s},$$

donde, $n_{i+1} \mid n_i$, para todo $i = 1, 2, \ldots, s-1$ y $n_s \geq 2$. Más aún, esta descomposición es única en el siguiente sentido: si $G = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$, es otra descomposición de G en suma directa de grupos cíclicos, donde $m_{i+1} \mid m_i$, para cada $t = 1, 2, \ldots, t-1$ y $m_t \geq 2$, entonces $s = t$ y $n_i = m_i$ para cada $i = 1, 2, \ldots, s$. Diremos que G es un grupo abeliano de tipo $(n_1, n_2, \ldots, n_s)$ y rango s.

El siguiente resultado se enuncia en la referencia [23] cuya demostración se puede encontrar en [46].

Teorema 2.8. *El grupo abeliano $E(\mathbb{F}_q)$ de rango 1 o 2 es de tipo (n_1, n_2), es decir, $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, donde $n_2 \mid n_1$ y además $n_2 \mid q-1$.*

El siguiente lema nos da la estructura de grupo de $E(\mathbb{F}_q)$ si E es supersingular (ver [23]).

Lema 2.2. *Sea $\#E(\mathbb{F}_q) = q + 1 - t$.*

i) Si $t^2 = q, 2q$, o $3q$, entonces $E(\mathbb{F}_q)$ es cíclico.

ii) Si $t^2 = 4q$, entonces o $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$ o $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$, dependiendo de si $t = 2\sqrt{q}$ o $t = -2\sqrt{q}$, respectivamente.

iii) Si $t = 0$ y $q \not\equiv 3 \pmod 4$, entonces $E(\mathbb{F}_q)$ es cíclico. Si $t = 0$ y $q \equiv 3 \pmod 4$, entonces o $E(\mathbb{F}_q)$ es cíclico o $E(\mathbb{F}_q) \cong \mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$.

Ahora, escribimos algunos resultados de estructura de grupos de $E(\overline{\mathbb{F}}_q)$. Tenemos que *$E$ es un grupo de torsión*, es decir, para cada punto $P \in E$ existe un entero positivo k tal

que $kP = \mathcal{O}$. El menor entero que satisface esto último se le conoce como *orden de* P. Se puede observar en la Tabla 2.3 que el punto racional $(28, 18)$ tiene orden 7.
Un *k-punto de torsión*, para un entero positivo k, es un punto $P \in E(\overline{\mathbb{F}}_q)$ que satisface $kP = \mathcal{O}$. Con $E(\mathbb{F}_q)[k]$ denotamos el subgrupo de k-puntos de torsión de $E(\mathbb{F}_q)$ con $k \neq 0$. Para ilustrar los resultados previos tenemos los siguientes ejemplos. En el primero, obtenemos la forma que tienen los puntos de orden 2. Además, obtenemos la cardinalidad del conjunto de puntos de una curva elíptica.

Ejemplo 2.4. Consideremos la curva elíptica $E/\mathbb{F}_q$, dada por la ecuación $y^2 = x^3 + ax + b$, donde la característica de $\mathbb{F}_q$ es distinta de 2 y 3. Un punto $P = (x, y) \in E(\mathbb{F}_q)$ tiene orden dos si $P = -P$, esto es, si y es tal que $y = -y$, por tanto $y = 0$. Sean x_1, x_2, x_3 las raíces del polinomio cúbico $x^3 + ax + b$. Como estamos considerando una curva tal que $\Delta \neq 0$, tenemos que las raíces son distintas. Así, el conjunto de 2-puntos de torsión está dado por $E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$.

Para ilustrar mejor el ejemplo previo veamos algunos casos específicos, para ello, trabajamos en campos de enteros módulo un número primo.

Ejemplo 2.5. Consideremos el campo $\mathbb{Z}_7$ y la curva elíptica con ecuación $y^2 = x^3 + 5x + 3$. Recordemos que, para campos de característica distinta de dos y tres, el discriminante está dado por $\Delta = -16(4a^3 + 27b^2)$, el cual es diferente de cero en nuestro caso, por tanto el polinomio cúbico $p(x) = x^3 + 5x + 3$ tiene tres raíces distintas. Veamos si el polinomio $p(x) = x^3 + 5x + 3$, tiene raíces en $\mathbb{Z}_7$. Dado que $\mathbb{Z}_7$ no tiene muchos elementos evaluamos $p(x)$ en cada uno de ellos, obteniendo: $p(0) = 3$, $p(1) = 2$, $p(2) = 0$, $p(3) = 3$, $p(4) = 3$, $p(5) = p(-2) = -1$ y $p(6) = p(-1) = 4$. Por tanto, 2 es la única raíz del polinomio cúbico en $\mathbb{Z}_7$. De aquí que, el polinomio se puede escribir como

$$0 = x^3 + 5x + 3 = (x - 2)(x^2 + 2x + 2).$$

Notemos que $x^2 + 2x + 2$ es un polinomio irreducible sobre $\mathbb{Z}_7$. Por tanto $\langle x^2 + 2x + 2\rangle$ es un ideal maximal (ver Apéndice A) en $\mathbb{Z}_7[x]$ y $\mathbb{K} = \mathbb{Z}_7[x]/\langle x^2 + 2x + 2\rangle$ es un campo cuyos elementos son de la forma $b_0 + b_1 x$ con b_0, $b_1 \in \mathbb{Z}_7$ y el elemento cero es $\langle x^2+2x+2\rangle$ (ver [13]). Como $\mathbb{K}$ es un campo de extensión de grado 2 o bien una extensión del campo $\mathbb{Z}_7$, por el Teorema $5G$ de la referencia [13] el polinomio x^2+2x+2 tiene como raíz $\overline{x} = x+\langle x^2+2x+2\rangle$. En efecto,

$$\begin{aligned}(x + \langle x^2 + 2x + 2\rangle)^2 + 2(x + \langle x^2 + 2x + 2\rangle) + 2 &= x^2 + \langle x^2 + 2x + 2\rangle + 2x + \langle x^2 + 2x + 2\rangle + 2 \\ &= \langle x^2 + 2x + 2\rangle = 0\end{aligned}$$

Así, $\overline{x}$ es raíz del polinomio cuadrático. Ahora, veamos quién es la otra raíz de $p(x)$, para esto, dividimos $x^3 + 5x + 3$ entre $(x-2)(x-\overline{x}) = x^2 - (\overline{x}+2)x + 2\overline{x}$. De donde obtenemos que la otra raíz es $-(2+\overline{x})$. Por tanto, los 2-puntos de torsión de la curva elíptica son

$$\{\mathcal{O}, (2, 0), (\overline{x}, 0), (-(2+\overline{x}), 0)\}.$$

Ejemplo 2.6. Ahora, en el mismo campo como en el ejemplo anterior, consideremos la curva cuya ecuación está dada por $y^2 = x^3 + 3x + 4$. Llamemos $p(x) = x^3 + 3x + 4$ y de manera similar al ejemplo previo, tenemos que el discriminante $\Delta \neq 0$, por tanto $p(x)$ tiene tres raíces distintas. Veamos si $p(x)$ tiene raíces en $\mathbb{Z}_7$. Como, $p(0) = 4$, $p(1) = 1$, $p(2) = 4$, $p(3) = 5$, $p(4) = 3$, $p(5) = 4$ y $p(6) = 0$, se tiene que 6 es una raíz de $p(x)$. Así, $p(x) = x^3+3x+4 = (x-6)(x^2+6x+4)$. Observemos que el polinomio x^2+6x+4 es irreducible sobre $\mathbb{Z}_7$. Por tanto, podemos construir el campo cociente $\mathbb{F} = \mathbb{Z}_7[x]/\langle x^2+6x+4\rangle$. De donde $\alpha = x + \langle x^2 + 6x + 4\rangle$ es también una raíz. Con esto, se deduce que $(x-6)(x-\alpha)$ divide a $p(x)$. Realizando dicho cociente de polinomios obtenemos que $-(6+\alpha)$ es otra raíz. Por lo tanto, los puntos de 2-torsión constituyen el conjunto

$$\{\mathcal{O}, (6,0), (\alpha,0), (-(6+\alpha),0)\}.$$

En los ejemplos que siguen determinamos el número de puntos que satisfacen la ecuación de una curva elíptica dada.

Ejemplo 2.7. Sea q una potencia de un primo impar tal que satisface que $q \equiv 2 \pmod 3$. Consideremos $b \in \mathbb{F}_q$ con $b \neq 0$ y la curva elíptica $E_1/\mathbb{F}_q : y^2 = x^3 + b$. Se tiene que la aplicación $f_b : x \longmapsto x^3 + b$ es una permutación. En efecto, consideremos $x_1, x_2 \in \mathbb{F}_q$ tales que $f_b(x_1) = f_b(x_2)$, esto es, $x_1^3 = x_2^3$. De aquí se cumple que $(x_1^3)^{-r} = (x_2^3)^{-r}$ para r tal que $q = 3r + 2$, puesto que $q \equiv 2 \pmod 3$. Así, para x_1 distinto de cero, $1 = (x_1)^{q-1} = (x_1)^{3r+1}$. Por tanto,

$$\begin{aligned} x_1^{3r}x_1 &= x_2^{3r}x_2 \\ x_1^{-3r}x_1^{3r}x_1 &= x_2^{-3r}x_2^{3r}x_2 \\ x_1 &= x_2 \end{aligned}$$

De donde se concluye que f_b es inyectiva y por tanto suprayectiva. De esta manera tenemos que f_b es una permutación. Por otro lado, se tiene que para cada uno de los $(q-1)/2$ elementos $x \in \mathbb{F}_q$ tales que $x^3 + b$ es un residuo cuadrático (ver Apéndice A, Sección A.3) de $\mathbb{F}_q$ distinto de cero es la primer coordenada de dos puntos de la curva E_1, a saber, tienen

la forma $(x, \pm\sqrt{x^3+b})$, entonces tenemos $q-1$ puntos de tal forma. Los otros puntos de E_1 son $(\sqrt[3]{-b}, 0)$ y $\mathcal{O}$. Por lo tanto, la cardinalidad de los puntos de la curva elíptica es $q+1$. Por el corolario previo tenemos que $t=0$, así que la curva es supersingular. Y por el inciso (iii) del Lema 2.2 las únicas dos posibilidades para el tipo de grupo de $E_1(\mathbb{F}_q)$ son $((q+1)/2, 2)$ y $q+1$, esto es,

$$E_1(\mathbb{F}_q) = \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2 \quad \text{o bien} \quad E_1(\mathbb{F}_q) = \mathbb{Z}_{q+1}.$$

Notemos que el único punto de orden dos es $(\sqrt[3]{-b}, 0)$, por tanto $E_1[2] \cong \mathbb{Z}_2$. Concluimos que $E_1(\mathbb{F}_q)$ es un grupo cíclico de orden $q+1$ puesto que si existe $P \in \mathbb{Z}_{\frac{q+1}{2}}$ tal que $2P = \mathcal{O}$, entonces $E_1(\mathbb{F}_q)[2] \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, lo cual contradice el hecho de que $E_1[2] \cong \mathbb{Z}_2$.

Ejemplo 2.8. Sea q potencia de un primo impar que satisface la congruencia $q \equiv 3 \pmod 4$. Consideremos $a \in \mathbb{F}_q$, con $a \neq 0$ y la curva elíptica $E_2/\mathbb{F}_q : y^2 = x^3 + ax$. En este caso, -1 no es residuo cuadrático en $\mathbb{F}_q$. En efecto, dado que $(q-1) \equiv 2 \pmod 4$, tenemos que $q-1 = 4k+2$, luego $(-1)^{(q-1)/2} = (-1)^{2k+1} = -1$. De donde se concluye que -1 no es un residuo cuadrático. Observemos que $(-x)^3 + a(-x) = -(x^3 + ax)$. Por tanto, para cada $x \in \mathbb{F}_q$ tal que $x^3 + ax \neq 0$, exactamente un elemento de $\{x, -x\}$ es la primer coordenada de dos puntos en $E_2(\mathbb{F}_q)$ esto debido a que -1 no es residuo cuadrático. Si $x \in \mathbb{F}_q$ con $x \neq 0$ que satisface $x^3 + ax = 0$, entonces $(x, 0)$ y $(-x, 0)$ son dos puntos en $E_2(\mathbb{F}_q)$ junto con $(0, 0)$ y $\mathcal{O}$. Así, el total de puntos en $E_2(\mathbb{F}_q)$ es $q+1$. Por tanto, $E_2(\mathbb{F}_q)$ es supersingular.

Por otro lado, se tienen tres puntos de orden dos en $E_2(\mathbb{F}_q)$, a saber, $P_1 = (0, 0)$, $P_2 = (\sqrt{-a}, 0)$, $P_3 = (-\sqrt{-a}, 0)$. Luego, P_2 y P_3 están en $E_2(\mathbb{F}_q)$ si y sólo si $\sqrt{-a} \in \mathbb{F}_q$, esto es, si a es no residuo cuadrático. Por tanto, $E_2(\mathbb{F}_q)$ es cíclico si a es residuo cuadrático en $\mathbb{F}_q$ puesto que $E_2(\mathbb{F}_q)[2] = \{\mathcal{O}, (0, 0)\} \cong \mathbb{Z}_2$. Mientras que $E_2(\mathbb{F}_q)$ es del tipo $(\frac{q+1}{2}, 2)$ si a es no residuo cuadrático, en este caso, se tienen cuatro 2-puntos de torsión, a saber $E_2(\mathbb{F}_q)[2] = \{\mathcal{O}, (0, 0), (\sqrt{-a}, 0), (-\sqrt{-a}, 0)\}$.

En los siguientes ejemplos se muestran casos particulares de los ejemplos previos.

Ejemplo 2.9. Consideremos $q = 11 = 3(3) + 2$ y la curva elíptica definida sobre el campo $\mathbb{Z}_{11}$ dada por la ecuación $E : y^2 = x^3 + 7$. La siguiente tabla muestra los residuos cuadráticos sobre $\mathbb{Z}_{11}$ y de donde se deduce que el conjunto de puntos $\mathbb{Z}_{11}$-racionales de la curva es

$$\{\mathcal{O}, (2, 2), (2, 9), (3, 1), (3, 10), (4, 4), (4, 7), (5, 0), (6, 5), (6, 6), (7, 3), (7, 8)\}.$$

x	0	1	2	3	4	5	6	7	8	9	10
x^3+7	7	8	4	1	5	0	3	9	2	2	6
x^2	0	1	4	9	5	3	3	5	9	4	1

Tabla 2.5: Obtención de puntos $\mathbb{Z}_{11}$-racionales de la curva $y^2 = x^3 + 7$ sobre $\mathbb{Z}_{11}$.

Para este ejemplo específico en la siguiente tabla mostramos los n-puntos de torsión para distintos valores de n. Cabe mencionar que en este caso $E[10] = E[2]$, $E[9] = E[3]$, $E[8] = E[4]$ y $E[11] = E[7] = E[5] = E[1]$.

$$E[1] = \{\mathcal{O}\}, \quad E[2] = \{\mathcal{O}, (5,0)\}, \quad E[3] = \{\mathcal{O}, (3,1), (3,10)\},$$
$$E[4] = \{\mathcal{O}, (2,2), (2,9), (5,0)\}, \qquad E[6] = \{\mathcal{O}, (3,1), (3,10), (5,0), (6,5), (6,6)\}.$$

Tabla 2.6: Ejemplos de los subgrupos de torsión de la curva elíptica definida sobre $\mathbb{Z}_{11}$ dada por la ecuación $y^2 = x^3 + 7$.

Ejemplo 2.10. Nuevamente, consideremos $q = 11 = 4(2) + 3$. El conjunto de puntos $\mathbb{Z}_{11}$-racionales que forman la curva elíptica dada por la ecuación $E : y^2 = x^3 + 5x$ es

$$\{\mathcal{O}, (0,0), (3,3), (3,8), (6,2), (6,9), (7,2), (7,9), (9,2), (9,9), (10,4), (10,7)\}.$$

En este caso, $a = 5$ y como se puede observar en la Tabla 2.5 es un residuo cuadrático, por tanto se tiene sólo un par de 2-puntos de torsión que son $\mathcal{O}$ y $(0,0)$.

Ahora, consideremos $a = -4$, es decir, consideremos la curva elíptica con ecuación $y^2 = x^3 - 4x$. Donde el conjunto de puntos de la curva elíptica es el siguiente

$$\{\mathcal{O}, (0,0), (2,0), (3,2), (3,9), (4,2), (4,9), (6,4), (6,7), (9,0), (10,5), (10,6)\}.$$

Dado que $-a = 4$ es un residuo cuadrático, el conjunto de 2-puntos de torsión consta de cuatro puntos, a saber, $\mathcal{O}$, $(0,0)$, $(2,0)$ y $(9,0)$.

Por otra parte, veamos a qué grupo es isomorfo el grupo de puntos racionales de las curvas elípticas descritas en los dos últimos ejemplos. Para ello, primero consideremos la curva $E_1 : y^2 = x^3 + 7$ del Ejemplo 2.9 sobre el mismo campo. Dado que $E_1[2] = \{\mathcal{O}, (5,0)\}$ y es isomorfo a $\mathbb{Z}_2$, concluimos que $E_1(\mathbb{Z}_{11})$ es un grupo cíclico de orden 12. Por lo tanto, $E_1 \cong \mathbb{Z}_{12}$.

Para el Ejemplo 2.10 y considerando la curva con ecuación $E : y^2 = x^3 + 5x$ tenemos que el orden del grupo es 12. Así, si escribimos $\#E(\mathbb{Z}_q) = q + 1 - t$ y dado que $q + 1 = 12$

obtenemos que $t = 0$. Por el inciso (iii) del Lema 2.2 y dado que $q \equiv 3 \pmod 4$ entonces o $E(\mathbb{Z}_q)$ es cíclico o bien $E(\mathbb{Z}_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$. Dado que 5 es residuo cuadrático concluimos que $E(\mathbb{Z}_{11})$ es cíclico y además de orden 12. De manera similar a la curva del Ejemplo 2.9 $E(\mathbb{Z}_{11}) \cong \mathbb{Z}_{12}$.

Por último, consideremos la curva $E_2 : y^2 = x^3 - 4x$ del Ejemplo 2.10. Nuevamente por el inciso (iii) del Lema 2.2 y dado que -4 es no residuo cuadrático, $E_2(\mathbb{Z}_{11})$ es del tipo $\left(\frac{q+1}{2}, 2\right)$. Por lo tanto $E_2(\mathbb{Z}_{11}) \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

Dado que ya conocemos a cerca de las propiedades de grupo que tiene el conjunto de puntos racionales de una curva elíptica, en el siguiente capítulo enfocamos nuestro estudio en cómo obtener de manera eficiente el múltiplo escalar de un punto racional utilizando la operación suma definida en las llamadas curvas de Koblitz.

Capítulo 3

Curvas de Koblitz

En este capítulo describimos una forma de obtener el múltiplo escalar de un punto racional de una curva elíptica, como también las representaciones que se le pueden dar a un número entero, entre ellas tenemos la representación binaria, en forma no adyacente, entre otros. La representación en forma no adyacente nos permitirá desarrollar una manera eficiente de obtener dicho múltiplo escalar. Describimos a las curvas conocidas como curvas de Koblitz las cuales, como se ha mencionado anteriormente, serán de nuestro interés en este trabajo. Cabe mencionar que los ejemplos de los algoritmos que se dan en este capítulo se implementaron en el software *SAGE*.

3.1. Múltiplo escalar de un punto racional

En el capítulo anterior se ha descrito una forma de sumar dos puntos racionales distintos y la forma de sumar un punto consigo mismo, lo que nos lleva a definir el múltiplo escalar de un punto racional.

Definición. Sea P un punto racional de una curva elíptica. El *múltiplo escalar de* P digamos k se define como la suma de P consigo mismo k veces, es decir,

$$k \cdot P = \underbrace{P + P + \cdots + P}_{k \text{ veces}}. \tag{3.1}$$

Hay varias formas de obtener el múltiplo escalar de un punto racional, los cuales se pueden obtener mediante las representaciones que se le pueden dar a los escalares.
El método binario utliza la representación binaria de los escalares y es una manera general de calcular el múltiplo escalar, el cual es la versión aditiva del algoritmo de elevar al

cuadrado y multiplicar. Para fines de comparación, a continuación mostramos el algoritmo correspondiente el cual se puede consultar en referencias como ver [43], [28].

Entrada: Entero n, un punto racional P de la curva elíptica
Salida: $Q \leftarrow P$, $R \leftarrow \mathcal{O}$
Mientras $n > 0$, hacer
Si n es impar, entonces $R \leftarrow R + Q$
$Q \leftarrow 2Q$, $n \leftarrow \lfloor n/2 \rfloor$
Salida: R

Algoritmo 2: Método binario para obtener un múltiplo escalar de un punto racional de una curva elíptica.

Describimos algunas formas de obtener el múltiplo escalar de un punto racional de una curva elíptica arbitraria, esto para motivar los algoritmos que se describirán, lo cuales son análogos entre sí. Dentro de los métodos que se utilizan para obtener dicho múltiplo escalar tenemos el método de la ventana (o bien, en inglés window methods) y el método de adición y sustracción, este último se describe a continuación.

Método de adición y sustracción

Como cada número entero tiene una representación binaria, de manera similar se tiene una representación conocida como la forma no adyacente.
El método de adición y sustracción es la técnica básica para obtener múltiplos escalares, que está basado en la forma no adyacente del coeficiente, la cual definimos a continuación (ver [11]).

Definición. Una representación en *forma no adyacente (o NAF por sus siglas en inglés, Non Adjacent Form)* de un entero positivo k es una expresión de la forma

$$k = \sum_{i=0}^{\ell-1} k_i 2^i, \tag{3.2}$$

donde para cada $0 \leq i \leq \ell - 1$, $k_i \in \{0, 1, -1\}$, $k_{\ell-1} \neq 0$ y tiene la propiedad de que no hay dos dígitos consecutivos distintos de cero. Decimos que la longitud de la NAF es ℓ.

Por ejemplo, consideremos $k = 27$, entonces la NAF de k es $27 = 2^5 - 2^2 - 1$, en este caso la longitud de la representación NAF de 27 es 6.
A continuación describimos las propiedades que satisface esta representación NAF, las cuales se pueden consultar también en las referencias [11], [39], [29].

Teorema 3.1. *Sea k un entero positivo.*

1. *k tiene una representación NAF única, la cual escribimos como $NAF(k)$.*

2. *$NAF(k)$ tiene el menor número de dígitos distintos de cero, de cualquier representación binaria con signo de k.*

3. *La longitud de $NAF(k)$ es como máximo una unidad más que la longitud de la representación binaria de k.*

4. *Si la longitud de $NAF(k)$ es ℓ, entonces $2^\ell/3 < k < 2^{\ell+1}/3$.*

5. *La densidad promedio de los dígitos no nulos entre todas las NAF de longitud ℓ es aproximadamente $1/3$.*

La representación descrita previamente se puede obtener de manera eficiente mediante el siguiente algoritmo (ver [39]).

Entrada: Un entero positivo n
Salida: $NAF(n)$
$c \leftarrow n$, $S \leftarrow \{\}$
Mientras $c > 0$ hacer
  Si c impar
    $u \leftarrow 2 - (c \bmod 4)$
    $c \leftarrow c - u$
  Si no
    $u \leftarrow 0$
  Agregar u al inicio de S
  $c \leftarrow c/2$
Salida: S

Algoritmo 3: Representación NAF de un entero positivo.

Para ilustrar el Algoritmo 3, en la Tabla 3.1 mostramos cómo se obtiene la representación de $n = 27$ paso a paso. Donde c es el cociente de dividir entre dos, u los coeficientes de las potencias de 2 en la ecuación (3.2) que se eligen de manera que el siguiente valor de c sea divisible por dos; y S es el vector de 0, 1, o -1 que forman la representación NAF. Como resultado se tiene la sucesión $[1, 0, 0, -1, 0, -1]$ o bien $27 = 2^5 - 2^2 - 1$.

c	u	S
27		
28	−1	$[-1]$
14	0	$[0,-1]$
7		
8	−1	$[-1,0,-1]$
4	0	$[0,-1,0,-1]$
2	0	$[0,0,-1,0,-1]$
1		
0	1	$[1,0,0,-1,0,-1]$

Tabla 3.1: Obtención paso a paso de la representación NAF del entero $n = 27$ utilizando el Algoritmo 3 implementado en el software *SAGE*.

El algoritmo previo se puede modificar de manera que obtengamos uno para la multiplicación escalar, esto es, el método de adición y sustracción, donde el costo del método depende de la longitud ℓ de la representación NAF (ver [39]). El algoritmo es el siguiente.

Entrada: Un entero positivo n y un punto racional P de una curva elíptica
Salida: El punto racional nP
$c \leftarrow n$, $Q \leftarrow \mathcal{O}$, $P_0 \leftarrow P$
Mientras $c > 0$ hacer
Si c impar
$u \leftarrow 2 - (c \text{ mód } 4)$, $c \leftarrow c - u$
Si $u = 1$, entonces $Q \leftarrow Q + P_0$
Si $u = -1$, entonces $Q \leftarrow Q - P_0$
$c \leftarrow c/2$, $P_0 \leftarrow 2P_0$
Salida: Q

Algoritmo 4: Método de adición y sustracción para hallar un múltiplo escalar de un punto racional de una curva elíptica.

Notación. En lo que sigue daremos ejemplos en donde será necesaria la siguiente notación para escribir polinomios, esto con el fin de representar de manera compacta los puntos racionales de una curva elíptica: listamos los coeficientes del polinomio dado, de donde obtenemos una sucesión binaria y formamos bloques de longitud 4. Una vez que se tienen éstos, los representamos en notación hexadecimal, como se muestra en el siguiente ejemplo.

Ejemplo 3.1. Consideremos el polinomio $x^{13} + x^{12} + x^{11} + x^{10} + x^7 + x^5 + x^3 + x + 1$ cuyos coeficientes divididos en bloques de cuatro son 0011 1100 1010 1011. Ahora convirtiendo a la base hexadecimal lo escribiremos como $3CAB \coloneqq x^{13}+x^{12}+x^{11}+x^{10}+x^7+x^3+x^5+x+1$.

Ejemplo 3.2. Retomando la representación NAF de $n = 27$ que se obtuvo en la tabla previa, mostramos un ejemplo del Algoritmo 4. Para ello, consideremos el campo $\mathbb{F}_{2^7}$, una curva elíptica dada por la ecuación $y^2 + xy = x^3 + x^2 + 1$ y un punto racional de dicha

curva $P = (x^2 + x + 1, x^5 + x^4 + x^3 + x)$ o bien utilizando la notación descrita $P = (07, 3A)$. En la siguiente tabla se muestra la forma en que se obtiene 27 veces P, resultando que $27 \cdot (x^2 + x + 1, x^5 + x^4 + x^3 + x) = 27 \cdot P = (9, 55) = (x^3 + 1, x^6 + x^4 + x^2 + 1)$.

c	u	$-P_0$	Q	P_0
27	–1	$(07, 3D)$	$(07, 3D)$	$(1F, 13)$
14				$(7F, 42)$
7	–1	$(7F, 3D)$	$(79, 44)$	$(4B, 35)$
4				$(33, 54)$
2				$(15, 5A)$
1	1		$(09, 55)$	$(53, 03)$

Tabla 3.2: Obtención del múltiplo escalar del punto racional P de $E(\mathbb{F}_{2^7})$ definida por $y^2 + xy = x^3 + x^2 + 1$, con dado por $P : (x^2 + x + 1, x^5 + x^4 + x^3 + x) = (07, 3A)$, mediante el Algoritmo 4 implementado en el software *SAGE*.

En la siguiente sección abordaremos el tema referente a las curvas elípticas propuestas por N. Koblitz, las cuales ofrecen propiedades matemáticas que garantizan tanto la resistencia ante intentos de calcular el logaritmo discreto como eficiencia en la implementación.

3.2. Curvas de Koblitz

Las *curvas anómalas binarias* fueron introducidas por Neal Koblitz en [16] de ahí que también son conocidas como *curvas de Koblitz* (o *curvas ABC*, por sus siglas en inglés Anomalous Binary Curve), son curvas elípticas con coeficientes en $\mathbb{F}_2$ y que son consideradas en un campo $\mathbb{F}_{2^m}$ que es extensión de $\mathbb{F}_2$, en este caso, el grado de extensión m se elige de manera que se genere una gran cantidad finita de puntos racionales sobre la curva logrando así un criptosistema seguro (ver [9]). Las cuales son un caso particular de la ecuación (2.17) y que describimos a continuación.

Definición. Una *curva anómala binaria* es una de las curvas E_0 y E_1 definidas sobre $\mathbb{F}_2$ dadas por la ecuación

$$E_a : y^2 + xy = x^3 + ax^2 + 1, \quad a \in \mathbb{F}_2. \tag{3.3}$$

Escribiremos $E_a(\mathbb{F}_{2^m})$ para hacer referencia al conjunto de puntos $\mathbb{F}_{2^m}$-racionales, que es en donde se realizarán los protocolos de llave pública. Tal grupo se debe elegir de manera que sea computacionalmente difícil resolver el problema de logaritmo discreto de sus elementos. Así, por ejemplo el orden $\#E_a(\mathbb{F}_{2^m})$ debe ser divisible por un número primo grande. Lo ideal sería que $\#E_a(\mathbb{F}_{2^m})$ sea un número primo o que sea producto de un primo grande por un número entero pequeño, esto sólo sucede si m es primo o en otro caso, cuando se tienen subgrupos $E_a(\mathbb{F}_{2^d})$ con d un divisor de m (ver [39]).
Cuando m es un número primo sólo se tiene un divisor propio, a saber, $d = 1$. Así, las

curvas de Koblitz sobre $\mathbb{F}_2$ son $E_0(\mathbb{F}_2) = \{\mathcal{O}, (0,1), (1,0), (1,1)\}$ y $E_1(\mathbb{F}_2) = \{\mathcal{O}, (0,1)\}$. Dado que $d = 1$ siempre es divisor de m, entonces tenemos que $E_a(\mathbb{F}_2)$ siempre es un subgrupo de $E_a(\mathbb{F}_{2^m})$, por tanto el orden $\#E_a(\mathbb{F}_{2^m})$ siempre es divisible por $\#E_a(\mathbb{F}_2)$. De donde tenemos la siguiente definición.

Definición. Una curva de Koblitz E_a tiene un grupo de orden *casi primo* sobre $\mathbb{F}_{2^m}$ si $\#E_a(\mathbb{F}_{2^m}) = hn$, donde n es un primo, h es llamada *cofactor* y está definida como

$$h = \begin{cases} 4, & \text{si } a = 0; \\ 2, & \text{si } a = 1. \end{cases} \tag{3.4}$$

Así, decimos que un entero es *casi primo* si es de la forma $N = h \cdot r$, donde h es igual a 2 o 4 y r es un número primo mayor que 2.

De acuerdo con [39], la cardinalidad de $E_a(\mathbb{F}_{2^m})$ nunca es primo para $m > 1$. A continuación mostramos algunos valores de m menores que 512 para los cuales el número de puntos racionales de las curvas de Koblitz son casi primos (ver [39], [11]).

Los valores de $m \leq 512$ para los cuales $\#E_0(\mathbb{F}_{2^m})$ es cuatro veces un primo son

$m = 5, 7, 13, 19, 23, 41, 83, 97, 103, 107, 131, 233, 239, 277, 283, 349, 409.$

Los valores de $m \leq 512$ para los cuales $\#E_1(\mathbb{F}_{2^m})$ es dos veces un primo son

$m = 3, 5, 7, 11, 17, 19, 23, 101, 107, 109, 113, 163, 283, 311, 331, 347, 359.$

Las curvas de mayor interés en criptografía son las de orden casi primo, por lo que procedemos a definir algunos conceptos.

Definición. Supongamos que $\#E_a(\mathbb{F}_{2^m}) = h \cdot r$ es casi primo. Definimos el *subgrupo principal de* $E_a(\mathbb{F}_{2^m})$ como su subgrupo de orden r.

Es más común realizar operaciones criptográficas en los subgrupos principales que en la curva entera. Tenemos el siguiente resultado que nos da una característica para determinar cuándo un punto racional de la curva está en el subgrupo principal.

Proposición 1. *Supongamos que $\#E_a(\mathbb{F}_{2^m})$ es casi primo y sea P un punto racional en $E_a(\mathbb{F}_{2^m})$. Entonces el punto racional P está en el subgrupo principal si y sólo si $P = hQ$, para algún Q en $E_a(\mathbb{F}_{2^m})$ y h como en la definición anterior.*

La prueba de este resultado se puede encontrar en [39]. Y como consecuencia de la proposición previa se tiene la siguiente que también determina cuándo un punto dado está en el subgrupo principal.

Proposición 2. *Si $a = 1$, entonces un punto racional $P = (x, y)$ está en el subgrupo principal si y sólo si $Tr(x) = 1$. Si $a = 0$, entonces P está en el subgrupo principal si y sólo si $Tr(x) = 0$ y $Tr(y) = Tr(\lambda x)$, donde λ es un elemento que satisface que $\lambda^2 + \lambda = x$ y Tr es la función traza.*

La definición de función traza se recuerda en el Apéndice A. Para realizar la demostración consideremos la ecuación de *Weierstrass* dada por

$$E : y^2 + xy = x^3 + ax^2 + b, \tag{3.5}$$

sobre $\mathbb{F}_{2^m}$. Recordemos que el orden de $E(\mathbb{F}_{2^m})$ siempre es par y divisible por 4 si y sólo si la traza de a es 0 (ver [39]). Además tenemos la siguiente proposición.

Proposición 3. *Sea (x_2, y_2) un punto en $E(\mathbb{F}_{2^m})$. Entonces $(x_2, y_2) = 2(x_1, y_1)$ para algún (x_1, y_1) en $E(\mathbb{F}_{2^m})$ si y sólo si $Tr(x_2) = Tr(a)$.*

Demostración. Considerando la ecuación (3.5) tenemos que $y^2 + xy + x^3 + ax^2 + b = 0$, con $a, b \in \mathbb{F}_{2^m}$ fijos. Ahora dividiendo la ecuación previa entre x^2 y haciendo el cambio de variables $z = y/x$, obtenemos (ver [35], [39]),

$$z^2 + zx + a + \frac{b}{x^2} = 0, \tag{3.6}$$

por el resultado 9 del Apéndice A la ecuación (3.6) tiene solución si y sólo si se cumple que $Tr(x + a + b/x^2) = 0$ y si z_0 es una solución entonces también lo es $z_0 + 1$. Así, dado un punto racional $P = (x_1, y_1)$, de la ecuación de la suma de un punto consigo mismo tenemos que x_2 satisface $x_2 = x_1^2 + \frac{b}{x_1^2}$. Por otro lado, dado que la función traza es lineal y recordando que $-a_1 = a_1$ para todo a_1 elemento de $\mathbb{F}_{2^m}$, entonces $z_1 = x_1/y_1$ debe satisfacer la ecuación (3.6). Por lo tanto, $Tr(x_1^2 + a + b/x^2) = Tr(x_2)$ o equivalentemente $Tr(a) = Tr(x_1^2 + b/x_1^2) = Tr(x_2)$. De aquí que la primera coordenada de cualquier punto de la forma $2P$, con P un punto arbitrario, satisface que $Tr(x) = Tr(a)$, de donde se obtiene el resultado. □

Proposición 4. *Supongamos que a tiene traza 0. Sea (x_4, y_4) un punto de $E(\mathbb{F}_{2^m})$. Entonces*

$$(x_4, y_4) = 4(x_1, y_1), \tag{3.7}$$

para algún (x_1, y_1) en E si y sólo si $Tr(x_4) = 0$ y

$$Tr(y_4) = Tr(\lambda x_4), \tag{3.8}$$

para algún $\lambda \in \mathbb{F}_{2^m}$ *que satisface que*

$$\lambda^2 + \lambda = x_4 + a. \tag{3.9}$$

Demostración. Supongamos primero que (3.7) se satisface para algún (x_1, y_1). Tomando $(x_2, y_2) = 2(x_1, y_1)$, entonces tenemos que $(x_4, y_4) = 2(x_2, y_2)$. Así, de la Proposición 3, se deduce que $Tr(x_4) = Tr(x_2) = 0$. Ahora sea

$$\lambda := x_2 + \frac{y_2}{x_2}, \tag{3.10}$$

entonces de la fórmula de doblado de puntos racionales se satisface (3.9) y

$$y_4 := x_2^2 + (\lambda + 1)x_4. \tag{3.11}$$

De aquí se tiene que $Tr(y_4) = Tr(x_2^2 + (\lambda + 1)x_4) = Tr(x_2^2) + Tr(\lambda x_4) + Tr(x_4)$. Dado que $Tr(x_2^2) = Tr(x_2)$ y $Tr(x_4) = Tr(x_2) = 0$, se cumple (3.8).
Por el contrario, supongamos que $Tr(x_4) = 0$ y que se satisface (3.8) para algún λ que es raíz de (3.9). Entonces (3.8) se cumple para cualquier solución λ de (3.9). Se deduce de la Proposición 3 que $(x_4, y_4) = 2(x_2, y_2)$, para algún (x_2, y_2) en $E(\mathbb{F}_{2^m})$. Se concluye que se cumple (3.10). Además, como (3.11) se satisface, entonces $y_4 + \lambda x_4 = x_2^2 + x_4$. De donde se obtiene que $Tr(x_2^2) = 0$ y también que $Tr(x_2) = 0$. Nuevamente, por la Proposición 3, $(x_2, y_2) = 2(x_1, y_1)$, para algún (x_1, y_1) en $E(\mathbb{F}_{2^m})$. Así, $(x_4, y_4) = 4(x_1, y_1)$. □

Con todo esto, se tiene la prueba de la Proposición 2. Por tanto, verificar si un punto está en el subgrupo principal es esencialmente gratis cuando $a = 1$, en cambio para $a = 0$, el costo es de una multiplicación de campo (ver [39]).

Por otro lado, tenemos que la operación central de esquemas criptográficos basados en curvas elípticas es la multiplicación escalar, operación análoga a la exponenciación en grupos multiplicativos (ver [4]). A continuación describimos la forma en que se define la multiplicación escalar en el grupo formado por el conjunto de puntos racionales de una curva elíptica junto con la operación definida en este mismo.

Dado que las curvas de Koblitz están definidas sobre $\mathbb{F}_2$ tienen la siguiente propiedad: *Si* $P = (x_1, y_1)$ *es un punto en* $E_a(\mathbb{F}_{2^m})$ *entonces también lo está el punto* (x_1^2, y_1^2). *Además, se puede verificar que (ver [39]),*

$$(x^4, y^4) + 2(x, y) = \mu \cdot (x^2, y^2), \tag{3.12}$$

para todo (x, y) *en* $E_a(\mathbb{F}_{2^m})$, *donde* $\mu = (-1)^{1-a}$.

La relación (3.12) se puede reescribir de manera más sencilla haciendo uso del endomorfismo de Frobenius, τ, sobre $E_a(\mathbb{F}_{2^m})$ (ver [9]),

$$\tau(x, y) := (x^2, y^2), \quad \text{para } (x, y) \in E_a(\mathbb{F}_{2^m}), \tag{3.13}$$

$$\tau(\mathcal{O}) := \mathcal{O}, \tag{3.14}$$

como

$$\tau(\tau P) + 2P = \mu\tau P, \quad \text{para todo } P \text{ en } E_a(\mathbb{F}_{2^m}). \tag{3.15}$$

De donde se sigue que doblar un punto racional puede reemplazarse por cálculos que involucren el endormorfismo de Frobenius, es decir, sumar un punto consigo mismo se puede ver como la aplicación del endomorfismo de Frobenius τ a dicho punto racional (ver [9]). Cabe mencionar que τ^ℓ indica hacer actuar ℓ veces dicho endomorfismo sobre el punto racional P.
Como la ecuación (3.15) se cumple para todo punto racional de la curva $E_a(\mathbb{F}_{2^m})$, entonces τ es tal que satisface el polinomio

$$g(\xi) = \xi^2 + 2 - \mu\xi, \tag{3.16}$$

esto es, $g(\tau) = \tau^2 + 2 - \mu\tau = 0$. Resolviendo explícitamente (3.16) tenemos que las soluciones son complejas y son las siguientes

$$\xi_1 = \frac{\mu + \sqrt{-7}}{2} \quad \text{y} \quad \overline{\xi_1} = \frac{\mu - \sqrt{-7}}{2}. \tag{3.17}$$

Ahora, consideremos el anillo de polinomios con coeficientes enteros en la variable ξ, $\mathbb{Z}[\xi]$. Sean $g_1(\xi) = u_{l-1}\xi^{l-1} + u_{l-2}\xi^{l-2} + \cdots + u_1\xi + u_0 \in \mathbb{Z}[\xi]$ y P un punto racional de E_a. Combinando el endomorfismo de Frobenius con la multiplicación escalar, se puede hacer actuar la función $g_1(\tau)$ en P (ver [11]), como sigue:

$$\begin{aligned} (g_1(\tau))(P) &= \left(u_{l-1}\tau^{l-1} + u_{l-2}\tau^{l-2} + \cdots + u_1\tau + u_0\right)(P), \\ &= u_{l-1}\tau^{l-1}(P) + u_{l-2}\tau^{l-2}(P) + \cdots + u_1\tau(P) + u_0 P. \end{aligned} \tag{3.18}$$

Dado que deseamos obtener una forma eficiente de calcular el múltiplo escalar de un punto racional de E_a, digamos k, la estrategia consiste en hallar para k una expresión de la forma,

$$k = u_n\xi^n + \cdots + u_0 \in \mathbb{Z}[\xi], \tag{3.19}$$

con n y los u_i pequeños, preferentemente que los u_i satisfagan la proposición: $u_i \in \{1, 0, -1\}$

y casi todos cero; esto para después calcular kP haciendo uso de (3.18). Es decir,

$$kP = (k)(P) = u_n\tau^n(P) + \cdots + u_1\tau(P) + u_0P. \tag{3.20}$$

3.2.1. Representación en forma no adyacente

Con el fin de hallar una expresión de la forma como en (3.19) para un número entero, en esta sección veremos cuándo un elemento de $\mathbb{Z}[\xi]$ es divisible por ξ. A partir de esto, definiremos la representación τNAF y las propiedades que satisface.

Como τ es tal que satisface $\xi^2 + 2 = \mu\xi$, cada elemento de $\mathbb{Z}[\xi]$ se podrá identificar con un elemento de la forma $\alpha = a_0 + a_1\xi$, con $a_0, a_1 \in \mathbb{Z}$ (ver [9], [11]), es decir, con elementos de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$. En particular para un entero k que tiene la forma como en (3.19). Empezamos definiendo la norma de α un elemento de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$, como sigue, donde entenderemos por *conjugado de* $\alpha = a_0 + a_1\xi$ como en los números complejos.

Definición. La *norma de* $\alpha = a_0 + a_1\xi \in \mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$ es el número entero que se obtiene al realizar el producto de α con su conjugado. De manera explícita,

$$N(a_0 + a_1\xi) = a_0^2 + \mu a_0 a_1 + 2a_1^2. \tag{3.21}$$

La norma definida previamente posee las propiedades que se enuncian en el siguiente teorema el cual se puede consultar en las referencias [11], [39].

Teorema 3.2. *Sean* $\alpha, \beta \in \mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$. *La función norma satisface las siguientes propiedades,*

i) $N(\alpha) \geq 0$ *y la igualdad se cumple si y sólo si* $\alpha = 0$.

ii) Los únicos elementos de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$ *con norma* 1, *son* 1 *y* -1.

iii) $N(\xi) = 2$ *y* $N(\xi - 1) = h$, *con* h *como en* (3.4).

iv) La función norma es multiplicativa, esto es, $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$, *para todo* $\alpha_1, \alpha_2 \in \mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$.

v) $N(\xi^m - 1) = \#E_a(\mathbb{F}_{2^m})$ *y* $N((\xi^m - 1)/(\xi - 1)) = n$, *con* n *como en* (3.4).

vi) Considerando la distancia de manera similar al plano complejo, esto es, la distancia euclidiana de un número complejo δ *al* 0 *está dada por* $\sqrt{N(\delta)}$, *en este caso tenemos que la desigualdad del triángulo toma la forma* $\sqrt{N(\alpha+\beta)} \leq \sqrt{N(\alpha)} + \sqrt{N(\beta)}$.

vii) $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ *es un anillo euclidiano respecto a la función norma. Esto es, si* $\alpha, \beta \in \mathbb{Z}[\xi]$ *con* $\beta \neq 0$*, existen* $\kappa, \rho \in \mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ *(no necesariamente únicos), tales que* $\alpha = \kappa\beta + \rho$ *y* $N(\rho) < N(\beta)$*.*

Para la demostración de la primera parte del inciso (v) del Teorema 3.2 se puede consultar la referencia [22], en la cual el resultado se obtiene en el desarrollo de una demostración. Para probar la segunda parte, esto es, para $N((\xi^m - 1)/(\xi - 1)) = n$. Como consideramos curvas de Koblitz de orden casi primo, entonces $\#E_a(\mathbb{F}_{2^m}) = h \cdot n$, con n un número primo y h como en (3.4). Por tanto, por la primera parte de este inciso, $N(\xi^m - 1) = \#E_a(\mathbb{F}_{2^m}) = h \cdot n$. Por otro lado, tenemos que $\xi - 1$ divide a $\xi^m - 1$, entonces

$$\xi^m - 1 = (\xi - 1)H(\xi), \tag{3.22}$$

con $H(\xi) = \xi^{m-1} + \xi^{m-2} + \cdots + 1$. Dado que la norma es multiplicativa, se tiene que $h \cdot n = \#E_a(\mathbb{F}_{2^m}) = N(\xi^m - 1) = N(\xi - 1)N(H(\xi)) = h \cdot N(H(\xi))$. De esta manera $N(H(\xi)) = n$. De lo previo y de (3.22) se concluye que $N((\xi^m - 1)/(\xi - 1)) = n$.

La *sucesión de Lucas* es una sucesión de números enteros que facilitan los cálculos que involucran irracionales cuadráticos (ver Apéndice A Sección A.6). En lo que sigue se usará la sucesión de Lucas para los números ξ_1, con ξ_1 como en (3.17) por lo que también se presentan algunas de sus propiedades.

Existen dos sucesiones U_k y V_k asociados a un número cuadrático irracional que difieren en la inicialización de los dos primeros términos de la relación de recurrencia (ver [9]) $L_{k+1} = \mu L_k - 2L_{k-1}$, $k \geq 1$, $\mu = (-1)^{1-a}$, donde a es como en 3.3, esto es, $a \in \mathbb{F}_2$; las cuales para el irracional cuadrático ξ_1 se definen de la siguiente forma

$$\begin{array}{lll} U_0 = 0,\ U_1 = 1 & \text{y} & U_{k+1} = \mu U_k - 2U_{k-1},\ \text{para} \quad k \geq 1; \\ V_0 = 2,\ V_1 = \mu & \text{y} & V_{k+1} = \mu V_k - 2V_{k-1},\ \text{para} \quad k \geq 1. \end{array} \tag{3.23}$$

Estas sucesiones cumplen las siguientes propiedades, los cuales se pueden consultar en la referencia [39].

- Se puede probar por inducción y también pueden probarse directamente resolviendo las relaciones de recurrencia lineales (3.23) de la forma usual que se cumple:

$$\begin{aligned} U_k &= (\xi^k - \overline{\xi}^k)/\sqrt{7}, \\ V_k &= \xi^k + \overline{\xi}^k. \end{aligned} \tag{3.24}$$

  En efecto, reescribiendo U_k tenemos que $U_{k+2} = \mu U_{k+1} - 2U_k$ con $k \geq 0$. Proponemos

una solución de la forma $U_k = cr^k$, entonces $cr^{k+2} = \mu cr^{k+1} - 2cr^k$. De donde $r^2 = \mu r - 2$; igualando a cero y resolviendo obtenemos que las soluciones son ξ_1 y $\overline{\xi}_1$. Dado que estas soluciones son linealmente independientes entonces también lo son ξ_1^k y $\overline{\xi}_1^k$. Por tanto, $U_k = c_1\xi^k + c_2\overline{\xi}^k = c_1\xi + c_2\overline{\xi^k}$. De los valores de U_0 y de U_1 se obtiene que $c_1 = -c_2$ y $c_1 = \frac{1}{\sqrt{-7}}$, de esta manera

$$U_k = \frac{1}{\sqrt{-7}}(\xi^k - \overline{\xi^k}). \tag{3.25}$$

De manera similar se obtiene que $V_k = c_1\xi + c_2\overline{\xi^k}$. Como en este caso $V_0 = 2$ y $V_1 = \mu$ entonces $c_1 = c_2 = 1$. Por tanto

$$V_k = \xi^k + \overline{\xi^k}. \tag{3.26}$$

- Si $\theta = \tan^{-1}(\sqrt{7})$, entonces (3.24) se puede escribir como

$$\begin{aligned} U_k &= \mu^{k+1}\, 2^{k/2+1}\ \operatorname{sen}(k\theta)/\sqrt{7}, \\ V_k &= \mu^k\, 2^{k/2+1}\ \cos(k\theta). \end{aligned} \tag{3.27}$$

De las propiedades de la norma definida tenemos que $|\xi_1| = \sqrt{\xi_1\overline{\xi_1}} = \sqrt{2}$. Por otro lado, si θ_1 es el argumento de ξ_1 entonces $\tan(\theta_1) = \sqrt{7}/\mu$. Dado que μ puede tomar el valor de 1 o de -1, analizamos el caso en que $\mu = -1$. Por tanto θ_1 es de la forma $\theta_1 = arctan(\sqrt{7}/\mu) + \pi = \mu\, arctan(\sqrt{7}) + \pi = \mu\theta + \pi$, por ser $arctan$ una función impar. De aquí que $\xi_1 = \sqrt{2}(\cos\theta_1 + \sqrt{-1}\operatorname{sen}\theta_1)$. De las ecuaciones (3.25) y (3.26) se deducen que $U_k = 2(2^{k/2})\mu^{k+1}\operatorname{sen}(k\theta)/\sqrt{7} = \mu^{k+1}2^{k/2+1}\operatorname{sen}(k\theta)/\sqrt{7}$ y $V_k = (2^{k/2+1})\mu^k\cos(k\theta)$, respectivamente.

- Se puede probar por inducción que $\xi^k = U_k\xi - 2U_{k-1}$, para $k \geq 1$.
Multiplicando la ecuación previa por $\overline{\xi^k}$, obtenemos que $U_k^2 - \mu U_k U_{k-1} + 2U_{k-1}^2 = 2^{k-1}$, para $k \geq 1$.

- El orden del grupo $\#E_a(\mathbb{F}_{2^m})$ se puede calcular como $\#E_a(\mathbb{F}_{2^m}) = 2^m + 1 - V_m$.
En efecto, por el inciso (iv) del Teorema 3.2 $N(\xi^m - 1) = \#E_a(\mathbb{F}_{2^m})$. Por otra parte, de la definición de norma se tiene que $N(\xi^m - 1) = (\xi^m - 1)\overline{(\xi^m - 1)}$. De aquí que $N(\xi^m - 1) = (\xi\overline{\xi})^m - (\xi^m + \overline{\xi}^m) + 1$. Utilizando la segunda relación de (3.24) y el hecho de que $N(\xi) = 2$ se concluye que $\#E_a(\mathbb{F}_{2^m}) = 2^m + 1 - V_m$.

Lema 3.1. *El elemento $c_0 + c_1\xi$ de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$ es divisible por ξ si y sólo si c_0 es*

par. Y es divisible por ξ^2 si y sólo si c_0 es par y

$$c_0 \equiv 2c_1 \pmod{4}. \tag{3.28}$$

Demostración. Sean $c_0 + c_1\xi \in \mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ y $\mu = (-1)^{1-a}$. Probemos la primera parte del lema. Para ello, supongamos que $c_0 + c_1\xi$ es divisible por ξ. Entonces existen d_0 y d_1, tales que $c_0 + c_1\xi = (d_0 + d_1\xi)\xi = -2d_1 + (d_0 + \mu d_1)\xi$. De donde se obtiene que c_0 es par. Ahora, supongamos que c_0 es par. Como $\xi^2 + 2 = \mu\xi$, entonces

$$\frac{c_0 + c_1\xi}{\xi} = \frac{(\mu\xi - \xi^2)c_0 + 2c_1\xi}{2\xi} = \frac{\mu c_0 + 2c_1}{2} - \frac{c_0}{2}\xi.$$

A partir de esto concluimos que $c_0 + c_1\xi$ es divisible por ξ. Ahora, probemos la segunda parte. Supongamos que ξ^2 divide a $c_0 + c_1\xi$. Por un lado cada múltiplo de ξ^2 es de la forma $(d_0 + d_1\xi)\xi^2 = (d_0 + d_1\xi)(\mu\xi - 2) = -2d_0 + (d_0\mu - 2d_1)\xi + \mu d_1(\mu\xi - 2) = -2(d_0 + \mu d_1) + (\mu d_0 - d_1)\xi$. Por tanto, $c_0 = -2(d_0 + \mu d_1)$ y $c_1 = (\mu d_0 - d_1)$ son tales que c_0 es par y

$$c_0 - 2c_1 = (-2d_0 - 2\mu d_1) - (2\mu d_0 - 2d_1) = -2d_0(\mu + 1) - 2d_1(\mu - 1).$$

Como $\mu \in \{-1, 1\}$ entonces $\mu + 1 \in \{0, 2\}$ y $\mu - 1 \in \{-2, 0\}$. Así, $2(\mu + 1) \in \{0, 4\}$ y $2(\mu - 1) \in \{-4, 0\}$. De esta manera se concluye que tanto $2(\mu + 1)$ como $2(\mu - 1)$ son congruentes con cero módulo 4.

Por último, supongamos que c_0 es par y que $c_0 \equiv 2c_1 \pmod 4$. Considerando el hecho de que $\xi^2 + 2 = \mu\xi$, tenemos que $2 = \xi(\mu - \xi)$, por tanto $4 = -\xi^2(1 + \mu\xi)$. Luego,

$$\begin{aligned} \frac{c_0 + c_1\xi}{\xi^2} &= \frac{-\xi^2(1 + \mu\xi)(c_0 + c_1\xi)}{4\xi^2} = \frac{-\xi^2(c_0 + (\mu c_0 + c_1)\xi + \mu c_1\xi^2)}{4\xi^2}, \\ &= -\frac{c_0 - 2\mu c_1}{4} - \frac{\mu c_0 + 2c_1}{4}\xi. \end{aligned}$$

Utilizando el hecho de que $\mu^2 = 1$, la igualdad previa se puede escribir como

$$\frac{c_0 + c_1\xi}{\xi^2} = -\frac{c_0 - 2\mu c_1}{4} - \mu\frac{c_0 + 2\mu c_1}{4}\xi. \tag{3.29}$$

De esta forma, si $c_0 \pm 2\mu c_1 \equiv 0 \pmod 4$ entonces ξ^2 divide a $c_0 + c_1\xi$. □

Para ilustrar el resultado previo consideremos $\mu = 1$, $c_0 = 6$ y $c_1 = 7$ los cuales satisfacen que $c_0 \equiv 2c_1 \pmod 4$. Utilizando (3.29) tenemos que $\frac{6+7\xi}{\xi^2} = 2 - 5\xi$. Por otro lado, $(2 - 5\xi)\xi^2 = (2 - 5\xi)(\mu\xi - 2) = 2\mu\xi - 4 - 5\mu\xi^2 + 10\xi = 2\mu\xi - 4 - 5\xi + 10\mu + 10\xi = 6 + 7\xi$.

Observemos que el lema previo nos da una forma de saber cuándo un elemento de $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ es divisible por ξ y a partir del cual tenemos la siguiente definición.

Definición. Una representación NAF ξ-ádica o ξNAF de un elemento de $k \in \mathbb{Z}[\xi]$ distinto de cero es una expresión de la forma

$$k = \sum_{i=0}^{\ell-1} u_i \xi^i, \tag{3.30}$$

con cada $u_i \in \{0, 1, -1\}$, $u_{\ell-1} \neq 0$ y dos dígitos consecutivos u_i no son distintos de cero. La longitud de ξNAF es ℓ.

Cabe mencionar que la representación NAF ξ-ádica se puede obtener mediante divisiones sucesivas entre ξ, donde los u_i son los residuos que se obtienen al realizar dicha división. Observemos que la forma de obtener esta representación es análoga a la forma en que se obtiene la expresión binaria de los enteros el cual se logra realizando divisiones sucesivas entre dos. Por otra parte, a partir del resultado previo tenemos el siguiente algoritmo para obtener la representación ξNAF (ver [39]).

Entrada: Enteros r_0, r_1
Salida: Representación ξNAF de $r_0 + r_1\xi$
$c_0 \leftarrow r_0$, $c_1 \leftarrow r_1$, $S \leftarrow \langle\rangle$
Mientras $c_0 \neq 0$ o $c_1 \neq 0$ hacer
  Si c_0 impar
    $u \leftarrow 2 - (c_0 - 2c_1) \pmod 4$
    $c_0 \leftarrow c_0 - u$
  Si no
    $u \leftarrow 0$
  Agregar u al inicio de S
  $(c_0, c_1) \leftarrow (c_1 + \mu c_0/2,\ -c_0/2)$
Salida: S

Algoritmo 5: Representación ξNAF de $r_0 + r_1\xi$, con r_0 y r_1 números enteros.

Ejemplo 3.3. Considerando nuevamente $n = 27$, en este caso, se escribiría de la forma $27 + 0 \cdot \xi$. Utilizando el algoritmo previo se tiene la sucesión $1, 0, 1, 0, 0, -1, 0, 0, 0, -1, 0, -1$. Por tanto, de acuerdo con (3.30) se tiene que ξNAF de 27 es $\xi^{11} + \xi^9 - \xi^6 - \xi^2 - 1$.

Observemos que el Algoritmo 5 se puede realizar debido a que sólo se tienen las operaciones suma y producto. Por otro lado, a partir del siguiente lema tenemos la unicidad de representación ξNAF.

Lema 3.2. *Sea α un elemento de $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$. Entonces sólo una de las siguientes afirmaciones se cumple*

1. *α es divisible por ξ,*
2. *$\alpha \equiv 1 \pmod{\xi^2}$,*
3. *$\alpha \equiv -1 \pmod{\xi^2}$.*

Demostración. Sea $\alpha = c_0 + c_1\xi$ un elemento de $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$. Si c_0 es par entonces por el Lema 3.1 tenemos que ξ divide a α. Ahora, si c_0 es impar entonces ya sea que $c_0 + 1$ o que $c_0 - 1$ satisface la ecuación (3.28). Así, nuevamente por el Lema 3.1 obtenemos que ξ^2 divide a $\alpha \pm 1$. Por tanto, $\alpha \equiv \pm 1 \pmod{\xi^2}$. □

De lo anterior y por el Algoritmo 5 garantizan la existencia y unicidad de la representación ξ-NAF. El siguiente resultado cuya prueba se encuentra en [39], nos da la densidad de números distintos de cero en la representación ξNAF de un elemento de $\mathbb{Z}[\xi]$ distinto de cero.

Proposición 5. *La densidad promedio entre las representaciones NAF ξ-ádicas de longitud ℓ está dada por*

$$\frac{2^{\ell}(3\ell - 4) - (-1)^{\ell}(6\ell - 4)}{9(\ell - 1)(2^{\ell} - (-1)^{\ell})}, \tag{3.31}$$

y por lo tanto asintóticamente es $1/3$.

Con este resultado tenemos que a lo más la tercera parte de la representación ξ-NAF es distinta de cero. De acuerdo con la referencia [9], por medio del ξNAF es posible construir un algoritmo para obtener el múltiplo escalar donde doblar un punto racional se reemplaza por una acción de Frobenius, el cual se puede utilizar para realizar de manera eficiente la suma de un punto racional P de una curva de Koblitz $E_a(\mathbb{F}_{2^m})$ consigo mismo tantas veces como se desee. Dicho algoritmo lo describimos a continuación (ver [39]).

Entrada: Un entero n, un punto P en $E_a(\mathbb{F}_{2^m})$
Salida: nP
$Q = \mathcal{O}$; $P_0 = P$;
$tn = \xi NAF(n)$ (o bien , $tn = \sum_{i=0}^{\ell-1} u_i \xi^i$) (vía 5)
Para cada i desde 0 a $\ell - 1$, hacer
Si $u_i == 1$, entonces $Q = Q + P_0$
Si $u_i == -1$, entonces $Q = Q - P_0$
$P_0 = \tau(P_0)$
Salida: Q

Algoritmo 6: Suma de un punto racional P consigo mismo n veces utilizando la representación ξ-NAF de n.

De esta manera se tiene una suma de la forma
$(k)(P) = (u_{\ell-1}\tau^{\ell-1} + \cdots + u_1\tau + u_0)(P) = u_{\ell-1}\tau^{\ell-1}(P) + \cdots + u_1\tau(P) + u_0(P)$.

A continuación mostramos algunos ejemplos de las sumas realizadas haciendo uso de los algoritmos previos, mencionando el tiempo de ejecución de los mismos en el software *SAGE*. En las Tablas 3.3 y 3.4 se muestran los resultados de múltiplos escalares de puntos racionales de curvas de Koblitz considerados en distintos grados de extensión que fueron obtenidos mediante dos métodos, a saber, el método binario que utiliza la representación binaria de los escalares junto con sumas y doblados de puntos racionales; y el método de adición y sustracción utilizando la representación ξNAF de los escalares. Cabe mencionar que la notación que se utiliza es la que se expone en el Ejemplo 3.1.

m	Punto	Escalar	Tiempo de ejecución con representación	
			Binaria	ξ-NAF
$a = 0$				
5	$x : 1F$ $y : 19$	7228	0.0045409355163574215	0.005641815185546875
7	$x : 7A$ $y : 25$	9621	0.0065252227783203125	0.006990623474121094
13	$x : 36DD3$ $y : 70F2$	9631	0.019952564239501952	0.012538881301879882
19	$x : 0B2BF$ $y : 16BD3$	8822	0.04337620735168457	0.0200229549407959
23	$x : 5DB422$ $y : 6B69DA$	2038	0.05904321670532227	0.03652124404907227
41	$x : 11C62991922$ $y : BD9058649A$	3423	0.1859287738800049	0.08968300819396972
83	$x : 1549D89F43204E7F93B71$ $y : 4435F47BB2C31456DDDEA$	7298	0.6263691902160644	0.3558107852935791
97	$x : 629D0FDF16C9F0F061C43A49$ $y : 95B5D463DE9DA961714808D8$	1255	0.8987803936	0.44836101532
103	$x : 754F28929DF20C6BE4D37BE22E$ $y : 44B619BB17E7241522E6A27A63$	3046	1.1535387992858888	0.5784142017364502
131	$x : 18E9E0435B568D5B56ECCFF9EF8037DA8$ $y : 322AED26669D666B9E5842F3EEBA9BBA8$	3495	1.856601619720459	0.8213678359985351

Tabla 3.3: Ejemplos de los tiempos de ejecución de los métodos binario y ξ-NAF para la multiplicación escalar con parámetro de la curva $a = 0$, los cuales fueron obtenidos mediante la implementación de los algoritmos 5 y 6 en el software *SAGE*.

m	Punto	Escalar	Tiempo de ejecución con representación	
			Binaria	ξ-NAF
$a = 1$				
5	$x : 1D \quad y : 1B$	9247	0.004696369171142578	0.005458127975463867
7	$x : 6E \quad y : 78$	8278	0.005950681686401367	0.005472145080566406
11	$x : 387 \quad y : 675$	9695	0.015240755081176758	0.010235481262207032
17	$x : 1FA9A \quad y : 197AD$	5043	0.03550271987915039	0.02885483741760254
19	$x : 3C8B7 \quad y : 7FF0C$	6312	0.036911630630493165	0.019169683456420897
23	$x : 1CD93F \quad y : 6E606D$	5183	0.06116719245910644	0.03385716438293457
101	$x : 14496DB03A659C6BBB66818521$ $y : 1BEEB2E74072542B0A943204DF$	4002	1.0309635639190673	0.5466420173645019
107	$x : DE2605FE67B34E054CEBFC05A7$ $y : 254FB77CDB495795323FAE2864D$	1757	1.182300615310669	0.5558903694152832
109	$x : 15A9BF95E1FEC8D2D49AA92736F3$ $y : 13495D84C822A87F73BCB3896AA2$	4000	1.1221933841705323	0.49723243713378906
113	$x : 129AC4134305F276FCCB1D42AC5D8$ $y : 2326437BD8E0C7E32F3F40C2A48E$	3918	1.3530833721160889	0.5318639755249024
163	$x : 43C6BF8797AB1A7F076821D7ABD55BE895DCC5DF9$ $y : 53988B631EBDB434518EF001F3896FAC487638F4A$	4549	2.2232872009277345	0.9308852195739746

Tabla 3.4: Ejemplos de los tiempos de ejecución de los métodos binario y ξ-NAF para la multiplicación escalar con parámetro de la curva $a = 1$, los cuales fueron obtenidos mediante la implementación de los algoritmos 5 y 6 en el software *SAGE*.

En los ejemplos previos se puede observar que entre mayor es el grado de extensión del campo considerado, se nota más la eficiencia del método que utiliza la representación ξ-NAF de los escalares respecto al método binario.
De los ejemplos mostrados anteriormente y algunos adicionales se concluye que el método para la multiplicación escalar utilizando curvas de Koblitz con la representación ξ-NAF es aproximadamente dos veces más rápido comparado con el método binario. Además, se realizó la comparación de los tiempos de ejecución de estos algoritmos con los que ya tiene implementado el software *SAGE*, los cuales fueron considerablemente más pequeños. De aquí se tiene una motivación para seguir investigando formas de obtener más eficiencia. En parte esta diferencia en rapidez de cálculo también puede estar motivada por una mayor habilidad de implementación de parte del equipo de *SAGE* y no sólo la parte matemática del algoritmo empleado.

A continuación tenemos algunas definiciones, resultados y algoritmos, los cuales se pueden consultar en la referencia [39]. Se espera que con esto se logre reducir más el tiempo de cálculo para sumar un punto consigo mismo un número arbitrario finito de veces.

3.2.2. Reducción modular en $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$

Lo que describimos a continuación consiste en generalizar la noción de reducción modular en el anillo de los enteros $\mathbb{Z}$ (ver [39]). Para ello, consideremos enteros c y d, con $d > 1$, si deseamos reducir c módulo d, es decir, deseamos hallar un entero ρ, tal que $\rho \equiv c \pmod{d}$, donde el entero ρ se puede obtener mediante división entera, como sigue.

Definamos para λ un número real $Round(\lambda) := \lfloor \lambda + 1/2 \rfloor$, entonces $\rho = c - kd$, donde $k := Round(c/d)$. También definimos la parte fraccionaria de λ como

$$((\lambda)) := \lambda - Round(\lambda). \tag{3.32}$$

Utilizando la parte fraccionaria de c/d, el proceso de reducción modular se puede describir como $\rho = d\left(\left(\frac{c}{d}\right)\right)$. De la definición (3.32), tenemos que $|((\lambda))| < 1/2$.

Para la generalización de la reducción modular en el anillo $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ primero se extienden las definiciones de redondeo y parte fraccionaria de λ. Para ello λ se considera de la forma $\lambda = \lambda_0 + \lambda_1\xi$, con λ_1 y λ_2 números reales. Este redondeo se puede realizar mediante el Algoritmo 7 (ver [39]), lo cual escribiremos como $(q_0, q_1) = Round(\lambda_0, \lambda_1)$, o bien $q_0 + q_1\xi = Round(\lambda_0 + \lambda_1\xi)$ y la parte fraccionaria de λ se define de manera similar como en (3.32).

Entrada: Números reales λ_0, λ_1 que definen a λ, con $\lambda := \lambda_0 + \lambda_1\xi$
Salida: Números reales q_0, q_1 que especifican a $q_0 + q_1\xi := Round(\lambda)$

$f_0 \leftarrow Round(\lambda_0)$, $f_1 \leftarrow Round(\lambda_1)$
$\eta_0 \leftarrow \lambda_0 - f_0$, $\eta_1 \leftarrow \lambda_1 - f_1$, $h_0 \leftarrow 0$, $h_1 \leftarrow 0$, $\eta \leftarrow 2\eta_0 + \mu\eta_1$
Si $\eta \geq 1$
    Si $\eta_0 - 3\mu\eta_1 < -1$, $h_1 \leftarrow \mu$
    Si no $h_0 \leftarrow 1$
Si no
    Si $\eta_0 + 4\mu\eta_1 \leq 2$, $h_1 \leftarrow \mu$
Si $\eta < -1$
    Si $\eta_0 - 3\mu\eta_1 \geq 1$, $h_1 \leftarrow -\mu$
    Si no $h_0 \leftarrow -1$
Si no
    Si $\eta_0 + 4\mu\eta_1 < -2$, $h_1 \leftarrow -\mu$
$q_0 \leftarrow f_0 + h_0$, $q_1 \leftarrow f_1 + h_1$
Salida: q_0, q_1

Algoritmo 7: Redondeo de $\lambda := \lambda_0 + \lambda_1\xi$, con λ_0 y λ_1 números reales.

Ejemplo 3.4. Sea $\lambda = 97.34568 + 30.6723\xi$. Utilizando la forma de redondeo dado en el

Algoritmo 7, se tiene que si $\mu = 1$, el vecino más cercano a λ es $\lambda_r = 97 + 31\xi$ y cuando $\mu = -1$, $\lambda_r = 98 + 31\xi$.

De manera análoga a la división de enteros consideremos un dividendo $\gamma = c_0 + c_1\xi$ y un divisor $\delta = d_0 + d_1\xi$ en $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$. Deseamos hallar un cociente $\kappa = q_0 + q_1\xi$ y un residuo $\rho = r_0 + r_1\xi$ de tal manera que $\gamma = \kappa\delta + \rho$ y tal que ρ sea de norma lo más pequeña posible. Para lograr esto, se obtiene κ mediante el redondeo de γ/δ y después resolvemos para ρ, esto es, $\frac{\gamma}{\delta} = \frac{\gamma\overline{\delta}}{N(\delta)} = \frac{g_0}{N(\delta)} + \frac{g_1\xi}{N(\delta)}$. De esta manera hallamos κ vía el Algoritmo 7 y obtenemos ρ mediante $\rho = \gamma - \kappa\delta$. El siguiente algoritmo nos da una forma de realizar la división en $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$ paso a paso (ver [39]).

Entrada: Dividendo $\gamma = c_0 + c_1\xi$ y el divisor $\delta = d_0 + d_1\xi$
Salida: Cociente $k = q_0 + q_1\xi$ y un residuo $\alpha = r_0 + r_1\xi$
$g_0 \leftarrow c_0d_0 + \mu c_0d_1 + 2c_1d_1$, $g_1 \leftarrow c_1d_0 - c_0d_1$
$N \leftarrow d_0^2 + \mu d_0d_1 + 2d_1^2$
$\lambda_0 \leftarrow g_0/N$, $\lambda_1 \leftarrow g_1/N$
$(q_0, q_1) \leftarrow Round(\lambda_0, \lambda_1)$
$r_0 \leftarrow c_0 - d_0q_0 + 2d_1q_1$, $r_1 \leftarrow c_1 - d_1q_0 - d_0q_1 - \mu d_1q_1$
Salida: q_0, q_1, r_0, r_1

Algoritmo 8: División en $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$.

Se puede observar del algoritmo previo que si obviamos el cociente y que sólo nos devuelva el residuo, se tiene un algoritmo que nos da la reducción modular. Esto es, nos devolvería $\rho = r_0 + r_1\xi$ que es congruente con γ módulo δ.

Ejemplo 3.5. Sean $\gamma = 25 + 13\xi$ y $\delta = 6 + 9\xi$ dos elementos de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$. Luego, utilizando el algoritmo previo con $\mu = 1$, obtenemos que la norma de δ es 252. El cociente y residuo que se obtienen al dividir γ entre δ son $3 + (-\xi)$ y $-11 + \xi$, respectivamente, es decir, $25 + 13\xi = (3 - \xi)(6 + 9\xi) + (-11 + \xi)$.

En la siguiente sección se dan algunos resultados los cuales apoyan la reducción de la longitud de la representación ξNAF.

3.3. Representación ξNAF reducida

En esta sección definimos la representación ξNAF reducida y se aplica al problema de multiplicación escalar eficiente de un punto racional de una curva de Koblitz.

Definición. Sea G un conjunto de puntos racionales de una curva de Koblitz y supongamos que γ y ρ son elementos de $\mathbb{Z}[\xi]/\langle\xi^2 - \mu\xi + 2\rangle$, tales que $(\gamma)(P) = (\rho)(P)$, para todo $P \in G$. Entonces decimos que $\xi NAF(\gamma)$ *y* $\xi NAF(\rho)$ *son equivalentes respecto a* G.

Según la referencia [39] esta terminología surge a partir del hecho de que para multiplicar un punto P de G por γ se puede utilizar ya sea $\xi NAF(\gamma)$ o bien $\xi NAF(\rho)$. El siguiente resultado da una condición de cuándo se dice que dos representaciones ξNAF son equivalentes respecto a un conjunto $G := E_a(\mathbb{F}_{2^m})$ de $\mathbb{F}_{2^m}$-puntos racionales de E_a.

Proposición 6. *Si γ y ρ son dos elementos de $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ con $\gamma \equiv \rho \ (mód\ (\xi^m - 1))$, entonces $(\gamma)(P) = (\rho)(P)$, para todo P en $E_a(\mathbb{F}_{2^m})$. Así, $\xi NAF(\gamma)$ y $\xi NAF(\rho)$ son equivalentes con respecto a $E_a(\mathbb{F}_{2^m})$.*

Demostración. Sea $P = (x, y)$ un punto arbitrario de $E_a(\mathbb{F}_{2^m})$. Aplicando el automorfismo de Frobenius m veces obtenemos que $\tau^m P = (x^{2^m}, y^{2^m})$. Como x y y son elementos de $\mathbb{F}_{2^m}$ y por el Teorema A.4 tenemos que $x^{2^m} = x$ y $y^{2^m} = y$, por tanto

$$\tau^m P = P. \tag{3.33}$$

Dado que P se eligió de manera arbitraria entonces (3.33) se cumple para todo P en $E_a(\mathbb{F}_{2^m})$. De donde se deduce que $(\tau^m - 1)(P) = \mathcal{O}, \ \ \forall P \in E_a(\mathbb{F}_{2^m})$. Por hipótesis tenemos que $\gamma \equiv \rho$ (mód $(\xi^m - 1)$), entonces existe un $k \in \mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ tal que $\gamma = \rho + k(\xi^m - 1)$. Así, $(\gamma)(P) = (\rho)(P) + (k(\tau^m - 1))P = (\rho)(P) + (k)(\mathcal{O}) = (\rho)(P) + \mathcal{O} = (\rho)(P), \ \ \forall P \in E_a(\mathbb{F}_{2^m})$. Por tanto, $(\gamma)(P) = (\rho)(P)$, para todo P en $E_a(\mathbb{F}_{2^m})$. □

Notemos que la proposición previa da la equivalencia en el grupo formado por los puntos racionales de una curva de Koblitz, pero se pueden restringir las hipótesis para obtener la equivalencia en el subgrupo principal, como en los siguientes resultados.

Proposición 7. *Sea P un punto del subgrupo principal de una curva de Koblitz de orden casi primo y definamos δ como*

$$\delta = \frac{\xi^m - 1}{\xi - 1}. \tag{3.34}$$

Entonces $(\delta)(P) = \mathcal{O}$.

Demostración. Por la Proposición 1 existe $Q \in E_a$ tal que $P = hQ$. Como se cumple que $(\tau^m - 1)P = \mathcal{O}$ para todo $P \in E_a$, en particular para Q. Así, $(\tau^m - 1)Q = \mathcal{O}$. Entonces $(\delta(\tau - 1))(Q) = \mathcal{O}$. Por tanto, $\mathcal{O} = \delta(\tau - 1)(\overline{\tau - 1})Q = (\delta N(\tau - 1))(Q) = (\delta)(hQ) = \delta P$. Donde $\overline{\tau - 1}$ representa el conjugado de $\tau - 1$. □

Teorema 3.3. *Sea P un punto del subgrupo principal de una curva de Koblitz de orden casi primo y definamos δ como en la proposición anterior. Si γ y ρ son elementos de $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ con $\gamma \equiv \rho \ \ (mód\, \delta)$, entonces $(\gamma)(P) = (\rho)(P)$. Así, $\xi NAF(\gamma)$ y $\xi NAF(\rho)$ son equivalentes con respecto al subgrupo principal.*

Demostración. Como $(\tau^m - 1)P = \mathcal{O}$ para todo punto racional P de una curva de Koblitz, en particular se cumple para P en el subgrupo principal. Por hipótesis tenemos que $\gamma \equiv \rho \pmod{\delta}$, entonces existe un k en $\mathbb{Z}[\xi]/\langle \xi^2 - \mu\xi + 2\rangle$ tal que $\gamma = \rho + k\delta$. Por tanto, $(\gamma)(P) = (\rho)(P) + (k)(\delta P)$. Por la Proposición 7 $(\gamma)(P) = (\rho)(P) + (k)(\mathcal{O}) = (\rho)(P)$. Así, $(\gamma)(P) = (\rho)(P)$. □

Con lo anterior ya podemos proceder a dar la definición de la representación ξNAF reducida sobre las curvas de Koblitz.

Definición. Supongamos que $E_a(\mathbb{F}_{2^m})$ tiene orden casi primo y que r es el orden del subgrupo principal. Sean n un entero positivo menor que $r/2$ y δ como en (3.34).
Definimos la representación *NAF ξ-ádica reducida de n* como $R\xi NAF(n) := \xi NAF(\rho)$, donde $\rho := n \pmod{\delta}$.

De acuerdo con la definición y teorema previos se concluye que $R\xi NAF(n)$ y $\xi NAF(\rho)$ son equivalentes respecto al subgrupo principal de $E_a(\mathbb{F}_{2^m})$. De esta manera $R\xi NAF(n)$ puede ser utilizado en lugar de $\xi NAF(n)$ para la multiplicación escalar en el subgrupo principal (ver [39]).
El siguiente teorema cuya demostración se puede consultar en [39] conduce a que esta última es una elección más eficiente. Antes de enunciar el resultado recordemos que el peso de Hamming de un vector es el número de sus entradas distintas de cero.

Teorema 3.4. *El peso promedio de Hamming entre las representaciones ξNAF reducidas de longitud ℓ es $m/3$.*

Además, al reemplazar $NAF(n)$ por $R\xi NAF(n)$ se elimina el doblado de puntos racionales y se mantiene constante el número de sumas de puntos racionales. De esta manera se obtiene aritmética eficiente sin utilizar doblado de puntos racionales, lo que se mencionaba en la parte introductoria de este capítulo.

3.3.1. Multiplicación escalar en curvas de Koblitz

Una vez que se tienen las herramientas a utilizar para la multiplicación escalar en curvas de Koblitz, a saber el análogo del método binario utilizando $R\xi NAF$, describimos los algoritmos para obtener la representación $R\xi NAF$ como para la multiplicación escalar.

El siguiente algoritmo da una forma de calcular la reducción de un entero n módulo δ, el cual será necesario para poder describir la forma de obtener la representación $NAF\xi$-ádica reducida (ver [39]).

Entrada: Entero n
Parámetros de la curva: $m,\ a,\ s_0,\ s_1,\ r$
Salida: Enteros $r_0,\ r_1$ que especifican $r_0 + r_1\xi := n \pmod{(\xi^m - 1)/(\xi - 1)}$
$d_0 \leftarrow s_0 + \mu s_1$
$\lambda_0 \leftarrow s_0 n/r$
$\lambda_1 \leftarrow s_1 n/r$
$(q_0,\ q_1) \leftarrow Round(\lambda_0,\ \lambda_1)$ (vía 7)
$r_0 \leftarrow n - d_0 q_0 - 2 s_1 q_1$
$r_1 \leftarrow s_1 q_0 - s_0 q_1$
Salida: $r_0,\ r_1$

Algoritmo 9: Reducción módulo $\delta = (\xi^m - 1)/(\xi - 1)$.

Ejemplo 3.6. Para ilustrar el algoritmo previo consideremos en $\mathbb{Z}_{2^7}$ con polinomio irreducible $x^7 + x + 1$ una curva de Koblitz con ecuación $y^3 + xy = x^3 + x^2 + 1$. Cabe mencionar que en este caso el número de puntos racionales de la curva es $142 = 2 * 71$ y $\delta = 7 + 2\xi$. De donde se obtienen los siguientes parámetros de la curva $(m, a, s_0, s_1, r) = (7, 1, 9, -2, 71)$ y sea $n = 35$. Utilizando el Algoritmo 9 implementado en el software *SAGE*, obtenemos que 35 es congruente con $3 + \xi$ módulo δ. En efecto,

$$35 = (3 + \xi) + (7 + 2\xi)(4 - \xi) = 31 + 2\xi - 2\xi^2 = 31 + 2\xi - 2\xi + 4 = 35.$$

De acuerdo con [39] el siguiente algoritmo, con el cual se calcula la representación NAF ξ-ádica reducida se obtiene combinando los algoritmos 9 y 5.

Entrada: Entero positivo n
Paramétros de la curva: $m,\ a,\ s_0,\ s_1,\ r$
Salida: Representación $R\xi NAF(n)$
$\rho \leftarrow n \pmod{\delta}$ (vía 9)
$S \leftarrow \xi NAF(\rho)$ (vía 5)
Salida: S

Algoritmo 10: Representación NAF ξ-ádica reducida.

Ejemplo 3.7. Consideremos nuevamente los parámetros de la curva del ejemplo previo. En este caso, tomemos $n = 27$. Utilizando el Algoritmo 10 implementado en el software *SAGE*, en la primera parte obtenemos que 27 es congruente con $-5 + \xi$ módulo $\delta = 7 + 2\xi$. En la segunda parte obtenemos que la representación ξNAF de $-5 + \xi$ es la sucesión $-1, 0, 0, 0, 0, 1$. Como se puede observar a diferencia de la representación ξNAF de 27 en el Ejemplo 3.3 en este caso si quisieramos obtener el múltiplo escalar de un punto racional de la curva dada conviene utilizar la representación ξNAF reducida, puesto que la longitud de la sucesión es menor.

Dado que $\tau P_0 = \tau(x_0, y_0) = (x_0^2, y_0^2)$ donde $P_0 = (x_0, y_0)$, pero si x_0 y y_0 están expresados en base normal, elevar al cuadrado se puede realizar mediante un corrimiento de elementos de su representación vectorial (ver Apéndice A.4.1). A tal rotación lo escribimos como $\sigma[P_0]$. A continuación mostramos un ejemplo de tal rotación en el campo de extensión $\mathbb{F}_{2^5}$, en donde la notación que se utiliza para representar a los elementos de dicho campo se expone en el Ejemplo 3.1.

Ejemplo 3.8. Consideremos el campo $\mathbb{F}_{2^5}$ con polinomio irreducible $x^5 + x^2 + 1$ que se escribe como 25 utilizando la notación mencionada. Sus elementos son

00	02	04	08	10	05	0A	14	0D	1A	11	07	0E	1C	1D	1F
1B	13	03	06	0C	18	15	0F	1E	19	17	0B	16	09	12	01

Tabla 3.5: Elementos del campo $\mathbb{F}_{2^5}$ con polinomio irreducible $x^5 + x^2 + 1$.

Un generador de la base normal es $08 = x^3$ y la base generada es $\{08, 0A, 0E, 1E, 13\}$. Ahora para ejemplificar la rotación tomemos $P = 0D$ un elemento de $\mathbb{F}_{2^5}$. El cuadrado de P es $P^2 = 1B$. Sus representaciones en base normal son $(0, 0, 0, 1, 1)$ y $(1, 0, 0, 0, 1)$, respectivamente. Como podemos observar el cuadrado se obtiene mediante el corrimiento de coordenadas, por tanto $P^2 = (1, 0, 0, 0, 1) = \sigma(0, 0, 0, 1, 1) = \sigma[P]$.

La rotación que hemos definido lo utilizamos en el siguiente algoritmo, donde aplicamos la NAF ξ-ádica para obtener un procedimiento que permite realizar la multiplicación eficiente en el subgrupo principal de $E_a(\mathbb{F}_{2^m})$, el cual se obtiene modificando el Algoritmo 5 como se describe a continuación (ver [39]).

Entrada: Entero positivo n, con $n < r/2$, P punto racional del subgrupo principal
Parámetros de la curva: $m,\ a,\ s_0,\ s_1,\ r$
Salida: nP
Calcular $(r_0, r_1) \leftarrow n \pmod{\delta}$ (vía 9)
$Q \leftarrow \mathcal{O}$, $P_0 \leftarrow P$
Mientras $r_0 \neq 0$ o $r_1 \neq 0$ hacer
  Si r_0 impar entonces
    $u \leftarrow 2 - (r_0 - 2r_1) \pmod 4$, $r_0 \leftarrow r_0 - u$
    Si $u == 1$, entonces $Q \leftarrow Q + P_0$
    Si $u == -1$, entonces $Q \leftarrow Q - P_0$
  $P_0 \leftarrow \tau P_0$ $(== \sigma[P_0])$
  $(r_0, r_1) \leftarrow (r_1 + \mu r_0/2, -r_0/2)$
Salida: Q

Algoritmo 11: Multiplicación escalar en curvas de Koblitz.

Ejemplo 3.9. Considerando nuevamente el campo $\mathbb{F}_{2^5}$ con polinomio irreducible x^5+x^2+1 cuyos elementos se pueden observar en el Ejemplo 3.8 y la curva elíptica con ecuación $E_0: \ y^2 + xy = x^3 + 1$, tenemos que el conjunto de puntos racionales que lo forman junto con el punto al infinito son los siguientes, la notación de los puntos racionales que se utiliza es la que se describe en el Ejemplo 3.1, los cuales se obtuvieron utilizando el software *SAGE*:

(00, 01)	(01, 00)	(01, 01)	(02, 1D)	(02, 1F)	(03, 0C)	(03, 0F)	(04, 12)
(04, 16)	(05, 1A)	(05, 1F)	(07, 18)	(07, 1F)	(09, 14)	(09, 1D)	(0B, 16)
(0B, 1D)	(0C, 05)	(0C, 09)	(0D, 06)	(0D, 0B)	(0F, 16)	(0F, 19)	(10, 09)
(10, 19)	(11, 03)	(11, 12)	(12, 06)	(12, 14)	(15, 07)	(15, 12)	(17, 0B)
(17, 1C)	(18, 0F)	(18, 17)	(1A, 0B)	(1A, 11)	(1B, 0F)	(1B, 14)	(1C, 09)
(1C, 15)	(1F, 06)	(1F, 19)					

Tabla 3.6: Puntos racionales de la curva $y^2 + xy = x^3 + 1$ sobre $\mathbb{F}_{2^5}$.

Como podemos notar el número de puntos racionales de la curva sobre el campo en cuestión es $\#E_0(\mathbb{F}_{2^5}) = 44 = 4 \cdot 11$. Eligiendo de manera arbitraria el punto racional $P = (x^2, x^4 + x) = (04, 12)$, calculamos el múltiplo escalar, $5 \cdot P$, utilizando el algoritmo 11. Para ello, consideramos $\delta = 3 + 2\xi$ y es tal que $N(\delta) = 11$. En este caso $r = 11$ con lo que obtenemos que $s_0 = 1$, $s_1 = -2$. Así, ya contamos con los parámetros necesarios para hacer uso del algoritmo mencionado. En la Tabla 3.7 se muestran los valores que toman los parámetros en cada paso para obtener

$$n \cdot P = 5(x^2, x^4 + x) = 5(04, 12) = (0D, 0B) = (x^3 + x^2 + 1, x^3 + x + 1).$$

r_0	r_1	u	$-P_0$	Q	P_0
1	1				
2	1	−1	$(04,16)$	$(04,16)$	$(10,09)$
0	−1			$(0D,0B)$	
−1	0				
0	0	−1	$(0D,06)$	$(0D,0B)$	$(1B,0F)$

Tabla 3.7: Obtención de un múltiplo escalar del punto racional $P = (x^2, x^4+x) = (04, 12)$ de la curva $y^2+xy = x^3+1$ sobre $\mathbb{F}_{2^5}$, a saber, $5P$, utilizando el Algoritmo 11 implementado en el software *SAGE*.

En el siguiente capítulo hablamos acerca del criptosistema ElGamal y vemos la forma en que utilizan las curvas elípticas en estos mismos. También describimos la forma existente de encajar un mensaje en una curva elíptica y realizamos su modificación para obtener un respectivo encajamiento en las curvas de Koblitz.

Capítulo 4

ElGamal con curvas elípticas

Como se describió en la Sección 1.6 el criptosistema propuesto por el egipcio Taher ElGamal está dado en el grupo multiplicativo $\mathbb{Z}_p^*$. En este capítulo describimos el análogo utilizando curvas elípticas definidas sobre un campo finito $\mathbb{F}_q$ con q elementos. Es por ello que en la primera sección describimos la forma de encajar un mensaje o cadena de caracteres en una curva elíptica primero definida en un campo finito con característica $p > 2$ con p primo y después realizamos algo similar en característica 2 utilizando las curvas de Koblitz; para que a partir de este encajamiento se pueda trabajar mensajes cifrados usando curvas elípticas. Además, mostramos algunos ejemplos de encajamiento y de cifrado implementados en el software *SAGE*.

4.1. Encajamiento

De acuerdo con las referencias [1], [17], [45] y trabajando con una curva elíptica con ecuación de la forma $y^2 = x^3 + ax + b$ definida sobre el campo $\mathbb{Z}_p$ con un número primo $p > 2$ de elementos, existe una manera de encajar una cadena de caracteres en dicha curva como se muestra a continuación.

Consideremos $m = (m_1, m_2, \ldots, m_r)$ un mensaje visto como cadena de números enteros, donde cada m_i, $1 \leq i \leq r$, es menor a un cierto número positivo N; y sea k un número entero positivo lo suficientemente grande de tal manera que la probabilidad de fallo al momento de encajar m_i, para cada $1 \leq i \leq r$ sea de $1/2^k$.
La forma de encajar m en los puntos racionales de una curva elíptica es relacionando cada m_i con un punto racional $P = (x_{m_i}, y_{m_i})$ de dicha curva tal que x_{m_i} esté relacionado con m_i, $1 \leq i \leq r$ y que P sea un punto de la curva. Para esto último al evaluar x_{m_i} en $x^3 + ax + b$ se obtiene $z = x_{m_i}^3 + ax_{m_i} + b$ y se verifica si z es o no residuo cuadrático

(por ejemplo utilizando el criterio de Euler enunciado en el Apéndice A). Si es residuo cuadrático asociamos y_{m_i} con $\sqrt{z}$ y si no repetimos el proceso. El siguiente algoritmo realiza lo descrito previamente donde cada x_{m_i} se toma como $\ell = m_i k + j$, con $0 \leq j \leq k-1$, el cual se puede consultar en las referencias [17], [1]. En la practica se recomienda tomar k en el intervalo $[30, 50]$.

Entrada: Mensaje $m = (m_1, m_2, \ldots, m_r)$, enteros $k \in [30, 50]$ y $N \in \mathbb{N}$
Parámetros de la curva: $a, b \in \mathbb{Z}_p$, p primo
Salida: Encajamiento de m en una curva elíptica
Para cada m_i, $1 \leq i \leq k$ hacer
$\ell = m_i k + j$, $x_{m_i} = \ell$, $z = x_{m_i}^3 + a x_{m_i} + b$
Si z es residuo cuadrático,
$y_{m_i} = \sqrt{z}$
Identificar $m_i \longleftrightarrow P_{m_i}$
Si no
Aumentar j en uno

Algoritmo 12: Encajamiento de un mensaje en una curva elíptica definida sobre $\mathbb{Z}_p$, con p primo impar.

Como se puede observar en el algoritmo previo, para realizar dicho encajamiento se necesitan realizar saltos de tamaño k, de ahí que se deba cumplir la desigualdad $Nk < p$.

A continuación mostramos un ejemplo del algoritmo previo donde consideramos el alfabeto con 26 caracteres, es decir, se utiliza codificación de mensajes, con esto nos estaremos refiriendo a que cada letra de dicho mensaje se identifica con los elementos de $\mathbb{Z}_{26}$ como se muestra en la siguiente tabla.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓
18	19	20	21	22	23	24	25

Tabla 4.1: Codificación de letras.

Ejemplo 4.1. Sea M el mensaje a encajar dado por M = "IREMOS A LA LUNA". Codificando el mensaje obtenemos $[8, 17, 4, 12, 14, 18, 0, 11, 0, 11, 20, 13, 0]$. Notemos que la longitud de dicho mensaje sin tomar en cuenta los espacios es 13. Con el fin de que este ejemplo sea ilustrativo tomamos $k = 13$, esto es, estamos tomando saltos de tamaño

13. Como cada entrada del mensaje codificado es menor que 26 podemos elegir $p = 347 > 26 * 13$.
Consideremos la curva elíptica sobre $\mathbb{Z}_{347}$ dada por la ecuación $y^2 = x^3+91x+204$. Veamos el proceso que se realiza para encajar el primer carácter del mensaje que lo hemos codificado como 8.
Iniciamos tomando $j = 0$, de esta manera se tiene que $\ell = 8 * 13 + 0 = 104$. Evaluamos ℓ en $x^3 + 91x + 204$. Obtenemos que $z = (104)^3 + 91 * 104 + 204$ mód $347 = 189$. Utilizamos el criterio de Euler (ver Sección A.3 del Apéndice A) para ver si z es residuo cuadrático. Luego, $189^{(347-1)/2} = 189^{173} \equiv 346 \not\equiv 1$ mód 347. Concluimos que z no es residuo cuadrático, por tanto aumentamos j en uno y así $\ell = 105$. Similarmente se obtiene que $z = 76$ y que tampoco es residuo cuadrático. Nuevamente aumentamos j en uno, por tanto $\ell = 106$. Con este valor de ℓ obtenemos que $z = 246$, el cual es residuo cuadrático puesto que $246^{173} \equiv 1$ mód 347. A partir del criterio de Euler se obtiene que $246^{(p+1)/4} = 196$ es una raíz, pero también lo es $p - 196 = 151$. Por conveniencia tomamos $y = 151$, de esta manera identificamos I con $(106, 151)$.

Se realiza un procedimiento similar para hallar el resto de los puntos que corresponden al encajamiento de nuestro mensaje, obteniendo como resultado como se muestra a continuación, el cual se obtuvo implementando el algoritmo previo en el software *SAGE*.

(106, 151),	(221, 242),	(53, 276),	(159, 60),	(183, 254),	(238, 204),	(1, 264)
(146, 163),	(1, 264),	(146, 163),	(262, 207),	(172, 228),	(1, 264).	

Tabla 4.2: Encajamiento de *"IREMOS A LA LUNA"* en la curva elíptica sobre $\mathbb{Z}_{347}$ dada por la ecuación $y^2 = x^3 + 91x + 204$, el cual se obtuvo implementando el Algoritmo 12 en el software *SAGE*.

En lo que sigue describimos una nueva forma de realizar algo similar para el caso de característica dos. Para ello, consideremos un mensaje $M = (m_1, m_2, \ldots, m_r)$ y una curva de Koblitz dada por la ecuación (3.3) $E_a : y^2 + xy = x^3 + ax^2 + 1, \quad a \in \mathbb{F}_2$.

Dado que deseamos resolver la ecuación previa tomamos un cierto valor de x en $\mathbb{F}_{2^m}$, digamos x_{m_i} para $1 \leq i \leq r$, entonces al evaluar el lado derecho obtenemos el valor $z := x_{m_i}^3 + ax_{m_i}^2 + 1$. Por tanto, la ecuación previa se puede escribir de la forma

$$y^2 + x_{m_i} y = z. \tag{4.1}$$

Tenemos dos casos, el primero de ellos es cuando x_{m_i} es igual a cero y el segundo es cuando se tiene lo contrario. Considerando el primer caso y dado que estamos en característica dos siempre se tiene solución puesto que la ecuación es de la forma $y^2 = 1$. Por tanto

basta tomar $y = 1$. Ahora, supongamos que x_{m_i} es distinto de cero, por el resultado 9 del Apéndice A la ecuación (4.1) tiene solución si y sólo si $Tr(zx_{m_i}^{-2}) = 0$, la solución se encuentra como se muestra a continuación. Reescribimos (4.1) como $x_{m_i}^{-2}y^2+x_{m_i}^{-1}y+x_{m_i}^{-2}z = 0$. Haciendo $u = x_{m_i}^{-1}y$, la ecuación previa se transforma en una de la forma $u^2 + u + \gamma = 0$, con $\gamma = x_{m_i}^{-2}z$. De acuerdo con la demostración que se presenta en la referencia [21] de que tomando un $\theta \in \mathbb{F}_{2^m}$ fijo con $Tr(\theta) = 1$, este θ existe dado que la función Tr es balanceada; entonces

$$u_0 = \gamma\theta^2 + (\gamma + \gamma^2)\theta^{2^2} + (\gamma + \gamma^2 + \gamma^4)\theta^{2^3} + \cdots + (\gamma + \gamma^2 + \cdots + \gamma^{2^{m-2}})\theta^{2^{m-1}} \tag{4.2}$$

es solución de $u^2 + u + \gamma = 0$. A partir de donde se concluye que las soluciones a la ecuación (4.1) son

$$y = x_{m_i}u_0, \quad \text{y} \quad y = x_{m_i}(u_0 + 1), \tag{4.3}$$

Con lo anterior y dado que trabajamos con curvas de Koblitz tenemos lo que necesitamos para proceder a realizar el encajamiento de un mensaje en estas curvas. Por ello, consideremos un mensaje o cadena de caracteres $M = m_1m_2m_3....m_r$, donde cada m_i con $1 \leq i \leq r$ es un entero menor a un cierto número positivo N. De manera similar al encajamiento con curvas elípticas definidas sobre campos con $p > 2$ elementos, la forma de encajar M es relacionando cada m_i con un punto $P = (x_{m_i}, y_{m_i})$ tal que x_{m_i} esté relacionado con m_i, $1 \leq i \leq k$. Así, al evaluar x_{m_i} en $E_a : y^2 + xy = x^3 + ax^2 + 1$ considerada sobre $\mathbb{F}_{2^m}$ toma la forma $y^2 + x_{m_i}y = z$ como en (4.1). Si tiene solución asociamos y_{m_i} con dicha solución dada por (4.3). Si no, repetimos tal proceso. El siguiente algoritmo realiza lo descrito previamente, donde cada x_{m_i} se toma como $\ell = m_ik + j$, con $0 \leq j \leq k - 1$; nuevamente k es un número entero positivo lo suficientemente grande de tal manera que la probabilidad de fallo al momento de encajar m_i para cada $1 \leq i \leq r$ sea de $1/2^k$.

Entrada: Mensaje $M = (m_1, m_2, \ldots, m_r)$, enteros $k \in [30, 50]$ y N
Parámetros de la curva: $a \in \mathbb{F}_2$
Salida: Encajamiento de M en una curva de Koblitz
Para cada m_i, $1 \leq i \leq k$ hacer
$\ell := m_ik + j$, $x_{m_i} = \ell$
$F : z = x_{m_i}^3 + ax_{m_i}^2 + 1$
Si F tiene solución y,
$y_{m_i} = y$
Identificar $m_i \longleftrightarrow P_{m_i}$
Si no
Aumentar j en uno

Algoritmo 13: Encajamiento de un mensaje en una curva de Koblitz.

A continuación mostramos un ejemplo de procedimiento descrito previamente utilizando el Algoritmo 13 con los datos correspondientes. Cabe mencionar que la notación con la que se trabaja es la expuesta en el Ejemplo 3.1.

Ejemplo 4.2. Considerando nuevamente el mensaje del Ejemplo 4.1 tenemos que su codificación es $[8, 17, 4, 12, 14, 18, 0, 11, 0, 11, 20, 13, 0]$ con 13 entradas. Nuevamente tomamos $k = 13$. Dado que cada entrada es menor que 26, en este caso m tiene que tomar un valor tal que $2^m > 26 * 13 = 338$. Tomamos el primer número entero que lo satisface, esto es, $m = 9$.
Como $\mathbb{F}_{2^9}$ es un campo de extensión del campo $\mathbb{F}_2$ tenemos que el polinomio irreducible es $x^9 + x^4 + 1$ y una base normal de $\mathbb{F}_{2^9}$ sobre $\mathbb{F}_2$ es el siguiente conjunto linealmente independiente generado por x^5,
$\{x^5, x^5 + x, x^5 + x^2 + x, x^5 + x^4 + x^2 + x, x^8 + x^5 + x^4 + x^2 + x, x^8 + x^7 + x^6 + x^5 + x^4 + x,$
$x^8 + x^6 + x^4 + x^3 + x + 1, x^8 + x^3 + 1, x^7 + x^2 + 1\}$,
la cual escrita en la notación mencionada toma la forma

$$\{020, 022, 026, 036, 136, 1F2, 15B, 109, 085\}.$$

Trabajemos con la curva de Koblitz con cardinalidad igual a 508 dada por la ecuación $y^2 + xy = x^3 + 1$.
Para ilustrar el procedimiento a realizar en el encajamiento realizaremos dicho proceso para el primer elemento de la codificación del texto, esto es $m_i = 8$. Como $0 \leq j \leq k - 1$, iniciamos con $j = 0$. De esta forma obtenemos que $\ell = 8 * 13 + 0 = 104 = 104$ mód 2^9. Para verlo como un elemento de $\mathbb{F}_{2^9}$, consideramos su representación binaria, los cuales serán los coeficientes de la base normal. De esta manera se obtiene que $x_8 = x^7+x^4+x^3+x^2+x+1$. Evaluando en la ecuación de la curva, tenemos que $y^2 + x_8 y = x^6 + x^5 + x^3 + x + 1$, o bien

$$y^2 + x_8 y + z_8 = 0, \tag{4.4}$$

donde $z_8 = x^6+x^5+x^3+x+1$. Se requiere resolver la ecuación previa que tiene la forma como en (4.1), por tanto se tiene solución si y sólo si $Tr(z_8 x_8^{-2}) = 0$. Realizando manipulaciones algebraicas se obtiene que $x_8^{-2} = 1 + x^2 + x^4 + x^7 + x^8$ y $z_8 x_8^{-2} = x + x^3 + x^8$, con traza igual a cero, de donde se concluye que la ecuación (4.4) tiene solución.
Hacemos $\gamma = x + x^3 + x^8$,así de acuerdo con (4.2) y tomando $\theta = 1$, obtenemos que $u_0 = \gamma^2 + \gamma^{2^3} + \gamma^{2^5} + \gamma^{2^7}$ o bien $u_0 = x + x^6 + x^8$. Por la ecuación (4.3) las soluciones a la ecuación (4.4) están dadas de la forma $y = x_8 u_0$ y $y = x_8(u_0 + 1)$. En nuestro caso, consideramos $y = x_8(u_0 + 1)$ lo cual resulta que está dada por la expresión $y = x^7 + x^6 + x^4 + x^3 + x^2 +$

$x+1$. Escribiendo esto en la notación mencionada obtenemos que $8 \hookrightarrow (09F, 0DF)$. El resto de los puntos del encajamiento se obtienen realizando un proceso similar, los cuales mostramos a continuación.

$(09F, 0DF)$	$(1A0, 062)$	$(0E2, 0EA)$	$(02F, 118)$	$(1DD, 0D7)$	$(1B4, 024)$	$(000, 001)$
$(01F, 0EF)$	$(000, 001)$	$(01F, 0EF)$	$(081, 1B4)$	$(0CF, 06B)$	$(000, 001)$	

Tabla 4.3: Encajamiento de *"IREMOS A LA LUNA"* en la curva $y^2 + xy = x^3 + 1$ considerada en $\mathbb{F}_{2^9}$, los cuales se obtuvieron mediante la implementación del Algoritmo 13 en el software *SAGE*.

Hasta esta parte hemos visto la forma de realizar multiplicación escalar en curvas elípticas, la manera de encajar un mensaje en dichas curvas y sobre todo en curvas de Koblitz. Falta describir el criptosistema ElGamal utilizando estas curvas lo cual hacemos en la siguiente sección.

4.2. ElGamal

Como en el primer capítulo, supongamos que A y B son dos usuarios y que B desea enviarle un mensaje cifrado a A, sólo que en este caso, desea utilizar el sistema de cifrado ElGamal con curvas elípticas. Entonces lo que A necesita realizar es, primero establecer su llave pública, como sigue (ver [46]):

Elige una curva elíptica E sobre un campo finito $\mathbb{F}_q$ tal que el problema de logaritmo discreto sea intratable en $E(\mathbb{F}_q)$ y un punto racional G de $E(\mathbb{F}_q)$ de orden primo. De manera secreta y aleatoria selecciona un entero a y calcula $P_A = aG$. Así, la llave pública de A es $(E(\mathbb{F}_q), \mathbb{F}_q, G, P_A)$ y la llave privada es a.
Para enviarle un mensaje cifrado a A, B realiza el siguiente proceso de cifrado, mientras que A recupera el mensaje realizando el proceso de descifrado:

Cifrado:
El usuario B debe obtener la llave pública de A, expresar su mensaje como una sucesión finita de puntos racionales $M = (\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_r)$ de la curva elíptica sobre $\mathbb{F}_q$, elegir de manera secreta y aleatoria un entero k y calcular

$$M_1 = kG, \quad M_2 = M + kP_A. \tag{4.5}$$

Por último envía M_1, M_2 a A, es decir, el mensaje cifrado es el par (M_1, M_2).

Descifrado:
El usuario A calcula

$$M = M_2 - aM_1. \tag{4.6}$$

Esto funciona, puesto que $M_2 - aM_1 = (M + kP_A) - a(kP) = M + k(aG) - akG = M$.

De esta manera si un tercero, digamos C, conoce la información pública de A, los puntos racionales M_1 y M_2 y si además puede calcular logaritmos discretos, entonces puede utilizar G y P_A para obtener a, pudiendo descifrar así el mensaje realizando $M_2 - aM_1$. También puede usar G y M_1 para hallar k y así puede calcular $M = M_2 - kP_A$. En cambio si no puede calcular logaritmos discretos entonces no hay forma conocida de obtener M. Cabe mencionar que es importante que B utilice un entero aleatorio k distinto cada vez que envíe un mensaje a A. Lo expuesto previamente se ilustra en el siguiente diagrama.

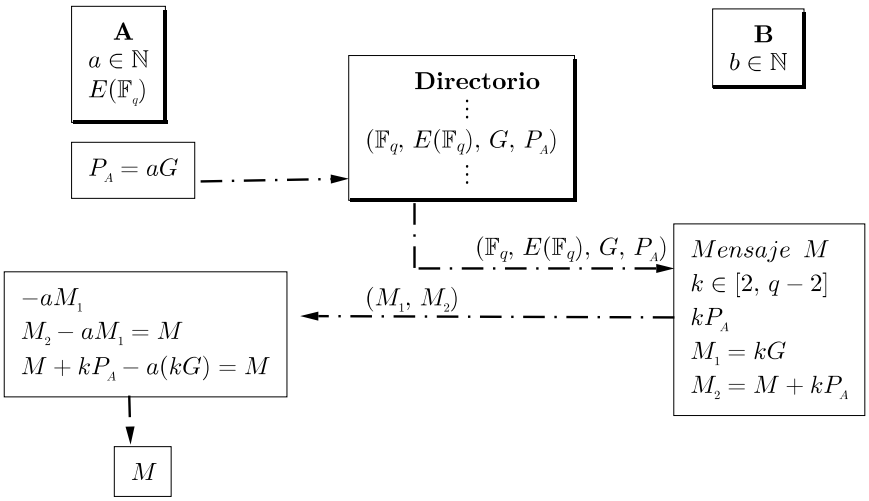

Figura 4.1: Diagrama del sistema ElGamal con curvas elípticas, donde A y B son dos usuarios del sistema, G un punto racional de una curva E sobre el campo $(\mathbb{F}_q)$. La llave pública del usuario A es $(E(\mathbb{F}_q), \mathbb{F}_q, G, P_A)$ mientras que su llave privada es a. El entero b es la llave privada del usuario B. El par (M_1, M_2) y M son los mensajes cifrado y en claro considerados como puntos racionales de la curva E.

4.2.1. Autenticación

Hasta ahora se han mencionado sistemas criptográficos que dos usuarios pueden utilizar para establecer una comunicación sin que ambas partes se tengan que reunir antes para establecer dicha comunicación. Por lo que resulta importante que ambas partes estén seguras del origen del mensaje, más aún si el mensaje es particularmente importante, es decir, el receptor de alguna manera debe estar seguro de que el mensaje cifrado que recibió

efectivamente es de quién dice ser y no de un tercero que se haga pasar por el emisor, a esto se le conoce como *autenticación*.
Por ejemplo cuando una persona desea desea realizar un retiro de una cuenta bancaria por teléfono, tal persona debe proporcionar alguna información personal que ambas partes conocen, es decir datos que fueron proporcionados al momento de abrir dicha cuenta bancaria, pero que un impostor no conoce.
Como se puede observar, en este caso se tienen tres participantes, un emisor, un receptor y un tercero no autorizado (oponente). El oponente puede actuar de dos maneras: que se haga pasar por el emisor o que espere a que el emisor envíe un mensaje y después sustituirlo por otro. El objetivo del oponente es que el receptor acepte su mensaje como el auténtico, en ese caso él gana (ver [38], [41]).

En criptografía de llave pública existe una forma de identificar un usuario, en el sentido que nadie más se pueda hacer pasar por el emisor. Sean A y B dos usuarios de un sistema, e_A y e_B sus respectivas funciones de encripción, recordemos que estas funciones son públicas, $\mathcal{M}$ y $\mathcal{C}$ conjuntos de posibles textos en claro y textos cifrados. Sea M un mensaje de B. No es suficiente que B le envíe $e_A(P)$ a A, dado que cualquiera que conozca e_A puede hacerlo de manera que no se puede saber si fue falsificado. En ese caso, B enviará $e_A e_B^{-1}(P)$. Por tanto, cuando A haya descifrado completamente el mensaje M aplicando su función de desencripción hallará una parte del mismo que no tiene coherencia, que es la parte $e_B^{-1}(P)$, de la cual A puede afirmar que el mensaje provino de B, para ello aplica la función de encripción de B, e_B, puesto que es pública. Dado que nadie más que B pudo haber aplicado la función e_B^{-1}, A sabe que el mensaje provino de B.

Observamos que de manera similar al caso del sistema ElGamal en $\mathbb{Z}_p^*$, este sistema con curvas elípticas el usuario A no puede estar seguro de si el mensaje que recibió realmente ha sido enviado por B o no. Por lo que hace falta que se involucre información que solamente pueda agregar el emisor. Para lograr esto, en la referencia [14] se describe un análogo a este criptosistema utilizando curvas elípticas, el cual se conoce como *criptosistema ElGamal con autenticación*. En este sistema, el proceso de cifrado involucra la información secreta del emisor de esta manera se puede saber que únicamente el usuario B pudo realizar dicho proceso y además logrando resistencia a ataques.

En otras palabras, supongamos que los usuarios A y B que desean comunicarse utilizando este sistema con autenticación, para ello ambas partes acuerdan de manera pública un generador, G, del grupo de puntos racionales de una curva elíptica sobre un campo finito $\mathbb{F}_q$ a utilizar. Además, sean a y b las respectivas llaves privadas de A y B. Los procesos de cifrado y descifrado se realizan como sigue:

Cifrado:
El usuario B obtiene la llave pública de A, expresa su mensaje como una sucesión finita de puntos racionales $M = (\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_r)$ de puntos racionales de la curva elíptica sobre $\mathbb{F}_q$, elegir de manera secreta y aleatoria un entero k y calcular

$$M_1 = kG, \quad M_2 = M + kP_A + bP_A. \tag{4.7}$$

Descifrado:
Obtiene la llave pública de B, P_B y calcula aP_B. Por último, realiza

$$M = M_2 - aM_1 - aP_B. \tag{4.8}$$

Funciona, puesto que
$M_2 - aM_1 - aP_B = M + kP_A + bP_A - a(kG) - a(bG) = M + k(aG) + b(aG) - a(kG) - a(bG) = M.$

De esta manera el usuario A recupera un mensaje coherente, con lo cual puede asegurar que el mensaje provino de B, dado que nadie más que B pudo haber agregado el término bP_A. Este sistema se ilustra en la siguiente figura.

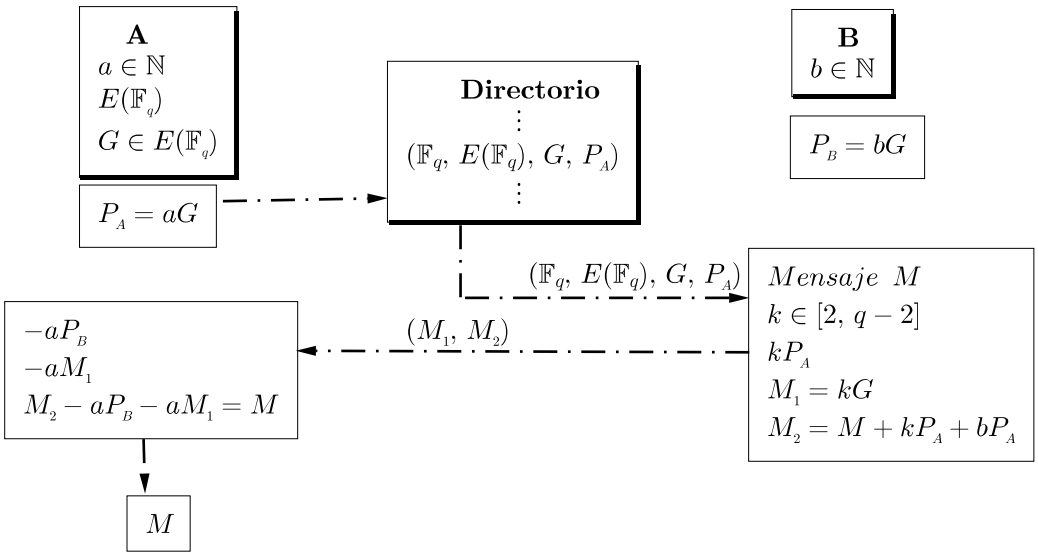

Figura 4.2: Diagrama de criptosistema ElGamal con autenticación, donde G se toma como el generador del grupo de puntos racionales de una curva elíptica; P_A y P_B son las llaves públicas de los usuarios A y B, respectivamente. Los mensajes en claro y cifrado son M y (M_1, M_2), respectivamente, vistos como puntos racionales de la curva.

Observemos que este sistema de cifrado se puede utilizar particularmente con curvas de Koblitz. A continuación describimos algunos ejemplos de curvas de Koblitz y además mostramos un ejemplo de este criptosistema.

4.2.2. Ejemplos

En esta sección mostramos más ejemplos de curvas de Koblitz, de encajamiento de un mensaje en estas curvas, como también un ejemplo del criptosistema ElGamal mediante el cifrado de un mensaje dado y considerando un alfabeto con 26 caracteres.

Dado que deseamos trabajar con un alfabeto con 26 caracteres a continuación mostramos un ejemplo de cifrado con autenticación en una curva definida considerada en $\mathbb{F}_{2^{13}}$.

Ejemplo 4.3. Elegimos de manera arbitraria la curva de Koblitz dada por la ecuación $E_0 : y^2 + xy = x^3 + 1$ sobre el campo $\mathbb{F}_{2^m} = \mathbb{F}_{2^{13}}$. El número de puntos racionales de la curva $E_0(\mathbb{F}_{2^{13}})$ es $8012 = 2^2 * 2003$, donde un generador es el punto racional $(11B3, 06BC)$, los cuales se obtuvieron utilizando *SAGE*.

Supongamos que el usuario B desea enviar el mensaje *"IREMOS A LA LUNA"* al usuario A. Tomando en cuenta la codificación de este mensaje de acuerdo con la Tabla 4.1, tenemos que el encajamiento de este mismo en la curva dada, realizado de manera similar como lo descrito en el Ejemplo 4.2, es el siguiente.

$(0443, 16B2)$	$(1B29, 0850)$	$(1559, 1CFB)$	$(146D, 0EAE)$	$(1E0A, 176D)$
$(1BC8, 0239)$	$(0000, 0001)$	$(0DFF, 18DE)$	$(0000, 0001)$	$(0DFF, 18DE)$
$(04A6, 12F4)$	$(0254, 1F2C)$	$(0000, 0001)$		

Tabla 4.4: Encajamiento del mensaje *"IREMOS A LA LUNA"* en una curva de Koblitz considerada en $\mathbb{F}_{2^{13}}$.

Ahora una vez que tenemos el mensaje como una sucesión de puntos racionales de la curva de Koblitz que estamos considerando, podemos utilizar el sistema ElGamal descrito previamente. Supongamos que 578 y 1455 elegidos de manera arbitraria, son las llaves privadas de A y B, respectivamente. Por tanto, haciendo uso del Algoritmo 11 obtenemos que las respectivas llaves públicas son

$$(1A3D, 0F3F) \quad \text{y} \quad (0133, 1FB6).$$

Considerando un entero arbitrario $k \in [2, 2^{13} - 1]$, $k = 4794$, obtenemos que el mensaje cifrado con autenticación es la siguiente sucesión de puntos racionales, los cuales se obtuvieron mediante la implementación del sistema ElGamal con autenticación en el software *SAGE*.

Con este mensaje cifrado y utilizando el proceso de descifrado, se recupera el mensaje original.

(1431, 0254)	(1F97, 08AB)	(05D7, 1BF6)	(194B, 0E41)	(1BD0, 1171)
(0C6F, 1DD8)	(1B39, 1BB5)	(0967, 1AFA)	(1B39, 1BB5)	(0967, 1AFA)
(19FA, 11D0)	(018B, 1C99)	(1B39, 1BB5)		

Tabla 4.5: Cifrado de *"IREMOS A LA LUNA"* en una curva de Koblitz dada por la ecuación $y^2 + xy = x^3 + 1$ considerada en $\mathbb{F}_{2^{13}}$, utilizando el sistema ElGamal con autenticación.

En lo que sigue mostraremos un ejemplo en donde se cifra un mensaje más largo, a saber, se cifra un fragmento tomado de la obra *"El principito"* de Antoine de Saint-Exupéry. Para ello describimos un modo de operación, el cual utiliza cifrado por bloques, es decir, el mensaje ahora se agrupa en bloques de cierto tamaño.
Dentro de los modos de operación se tienen: ECB (Electronic Code Book mode), CBC (Cipher Block Chaining mode), entre otros. Para realizar una lectura a fondo de los modos de operación algunas de las referencias que se pueden consultar son [42] y [30]. Para nuestro ejemplo usaremos CBC. En el modo de operación CBC se utiliza cifrados por bloques, es decir, para cifrar un mensaje M, éste se divide en bloques de cierta longitud y se cifra cada uno de estos bloques. El bloque cifrado C_i no sólo depende del bloque del texto en claro y de la clave privada, sino de todos lo bloques de texto en claro anteriores y de un valor inicial VI. Además, a partir del uso de este valor inicial, VI, el texto cifrado resultante es aleatorio. A continuación describimos la forma de cifrar utilizando este modo de operación.

Definición. Sean e_k y e_k^{-1} las funciones de encripción y desencripción por bloques de tamaño b, $\mathcal{M}_i$ y C_i bloques de longitud b y sea VI valor inicial que será utilizado una única vez. Definamos $C_0 = VI$ y los procesos de cifrado y descifrado se realizan de la siguiente manera:
Cifrado: $C_i = e_k(\mathcal{M}_i + C_{i-1}), \quad i \geq 1.$
Descifrado: $\mathcal{M}_i = e_k^{-1}(C_i) - C_{i-1}, \quad i \geq 1.$

Con este modo de operación aunque en el mensaje en claro se tengan bloques iguales esto no se ve reflejado en el texto cifrado puesto que quedan cifrados de manera diferente.

Ejemplo 4.4. Para desarrollar nuestro ejemplo tomemos una curva de Koblitz con parámetro $a = 0$ considerada en el campo $\mathbb{F}_{2^{23}}$. En este caso la curva tiene $2^2 * 2095853$ puntos racionales, donde un generador de dicha curva es el punto racional:

$$(x^{20} + x^{12} + x^9 + x^3 + x^2 + 1,\, x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^9 + x^8 + x^6 + x^3),$$

o bien $(10120D, 76348)$ utilizando la notación del Ejemplo 3.1. Cabe mencionar que tanto

la cardinalidad como el generador de la curva se obtuvieron mediante instrucciones que tiene el software *SAGE*.

Consideremos el siguiente fragmento que corresponde a la obra *"El principito"* de Antoine de Saint-Exupéry. Esta obra actualmente es de dominio público y se puede descargar libremente de la siguiente dirección: *http:www.elejandria.com/*
"EXAMINELO ATENTAMENTE PARA QUE SEPAN RECONOCERLO SI ALGUN DIA VIAJANDO POR AFRICA CRUZAN EL DESIERTO SI POR CASUALIDAD PASAN POR AHI NO SE APRESUREN SE LOS RUEGO Y DETENGASE UN POCO PRECISAMENTE BAJO LA ESTRELLA SI UN NINO LLEGA HASTA USTEDES SI ESTE NINO RIE Y TIENE CABELLOS DE ORO Y NUNCA RESPONDE A SUS PREGUNTAS ADIVINARAN ENSEGUIDA QUIEN ES SEAN AMABLES CON EL Y COMUNIQUENME RAPIDAMENTE QUE HA REGRESADO NO ME DEJEN TAN TRISTEX"
Realizando la codificación correspondiente se obtiene la siguiente sucesión con 360 elementos, donde los primeros 10 dígitos se toman de la forma $0d$ con $0 \leq d \leq 9$.

04	23	00	12	08	13	04	11	14	00	19	04	13	19	00	12	04	13	19	04
15	00	17	00	16	20	04	18	04	15	00	13	17	04	02	14	13	14	02	04
⋮																			
14	13	14	12	04	03	04	09	04	13	19	00	13	19	17	08	18	19	04	23

Tabla 4.6: Codificación del fragmento tomado de la obra *"El principito"* de Antoine de Saint-Exupéry.

Ahora consideremos hacer bloques de tamaño tres, es decir, para formar los dos primeros bloques tomamos 04, 23, 00 y 12, 08, 13 de la codificación, obteniendo los enteros 042300 y 120813 respectivamente, y así sucesivamente. Los bloques obtenidos se muestran a continuación. Cabe mencionar que la X que se agrega al final del fragmento es para que la longitud del mensaje sin considerar los espacios resulte mútiplo de 3.

042300	120813	041114	001904	131900	120413	190415	001700	162004	180415
001317	040214	131402	...						
			...	141204	030409	041319	001319	170818	190423

Tabla 4.7: Fragmento visto como bloques de longitud 3.

Realizamos el encajamiento de estos bloques haciendo uso del algoritmo descrito en 13, obteniendo:

(4E8C82, 66C1F5)	(4B085A, 3841CA)	(4F2818, 3AAFAB)	(1975E6, 546AB7)	(4A472B, 65E987)
(517069, 16A095)	(2E3124, 34B5E0)	(6E281, 14639A)	(54EBC2, 545C3A)	(32D70C, 14A750)
(7F560B, 230A34)	(500246, 1D9FAC)	(451AA6, 3D6A9E)	...	
			...	(63ACD1, 4AEEA1)
(2187909, 27A106)	(6BE426, 58B5C3)	(7B522A, 1A2973)	(5BA669, 3009C8)	(1E386F, 1CE96D)

Tabla 4.8: Encajamiento de un fragmento de la obra *"El principito"* de Antoine de Saint-Exupéry.

Ahora, supongamos que el usuario B desea enviarle el fragmento previo al usuario A cifrando el mensaje con el criptosistema ElGamal con autenticación utilizando puntos racionales de una curva de Koblitz. Para que B pueda realizar dicha tarea debe tener la llave pública de A, para ello consideremos que $k_a = 1509254$ y $k_b = 1883318$ son las respectivas llaves privadas de A y B. A partir de esto obtenemos que las correspondientes llaves públicas son:

$$P_A = (57BC59, 62CAFE) \quad \text{y} \quad P_B = (F140C, 338E2A).$$

Considerando un entero $k \in [2, 2^{23} - 1]$, $k = 5264258$ y eligiendo de manera arbitraria un valor inicial $VI = (758BA4, 028657)$, obtenemos que el mensaje cifrado es la sucesión de puntos racionales que se muestra en la Tabla 4.9.
Para ilustrar la forma en que se obtuvo el cifrado, a continuación mostramos la forma en que se cifró el primer bloque que se ve como el primer punto racional que se tiene en la tabla previa, es decir, ciframos $\mathcal{M}_1 = (4E8C82, 66C1F5)$. Dado que usaremos el modo CBC, primero calculamos $\mathcal{M}_1 + VI$, obteniendo $(4CC65E, 182854)$. Ahora para hacer uso del sistema ElGamal con autenticación realizamos los siguientes cálculos

$$k * P_A = (4F22C1, 4C8FDB);\ k_b * P_A = (584F08, 506E65);\ M_1 = (5DFAD5, 5F950A).$$

Una vez que se tienen estos datos ya podemos utilizar (4.7) para obtener M_2, así

$$M_2 = (794675, 3AB3D1). \tag{4.9}$$

Como se puede observar, el punto racional dado en (4.9) es el primer punto racional de la tabla siguiente. Se procede de manera similar para el resto de los puntos racionales del encajamiento para obtener el cifrado.

(794675, 3AB3D1)	(4B536, 64244B)	(693711, 66B330)	(3850BE, 27282F)	(B510E, 197038)
(569994, 672DD7)	(4E15DB, 714E53)	(1B695F, 294002)	(5DEA6, EAB44)	(44E773, 1736DC)
(62F755, 5B5DD8)	(645086, 7B048B)	(175C53, 5323DA)	...	
			...	(3F0267, 74FB2C)
(1102ED, 2C14E4)	(507A00, 25EC83)	(54D8F7, 5A5C52)	(DB1AD, 2A1E67)	(40EF1F, 70EA6E)

Tabla 4.9: Cifrado de un fragmento de la obra *"El principito"* de Antoine de Saint-Exupéry, haciendo uso del sistema ElGamal con autenticación utilizando los puntos racionales de una curva de Koblitz.

Ilustramos la forma de realizar el proceso de descifrado para el primer elemento del texto cifrado, esto es, para $M_2 = (794675, 3AB3D1)$. Para ello recordemos que la clave pública de B es $P_{_B} = (F140C, 338E2A)$. Ahora el usuario A utiliza su clave privada $k_a = 1509254$ y el Algoritmo 11 para obtener k_aP_B, es decir, obtiene $1509254P_B = (584F08, 506E65)$. Nuevamente, dado que usamos modo CBC con valor inicial $VI = (758BA4, 028657)$, primero desciframos M_2 utilizando (4.8) y después le sumaremos el negativo de VI. Para ello son necesarios los siguientes cálculos.

$$\begin{array}{ll} k_aM_1 = (4F22C1,\ 4C8FDB); & -k_aP_{_B} = (584F08,\ 08216D); \\ -k_aM_1 = (4F22C1,\ 03AD1A); & -VI = (758BA4,\ 770DF3). \end{array}$$

Utilizando (4.7) obtenemos que

$$\begin{aligned} M_2 + (-k_aM_1) + (-k_aP_{_B}) &= (794675, 3AB3D1) + (4F22C1,\ 03AD1A) \\ &\quad +(584F08,\ 08216D), \\ &= (4CC65E,\ 182854). \end{aligned} \tag{4.10}$$

Luego, restándole el valor inicial a (4.10) recuperamos el mensaje original

$$(4CC65E,\ 182854) + (758BA4,\ 770DF3) = (4E8C82,\ 66C1F5) = \mathcal{M}_1.$$

Continuando de manera similar para el resto de los puntos racionales en el mensaje cifrado, se puede verificar que se obtiene el mensaje original, es decir, la sucesión de puntos racionales que se obtiene coincide con la sucesión dada en el encajamiento.
Cabe mencionar que en este caso, la autenticación se puede observar al momento de descifrar, dado que si no se obtiene el mensaje original, entonces quiere decir que el mensaje provino de alguien que no es quien dice ser.

En el Apéndice C se pueden observar la sucesión completa de la codificación, los bloques, el encajamiento y cifrado del fragmento.

Conclusiones

En este trabajo se bosquejan los tipos de criptosistemas conocidos como de llave pública que surgen a partir de las desventajas que presentan los llamados de llave privada. Además, que las conocidas funciones unidireccionales tienen aplicación en criptografía, dentro de las cuales tenemos el problema de logaritmo discreto en el grupo formado por el conjunto de puntos racionales de una curva elíptica con la operación suma definida en el mismo. También se realizó un estudio de curvas elípticas, leyes y estructura de grupo que poseen junto con la operación definida.

Como se puede notar en los capítulos 2 y 3, las curvas se pueden clasificar respecto a que si cumplen o no ciertas características, como en el caso de las curvas de Koblitz. Además cabe mencionar que, aunque no se trató en el presente trabajo, se pueden tener distintas coordenadas para estas curvas, dentro de ellas se tienen coordenadas proyectivas, coordenadas Jacobianas y coordenadas de Edward. Para mayor información sobre estos temas se pueden consultar por ejemplo [46], [11].

Considerando lo que se describió en el capítulo previo, en característica dos se tiene encajamiento de un mensaje, similar al que se tiene en característica p, con p primo distinto de 2 y 3, en donde se realizan saltos de tamaño k, donde k es la longitud del mensaje a cifrar.

De acuerdo con los algoritmos presentados durante el desarrollo de este trabajo de tesis podemos concluir que hay una forma eficiente de obtener múltiplo escalar de puntos racionales de curvas elípticas definidas sobre campos de característica dos y en particular en curvas de Koblitz sin utilizar el doblado de puntos racionales. Además, con los resultados obtenidos en la Sección 3.2.1 respecto a los tiempos de ejecución, se concluye que el método para obtener múltiplo escalar utilizando la representación ξ-NAF es aproximadamente dos veces más rápido en comparación con el método binario de suma y doblado.

Se agregó la propiedad de autenticación al cifrado de datos, con una ligera modificación y sin cambiar demasiado el número total de operaciones. Que como se puede observar, esta propiedad de autenticación también se puede utilizar en las curvas de Koblitz.

Apéndice A

Álgebra

En este apéndice se enuncian sin demostración algunos resultados y conceptos básicos de álgebra que son utilizados a lo largo del escrito. El lector interesado puede encontrar la justificación y un tratamiento más profundo de estos temas en las referencias [8], [23], [11], [13], [24], [19], [10] y [34].

A.1. Grupos

Teorema A.1. *Un subgrupo de un grupo cíclico es cíclico.*

Teorema A.2. *Sea H un subgrupo de un grupo finito G. Entonces el orden de H es un divisor del orden de G.*

Corolario A.2.1. *Todo grupo de orden primo es cíclico.*

Teorema A.3. *El orden de un elemento de un grupo finito divide al orden del grupo.*

Teorema A.4. *Si G es un grupo finito de orden n, entonces $a^n = e$, para todo a en G.*

Teorema A.5. *Cualquier grupo abeliano finito es el producto (suma) directo(a) de grupos cíclicos.*

Teorema A.6. *Un grupo abeliano finito G es isomorfo a un grupo de la forma*

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}, \tag{A.1}$$

con n_i divisor de n_{i+1}, con $i = 1, 2, \ldots, s-1$ y donde los enteros n_i son determinados de manera única por G.

A.2. Anillos

Definición. Un conjunto no vacío R es un *anillo asociativo* si en R están definidas dos operaciones, denotadas por "$+$" y "$\cdot$", respectivamente tales que para cualesquiera a, b, c en R:

1. $a + b \in R$.
2. $a + b = b + a$.
3. $(a + b) + c = a + (b + c)$.
4. Existe $0 \in R$ tal que $a + 0 = a$, $\forall a \in R$.
5. Existe $-a \in R$ tal que $a + (-a) = 0$.
6. $a \cdot b \in R$.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
8. $a \cdot (b+c) = a \cdot b + a \cdot c$ y $(b+c) \cdot a = b \cdot a + c \cdot a$, (las dos leyes distributivas).

Cabe mencionar que escribiremos $(R, +, \cdot)$ para hacer referencia a un anillo con operaciones $+$ y $\cdot$. Decimos que $(R, +, \cdot)$ es *conmutativo* si la operación $\cdot$ es conmutativa, es decir, si se cumple que para a, $b \in R$ se cumple que $a \cdot b = b \cdot a$.

Definición. Un subconjunto U de un anillo $(R, +, \cdot)$ es un *ideal de* R si U es un subgrupo de R bajo la adición y para todo $u \in U$ y $r \in R$, tanto ur como ru están en U.

Definición. Un ideal $M \neq R$ de un anillo $(R, +, \cdot)$ es *ideal maximal de* R si siempre que U es un ideal de R tal que $M \subset U \subset R$ se tiene que $U = R$ o $U = M$.

A.3. Residuos cuadráticos

Definición. Si p es un número primo impar, $a \not\equiv 0 \pmod{p}$ es un *residuo cuadrático módulo* p si $x^2 \equiv a \pmod{p}$ tiene solución. Cuando la congruencia carece de solución a es llamado *no-residuo cuadrático módulo* p.

Teorema A.7. *Si a es un entero no divisible por el primo impar p. Entonces la congruencia $x^2 \equiv a \ (mód\, p)$ es soluble para algún entero x si y sólo si $a^{(p-1)/2} \equiv 1 \ (mód\, p)$. Esto se le conoce como criterio de Euler.*

A.4. Campos finitos

En esta parte tratamos acerca de campos finitos y la construcción de los mismos a partir de polinomios irreducibles. Para ello, definimos lo que entenderemos por campos

finitos, congruencia de polinomios, entre otros.

Definición. Un anillo conmutativo $(R, +, \cdot)$ es un *campo* si $R^* = R \setminus \{0\}$ es un grupo conmutativo bajo la operación producto "$\cdot$". El campo es *finito* si la cardinalidad de R es finita.

Definición. Sea $\mathbb{K}$ subconjunto de un campo $\mathbb{F}$, $\mathbb{K}$ *es subcampo de* $\mathbb{F}$ si es un campo bajo las operaciones de $\mathbb{F}$. En este contexto $\mathbb{F}$ es llamado *extensión del campo* $\mathbb{K}$.

Definición. Un campo $\mathbb{K}$ es de *característica* n si n es el menor entero positivo tal que $nx = 0$ para todo $x \in \mathbb{K}$. Cuando no existe tal n entonces el campo es de característica 0.

Definición. Sean $p(x), q(x)$ y $r(x)$ elementos del anillo de polinomios $\mathbb{F}[x]$ con $p(x)$ distinto del polinomio cero. Entonces $r(x)$ *y* $q(x)$ *son congruentes módulo* $p(x)$, si existe $h(x)$ en $\mathbb{F}[x]$ tal que $r(x) - q(x) = p(x)h(x)$. Escribiremos $r(x) \equiv q(x) \pmod{p(x)}$ para hacer referencia a ello.

La clase de equivalencia del polinomio $q(x) \in \mathbb{F}[x]$ módulo $p(x)$ consiste de los polinomios $r(x) \in \mathbb{F}[x]$ tales que $q(x) - r(x)$ es un múltiplo de $p(x)$. Esto es, si n es el grado del polinomio $p(x)$ y $grad(r(x))$ es el grado de $r(x)$, tenemos que

$$[q(x)] = \{r(x) : q(x) = p(x)h(x) + r(x), h(x), r(x) \in \mathbb{F}[x],\ grad(r(x)) < n\} = [r(x)],$$

donde $[r(x)]$ es la clase de equivalencia de $r(x)$ y este último el representante de la misma. Con $\mathbb{F}[x]/\langle p(x)\rangle$ indicamos el conjunto de clases de equivalencia módulo $p(x)$. En otras palabras, $\mathbb{F}[x]/\langle p(x)\rangle = \{[b_0 + b_1x + \cdots + b_{n-1}x^{n-1}] : b_i \in \mathbb{F},\ 0 \le i < n\}$.
Debido a que los polinomios $h(x)$ y $r(x)$ se hallan mediante el algoritmo de la división extendida y por la unicidad de $r(x)$ los coeficientes $b_0, b_1, \ldots, b_{n-1}$ son únicos. A partir de esto, tenemos que $\mathbb{F}[x]/\langle p(x)\rangle$ es finito si $\mathbb{F}$ lo es. Así, si $\mathbb{F}$ tiene m elementos y n es el grado del polinomio $p(x)$ entonces $\mathbb{F}[x]/\langle p(x)\rangle$ tiene m^n elementos.

Definición. Un polinomio $p(x)$ en $\mathbb{F}[x]$ es *irreducible sobre el campo* $\mathbb{F}$ si siempre que $p(x) = a(x)b(x)$ con $a(x)$, $b(x) \in \mathbb{F}[x]$, entonces ya sea $a(x)$ o $b(x)$ tiene grado cero (es decir, es una constante distinta de cero).

Teorema A.8. *Para* $p(x) \in \mathbb{F}[x]$*, el anillo de clases de residuos* $\mathbb{F}[x]/\langle p(x)\rangle$ *es un campo si y sólo si* $p(x)$ *es irreducible sobre* $\mathbb{F}$*, donde* $\langle p(x)\rangle$ *es el ideal generado por* $p(x)$*.*

Corolario A.8.1. *Sea* $\mathbb{F}$ *un campo finito, entonces* $\mathbb{F}$ *tiene por característica un número primo* p *y tiene* p^n *elementos.*

Corolario A.8.2. *Si el campo finito $\mathbb{F}$ tiene p^n elementos, entonces todo $a \in \mathbb{F}$ satisface que $a^{p^n} = a$.*

Lema A.1. *Para todo número primo p y todo entero positivo m existe un único campo con p^m elementos. A este campo lo escribiremos como $\mathbb{F}_{p^m}$ o bien como $GF(p^m)$.*

Teorema A.9. *Sea $\mathbb{F}_q$ un campo finito con $q = p^n$ elementos. Entonces cada subcampo de $\mathbb{F}_q$ tiene orden p^m, donde m es un entero positivo divisor de n. De manera inversa, si m es un entero positivo divisor de n entonces existe exactamente un subcampo de $\mathbb{F}_q$ con p^m elementos.*

Lema A.2. *Para cada campo finito $\mathbb{F}_q$, el grupo multiplicativo, $\mathbb{F}_q^*$, de elementos no cero de $\mathbb{F}_q$ es cíclico de orden $q-1$.*

Definición. Un generador del grupo cíclico $\mathbb{F}_q^*$ es llamado *elemento primitivo de* $\mathbb{F}_q$.

A continuación mostramos la forma de realizar una construcción de campos finitos a partir de polinomios, además presentamos un ejemplo de la misma.
En $\mathbb{F}[x]/\langle p(x)\rangle$ se pueden definir dos operaciones, suma y producto, como sigue: Sean $r_1(x)$ y $r_2(x)$ elementos de $\mathbb{F}[x]/\langle p(x)\rangle$, definimos

$$[r_1(x)] + [r_2(x)] \coloneqq [r_1(x) + r_2(x)] \quad \text{y} \quad [r_1(x)][r_2(x)] \coloneqq [r_1(x)r_2(x)].$$

Considerando esta definición se puede obtener que el neutro es la clase del polinomio $p(x)$ y que el inverso aditivo de $[r(x)]$ es $[p(x) - r(x)]$. A pesar de que en $\mathbb{F}[x]/\langle p(x)\rangle$ se tienen definida dos operaciones, es un campo si y sólo si $p(x)$ es irreducible, esto se debe al Teorema A.8. Para ilustrar lo anterior, veamos un ejemplo.

Ejemplo A.1. Consideremos el polinomio $p(x) = x^4 + x + 1$ irreducible sobre $\mathbb{F}_2$, donde los elementos de $\mathbb{F}_2[x]/\langle x^4 + x + 1\rangle$ son los polinomios con coeficientes en $\mathbb{F}_2$ de grado menor que 4. Como el grado de $p(x)$ coincide con el grado de extensión de $\mathbb{F}_2$, el cociente anterior es un campo con 2^4 elementos. Enseguida se muestran tales elementos y se ilustran las operaciones definidas.

$$\mathbb{F}_2[x]/\langle x^4+x+1\rangle = \{[0], [1], [x], [x^2], [x^3], [x+1], [x^2+x], [x^3+x^2], [x^3+x+1], [x^2+1], \\ [x^3+x], [x^2+x+1], [x^3+x^2+x], [x^3+x^2+x+1], [x^3+x^2+1], [x^3+1]\}.$$

Considerando que $x^4 = x + 1$, una base de este campo es $\mathcal{B} = \{\beta_1, \beta_2, \beta_3, \beta_4\}$ con $\beta_1 = x^3$, $\beta_2 = x^3 + x^2$, $\beta_3 = x^3 + x^2 + x + 1$ y $\beta_4 = x^3 + x$. A continuación se ejemplifica la suma de elementos de este campo vistos como combinación lineal de la base $\mathcal{B}$, esto es, se muestran los coeficientes de cada elemento de la base.

		β_1	β_2	β_3	β_4			β_1	β_2	β_3	β_4
$[x^0] = [1]$	=	1	1	1	1	$[x^8] = [x^2+1]$	=	0	0	1	1
$[x^1] = [x]$	=	1	0	0	1	$[x^9] = [x^3+x]$	=	0	0	0	1
$[x^2] = [x^2]$	=	1	1	0	0	$[x^{10}] = [x^2+x+1]$	=	1	0	1	0
$[x^3] = [x^3]$	=	1	0	0	0	$[x^{11}] = [x^3+x^2+x]$	=	1	1	0	1
$[x^4] = [x+1]$	=	0	1	1	0	$[x^{12}] = [x^3+x^2+x+1]$	=	0	0	1	0
$[x^5] = [x^2+x]$	=	0	1	0	1	$[x^{13}] = [x^3+x^2+1]$	=	1	0	1	1
$[x^6] = [x^3+x^2]$	=	0	1	0	0	$[x^{14}] = [x^3+1]$	=	0	1	1	1
$[x^7] = [x^3+x+1]$	=	1	1	1	0						

Tabla A.1: Suma de algunos elementos del campo cociente $\mathbb{F}_2[x]/\langle x^4+x+1\rangle$.

Ahora haciendo uso de la tabla previa, en la siguiente mostramos el producto de algunos elementos del campo. De donde se puede observar que $[x^6][x^7] = [x^{13}]$ y de la Tabla A.1 se tiene que $[x^{13}] = [x^3+x^2+1]$.

$\cdot$	$[1]$	$[x]$	$[x^2]$	$[x^3]$	$[x^4]$	$[x^5]$	$[x^6]$	$[x^7]$	$[x^8]$	$[x^9]$
$[1]$	$[1]$	$[x]$	$[x^2]$	$[x^3]$	$[x^4]$	$[x^5]$	$[x^6]$	$[x^7]$	$[x^8]$	$[x^9]$
$[x^6]$	$[x^6]$	$[x^7]$	$[x^8]$	$[x^9]$	$[x^{10}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$
$[x^7]$	$[x^7]$	$[x^8]$	$[x^9]$	$[x^{10}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$	
$[x^8]$	$[x^8]$	$[x^9]$	$[x^{10}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$		
$[x^9]$	$[x^9]$	$[x^{10}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$			
$[x^{10}]$	$[x^{10}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$				
$[x^{11}]$	$[x^{11}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$					
$[x^{12}]$	$[x^{12}]$	$[x^{13}]$	$[x^{14}]$	$[1]$						
$[x^{13}]$	$[x^{13}]$	$[x^{14}]$	$[1]$							
$[x^{14}]$	$[x^{14}]$	$[1]$								

Tabla A.2: Producto de algunos elementos del campo cociente $\mathbb{F}_2[x]/\langle x^4+x+1\rangle$.

Observemos que se pueden construir campos con cierta cantidad de elementos, en este caso mostramos uno con 16 elementos. Como se mencionó anteriormente, el número de elementos de todo campo finito es una potencia de un primo. Se pueden consultar las referencias como [19], [32] para ver otro ejemplo y donde se puede ver más a profundidad la construcción de campos finitos.

Cabe mencionar que en los ejemplos 3.8 y 3.9 realmente se trabajaron con los representantes de clase. Es fácil probar que la suma y el producto están bien definidos.

A.4.1. Bases normales

El campo $\mathbb{F}_{2^m}$ se puede ver como un espacio vectorial de dimensión m sobre $\mathbb{F}_2$. Esto es, existe un conjunto de m elementos, digamos $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}$ en $\mathbb{F}_{2^m}$, tales que cada

$\alpha \in \mathbb{F}_{2^m}$ se puede escribir de manera única de la forma

$$\alpha = \sum_{i=0}^{m-1} a_i \alpha_i, \quad a_i \in \{0, 1\}, \quad 0 \leq i \leq m-1. \tag{A.2}$$

Así podemos representar a α como un vector $(a_0, a_1, \ldots, a_{m-1})$ de ceros y unos.

En general existen distintas bases de $\mathbb{F}_{2^m}$ sobre $\mathbb{F}_2$, dentro de ellas se tiene la base normal. Una *base normal de* $\mathbb{F}_{2^m}$ *sobre* $\mathbb{F}_2$ es una base de la forma

$$\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{m-1}}\}, \quad \beta \in \mathbb{F}_{2^m}. \tag{A.3}$$

Esta base siempre existe debido al siguiente resultado que también se puede ver en la referencia [19].

Lema A.3. *Para cualquier campo finito* $\mathbb{K}$ *y cualquier extensión* $\mathbb{F}$ *de* $\mathbb{K}$*, existe una base normal de* $\mathbb{F}$ *sobre* $\mathbb{K}$*.*

Así, dado un elemento $\alpha \in \mathbb{F}_{2^m}$ se puede escribir como $\alpha = \sum_{i=0}^{m-1} a_i \beta^{2^i}$ con $a_i \in \{0, 1\}$ para $0 \leq i \leq m-1$.

Una forma de verificar si una base es normal es mediante el criterio dado por el siguiente teorema (ver [1]).

Teorema A.10. *Para* $\beta \in \mathbb{F}_{q^m}$*,* $\{\beta, \beta^q, \ldots, \beta^{q^{m-1}}\}$ *es una base normal de* $\mathbb{F}_{q^m}$ *sobre* $\mathbb{F}_q$ *si y sólo si los polinomios* $x^m - 1$ *y* $\beta x^{m-1} + \beta^q x^{m-2} + \cdots \beta^{q^{m-2}} x + \beta^{q^{m-1}}$ *son primos relativos en* $\mathbb{F}_{q^m}[x]$*.*

Como elevar al cuadrado es una operación lineal en $\mathbb{F}_{2^m}$ tenemos que

$$\alpha^2 = \sum_{i=0}^{m-1} a_i^2 \beta^{2^{i+1}} = \sum_{i=0}^{m-1} a_{i-1} \beta^{2^i},$$

con los subíndices de a_i reducidos módulo m. Por tanto, $\alpha^2 = (a_{m-1}, a_0, a_1, \ldots, a_{m-2})$ en esta base normal. De donde tenemos que la representación en base normal de $\mathbb{F}_{2^m}$ da mucha ventaja, dado que elevar al cuadrado un elemento de campo se puede realizar mediante una rotación de elementos de la representación vectorial, operación que se puede implementar sin costo computacional (ver [23]). Tal propiedad es utilizada para realizar aritmética eficiente en campos finitos de caraterística dos.

A.5. Función traza

Definición. Con Tr haremos referencia a la función traza, $Tr : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2$ definida por $Tr : \alpha \longmapsto \alpha + \alpha^{2^1} + \alpha^{2^2} + \cdots + \alpha^{2^{m-1}}$.

Cabe mencionar que Tr es una $\mathbb{F}_2$-transformación lineal y suprayectiva. De manera general tenemos las siguientes propiedades que satisface la función traza.

Proposición 8. *Para $\alpha, \beta \in \mathbb{F}_{2^m}$, $c \in \mathbb{F}_2$, la función traza tiene las siguientes propiedades*

1. $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
2. *Tr es una transformación lineal de $\mathbb{F}_{2^m}$ sobre $\mathbb{F}_2$, donde $\mathbb{F}_{2^m}$ y $\mathbb{F}_2$ son considerados como espacios vectoriales sobre $\mathbb{F}_2$.*
3. $Tr(c) = mc$.
4. $Tr(\alpha^2) = Tr(\alpha)$.

Proposición 9. *La ecuación cuadrática*

$$x^2 + ax + b = 0, \quad a, b \in \mathbb{F}_{2^m}, \quad a \neq 0, \tag{A.4}$$

tiene una solución en $\mathbb{F}_{2^m}$ si y sólo si $Tr(a^{-2}b) = 0$. Si x_1 es una solución entonces la otra solución es $x_1 + a$.

A continuación enunciamos un resultado que nos indica cuándo un elemento de $\mathbb{F}_{2^m}$ tiene traza cero.

Teorema A.11. *Sea $\alpha \in \mathbb{F}_{2^m}$. $Tr(\alpha) = 0$ si y sólo si existe $\beta \in \mathbb{F}_{2^m}$ tal que $\alpha = \beta + \beta^2$.*

Este β existe, dado que en el siguiente teorema se puede fijar θ elemento de $\mathbb{F}_{2^m}$ tal que $Tr(\theta) = 1$ el cual existe dado que Tr es balanceada

Teorema A.12. *Sean α y θ elementos de $\mathbb{F}_{2^m}$. Si β está definida por*

$$\beta = \alpha\theta^2 + (\alpha + \alpha^2)\theta^{2^2} + \cdots + (\alpha + \alpha^2 + \cdots + \alpha^{2^{m-2}})\theta^{2^{m-1}}, \tag{A.5}$$

entonces $\beta + \beta^2 = \alpha(Tr(\theta) - \theta) - \theta(Tr(\alpha) - \alpha)$.

A.6. Irracionales cuadráticos

Definimos a los irracionales cuadráticos como también algunas de sus propiedades. Para una lectura profunda al respecto se puede consultar la referencia [34].

Definición. El número real α es llamado *irracional cuadrático* si α es irracional y si α es raíz de un polinomio cuadrático con coeficientes enteros, es decir, $A\alpha^2 + B\alpha + C = 0$, donde A, B y C son números enteros.

Definición. Un *cuadrado perfecto* es un número que se puede escribir como producto de algún número entero por si mismo, es decir, $\sqrt{x} = a$ con $a \in \mathbb{Z}$.

Lema A.4. *El número real α es irracional cuadrático si y sólo si existen enteros a, b y c con $b > 0$ y $c \neq 0$ tal que b no es un cuadrado perfecto y*

$$\alpha = \frac{a + \sqrt{b}}{c}. \tag{A.6}$$

Definición. Sea $\alpha = \frac{a+\sqrt{b}}{c}$ un irracional cuadrático entonces el *conjugado* de α escrito como $\overline{\alpha}$ se define como $\alpha = \frac{a-\sqrt{b}}{c}$.

Lema A.5. *Si el irracional cuadrático α es una raíz del polinomio $Ax^2 + Bx + C = 0$, entonces la otra raíz del polinomio es el conjugado de α.*

Lema A.6. *Si $\alpha_1 = \frac{a_1+b_1\sqrt{d}}{c_1}$ y $\alpha_2 = \frac{a_2+b_2\sqrt{d}}{c_2}$ son irracionales cuadráticos, entonces*

1. $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_1} + \overline{\alpha_2}$,
2. $\overline{\alpha_1 - \alpha_2} = \overline{\alpha_1} - \overline{\alpha_2}$,
3. $\overline{\alpha_1\alpha_2} = \overline{\alpha_1}\overline{\alpha_2}$,
4. $\overline{\alpha_1/\alpha_2} = \overline{\alpha_1}/\overline{\alpha_2}$.

A.7. Problema de logaritmo discreto

A continuación enunciamos lo que se conoce como *problema de logaritmo discreto* en un grupo multiplicativo. De manera similar se puede escribir para un grupo aditivo.

Dados un grupo $(G, \cdot)$, un elemento $\alpha \in G$ de orden n y un elemento $\beta \in \langle\alpha\rangle$, hallar el elemento único $k \in \mathbb{Z}_n$ tal que $\alpha^k = \beta$ lo que escribimos como $k = log_\alpha\beta$.

La aplicación del problema de logaritmo discreto en criptografía surge a partir de que calcular logaritmos discretos es (probablemente) difícil, pero la exponenciación se puede realizar eficientemente.

Apéndice B

Propiedades de grupo de $E(\mathbb{K})$

Antes de verificar que la operación suma junto con el conjunto formado por los puntos racionales de una curva elíptica sobre un campo cumplen las propiedades de grupo, se enuncian algunos resultados previos los cuales serán necesarios para la mejor comprensión de las pruebas de dichas propiedades y que también se pueden consultar en las referencias [2], [23], [31], [37], [36], [44]. Para ello, consideremos un campo $\mathbb{K}$ y la ecuación de la curva elíptica E sobre $\mathbb{K}$ dada por

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{B.1}$$

cuya ecuación homogénea (respecto a la variable Z) es

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

Podemos observar que las expresiones dadas en (B.1) y (B.2) son las que nos permiten trabajar en el espacio afín y en el espacio proyectivo, respectivamente.
Dado que la ecuación de una curva elíptica en el plano proyectivo está expresada por (B.2), tenemos el siguiente resultado que nos proporciona la forma que tienen las rectas proyectivas que intersecan a dicha curva en el punto $\mathcal{O}$.

Proposición 10. *Las rectas proyectivas de la forma $X = cZ$ son las únicas rectas diferentes de $Z = 0$ que intersecan a la curva en el punto al infinito $\mathcal{O} = [0 : 1 : 0]$.*

Demostración. Consideremos la ecuación general de una recta proyectiva que es la dada por $\alpha_1X + \alpha_2Y + \alpha_3Z = 0$. Como el punto $\mathcal{O} = [0 : 1 : 0]$ es el único punto en la curva entonces $\mathcal{O}$ debe satisfacer la ecuación de la curva, por tanto obtenemos que $\alpha_2 = 0$. Por tanto la ecuación de la recta es de la forma $\alpha_1X + \alpha_3Z = 0$. Como por hipótesis se está

considerando $Z \neq 0$, entonces $\alpha_1 \neq 0$. Así $X = -\alpha_3 Z/\alpha_1$. Hacemos $c = -\alpha_3/\alpha_1$. Por tanto $X = cZ$. □

Ahora, consideremos el anillo de polinomios en las variables X, Y, y Z, $\mathbb{K}[X,Y,Z]$.

Definición. Sea $F \in \mathbb{K}[X,Y,Z]$ un polinomio homogéneo, la *curva proyectiva* ζ definida por F es el conjunto de soluciones $[X:Y:Z] \in \mathbb{P}^2_{\mathbb{K}}$ de $F(X,Y,Z) = 0$.

A continuación definimos cuándo diremos que una curva es irreducible.

Definición. Si ζ es una curva dada por una ecuación $\zeta : \phi(x,y) = 0$, y ϕ se puede ver como un producto de polinomios irreducibles $\phi(x,y) = p_1(x,y)p_2(x,y)\cdots p_n(x,y)$. Entonces los *componentes irreducibles de la curva* ζ son las curvas $p_1(x,y) = 0$, $p_2(x,y) = 0$, ..., $p_n(x,y) = 0$. Diremos que ζ *es irreducible* si tiene sólo un componente irreducible, o de manera equivalente, si $\phi(x,y)$ es un polinomio irreducible. Si ζ_1 y ζ_2 son dos curvas, diremos que ζ_1 *y* ζ_2 *no tienen componentes comunes* si sus componentes irreducibles son distintos.

El siguiente teorema se le conoce como Teorema de Bezout el cual nos dice la cantidad de puntos que se tienen en la intersección de dos curvas proyectivas, cuya demostración se puede consultar en las referencias como [12], [44], [37].

Teorema B.1. *Sean* $\mathbb{K}$ *un campo algebraicamente cerrado;* $F, G \in \mathbb{K}[X,Y,Z]$ *polinomios homogéneos de grados* m *y* n*, respectivamente, tales que no tienen factor común irreducible;* $\zeta_F = \{[X:Y:Z] \in \mathbb{P}^2_{\mathbb{K}} : F(X,Y,Z) = 0\}$, $\zeta_G = \{[X:Y:Z] \in \mathbb{P}^2_{\mathbb{K}} : G(X,Y,Z) = 0\}$. *Entonces el conjunto* $\zeta_F \cap \zeta_G$ *es finito y tenemos que* $\sum_{P \in \zeta_F \cap \zeta_G} I(P : \zeta_F, \zeta_G) = mn$*, donde* $I(P : \zeta_F, \zeta_G)$ *representa la multiplicidad del punto racional* P *en la intersección de* ζ_F *y* ζ_G.

A partir del teorema previo se obtiene el siguiente corolario que nos da la cantidad de puntos que se tendrán en la intersección de un recta con un curva proyectiva.

Corolario B.1.1. *Sean* $\mathbb{K}$ *un campo algebraicamente cerrado y* $F \in \mathbb{K}[X,Y,Z]$ *un polinomio homogéneo de grado* d*. Sea* $\zeta : F(X,Y,Z) = 0$ *una curva proyectiva de grado* d *y* L *una recta que no está contenida en* ζ*. Entonces* $\zeta \cap L$ *tiene exactamente* d *puntos contados con multiplicidad.*

Cabe mencionar que si L es una recta en $\mathbb{P}^2_{\mathbb{K}}$ y E una curva elíptica E sobre un campo $\mathbb{K}$ dada por la ecuación (B.2); por el corolario previo $E(\mathbb{K}) \cap L$ tiene tres puntos P, Q y R contando multiplicidad.

En lo que sigue se verifican las propiedades de grupo que satisface la operación suma definida en el conjunto de puntos racionales de una curva elíptica sobre un campo $\mathbb{K}$.
De la definición de la operación suma se tiene que es cerrada y conmutativa. Para probar que $P + \mathcal{O} = P$ para todo $P \in E(K)$, se tienen dos casos, cuando $P = \mathcal{O}$ y cuando $P \neq \mathcal{O}$. Si $P = \mathcal{O}$ entonces por el Corolario B.1.1 la recta tangente al punto al infinito dada por la ecuación $Z = 0$ interseca a $E(\mathbb{K})$ en $\mathcal{O}$ tres veces, de esta manera se tiene que $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Ahora consideremos el caso en que P es distinto de $\mathcal{O}$. La recta que pasa por P y $\mathcal{O}$ es una recta vertical, entonces el otro punto de intersección es el negativo de P, por tanto el simétrico de $-P$ es P. Con ambos casos se concluye que $P + \mathcal{O} = P$ para cada $P \in E(\mathbb{K})$. Además, del argumento previo también se tiene que sumar P con $-P$ se obtiene $\mathcal{O}$, por tanto $P + (-P) = \mathcal{O}$ para cada $P \in E(\mathbb{K})$. Por último falta verificar que se cumple la asociatividad de la operación, por lo que a continuación damos algunas definiciones y resultados.

B.0.1. Asociatividad

Con el objetivo de dar una demostración de la propiedad asociativa de la operación suma definida en una curva elíptica sobre un campo $\mathbb{K}$, a continuación damos algunas definiciones y resultados los cuales serán necesarios para la realización de la prueba. Estos resultados se pueden consultar en las referencias dadas al inicio de este apéndice para una lectura a mayor profundidad.

Los divisores son útiles para realizar un seguimiento de ceros y polos de una función racional. A continuación definimos lo que entenderemos por divisor.

Definición. Sea $\mathbb{K} = \mathbb{F}_q$ y $E(\mathbb{K})$ una curva elíptica sobre $\mathbb{K}$. Un *divisor* D es una suma de $\overline{\mathbb{F}}_q$-puntos racionales de la forma $D = \sum_{P \in E(\mathbb{K})} \eta_P(P)$, donde $\eta_P \in \mathbb{Z}$ y es tal que $\eta_P = 0$ para todos salvo un número finito de $P \in E(\mathbb{K})$. El *grado de un divisor* D es el entero $grad(D) = \sum_{P \in E(\mathbb{K})} \eta_P$.

El conjunto de divisores de $E(\mathbb{K})$, $Div(E(\mathbb{K})$, forma un grupo aditivo abeliano generado por los puntos racionales de $E(\mathbb{K})$, donde la operación es la dada por la siguiente igualdad

$$\sum_{P \in E(\mathbb{K})} \eta_P(P) + \sum_{P \in E(\mathbb{K})} m_P(P) = \sum_{P \in E(\mathbb{K})} (\eta_P + m_P)(P).$$

Escribiremos como $Div^0(E(\mathbb{K}))$ el conjunto de todos los *divisores de grado* 0, esto es, $Div^0(E(\mathbb{K})) = \{D \in Div(E(\mathbb{K})) : grad(D) = 0\}$.

Definición. Sean $D_1, D_2 \in Div(E(\mathbb{K})$. En $Div(E(\mathbb{K})$ se define el orden $\geq$ de manera que

$D_1 \geq D_2$ cuando se cumple que $\eta_P \geq m_P$ para cada $P \in E(\mathbb{K})$. Donde $D_1 = \sum_{P \in E(\mathbb{K})} \eta_P(P)$ y $D_2 = \sum_{P \in E(\mathbb{K})} m_P(P)$.

Definición. Si consideramos una curva elíptica sobre un campo $\mathbb{K}$ con ecuación de la forma $r(x,y) = 0$, donde $r(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$, con $r \in \mathbb{K}[x,y]$, entonces el *anillo de coordenadas de E sobre* $\mathbb{K}$, el cual escribimos como $\mathbb{K}[E]$ es el dominio entero $\mathbb{K}[E] = \mathbb{K}[x,y]/\langle r \rangle$, donde $\langle r \rangle$ es el ideal en $\mathbb{K}[x,y]$ generado por r. De manera similar se define $\overline{\mathbb{K}}[E] = \overline{\mathbb{K}}[x,y]/\langle r \rangle$.

Sea ℓ un elemento de $\overline{\mathbb{K}}[E]$ cualesquiera, entonces podemos pensar en sustituir y^2 por $y^2 - r(x,y)$ para así obtener una representación de la forma

$$(x,y) = v(x) + yw(x), \quad \text{con} \quad v(x), w(x) \in \overline{\mathbb{K}}[x]. \tag{B.3}$$

Ahora, sean $f_1, f_2, g_1, g_2 \in \mathbb{K}[E]$ con g_1 y g_2 distintos del polinomio cero en $\mathbb{K}[E]$. Definimos la relación de equivalencia $\sim$ como $f_1/g_1 \sim f_2/g_2$ si y sólo si $f_1g_2 = f_2g_1$.

Definición. El *campo de funciones racionales de E sobre* $\mathbb{K}$, $\mathbb{K}(E)$ es el conjunto de clases de equivalencia de cocientes de la forma f_1/g_1 con $f_1, g_1 \in \mathbb{K}[E]$ y $g_1 \neq 0$. Donde las operaciones de campo se definen de manera natural como en un anillo de polinomios.

De manera similar, $\overline{\mathbb{K}}(E)$ el campo de funciones de E sobre $\overline{\mathbb{K}}$ es el campo de funciones racionales de $\overline{\mathbb{K}}[E]$. Los elementos de $\overline{\mathbb{K}}(E)$ son los que llamaremos *funciones racionales*.

Definición. Sean $\phi \in \overline{\mathbb{K}}(E)^*$ una función racional distinta de cero y $P = (x_0, y_0) \in E(\mathbb{K})$ diferente del punto $\mathcal{O}$. Diremos que ϕ *está definida en* P si existe una representación de la forma $\phi = f/g$, con $f, g \in \overline{\mathbb{K}}[E]$ tal que $g(x_0, y_0) \neq 0$. Por tanto si ϕ está definida sobre P lo escribimos como $\phi(P) = \frac{f(x_0,y_0)}{g(x_0,y_0)} = \frac{f(P)}{g(P)}$. Si se cumple que $\phi(P) = 0$, entonces decimos que ϕ *tiene un cero en* P. Si ϕ no está definida en P diremos que ϕ *tiene un polo en* P y en ese caso escribimos $\phi(P) = \infty$.

Ejemplo B.1. Sea $\mathbb{K} = \mathbb{F}_q$ con característica de $\mathbb{F}_q$ distinta de 2 y de 3. Consideremos la curva elíptica sobre $\mathbb{K}$ con ecuación $E : y^2 = x^3 - x$; un punto racional $P = (1,0) \in E(\mathbb{K})$ y $\phi = (x^2 - x)/y \in \overline{\mathbb{K}}(E)$. Observemos que si ϕ lo consideramos como un cociente de polinomios, esto es, $\phi \in \overline{\mathbb{K}}(x,y)$ entonces ϕ no está definido en P. Sin embargo, como un elemento de $\overline{\mathbb{K}}(E)$ tenemos que $\phi = \frac{x^2-x}{y} = \frac{y(x^2-x)}{y^2} = \frac{y(x^2-x)}{x^3-x} = \frac{(x^2-x)}{(x^2-x)(x+1)} = \frac{y}{x+1}$, de donde se tiene que $\phi(P) = 0$.

Con el objetivo de definir el valor de ϕ en el punto $\mathcal{O}$, sea $\ell \in \overline{\mathbb{K}}[E]$, de acuerdo con (B.3) ℓ se puede escribir de la forma $\ell(x,y) = v(x) + yw(x)$ donde $v(x), w(x) \in \overline{\mathbb{K}}[x]$.

Definición. Se define el *grado de* ℓ como $grad(\ell) = \max\{2\,grad_x(v),\ 3 + 2\,grad_x(w)\}$.

Supongamos que $\phi = f/g$ es una función racional con $f, g \in \overline{\mathbb{K}}[x,y]/\langle r\rangle$. Si se cumple que $grad(f) < grad(g)$ hacemos $\phi(\mathcal{O}) = 0$. Si $grad(f) > grad(g)$ entonces $\phi(\mathcal{O}) = \infty$. Si $grad(f) = grad(g)$, se tienen dos casos. Si $grad(f)$ es par entonces escribiendo f y g en forma canónica tendrán como términos de grado más alto ax^d y bx^d, respectivamente, para algunos a y b en $\mathbb{K}$ y algún entero d. Entonces $\phi(\mathcal{O}) = a/b$. De manera similar si $grad(f)$ es impar, así los términos de mayor grado tendrán la forma ayx^d y byx^d. Nuevamente $\phi(\mathcal{O}) = a/b$.

Teorema B.2. *Para cada punto racional P de $E(\mathbb{K})$ existe una función racional $u \in \overline{\mathbb{K}}(E)$ tal que es cero en P con la siguiente propiedad: Si ϕ es cualquier función racional distinta de cero, entonces $\phi = u^d s$ para algún entero d y alguna función racional $s \in \overline{\mathbb{K}}(E)$ tal que es finita y no es cero en P, es decir, $s(P) \neq 0, \infty$. Además, el número d no depende de la elección de u.*

La prueba del teorema previo se puede encontrar en la referencia [2]. A partir de este resultado tenemos la siguiente definición.

Definición. Una función u que satisface el teorema previo se le llama *parámetro uniformizador de P.*

Definición. Si ϕ es una función racional tal que $\phi = u^d s$, donde u es un parámetro uniformizador de P, diremos que *el orden de ϕ en P* es d y lo escribimos como $ord_P(\phi) = d$.

Proposición 11. *El punto P es un cero de ϕ si y sólo si $ord_P(\phi) > 0$, en ese caso, su multiplicidad se define como $ord_P(\phi)$. Similarmente, el punto P es un polo si y sólo si $ord_P(\phi) < 0$, en ese caso, su multiplicidad se define como $-ord_P(\phi)$.*

La proposición previa se puede consultar en las referencias [23], [31]. Por otro lado, las pruebas de los siguientes dos resultados se pueden hallar en la referencia [2].

Teorema B.3. *Sea ϕ una función racional en $E(\mathbb{K})$. Entonces $\sum_{P\in E(\mathbb{K})} ord_P(\phi) = 0$.*

Lema B.1. *Sea ϕ un polinomio en $E(\mathbb{K})$. La suma de las multiplicidades de los ceros de ϕ es igual al grado de ϕ.*

Dado que una función ϕ tiene un número finito de polos y ceros en $E(\mathbb{K})$ se define el *divisor de ϕ, $div(\phi)$* como $div(\phi) = \sum_{P\in E(\mathbb{K})} ord_P(\phi)(P)$.
Sean $\phi_1, \phi_2 \in \overline{\mathbb{K}}(E)$, se tienen las siguientes propiedades

$$div(\phi_1\phi_2) = div(\phi_1) + div(\phi_2), \tag{B.4}$$

$$div(\phi_1/\phi_2) = div(\phi_1) - div(\phi_2). \tag{B.5}$$

Teorema B.4. *Si ϕ es función racional distinta de cero entonces $div(\phi) \in Div^0$. Más aún, $div(\phi) = 0$ si y sólo si $\phi \in \overline{\mathbb{K}}^*$.*

La prueba del teorema previo se puede consultar en las referencias [36], [23]. A continuación se da la definición de cuándo se dice que un divisor es principal.

Definición. Un divisor $D \in Div(E(\mathbb{K}))$ es *principal* si es de la forma $D = div(\phi)$ para alguna ϕ función racional distinta de cero.

El siguiente teorema nos da una caracterización de divisores principales, el cual se puede consultar en las referencias [23], [2].

Teorema B.5. *Sea $D = \sum_{P \in E(\mathbb{K})} \eta_P(P)$ un divisor. Entonces D es principal si y sólo si $\sum_{P \in E(\mathbb{K})} \eta_P = 0$ y $\sum_{P \in E(\mathbb{K})} \eta_P P = \mathcal{O}$.*

Consideremos $Prin(E(\mathbb{K}))$ el conjunto de todos los divisores principales. Tenemos la siguiente afirmación cuya demostración se encuentra en [31] y que también se puede consultar en [23] .

Proposición 12. *El conjunto $Prin(E(\mathbb{K}))$ forma un subgrupo de Div^0.*

De acuerdo con la proposición previa tenemos que todos los divisores principales tienen grado cero.

Los divisores nos proporcionan otra forma de interpretar la intersección de curvas. Por ejemplo supongamos que se consideran dos curvas ζ_1 y ζ_2 las cuales no tiene un factor común, representados por polinomios en dos variables. Elegimos ϕ para la curva ζ_2, podemos analizar los divisores asociados a ϕ en la primera curva. Por definición tenemos que $div(\phi) = \sum_{P \in \zeta_1}(\eta_P)P$. Pero los ceros de ϕ son los puntos en los cuales se intercan las dos curvas y por el teorema de Bezout sabemos el número de puntos en dicha intersección. Por lo que de manera alternativa podemos escribir $div(\phi)$ como

$$div(\phi) = \sum_{P \in \zeta_1 \cap \zeta_2} I(P)P - \sum_{Q \in T \cap \zeta_2} \eta_Q Q;$$

donde I es como el teorema de Bezout y T es el conjunto de polos de ϕ contados con multiplicidad. A continuación definimos una relación de equivalencia entre dos divisores.

Definición. Diremos dos divisores D_1 y D_2 son *equivalentes*, $D_1 \sim D_2$, si $D_1 - D_2$ es un divisor principal.

Ejemplo B.2. Consideremos los puntos racionales P, Q, $P+Q$ y $\mathcal{O}$ de una curva elíptica $E(\mathbb{K})$ fija. Definamos los divisores $D_1 = P+Q$ y $D_2 = (P+Q)+\mathcal{O}$. Sean las rectas proyectivas $\mathcal{L}_1$ que pasa por P y Q; y $\mathcal{L}_2$ la que pasa por $P+Q$ y $\mathcal{O}$. Luego, $\mathcal{L}_1$ y $\mathcal{L}_2$ intersecan a $E(\mathbb{K})$ en un punto racional común, digamos $R = -(P+Q)$. Considerando que L_1 y L_2 son las respectivas ecuaciones de $\mathcal{L}_1$ y $\mathcal{L}_2$. Entonces tenemos que $div(L_1) = P+Q-(P+Q)$ y $div(L_2) = (P+Q)-(P+Q)+\mathcal{O}$. Definimos la función racional f en $E(\mathbb{K})$ como $f = L_1/L_2$. De esta manera obtenemos que

$$\begin{aligned} div(f) &= div(L_1) - div(L_2) = P+Q-(P+Q)-((P+Q)-(P+Q)+\mathcal{O}), \\ &= P+Q-((P+Q)+\mathcal{O}) = D_1 - D_2. \end{aligned}$$

De aquí que $D_1 = P+Q$ y $D_2 = (P+Q)+\mathcal{O}$ son equivalentes.

En lo que sigue, el objetivo es establecer un isomorfismo entre el grupo formado por los puntos racionales y el grupo de clases de divisores de grado cero de $E(\mathbb{K})$, para ello empezamos definiendo el espacio de Riemman-Roch.

Definición. Sea D un divisor. Definimos el *espacio de Riemann-Roch de D* como el conjunto

$$\mathcal{L}(D) = \{g \in \overline{\mathbb{K}}(E)^* : div(g) \geq -D\} \cup \{0\}, \tag{B.6}$$

donde $\overline{\mathbb{K}}(E)^*$ es el conjunto de funciones racionales en $E(\overline{\mathbb{K}})$ distintos de cero.

Proposición 13. *Para un divisor $D \in Div(E(\mathbb{K}))$, el conjunto $\mathcal{L}(D)$ es un espacio vectorial sobre $\overline{\mathbb{K}}(E)$.*

La demostración de la proposición previa se puede consultar en la referencia [31].

Proposición 14. *Sean D_1 y D_2 divisores tales que $D_1 \sim D_2$. Entonces los espacios $\mathcal{L}(D_1)$ y $\mathcal{L}(D_2)$ son isomorfos.*

Demostración. Sean D_1 y D_2 dos divisores equivalentes, entonces existe una función racional f distinta de cero tal que

$$D_1 - D_2 = div(f). \tag{B.7}$$

Sean $\mathcal{L}(D_1)$ y $\mathcal{L}(D_2)$ los respectivos espacios de Riemann-Roch de D_1 y D_2. Supongamos que $g \in \mathcal{L}(D_1)$ entonces $div(g) \geq -D_1$. Por (B.4) tenemos que $div(gf) = div(g) + div(f)$. De (B.7) y como $div(g) \geq -D_1$ se tiene que $div(g) + D_1 - D_2 \geq -D_2$. De esta manera concluimos que $div(gf) \geq -D_2$. Por definición $gf \in \mathcal{L}(D_2)$. Por otro lado, supongamos

que $g \in \mathcal{L}(D_2)$, en este caso, $div(g) \geq -D_2$. Por la relación (B.5) y por (B.7) $div(g/f) = div(g) - div(f) = div(g) - (D_1 - D_2)$. Como $div(g) \geq -D_2$ entonces $div(g/f) \geq -D1$. Así por definición $gf \in \mathcal{D}$.
Con lo anterior definimos el isomorfismo de entre $\mathcal{L}(D_1)$ y $\mathcal{L}(D_2)$ como

$$\begin{array}{c} \sigma : \mathcal{L}(D_1) \longrightarrow \mathcal{L}(D_2) \\ g \longmapsto gf \end{array} \quad \text{y} \quad \begin{array}{c} \sigma^{-1} : \mathcal{L}(D_2) \longrightarrow \mathcal{L}(D_1) \\ g \longmapsto g/f. \end{array}$$

□

Proposición 15. *Si D es un divisor tal que $grad(D) < 0$ tenemos que su espacio de Riemann-Roch es $\mathcal{L}(D) = \{0\}$.*

Demostración. Supongamos que $f \in \mathcal{L}(D)$ con f distinto de cero y que $grad(D) < 0$. Entonces $div(f) \geq -D$. Por otro lado, el grado de $div(f)$ es igual a cero, por tanto $0 \geq grad(-D) = -grad(D)$. De donde se concluye que $0 \leq grad(D)$, lo cual contradice la hipótesis de que $grad(D) < 0$; esto surge a partir de suponer que f no es cero, por lo que $f = 0$. □

Sea $\ell(D)$ la dimensión de $\mathcal{L}(D)$. La prueba de los siguientes resultados se pueden encontrar en las referencias [36], [31].

Teorema B.6 (Riemann-Roch). *Sea $\mathcal{C}$ una curva suave y $K_{\mathcal{C}}$ un divisor canónico en $\mathcal{C}$. Entonces existe un entero $g \geq 0$, el cual llamamos género de $\mathcal{C}$, que satisface la relación $\ell(D) - \ell(K_{\mathcal{C}} - D) = grad(D) - g + 1$, para todos los divisores D.*

Corolario B.6.1. *Para una curva fija $\mathcal{C}$ tenemos que*

1. *$\ell(K_{\mathcal{C}}) = g$,*
2. *$grad(K_{\mathcal{C}}) = 2g - 2$,*
3. *Si $grad(D) > 2g - 2$, entonces $\ell(D) = grad(D) - g + 1$.*

Proposición 16. *El género de una curva elíptica es 1.*

Como una curva elíptica es de género 1 el siguiente corolario se obtiene a partir del teorema de Riemann-Roch.

Corolario B.6.2. *En una curva elíptica la condición $grad(D) > 0$ implica que*

$$\ell(D) = grad(D). \tag{B.8}$$

Grupo de Picard

A continuación definimos el grupo de clases de divisores o bien grupo de Picard. Esto es, nos dice cuales son los divisores que no son principales. En particular, se tiene que $Prin(E(\mathbb{K})) \subseteq Div^0$, por lo que veremos qué divisores de grado cero no son principales

Definición. El grupo cociente $Div^0/Prin(E(\mathbb{K}))$ es llamado *grupo de Picard de* $E(\mathbb{K})$ *de grado cero* o *grupo de clases de divisores de grado cero de* $E(\mathbb{K})$, el cual escribimos como $Pic^0(E(\mathbb{K}))$.

Proposición 17. *Sean* P *y* Q *dos puntos racionales de una curva elíptica sobre* $\mathbb{K}$. *Entonces* $P \sim Q$ *si y sólo si* $P = Q$.

Demostración. Consideremos P y Q dos puntos racionales de una curva elíptica $E(\mathbb{K})$. Supongamos que $P \sim Q$, entonces tenemos que $div(f) = P - Q$, para alguna función racional en $E(\mathbb{K})$ distinta de cero; o bien reescribiendo esto, $div(f) + Q = P > 0$. Por (B.6) tenemos que $f \in \mathcal{L}(Q)$. Por el Corolario B.6.2 tenemos que $\ell(\mathcal{L}(Q)) = grad(Q) = 1$. Luego tenemos que el ideal generado por Q, $\langle Q \rangle$ es un subconjunto de $\mathcal{L}(Q)$ y ambos de dimensión 1. Por tanto se tiene la igualdad. Esto implica que f es una constante, así $div(f) = 0$. De esta manera se concluye que $P = Q$.
Ahora supongamos que $P = Q$ entonces $D = P - Q = 0$. Por tanto D es principal, lo que implica que $P \sim Q$. □

Proposición 18. *Sea* D *un divisor de grado* 0. *Existe un punto racional* P *de una curva elíptica sobre* $\mathbb{K}$ *el cual satisface* $D \sim P - \mathcal{O}$. *Además, este punto es único.*

Demostración. Sea D un divisor de grado cero, esto es, $grad(D) = 0$. Por otro lado, $grad(D+\mathcal{O}) = grad(D)+grad(\mathcal{O}) = 1$. Por el Corolario B.6.2, $\mathcal{D} + \mathcal{O} = grad(D+\mathcal{O}) = 1 > 0$, esto es, $\mathcal{D} + \mathcal{O}$ es generado por un elemento. Sea $f \in \mathcal{D} + \mathcal{O}$ distinto de cero, entonces por definición $div(f)+D+\mathcal{O} \geq 0$, o bien, $div(f) \geq -D-\mathcal{O}$. Lo que implica que existe un punto P tal que $div(f) = -D-\mathcal{O}+P$, de manera que $grad(-D-\mathcal{O}+P) = 0$, es decir, $grad(div(f)) = 0$. Luego por definición tenemos que $D \sim P - \mathcal{O}$. Para la unicidad, supongamos que existe otro punto $\tilde{P}$ tal que $D \sim \tilde{P} - \mathcal{O}$. Entonces $P - \mathcal{O} \sim \tilde{P} - \mathcal{O}$. Por la Proposición 17 tenemos que $\tilde{P} = P$. Por tanto el punto P es único. □

Ahora definamos una función $\sigma : D^0 \to E(\mathbb{K})$ dada por $D \to P - \mathcal{O}$ como en la proposición previa. La función σ es suprayectiva puesto que si tomamos cualquier punto racional P de $E(\mathbb{K})$, entonces tenemos que $P - \mathcal{O} \sim P - \mathcal{O}$ y por tanto $\sigma(P - \mathcal{O}) = P$.

Proposición 19. *Sean* $D_1, D_2 \in Div^0$. *Entonces* $\sigma(D_1) = \sigma(D_2)$ *si y sólo si* $D_1 \sim D_2$.

Demostración. Sean D_1 y D_2 divisores de grado cero. Supongamos que $P = \sigma(D_1)$ y $Q = \sigma(D_2)$, esto es, $D_1 \sim P - \mathcal{O}$ y $D_2 \sim Q - \mathcal{O}$. Entonces por definición existen dos funciones racionales en $E(\mathbb{K})$ tales que $div(f_1) = P - \mathcal{O} - D_1$ y $div(f_2) = Q - \mathcal{O} - D_2$. Así, $div(f_1/f_2) = div(f_1) - div(f_2) = P - \mathcal{O} - D_1 - (Q - \mathcal{O} - D_2) = P - Q - (D_1 - D_2)$. Por tanto tenemos que $P - Q \sim D_1 - D_2$. De esta manera, si suponemos que $\sigma(D_1) = \sigma(D_2)$, entonces $P = Q$ y por tanto $D_1 - D_2 \sim 0$, lo que implica que $D_1 \sim D_2$. Recíprocamente, si $D_1 \sim D_2$ entonces tenemos que $P - Q \sim \mathcal{O}$. Luego, por la Proposición 17 concluimos que $P = Q$. □

Por la proposición previa σ induce una biyección, $\tilde{\sigma} : Pic^0(E(\mathbb{K})) \to E(\mathbb{K})$ con inversa $\kappa : E(\mathbb{K}) \to Pic^0(E(\mathbb{K}))$ que asigna a P a la clase de divisores $P - \mathcal{O}$.

Teorema B.7. *Existe un homomorfismo entre una curva elíptica $E(\mathbb{K})$ y $Pic^0(E(\mathbb{K}))$.*

Demostración. Sean P y Q puntos racionales fijos de una curva elíptica $E(\mathbb{K})$ y sea L_1 la recta que pasa por ellos, esta recta interseca a $E(\mathbb{K})$ en un tercer punto, digamos R. Tomemos L_2 la recta que pasa por R y $\mathcal{O}$. Por la ecuación (B.2) $Z = 0$ interseca a $E(\mathbb{K})$ en el punto $\mathcal{O}$ con multiplicidad tres. Entonces se cumplen $div(L_1/Z) = P + Q + R - 3\mathcal{O}$, $div(L_2/Z) = R + (P + Q) + \mathcal{O} - 3\mathcal{O} = R + (P + Q) - 2\mathcal{O}$. Por lo tanto, obtenemos que

$$\begin{aligned} div(L_1/L_2) &= div(L_1/Z) - div(L_2/Z) \\ &= P + Q + R - 3\mathcal{O} - (R + (P + Q) - 2\mathcal{O}); \\ &= P + Q + (P + Q) - \mathcal{O}. \end{aligned}$$

Como L_1/L_2 es función racional entonces $div(L_1/L_2) \sim 0$. Así, $P - \mathcal{O} + Q - \mathcal{O} - (P+Q) + \mathcal{O} = 0$. De la definición de κ obtenemos que $\kappa(P) + \kappa(Q) = \kappa(P + Q)$. Por tanto κ es dicho homomorfismo entre $E(\mathbb{K})$ y $Pic^0(E(\mathbb{K}))$. □

Una consecuencia de este teorema es la propiedad asociativa de la operación suma definida en el conjunto de puntos racionales de una curva elíptica sobre $\mathbb{K}$. Para verificar esto, consideremos los puntos racionales P, Q y R de $E(\mathbb{K})$ y realicemos lo siguiente

$$\begin{aligned} \kappa((P + Q) + R) &= \kappa(P + Q) + \kappa(R) = \kappa(P) + \kappa(Q) + \kappa(R), \\ &= \kappa(P) + \kappa(Q + R) = \kappa(P + (Q + R)). \end{aligned}$$

Aplicando función inversa $\tilde{\sigma}$ obtenemos que $(P + Q) + R = P + (Q + R)$.

Con todo esto, se concluye que el conjunto de puntos racionales de una curva elíptica E sobre un campo $\mathbb{K}$ junto con la operación suma definida forman un grupo abeliano.

Apéndice C

Ejemplo de cifrado

Para el ejemplo que se desarrolla en este parte, tomamos una curva de Koblitz con parámetro $a = 0$ considerada en el campo $\mathbb{F}_{2^{23}}$, en este caso, se tiene que la curva tiene $2^2 * 2095853$ puntos racionales, donde un generador de la curva es el punto racional: $(x^{20} + x^{12} + x^9 + x^3 + x^2 + 1, x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^9 + x^8 + x^6 + x^3)$. O bien, utilizando la notación del Ejemplo 3.1, $(10120D, 76348)$. Además, consideremos el siguiente fragmento que corresponde a la obra *"El principito"* de Antoine de Saint-Exupéry. Esta obra actualmente es de dominio público y se puede descargar libremente de la siguiente dirección: *http:www.elejandria.com/*

"EXAMINELO ATENTAMENTE PARA QUE SEPAN RECONOCERLO SI ALGUN DIA VIAJANDO POR AFRICA CRUZAN EL DESIERTO SI POR CASUALIDAD PASAN POR AHI NO SE APRESUREN SE LOS RUEGO Y DETENGASE UN POCO PRECISAMENTE BAJO LA ESTRELLA SI UN NINO LLEGA HASTA USTEDES SI ESTE NINO RIE Y TIENE CABELLOS DE ORO Y NUNCA RESPONDE A SUS PREGUNTAS ADIVINARAN ENSEGUIDA QUIEN ES SEAN AMABLES CON EL Y COMUNIQUENME RAPIDAMENTE QUE HA REGRESADO NO ME DEJEN TAN TRISTEX"

Realizando la codificación correspondiente se obtiene la siguiente sucesión con 360 elementos, donde los primeros 10 dígitos se toman de la forma $0d$ con $0 \leq d \leq 9$.

04 23 00 12 08 13 04 11 14 00 19 04 13 19 00 12 04 13 19 04
15 00 17 00 16 20 04 18 04 15 00 13 17 04 02 14 13 14 02 04
17 11 14 18 08 00 11 06 20 13 03 08 00 21 08 00 09 00 13 03
14 15 14 17 00 05 17 08 02 00 02 17 20 25 00 13 04 11 03 04
18 08 04 17 19 14 18 08 15 14 17 02 00 18 20 00 11 08 03 00
03 15 00 18 00 13 15 14 17 00 07 08 13 14 18 04 00 15 17 04
18 20 17 04 13 18 04 11 14 18 17 20 04 06 14 24 03 04 19 04
13 06 00 18 04 20 13 15 14 02 14 15 17 04 02 08 18 00 12 04
13 19 04 01 00 09 14 11 00 04 18 19 17 04 11 11 00 18 08 20
13 13 08 13 14 11 11 04 06 00 07 00 18 19 00 20 18 19 04 03
04 18 18 08 04 18 19 04 13 08 13 14 17 08 04 24 19 08 04 13
04 02 00 01 04 11 11 14 18 03 04 14 17 14 24 13 20 13 02 00
17 04 18 15 14 13 03 04 00 18 20 18 15 17 04 06 20 13 19 00
18 00 03 08 21 08 13 00 17 00 13 04 13 18 04 06 20 08 03 00
16 20 08 04 13 04 18 18 04 00 13 00 12 00 01 11 04 18 02 14
13 04 11 24 02 14 12 20 13 08 16 20 04 13 12 04 17 00 15 08
03 00 12 04 13 19 04 16 20 04 07 00 17 04 06 17 04 18 00 03
14 13 14 12 04 03 04 09 04 13 19 00 13 19 17 08 18 19 04 23

Ahora lo que realizamos es hacer bloques de cierto tamaño, es este caso tomamos bloques de tres, es decir, para formar los dos primeros bloques, tomamos $04, 23, 00$ y $12, 08, 13$ de donde se obtienen los enteros 42300 y 120813, respectivamente y así sucesivamente hasta terminar. Obteniendo la siguiente sucesión de bloques, los cuales se obtuvieron realizando algoritmos en *SAGE* que se muestran con los nombres $codif(Msj)$ y $HaceBlok(TB, MSJ)$ en el Apéndice D. Cabe mencionar que la X que se agrega al final del fragmento es para que la longitud del mensaje sin considerar los espacios resulte un mútiplo de 3.

042300 120813 041114 001904 131900 120413 190415 001700 162004 180415
001317 040214 131402 041711 141808 001106 201303 080021 080009 001303
141514 170005 170802 000217 202500 130411 030418 080417 191418 081514
170200 182000 110803 000315 001800 131514 170007 081314 180400 151704
182017 041318 041114 181720 040614 240304 190413 060018 042013 151402
141517 040208 180012 041319 040100 091411 000418 191704 111100 180820
131308 131411 110406 000700 181900 201819 040304 181808 041819 041308
131417 080424 190804 130402 000104 111114 180304 141714 241320 130200
170418 151413 030400 182018 151704 062013 190018 000308 210813 001700
130413 180406 200803 001620 080413 041818 040013 001200 011104 180214

130411	240214	122013	081620	041312	041700	150803	001204	131904	162004
070017	040617	041800	031413	141204	030409	041319	001319	170818	190423

Trabajando con los bloques obtenidos realizamos el encajamiento haciendo uso del algoritmo descrito en 13, obteniendo:

(4E8C82,66C1F5)	(4B085A,3841CA)	(4F2818,3AAFAB)	(1975E6,546AB7)	(4A472B,65E987)
(517069,16A095)	(2E3124,34B5E0)	(6E281,14639A)	(54EBC2,545C3A)	(32D70C,14A750)
(7F560B,230A34)	(500246,1D9FAC)	(451AA6,3D6A9E)	(4433A7,3B97A7)	(4EAF1A,626C7F)
(730BAC,2AF1F)	(6BB01F,6EF138)	(29490E,7F4396)	(D6442,6BCB79)	(70423C,6F94E2)
(7C47B1,6EE765)	(525C27,375928)	(2C446D,6C2C55)	(360DFD,3567A9)	(732433,24F248)
(613647,142D22)	(6C3661,8B46D)	(245615,3F132C)	(DC700,44CC46)	(6716F3,ED65C)
(165D9F,145DD4)	(D2C41,692D33)	(6C3ECA,494B70)	(32AAAA,58E85C)	(38B6E8,230160)
(484C10,3D3C27)	(565805,DA6AF)	(343365,5C9BE0)	(749424,388263)	(4228EE,507578)
(6BE577,4D6B73)	(6BA636,4CACC5)	(4F2818,3AAFAB)	(357720,3F4030)	(22E4DD,2A8C1)
(353D68,2FB619)	(2A3505,1FA4AC)	(366D36,68FC27)	(482B47,68A67B)	(1EDFC,440A51)
(6C2593,2CAC24)	(402263,6841C7)	(642B01,18C0D7)	(6BE426,58B5C3)	(4E7F55,3CEE42)
(60F725,655E29)	(785552,57F69C)	(769E85,A281D)	(2C9826,43040)	(635178,7DA7A3)
(296BF6,31D0EC)	(7551EF,3EFE36)	(2E53AD,3A1ECA)	(5B3E12,3E3A61)	(38CB4B,1E7E7E)
(2CFF77,328187)	(51E825,365189)	(B6AF6,204189)	(4A6E86,6E3820)	(32930D,772D0D)
(2774C7,610A32)	(72351E,30A3E3)	(482772,41D44A)	(37554C,55463F)	(47EB4C,AEEC)
(32AC9B,51C3F4)	(1FEAD3,3486A4)	(5B6178,17445E)	(68E1EA,3BEF4F)	(3FB53,4744A2)
(3E6F75,444DBB)	(218696,318E56)	(E1A01,44E34A)	(6FA354,39D7F6)	(4228EE,507578)
(28DC79,71927E)	(7D1F1E,341AF0)	(74E987,611606)	(5736F4,16D9D)	(6E281,14639A)
(711675,77C1DC)	(64B407,704D2E)	(1C1BB5,765BC8)	(BB423,2B028C)	(6D431A,5B55F9)
(4A2C84,523A9A)	(7362AC,4F801E)	(1C717A,3F4805)	(3ABC4A,45CF68)	(5660DF,25B236)
(0613647,142D22)	(4E63BC,14CF)	(120E9D,63E8C6)	(50B36A,348FDE)	(7B8601,547F4F)
(16549A,5B255)	(48F35A,728C45)	(85578,681DAF)	(7FA027,C5A9)	(54EBC2,545C3A)
(18ACEB,2CF05E)	(64A7F5,74EDD6)	(2800E4,567DF5)	(2DEC20,58A5F4)	(63ACD1,4AEEA1)
(2187909,27A106)	(6BE426,58B5C3)	(7B522A,1A2973)	(5BA669,3009C8)	(1E386F,1CE96D)

Ahora, supongamos que el usuario B desea enviarle el fragmento previo al usuario A realizando un cifrado con el criptosistema ElGamal con autenticación utilizando puntos racionales de una curva de Koblitz. Para que B pueda realizar dicha tarea debe tener la llave pública de A, para ello consideremos que 1509254 y 1883318 son las respectivas llaves privadas de A y B. A partir de esto se tienen que las correspondientes llaves públicas son:

$$(57BC59, 62CAFE) \quad \text{y} \quad (F140C, 338E2A), \text{ respectivamente.}$$

Considerando un entero $k \in [2,\, 2^{23} - 1]$, $k = 5264258$ y eligiendo de manera arbitraria un valor inicial $VI = (758BA4, 028657)$, obtenemos que el mensaje cifrado es la siguiente

sucesión de puntos racionales.

(794675, 3AB3D1)	(4B536, 64244B)	(693711, 66B330)	(3850BE, 27282F)	(B510E, 197038)
(569994, 672DD7)	(4E15DB, 714E53)	(1B695F, 294002)	(5DEA6, EAB44)	(44E773, 1736DC)
(62F755, 5B5DD8)	(645086, 7B048B)	(175C53, 5323DA)	(6BF549, 790434)	(58C3D4, 60D765)
(34E921, 6468A3)	(259C47, 333F36)	(455E34, 2774AB)	(E48AF, 26B12A)	(1327E8, A0B5A)
(68028A, 42A324)	(7C3476, 114EDB)	(69F2FA, 48CCF7)	(401F72, 65F215)	(55183A, 2C63E6)
(47001C, 54D49E)	(6B7000, 41176E)	(7028F8, 2320EB)	(6F5167, 7F2958)	(5D8725, 3AAB9B)
(5F779F, 1F042A)	(99F03, 4BF535)	(70D04A, 1B0FED)	(BF953, 375846)	(6749CE, 14DE47)
(41C4BD, 5AF7C7)	(E46EB, 193390)	(159CDF, 1C69E6)	(5418AA, 66B498)	(5B3B01, 5E183)
(4A981F, 41D8EE)	(66EC92, 3A0C08)	(1702C5, 54F61C)	(04908FA, 445F9E)	(67504A, 51DE87)
(31C9F7, 734854)	(3FEA2F, 401549)	(76C500, 593219)	(2C30DC, 6779D)	(2B56E1, 280D05)
(3982D5, 617223)	(2CCB6B, 69156A)	(608835, 6B1991)	(2CCEE2, 27446F)	(6E8C24, 426B77)
(5F1E7C, 40CAA3)	(2FCA5F, 680EC6)	(7F4BCD, 34A759)	(26A70E, 2CB413)	(74D2FD, 76DBB8)
(376C42, 5A534A)	(431CF0, 56BE1A)	(22A698, 8C2A8)	(5078E1, 321659)	(70D64B, 57C228)
(78590B, 496648)	(1ED6D7, 2CF4B)	(50AC76, 5B0880)	(13B2C7, 4B367F)	(54DC57, 470C05)
(78FFCF, 79F341)	(68A6DA, 59EB90)	(79A351, 6787D2)	(5F12BA, 63C667)	(1C06A1, 5339F0)
(69535D, 281865)	(3C00D9, 1576BE)	(387D0C, 75EC93)	(16FA73, 8C55)	(1B08B5, 4A7BF4)
(10F4BD, 47C86E)	(739B10, 72C503)	(25FDEA, 4F2E34)	(48137, 7FED91)	(18C3FE, 4E16C1)
(40B7AE, 52375A)	(525DA5, 2A8B3)	(7B3A47, 1B735E)	(584A80, 75CF65)	(585098, 5AD246)
(3BADD0, 7487FE)	(641630, 7AF03F)	(48A0B2, 1FD806)	(6E071E, 39FE6C)	(7E69AD, 1C0B62)
(1BE77C, 3C0617)	(325787, 6A4DC5)	(29EBE6, 4E4F2D)	(794C15, 520D6C)	(7101AD, 39E40)
(4C882F, 3F7210)	(222B18, 6B54E6)	(CD84, 1F93C6)	(2DEF55, 3E58F5)	(452C3B, 7FC904)
(2A8ACC, 60975E)	(4C0C2F, 3B323F)	(2E9CFE, 13ECEF)	(389588, 72D3A9)	(69AB57, 2AAEE8)
(5CCD4F, 43C1FF)	(539F0D, 290DE6)	(6BD53A, 666B6A)	(780883, 386AE3)	(3F0267, 74FB2C)
(1102ED, 2C14E4)	(507A00, 25EC83)	(54D8F7, 5A5C52)	(DB1AD, 2A1E67)	(40EF1F, 70EA6E)

Por último utilizando el proceso de descifrado se puede verificar que se obtiene el mensaje original, es decir, la sucesión de puntos racionales que se obtiene coincide con la sucesión dada en el encajamiento.

Apéndice D

Códigos *SAGE*

En esta parte mostramos los códigos de *SAGE* que se realizaron y utilizaron para la construcción de ejemplos mostrados en este trabajo de tesis. Cabe mencionar que los manuales de *SAGE* que se pueden encontrar en la dirección *http://www.sagemath.org/es/*.

```
assume("00=0","1=01","2=02","3=03","4=04","5=05","6=06","7=07","8=08","9=09")
def codif(Msj):
# Codigo que recibe como parametro una cadena de caracteres y devuelve
# su codificacion
    cod=[]
    Alf={"A":'%02d'%(0,),"B":'%02d'%(1,),"C":'%02d'%(2,),"D":'%02d'%(3,),
         "E":'%02d'%(4,),"F":'%02d'%(5,),"G":'%02d'%(6,),"H":'%02d'%(7,),
         "I":'%02d'%(8,),"J":'%02d'%(9,),"K":'%02d'%(10,),"L":'%02d'%(11,),
         "M":'%02d'%(12,),"N":'%02d'%(13,),"O":'%02d'%(14,),"P":'%02d'%(15,),
         "Q":'%02d'%(16,),"R":'%02d'%(17,),"S":'%02d'%(18,),"T":'%02d'%(19,),
         "U":'%02d'%(20,),"V":'%02d'%(21,),"W":'%02d'%(22,),"X":'%02d'%(23,),
         "Y":'%02d'%(24,),"Z":'%02d'%(25,)}
    lon=len(Msj)
    for  k in range(lon):
        if Msj[k] != " ": ban=Msj[k]; cod.append(Alf[ban])
    return cod

def CoefIguaLen(lista,m):
    band=list(np.zeros((m,),dtype=int))
    for k in range(len(lista)): band[k]=lista[k]
    return band

def rotaLista(lista): return lista[-1: ] + lista[: -1]
```

```
def AFNormal(CBNEx,m,lista):
    PC=0
    for k in range(m): PC=PC + lista[k]*CBNEx[k]
    return PC

def CBNgen(m):
# Codigo que obtiene la base normal de F_{2^m}
    K1=K.list(); ran=0; el=K1[0]; j=0;
    while el in K and ran!=m:
        ban = 0; CBNCoef = list(); CBNExp = list();
        for k in range(0,m,1):
            ban = el^(2^k); CBNExp.append(ban);
            CBNCoef.append(CoefIguaLen(ban.polynomial().list(),m))
        j=j+1; el=K1[j];  M=matrix(CBNCoef); ran=rank(M)
    return CBNCoef,CBNExp

def trasforma(el,m):
    binar=el.digits(base=2);  binar=CoefIguaLen(binar,m);
    CB, ge= CBNgen(m);   ban=AFNormal(ge,m,binar)
    return ban

def traza(m,exp):
    sum=0
    for k in range(m): sum = sum + exp^(2^k)
    return sum

def solucion(XX,traz,m,a):
# Codigo que obtiene la solucion de la ecuacion cuadratica en caracteristica dos
    if XX!=0:
        u0=0;
        gamma=traz* XX^(-2);
        for t in range(1,m):
            for k in range(t): u0=u0 +gamma^(p^k)
        y1=XX*(u0 +1)
    if XX==0:  y1=1
    return y1

def HaceBlok(TB,MSJ):
    bloquesstr=[]; bloqueint=[];  j=0;
    while j<len(MSJ):  ban ="";
        for k in range(TB): ban = ban + MSJ[j+k]
        bloquesstr.append(ban)
        bloqueint.append(int(ban));  j=j+TB
```

```
    return [bloquesstr, bloqueint]

def multi161(num, mul):
    res=ListRev(CoefIguaLen((2^mul * num).digits(base=2),m))
    return res

Tabula=[[0,0,0,0,0 ],[0,0,0,0,1],[0,0,0,1,0],[0,0,0,1,1],[0,0,1,0,0],
[0,0,1,0,1],[0,0,1,1,0],[0,0,1,1,1],[0,1,0,0,0],[0,1,0,0,1],[0,1,0,1,0],
[0,1,0,1,1],[0,1,1,0,0],[0,1,1,0,1],[0,1,1,1,0],[0,1,1,1,1],[1,0,0,0,0],
[1,0,0,0,1],[1,0,0,1,0],[1,0,0,1,1],[1,0,1,0,0],[1,0,1,0,1],[1,0,1,1,0],
[1,0,1,1,1],[1,1,0,0,0],[1,1,0,0,1],[1,1,0,1,0],[1,1,0,1,1],[1,1,1,0,0],
[1,1,1,0,1],[1,1,1,1,0],[1,1,1,1,1]];

def Agreg1(nu,Lis,mul):
    ban=mul;  bandera=Lis; lonL=len(bandera)-1;
    for k in range(ban-1,-1,-1):
        bandera[lonL]= (bandera[lonL] + Tabula[nu][k])%2
        lonL=lonL-1
    return bandera

def encajapm(mul,Lista):
# Codigo  que realiza el encajamiento de una cadena de caracteres
# previamente codificados
    en=[]; k=2^mul; p=2^m
    for el in Lista:  j=0;
        while j < k:
            LL=multi161(el, mul)
            lista=Agreg1(j,LL,mul); elem=K(Expr(lista))
            if elem !=0:
                z=K(elem^3 + a* elem^2 +1)
                gamma=z* elem^(-2); tr=traza(m,gamma);
                if tr==0:
                    rz= solucion(elem,z,m); en.append(E(elem,rz));  j=k;
                else: j=j+1;
            else:
                rz=solucion(elem,z,m); en.append(E(elem,rz));  j=k;
    return en

def RoundingOff(lambda0, lambda1, a):
    mu =(-1)^(1-a);
    f0 = floor(lambda0 + 1/2); f1 = floor(lambda1 + 1/2);
    n0 = lambda0 - f0; n1 = lambda0 - f1;
    h0 = 0; h1 = 0; eta = 2*n0 + mu*n1;
```

```
    if eta >= 1:
        if n0 - 3*mu*n1 < -1: h1 = mu
        else: h0 = 1
    else:
        if n0 + 4*mu*n1 >= 2: h1 = mu
    if eta < -1:
        if n0 - 3*mu*n1 >= 1: h1 = -mu
        else: h0 = -1
    else:
        if n0 + 4*mu*n1 < -2: h1 = -mu
    q0 = f0 + h0; q1 = f1 + h1
    return q0,q1

def ReduccionModular(a, s0, s1, r, nn):
    mu =(-1)^(1-a); d0 = s0 + mu*s1
    lam0 = s0*nn/r; lam1 = s1*nn/r
    q0,q1 = RoundingOff(lam0, lam1, a)
    r0 = nn - d0*q0 - 2*s1* q1
    r1 = s1*q0 - s0*q1
    return r0,r1

def ConvABNormal(CBNc,CBNex,expr,m):
    v = expr.list();
    exprC = vector(CoefIguaLen(v,m))
    Mat = matrix(GF(2),CBNc).transpose()
    solu = Mat.solve_right(exprC)
    exprNew = 0
    for k in range(m):
        exprNew =  exprNew + solu[k]*CBNex[k].polynomial()
    if exprNew==expr:
        soluNew=vector(rotaLista(list(solu)))
        expnew=0
        for k in range(m):
            expnew=expnew + soluNew[k]*CBNex[k].polynomial()
        return expnew

def MultiplicacionEsc(n,Punto):
# Obtiene el multiplo escalar de un punto de una curva
    if n == -1: return E(Punto[0],Punto[0] + Punto[1])
    else:
        Q=E(0); P00 = Punto;
        r0,r1=ReduccionModular(a, s0, s1, r, n);
        while r0!= 0 or r1!=0:
```

```
            if r0%2 == 1: u = 2-((r0-2*r1)%4)
            else: u = 0
            r0 = r0 - u
            if u == 1: Q = Q + P00
            if u == -1: Q = Q - P00
            P0x=P00[0].polynomial(); P0y=P00[1].polynomial();
            P00x = ConvABNormal(CbC,CbEx,P0x,m)
            P00y = ConvABNormal(CbC,CbEx,P0y,m)
            P00 = E(P00x,P00y)
            [r0,r1] = [r1 + mu*r0/2, -r0/2]
        return Q

def Um(t):
    if t == 0: return 0;
    else:  if t == 1: return 1;
           else: return mu*Um(t-1) - 2*Um(t-2)

def tauk(t): return Um(t)*T - 2*Um(t-1)

def cocientauk(t):
    suma=1;
    for j in range(1,t): suma=suma + tauk(j)
    [d0,d1]=suma.coefficients(sparse=false)
    [s0,s1]=[d0+mu*d1, -d1]
    return [s0,s1]

def CalParam():
    if a == 0: r = CarE/4;
    else: r = CarE/2;
    s= cocientauk(m);
    return r, s

def cifra(C, k,Xac,Xbc,Xb,M, VI):
# Cifra un mensaje M, dadas, C: generador de la curva eliptica
# y^2 = x^3 + ax + b, k: entero aleatorio, Xac y Xbc: Claves publicas
# de A y B, respectivamente, Xb: llave privada de B, VI: valor inicial
    Cifrado=list()
    Pc =MultiplicacionEsc(k,C)
    Pkc = MultiplicacionEsc(k,Xac)
    Pbx = MultiplicacionEsc(Xb,Xac)
    for el in M:
        c = el+ VI + Pkc + Pbx; VI=c;
        Cifrado.append(c)
```

```
    return [Pc,Cifrado]
def descifra(c,C,Xbc,Xa, VI):
# Descifra el mensaje c, dadas, C: generador de la curva eliptica
# y^2 = x^3 + ax + b, Xbc: llave publica de B, Xa: llave privada de A
    Pabc=MultiplicacionEsc(Xa,Xbc)
    mPabc =MultiplicacionEsc(-1, Pabc)
    c1=MultiplicacionEsc(Xa,c[0])
    mc1 = MultiplicacionEsc(-1,c1)
    Cifc=c[1]; Descifrado=list()
    for el in Cifc:
        M1 = el + mPabc
        M = M1 + mc1-VI; VI= el;
        Descifrado.append(M)
    return Descifrado
```

Bibliografía

[1] Ángel, J. J. A. *Criptografía y curvas elípticas.* Tesis de maestría. UAM-I, 1998.

[2] Charlap, L. S., and Robbins, D. P. An elementary introduction to elliptic curve. *CRD Expository Report* **31** (December 1988), 1–51.

[3] Cohen, H., Gerahard Frey, R. A., Christophe Doche, T. L., and Kim Nguyen, F. V. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall/CRC, 2006.

[4] Cruz, J. M. *Multiplicación escalar en curvas de Koblitz: Arquitectura en Hardware Reconfigurable.* Tesis de maestría. IPN, 2005.

[5] den Boer, B. Diffie-Hellman is as strong as discrete log for certain primes. *Advances in Cryptology CRYPTO' 88, LNCS* **403** (1988), 530–539.

[6] Diffie, W., and Hellman, M. E. New directions in cryptography. *IEEE Transactions on information theory* **31** (1983), 469–472.

[7] ElGamal, T. A public key cryptosystems and a signature scheme based on discrete logarithms. *IEEE Transactions on information theory IT-***22** (1976), 644–654.

[8] Fraleigh, J. B. *Algebra abstracta: primer curso.* Mexico, Sitesa, 1988. Traducido de: A first course in abstract algebra, third edition.

[9] García, A. J., and Penagos, C. M. *Implementación eficiente de algoritmos criptográficos usando curvas de Koblitz.* Tesis de maestría. Fundación Universidad del Norte, 2008. https://www.exploit-db.com/docs/spanish/14963-[spanish]-elliptic-curve-cryptography-anomalous-curves.pdf.

[10] Gutiérrez, J. N. Fundamentos matemáticos de códigos y criptografía. Notas de clase, Otoño, 2015. https: //sites.google.com/site/cdematem/.

[11] Hankerson, D., Menezes, A., and Vanstone, S. *Guide to elliptic curve cryptography*. Springer, 2003.

[12] Hartshorne, R. *Algebraic Geometry*. Graduate Texts in Mathematics **52**. Springer, 1977.

[13] Herstein, I. N. *Álgebra moderna*. México: Trillas, 1990, (reimp. 2012). Traducido de: Topics in algebra, first edition.

[14] Kakish, M. Authenticated and secure ElGamal cryptosystem over elliptic curves. *Internat. J. of Research and Reviews in Applied Sciences, IJRRAS* **10** (2000), 306–313.

[15] Koblitz, N. Elliptic curve cryptosystems. *Mathematics of Computation* **48**, *No.177* (January 1987), 203–209.

[16] Koblitz, N. CM-Curves with good cryptographic properties. *J. Feigenbaum: Advances in Cryptology-CRYPTO'91, LNCS* **576** (1992), 279–287.

[17] Koblitz, N. *A course in number theory and cryptography*, second ed. Graduate Texts in Mathematics **114**. New York, N.Y. Editorial Spring-Verlag, 1994.

[18] Koblitz, N., Menezes, A., and Vanstone, S. The state of elliptic curve cryptography. *Designs, Codes and Cryptography* (2000), 173–193.

[19] Lidl, R., and Niederreiter, H. *Introduction to finite fields and their applications*. Press Syndicate of the University of Cambridge, 1986.

[20] Maurer, U. M. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. *Advances in Cryptology CRYPTO' 94, LNCS* **839** (1994), 271–281.

[21] McEliece, R. J. *Finite fields for computer scientists and engineers*. Kluwer Academic Publishers, 1989.

[22] Meier, W., and Staffelbach, O. Efficient multiplication on certain nonsupersingular elliptic curves. *E. F. Brickell: Advances in Criptology-CRYPTO'92, LNCS* **740** (1993), 333–344.

[23] Menezes, A. *Elliptic curve public key cryptosystems*. The Kluwer International Series in Engineering and Computer Science. Springer, 1995.

[24] Menezes, A. J. *Applications of finite fields.* The Kluwer International Series in Engineering and Computer Science. Springer Science +Bussienes media, LLC, 1993.

[25] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. *Handbook of applied cryptography.* Massachusetts Institute of Technology, June 1996.

[26] Miller, V. S. Use of elliptic curves in cryptography. *H. C. Williams: Advances in Cryptology-CRYPTO'85, LNCS 218* (1986), 417–426.

[27] Molin, R. A. *An introduction to cryptography*, second ed. Chapman & Hall/CRC, 2007.

[28] Morain, F., and Olivos, J. Speeding up the computations on an elliptic curve using addition-subtraction chains. *Informatique théoroique et applications/ Theoretical informatics and applications* **24***, No. 6* (1990), 531–544.

[29] Okeya, K., Schmidt-Samosa, K., Spahn, C., and Takagi, T. Signed binary representations revisited. *M. Franklin: CRYPTO 2004, LNCS 3152* (2004), 123–139.

[30] Paar, C., and Pelzl, J. *Understanding cryptography.* Springer, 2010.

[31] Pérez, I. *Associative property on the group of elliptic curves.* Tesis de licenciatura. Pontificia Univerisdad Católica del Perú, Septiembre 2017.

[32] Reyes, F. *Curvas elípticas y su aplicación en criptografía.* Tesis de licenciatura. UTM, Universidad Tecnológica de la Mixteca, Enero 2015. http://jupiter.utm.mx/~tesis_dig/12548.pdf.

[33] Rivest, R., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Comunications of the ACM* **21** (1978), 120–126.

[34] Rosen, K. H. *Elementary number theory and its applications.* Addison-Wesley, 1986.

[35] Seroussi, G. Compact representation of elliptic curve points over $\mathbb{F}_{2^n}$. *Copyright Hewlett-Packard Company* (September 1998). http://www.hpl.hp.com/techreports/98/HPL-98-94R1.pdf.

[36] Silverman, J. H. *The arithmetic of elliptic curves*, second ed. Graduate Texts in Mathematics **106**. Springer, 2008.

[37] Silverman, J. H., and Tate, J. *Rational points on elliptic curve*. Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[38] Simmons, G. J. Authentication theory/coding theory. *Advances in Cryptology CRYPTO' 84, LNCS* **196** (1985), 411–431.

[39] Solinas, J. Efficient arithmetic on Koblitz curves. *Designs, Codes and Cryptography* **19** (2000), 195–249.

[40] Stallings, W. *Cryptography and network security principles and practice*, fifth ed. Prentice Hall, 2006.

[41] Stinson, D. R. Some constructions and bounds for authentications codes. *Journal of Cryptology* **1** (January 1988), 37–51.

[42] Stinson, D. R. *Cryptography: theory and practice*. Boca Raton, FL, CRC Press, 1995.

[43] Sullivan, N. T. *Fast algorithms for arithmetic on elliptic curves over prime fields.* Tesis de maestría. Calgary, Alberta, January 2007.

[44] Testa, D., and Anni, S. Ma426: Elliptic curves, Dember 2014.

[45] Washington, L. C. *Introduction to cryptography with coding theory*, second ed. Departament of Mathematics, 2006.

[46] Washington, L. C. *Elliptic curves number theory and cryptography*, second ed. Champam & Hall / CRC, 2008.