UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

"Ataques Tipo MOV en Subgrupos de Curvas Elípticas"

T E S I S

QUE PARA OBTENER EL TITULO DE:

M A T E M A T I C O

P R E S E N T A :

DAVID JOSE MIRELES MORALES

FACULTAD DE CIENCIAS
UNAM

DIRECTOR DE TESIS: DR. FLORIAN LUCA

2005

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:
"Ataques Tipo MOV en Subgrupos de Curvas Elípticas"

realizado por ***David José Mireles Morales***

con número de cuenta ***402038230*** , quien cubrió los créditos de la carrera de:
Matemáticas

Dicho trabajo cuenta con nuestro voto aprobatorio.

A t e n t a m e n t e

Director de Tesis Propietario	***Dr. Florian Luca***
Propietario	***Dr. Javier Páez Cárdenas***
Propietario	***M. en C. Ana Irene Ramírez Galarza***
Suplente	***Dr. Alberto Gerardo Raggi Cárdenas***
Suplente	***M. en C. José Antonio Gómez Ortega***

Consejo Departamental de *Matemáticas*

M. en C. Alejandro Bravo Mojica

FACULTAD DE CIENCIAS
CONSEJO DEPARTAMENTAL
DE
MATEMATICAS

Ataques Tipo MOV en Subgrupos de Curvas Elípticas

David José Mireles Morales

Febrero de 2005

A la memoria de mis abuelos
Atilano, Betty, José y Andrés.

A mi abuela Caro,
con todo mi amor.

A mis padres David y Dey
y a mi hermano Juan,
porque me han hecho ser quien soy.

A Rebeca
por su amor,
que nuestros sueños
se hagan realidad.

Agradecimientos

Antes que nada quiero agradecer a mis padres todo lo que me han dado, de no ser por su apoyo incondicional esta historia sería muy diferente. A mi padre le doy gracias por ser mi primer maestro de matemáticas y por despertar en mí las ganas de entender, por su gran curiosidad científica y su cariño. Agradezco a mi madre su paciencia y preocupación, de ella adquirí el hábito de la lectura que tanto significa para mí, pero sobre todo le agradezco el amor que siempre me ha dado. Gracias también a Juan, quien ha puesto un poco de música (de cello) en nuestras vidas y es un excelente compañero para hacer matemáticas.

Agradezco a mi abue Caro, por ser una abuelita consentidora, moderna y cariñosa, al Lic. Pepe Valencia el haber compartido su experiencia y conocimientos conmigo, a mis tíos Hernan y Laura, por adoptarme como sobrino así como yo los adopté de tíos, al tío Bernardo que hizo la auditoría de ISO a esta tesis, a la tía Carmina por todo lo que me enseñó en materias que ninguno de mis padres entendía, a la tía Lourdes Hernández que estuvo con nosotros en las buenas y en las malas. A mis primos Daniel, Francisco, Lía y Vero. Quiero también agradecer a mamá Lupe el cariño que siempre ha tenido conmigo.

Le doy gracias a Florian Luca por haberme tomado como su estudiante en todo el sentido de la palabra, le agradezco también toda la confianza que depositó en mí y todas las oportunidades que puso a mi alcance. A mis profesores Alejandro Illanes y Verónica Martínez, quienes me dieron una probadita de lo que son las matemáticas y me convencieron con ella, a José Antonio Gómez le agradezco la oportunidad que me dio de ser su ayudante, es un verdadero honor. Quiero agradecer también a Leon Kushner haberme enseñado a trabajar a lo largo de sus cursos. A Javier Páez agradezco los valiosos consejos que siempre ha sabido darme y el haberme enseñado a tomar un café capuchino como se debe. A Ana Irene Ramírez le doy gracias porque

para ella cada alumno es una persona diferente y única. De todos ustedes aprendí mucho más que matemáticas.

Quisiera mencionar también a María Luisa Pérez Seguí, a Ignacio Barradas y en general a todo el equipo que hace posible la Olimpiada Mexicana de Matemáticas, participar en ella es una de las mejores experiencias que he tenido y fue definitivo en mi elección de carrera. Espero poder seguir participando mucho tiempo. Agradezco muy especialmente a Lucy Parra, quien siempre sabe tener una sonrisa para regalar y sin quien ningún trámite sería posible.

A todos mis amigos de la vocacional: a Samuel y Alma, que estuvieron conmigo desde el principio, a Manuel Tierno, Carlos Juárez , Carlos Ramírez, Diego y Sid les agradezco su fiestera amistad y el haber compartido conmigo momentos irrepetibles, son un grupo de amigos inolvidable. A Sandra porque es una persona que se sabe hacer querer y finalmente a Sofi, quien me convenció de que levantarme los domingos temprano para hacer ejercicio es divertido y que siempre ha estado cuando la he necesitado, gracias Sofi. A todos ustedes gracias por su amistad, tienen un lugar en la historia de mi vida.

A mis amigos de Ciencias: a Juan Manuel, de quien podría decir muchas cosas, pero ninguna mejor que gracias por tu amistad, es única. A Omar el saber compartir su gran talento cuando se lo pedí, a Daniel Labardini cuya dedicación es un ejemplo, a Pedro Antonio Ricardo Martín Solórzano Mancera cuyo afán por la precisión es un modelo a seguir, a Rocio Navarro por ser la cordura en la nave de los locos, a Pedro Valencia , a Francisco Barrios y a Mariano Zerón por compartir (entre muchas otras cosas) la boyardía conmigo. A Serena, quien siempre está de buenas. A todos los que alguna vez fueron a los cafés de los miércoles gracias, fueron unas reuniones irrepetibles.

Gracias Rebe, por caminar este tiempo de la mano conmigo. Gracias por compartir mis sueños de atardeceres y perros orejones. Gracias por quererme y darme tu amor como lo has hecho. Espero esta sea sólo una de las muchas páginas que escribiremos juntos. Esta tesis es para ti con todo mi amor.

Vaya también un reconocimiento a Alicia y Beto, sin quien ningún trabajo en criptografía sería posible.

Gracias por todo.

Davo

Contenido

Introducción

El objetivo de este trabajo es presentar el artículo [LMS], junto con los prerrequisitos teóricos necesarios para entenderlo. En el mencionado artículo se calcula la probabilidad de que una curva elíptica sea susceptible a un cálculo de logaritmos discretos usando el algoritmo **MOV**.

La importancia de estos resultados se debe a que la posibilidad de calcular logaritmos discretos se traduce en la vulnerabilidad de los esquemas criptográficos que hacen uso de curvas elípticas para su ejecución. La estructura del trabajo es entonces la siguiente:

En el capítulo 1 introducimos el concepto de criptografía de clave pública, presentamos además varios algoritmos criptográficos que hacen uso de un grupo abeliano y observamos cómo la seguridad de dichos algoritmos depende, entre otras cosas, de que el cálculo de logaritmos discretos sea difícil en los grupos con los cuales los algoritmos son efectuados.

Los capítulos 2 y 3 están enfocados a desarrollar la teoría necesaria para entender el algoritmo MOV y demostrar el teorema de Hasse-Weil. De manera más específica, en el capítulo 2 introducimos el concepto de curva elíptica y demostramos que sus puntos pueden ser dotados de manera natural de una estructura de grupo abeliano. Describimos una forma estándar para los endomorfismos de una curva elíptica (que son automorfismos de grupo dados por funciones algebraicas) y demostramos teoremas que relacionan el grado del endomorfismo con el número de puntos en el núcleo del endomorfismo. Caracterizamos también las funciones racionales que van de una curva elíptica al campo en términos de sus divisores.

En el tercer capítulo construimos el apareo de Weil, que resultará ser una herramienta de gran importancia en la demostración de los resultados más avanzados sobre curvas elípticas que nos interesan, entre ellos el teorema de Hasse-Weil. En este mismo capítulo construimos el algoritmo MOV (llamado así por sus creadores: Menezes, Okamoto y Vanstone) que reduce el problema

de cálculo de logaritmos discretos en una curva elíptica sobre un campo finito al del cálculo de logaritmos discretos en una extensión del campo base de la curva, esto resulta útil si la extensión no es de grado muy grande, puesto que se cuenta con el método de cálculo de índices para el cálculo de logaritmos discretos en campos finitos. El MOV hace uso extensivo del apareo de Weil.

Finalmente el capítulo 4 consiste de la presentación del artículo [LMS], en éste, dada una curva elíptica $\mathbf{E}[\mathbb{F}_p]$, calculamos la probabilidad de éxito del algoritmo MOV en el grupo de todos los puntos de $\mathbf{E}[\mathbb{F}_p]$, el subgrupo cíclico más grande de $\mathbf{E}[\mathbb{F}_p]$ y el subgrupo de orden primo más grande de $\mathbf{E}[\mathbb{F}_p]$. Mostramos que en todos estos casos la probabilidad de éxito del MOV es exponencialmente pequeña.

Incluimos además dos apéndices, en el primero presentamos varios algoritmos mencionados en la parte principal de este trabajo, esto pensando que la naturaleza de una tésis relacionada con la criptografía es escencialmente algorítmica. Entre los algoritmos presentados están la reducción de Pohlig-Hellman, el método ρ de Pollard y el método del cálculo de índices, todos estos algoritmos son usados para el cálculo de logaritmos discretos en distintas situaciones. Presentamos también el algoritmo de Schoof para el cálculo del orden de una curva elíptica sobre un campo finito.

En el segundo apéndice aprovechamos toda la teoría desarrollada en los capítulos 2 y 3 para demostrar las conjeturas de Weil en el caso particular de una curva elíptica. Esto se logra calculando explícitamente la función zeta asociada a una curva sobre un campo finito.

Nos parece importante mencionar que la gran mayoría de los teoremas relacionados con curvas elípticas son demostrados usando métodos elementales, en contraste con la literatura clásica, donde los teoremas son demostrados usando conceptos avanzados de geometría algebraica. Esto nos parece apropiado, pues la exposición resulta en gran medida autocontenida y la comprensión de las demostraciones no depende de un gran cantidad de conceptos avanzados. Es así que los únicos prerrequisitos para el entendimiento de esta tesis son conocimientos básicos de álgebra moderna y teoría de números.

Finalmente el autor se disculpa por cualquier error u omisión en esta tesis. Usando una frase de un buen amigo, espero encuentren muchos errores, porque eso querrá decir que leyeron este trabajo.

David José Mireles Morales
Ciudad Universitaria, 7 de febrero de 2005.

Capítulo I

Preliminares Criptográficos

...Amparo aprovechó un descuido de Amaranta y le entregó una carta a Rebeca Buendía...(Rebeca) dobló la carta con la punta de los dedos y se la escondió...
Gabriel García Márquez, Cien años de soledad.

I.1 Criptografía

El problema que la criptografía busca resolver es el de dos individuos a los cuales llamaremos Alicia y Beto, quienes pretenden intercambiar información de manera segura y sin embargo no tienen certeza de que el mensaje no será interceptado en su trayectoria, dicho de otra manera, se busca transmitir información confidencial usando un canal inseguro. La solución que la criptografía plantea es transformar el mensaje usando una clave y enviar el mensaje transformado, de manera tal que alguien que intercepte la comunicación no pueda entender lo que se envía, mientras el destinatario del mensaje puede simplemente revertir la transformación y de esta manera entender lo que se le envía; puesto en términos más formales, la idea es la siguiente:

Al mensaje original m que Alicia le quiere enviar a Beto lo llamaremos *mensaje en texto llano*, Alicia conoce una función $f : \mathcal{M} \longrightarrow \mathcal{C}$, donde $\mathcal{M}$ es el conjunto de mensajes en texto llano y $\mathcal{C}$ es su imagen, a los elementos de $\mathcal{C}$ los llamaremos *criptomensajes*; las restricciones que le impondremos a f es que sea una función biyectiva y que alguien que sólo conoce $f(m)$ no pueda recuperar m fácilmente. Una vez que Alicia y Beto han acordado una tal f, para intercambiar mensajes de manera segura lo único que debe hacer

Alicia para mandarle un mensaje a Beto es tomar su mensaje m, calcular $f(m)$ y enviarle esta información a Beto. Al recibir $f(m)$ lo que Beto debe hacer es aplicarle f^{-1} para recuperar m. Usualmente, se usan algoritmos criptográficos públicamente conocidos y lo que se hace para conservar la seguridad es que f, $\mathcal{M}$ y $\mathcal{C}$ dependan de cierta clave k, que es el elemento que Alicia y Beto deben mantener secreto para asegurar su confidencialidad.

Ejemplo I.1.1. Presentamos aqui *el criptosistema de Pohlig-Hellman* como ejemplo. Para intercambiar mensajes de manera segura Alicia y Beto deben hacer lo siguiente:

1. Eligen un número primo P muy grande.
2. Codifican sus mensajes como enteros M que cumplan $0 \leq M < P$.
3. Eligen dos números d y e que cumplan $ed \equiv 1 \pmod{P-1}$.
4. Para codificar un mensaje calculan $C = M^d$. Envian C.
5. Al recibir C, lo único que deben hacer para decodificarlo es encontrar el número N tal que $N \equiv C^e \pmod{P}$ y $0 \leq N < P$. El pequeño Teorema de Fermat asegura que $M = N$. Recuperando de este modo el mensaje original.

En la notación de la discusión anterior, la clave consiste de los números P, d y e. Notemos que para que el algoritmo sea seguro, d y e deben permanecer en secreto. Esto hace al esquema impráctico para ciertas aplicaciones, como veremos en el resto de esta sección.

Hasta 1976 todos los protocolos criptográficos adolecían de una deficiencia fundamental, ésta consistía en que alguien que conociera f podía calcular f^{-1} en un tiempo de orden de magnitud igual al que tomaba la implementación del criptosistema (como en nuestro ejemplo anterior, pues si conocemos P y d , podemos calcular e. Para hacer esto sólo hay que hacer uso del algoritmo de la división, el cual toma un tiempo de magnitud semejante al que cuesta la encripción o decripción de los mensajes); hoy día a este tipo de criptosistemas se les conoce como *sistemas de clave privada* o *simétricos* . Estos sistemas tienen claras desventajas, por ejemplo, dos individuos que no habían tenido contacto previo no podían intercambiar información de manera confidencial hasta no haberse puesto de acuerdo en la clave k que iban a usar, para lo

cual deberían hacer uso de un medio seguro, elemento con el que suponíamos no contaban por principio de cuentas.

Es así como Diffie y Hellman proponen en [DH] lo que es hoy conocido como *criptosistemas de clave pública* o *asimétricos*, protocolos donde el conocimiento de f no es suficiente para determinar f^{-1} de manera rápida. El algoritmo que Diffie y Hellman proponen es un protocolo para obtener una clave k que después será usada en un sistema simétrico.

Algoritmo de intercambio de clave de Diffie-Hellman
Desde este momento, y a menos que se indique lo contrario, denotaremos por G a un grupo abeliano finito donde las operaciones de grupo sean fáciles de calcular y en el cual tengamos la posibilidad de obtener elementos de forma azarosa. Así mismo, $P \in G$ denotará a un elemento de orden muy grande $N = \text{ord}(P)$, tal que N sea primo o sólo tenga un par de factores primos, ambos muy grandes. A un grupo con estas características lo llamaremos un grupo apropiado para fines criptográficos. Para intercambiar una clave, lo que Alicia y Beto deben hacer es lo siguiente:

1. Alicia y Beto se ponen de acuerdo , públicamente si se desea, en un grupo G y un elemento $P \in G$.

2. Alicia escoge al azar un entero $a \in \{1, 2, \ldots, N-1\}$, que debe mantener en secreto y calcula aP.

3. Beto escoge al azar un entero $b \in \{1, 2, \ldots, N-1\}$, que debe mantener en secreto y calcula bP.

4. Alicia y Beto intercambian aP y bP.

5. Usando a y bP, elementos que Alicia conoce, calcula $a(bP) = abP$.

6. Usando b y aP, elementos que Beto conoce, calcula $b(aP) = abP$.

7. Ahora Alicia y Beto pueden usar abP como clave para un sistema simétrico.

Podemos preguntarnos ahora porqué es que este algoritmo funciona. Para justificar su seguridad pensemos en alguien a quien llamaremos Eva, que obtuvo toda la información que estuvo en tránsito. Lo que Eva conoce es G, P, aP, bP, así que para obtener la clave que Alicia y Beto usarán, Eva debería ser capaz de resolver el siguiente problema:

Problema de Diffie-Hellman
Dados $P, aP, bP \in G$, calcular abP.

Profundamente relacionado con el problema anterior está el *Problema del Logaritmo Discreto*, por el cual nos referimos a lo siguiente:

Problema del Logaritmo Discreto
Dados $g, h \in G$, encontrar el menor natural x que satisface $h = g^x$, si es que existe, y si no existe determinarlo.

Si Eva sabe resolver el **PLD** (Problema del Logaritmo Discreto) en G, puede usar P y aP para calcular a, una vez hecho esto, le bastará calcular $a(bP)$ para obtener abP. Sin embargo, no se sabe si existe una forma de resolver el Problema de Diffie-Hellman sin calcular logaritmos discretos. El protocolo de Diffie Hellman no es propiamente un algoritmo de clave pública en el sentido en el que lo habíamos planteado previamente, pues si bien resuelve el problema de intercambio de información entre dos individuos que no han tenido contacto previo, no consta de una función $f : \mathcal{M} \longrightarrow \mathcal{C}$, donde el conocimiento de f no sea suficiente para calcular f^{-1}. Presentamos ahora un protocolo que es propiamente un criptosistema de clave pública, el cual se debe a T. ElGamal, quien lo introdujo en [ElG].

Protocolo de Encripción de ElGamal
Como es costumbre, Alicia le quiere enviar un mensaje a Beto. Primero Beto establece su clave pública como sigue: Escoge un grupo apropiado para fines criptográficos G, escoge también un elemento $P \in G$, de orden primo o con sólo un par de factores primos, ambos muy grandes. Elige un número entero s que mantendrá secreto y calcula $B = sP$. El grupo G y los elementos P y B conforman la clave pública de Beto. Estos son publicados. La clave secreta de Beto es el entero s. Para enviar un mensaje secreto a Beto, Alicia hace lo siguiente:

1. Consigue la clave pública de Beto.
2. Expresa su mensaje como un elemento $M \in G$.
3. Escoge en secreto un entero k al azar y calcula $M_1 = kP$.
4. Calcula $M_2 = M + kB$.
5. Envía (M_1, M_2) a Beto.

Beto efectúa la decripción calculando

$$M = M_2 - sM_1.$$

Esta decripción funciona porque

$$M_2 - sM_1 = (M + kB) - s(kP) = M + skP - skP = M.$$

Si hacemos el análisis correspondiente, Eva, quien obtuvo toda la información públicamente disponible conoce la clave pública de Beto y los elementos M_1 y M_2. Si Eva puede calcular logaritmos discretos en G, puede usar P y B para encontrar s, el cual a su vez puede usar para decriptar el mensaje calculando $M_2 - sM_1$. De igual manera podría usar P y M_1 para encontrar k, pudiendo entonces calcular $M = M_2 - kB$. Es de esta manera como al tener Eva la capacidad de encontrar logaritmos discretos en G el sistema se vuelve inseguro, sin embargo aún no se sabe si hay forma de encontrar M sin calcular logaritmos discretos, aunque la opinión de la mayoría es que encontrar M es tan difícil como resolver el **PLD** en G.

Para mantener la seguridad del protocolo es importante que Alicia use un valor diferente de k cada vez que envíe un mensaje a Beto. Para ver esto consideremos el siguiente ejemplo: supongamos que Alicia usa el mismo valor de k para dos mensajes M y M'. Eva reconoce esto porque $M_1 = M_1'$. Usando esto Eva puede calcular $M_2' - M_2 = M' - M$. Si Eva tiene forma de conocer el contenido de un mensaje, por ejemplo, si M es un mensaje que Alicia le habia mandado a Eva anteriormente, entonces Eva puede encontrar M' calculando $M' = M - M_2 + M_2'$. Es así como en este caso el conocimiento de un mensaje en texto llano M permite a Eva deducir otro mensaje en texto llano M'.

Es claro que los protocolos de Diffie-Hellman, encripción y firma digital de ElGamal y DSA (que más adelante introduciremos) son inseguros si en G se sabe resolver el **PLD**. Se cree, aunque no se ha probado, que hay grupos donde resolver el **PLD** es de hecho equivalente a resolver algunos de los protocolos anteriores. Sin embargo, hay ciertos grupos G para los cuales se ha probado que resolver el Problema de Diffie-Hellman es equivalente en un tiempo polinomial a resolver el **PLD** en G, para ver los detalles se puede consultar [Mau] y [MW], vale la pena mencionar que la reducción del **PLD** al Problema de Diffie-Hellman usa curvas elípticas, las cuales introduciremos en el siguiente capítulo.

I.2 Firmas Digitales

La criptografía moderna, en la forma en que es usada hoy en el mundo comercial, está ocupada de un número considerable de problemas. De estos, los más importantes son:

1. Confidencialidad: Un mensaje enviado por Alicia a Beto no puede ser entendido por nadie más.

2. Autenticidad: Beto sabe que sólo Alicia pudo haber enviado el mensaje que recibió.

3. Integridad: Beto sabe que el mensaje de Alicia no ha sido modificado mientras estaba en tránsito.

4. No-Repudio: Es imposible que Alicia se arrepienta después y diga que el mensaje no fue enviado por ella.

Para entender la importancia de estas cuatro propiedades consideremos el siguiente escenario: Alicia desea comprar un artículo de Beto usando el internet. Alicia envía sus instrucciones a Beto, las cuales contienen su número de tarjeta de crédito y detalles de pago. Alicia desea que esta información permanezca confidencial, pues no quiere que nadie conozca su número de tarjeta de crédito o lo que está comprando. Beto necesita saber que el mensaje en verdad viene de Alicia y no de un impostor. Alicia y Beto necesitan estar seguros que la integridad del mensaje será preservada, por ejemplo, que un tercero no cambiará el monto de la compra. Finalmente, Beto requiere de la propiedad de No-Repudio, es decir, que Alicia no pueda decir después que no envió instrucciones de compra.

La propiedad de confidencialidad es resuelta usando los protocolos que hemos descrito anteriormente, sin embargo cabe preguntarse cómo obtener las otras tres propiedades arriba mencionadas. Una buena fuente de inspiración siempre es la forma en la que estos problemas se resuelven en la vida diaria; después de un poco de reflexión, no es difícil darse cuenta de que estos problemas son resueltos con la firma autógrafa de los documentos. Repasemos entonces las propiedades requeridas: Autenticidad, se supone que nadie más puede hacer nuestra firma autógrafa, puesto que ésta refleja rasgos y características muy particulares de cada persona; Integridad, si un documento está firmado y no tiene tachaduras o enmendaduras, se acepta que la persona

que lo firmó está de acuerdo con los términos estipulados en la hoja de papel. Por último, llegamos al No-Repudio, si un documento tiene la firma de una persona es imposible que esta persona niegue haber aceptado los términos del documento (aquí podríamos entrar en la polémica del análisis grafológico y las falsificaciones, pero no es lo que nos interesa). Hemos visto cómo hasta cierto punto la firma autógrafa es el medio por el cual se garantizan las tres propiedades requeridas, así que no está de más buscar una especie de firma para resolver estos problemas en nuestra situación.

Es así como llegamos al siguiente escenario, supongamos que Alicia desea firmar un documento. La forma clásica de hacer esto es escribiendo su firma en un pedazo de papel que contenga el documento. Pensemos ahora que el documento es electrónico, por ejemplo, un archivo de una computadora. Una solución inocente sería digitalizar la firma de Alicia y anexarla al archivo que contiene el documento. En este caso un impostor puede copiar la firma y anexarla a otro documento. Este razonamiento hace claro que se deben tomar medidas para que la firma dependa del documento de tal manera que no se pueda usar de nuevo. Al mismo tiempo que la firma no debe ser falsificable y debe depender del documento, el destinatario del archivo necesita tener la capacidad de verificar que la firma es válida, así que además es necesario tener la certeza de que si un documento incluye una firma que es declarada como válida, sólo Alicia lo pudo haber firmado. Llegamos así a nuestra propuesta para resolver los problemas anteriormente descritos: al final de cada documento se debe incluir una *firma digital* que dependa del documento de tal modo que el cambio de algún dato en el documento genere también un cambio en la firma digital, dado un documento y su firma debe ser posible verificar que coinciden y además necesitamos la seguridad de que sólo el remitente pudo haber calculado la firma. Invito al lector a considerar lo complejo de la situación antes de leer los protocolos de firma digital que exponemos a continuación:

Protocolo de Firma Digital de ElGamal

Para firmar un documento, Alicia debe establecer una clave privada de manera idéntica al caso de encripción de ElGamal, es decir: un grupo G apropiado para usos criptográficos, un elemento $A \in G$ de orden N muy grande y primo o con sólo un par de factores y un entero a con el que calcula $B = aA$. Finalmente, elige una función $f : G \longrightarrow \mathbb{Z}$ la cual no necesita tener ninguna propiedad especial, salvo que su imagen debe ser grande y sólo un pequeño número de elementos de G deben tener el mismo valor bajo f.

La clave pública de Alicia consiste de G, f, A y B. Mantiene a en secreto. El entero N no necesita ser hecho público, aunque su conocimiento no afecta la seguridad del sistema. Para firmar un documento, Alicia hace lo siguiente:

1. Representa el documento como un entero m (si $m > N$, elige un elemento diferente o una función de Hash, ver más adelante).
2. Elige un entero k al azar con $m.c.d.(k, N) = 1$ y calcula $R = kA$.
3. Calcula $s \equiv k^{-1}(m - af(R)) \pmod{N}$.

El mensaje firmado consiste de (m, R, s). Notemos que los elementos m, s son enteros, mientras R es un elemento de G. Veamos también que para la firma Alicia no necesita mantener el mensaje m en secreto, si desea hacerlo entonces debe usar alguna forma de encripción. Beto verifica la firma como sigue:

1. Obtiene la clave pública de Alicia.
2. Calcula $V_1 = f(R)B + sR$ y $V_2 = mA$.
3. Si $V1 = V2$, declara la firma como válida

Veamos cómo siempre que un mensaje es firmado correctamente se cumple la ecuación de verificación:

$$V_1 = f(R)BsR = (f(R)a)A + skA = (f(R)a)A + (m - af(R))A = mA = V_2.$$

Hemos usado el hecho de que $sk \equiv m - af(R) \pmod{N}$, que es equivalente a que $sk = m - af(R) + zN$ para algún entero z. Entonces,

$$skA = (m - af(R))A + zNA = (m - af(R))A + e = (m - af(R))A.$$

Esto explica porqué se definió s usando congruencias módulo N.

Si Eva puede calcular logaritmos discretos en G, entonces puede usar el conocimiento de A y B para encontrar a, acabando así con la seguridad del protocolo, puesto que podría poner la firma de Alicia en cualquier mensaje. Alternativamente, Eva puede usar A y R para encontrar k, puesto que conoce $s, f(R), m$; puede usar entonces $ks \equiv m - af(R) \pmod{N}$ para encontrar

a. Si $d = mcd(f(R), N) \neq 1$, entonces $af(R) \equiv m - ks \pmod{N}$ tiene d soluciones para a y si d es pequeño, Eva puede intentar con cada posibilidad hasta obtener un a que cumpla $B = aA$. Puede entonces usar a como antes para falsificar la firma de Alicia en cualquier mensaje.

Como hemos visto, para asegurar un esquema de firma seguro, Alicia debe mantener a y k en secreto. También debe usar un valor diferente de k para cada firma, como ejemplifica lo siguiente: supongamos que ella firma los mensajes m y m' usando el mismo valor de k, para obtener los mensajes firmados (m, R, s) y (m', R, s'). Eva se da cuenta inmediatamente de que el mismo valor de k se ha usado dos veces, puesto que el valor de R es el mismo para ambas firmas. Las ecuaciones para s, s' resultan en lo siguiente:

$$ks \equiv m - af(R) \pmod{N} \quad , \quad ks' \equiv m' - af(R) \pmod{N}.$$

Restando obtenemos $k(s - s') \equiv m - m' \pmod{N}$ y si hacemos $d = \text{mcd}(s - s', N)$, entonces existen d valores posibles para k. Eva puede intentar con cada uno hasta llegar al que cumpla $R = kA$. Una vez que conoce k puede encontrar a como explicamos anteriormente.

Es claro que si Eva puede encontrar logaritmos discretos en G, entonces tiene forma de generar firmas falsas, sin embargo, tal vez no es necesario que Eva sepa encontrar logaritmos discretos para poder falsificar la firma de Alicia en algún otro mensaje m. Todo lo que Eva debe hacer es generar R, s tales que la ecuación de verificación $V_1 = V_2$ se cumpla. Esto quiere decir que debe encontrar $R \in G$ y un entero s tales que

$$f(R)B + sR = mA.$$

Si empieza por elegir el elemento $R \in G$, entonces necesita poder resolver el problema del logaritmo discreto $sR = mA - f(R)B$ para el entero s. Si decide escoger primero s, entonces debe ser capaz de encontrar R. Esto parece ser tan complejo como el problema del logaritmo discreto, aunque no ha sido analizado tan profundamente. Cabe aclarar que nadie ha descartado la posibilidad de encontrar un algoritmo que calcule R y s simultaneamente. Hay formas de usar un mensaje con una firma válida para generar otro mensaje con una firma válida (ver el ejemplo I.2.1), sin embargo, los mensajes así generados tienen una muy baja probabilidad de tener sentido.

En la práctica, una desventaja del sistema de ElGamal es que el mensaje firmado (m, R, s) tiene una longitud de tres veces la del mensaje original, es

por eso que usualmente se usa una *función de Hash* H y lo que se hace es aplicarle el protocolo de firma digital a $H(m)$ en vez de a m. Una función criptográfica de Hash es una función que toma entradas de longitud arbitraria, a veces mensajes de millones de bits, y regresa valores de longitud fija, por ejemplo 160 bits. Es a $H(m)$, el valor de la función de Hash aplicada a m, que se le aplican los protocolos de firma digital. Una función de Hash apropiada para fines criptográficos debe tener las siguientes características:

1. Dado m, $H(m)$ se puede calcular rápidamente.

2. Dado y no es factible encontrar m tal que $H(m) = y$. Esto se conoce como que H es resistente a las preimágenes.

3. No es factible encontar dos mensajes m_1 y m_2 con $H(m_1) = H(m_2)$. Esto se conoce como ser resistente a las colisiones.

Es claro que la razón de exigirle (2) y (3) a una función de Hash es evitar que un impostor produzca mensajes con un valor de Hash deseado o dos mensajes con el mismo valor de Hash, con lo que tendría la posibilidad de generar firmas válidas sin el conocimento de la clave secreta del emisor. Hay disponible una cantidad razonable de funciones de Hash, por ejemplo MD5 (Rivest), con una salida de 128-bits y SHA (Secure Hash Algorithm, NIST) con una salida de 160-bits (ver [MOV2]).

La ventaja del uso de la función de Hash es que un mesaje de millones de bits de largo tiene una firma de sólo unos cuantos cientos de bits, y aun así, gracias a las propiedades exigidas a H, es difícil encontrar otro mensaje con la misma firma; con esto garantizamos la seguridad en el esquema de firma, al tiempo que lo aceleramos considerablemente.

Parece apropiado comentar aquí que aunque es común introducir las técnicas de clave pública en el contexto de la protección de la confidencialidad, los protocolos de clave pública son usualmente imprácticos para estos propósitos, puesto que son ordenes de magnitud más lentos que los protocolos simétricos. El uso de la clave pública en la confidencialidad está usualmente limitado a la transmisión de claves que después serán usadas para un algoritmo simétrico. Por otro lado, las firmas digitales que proporcionan las propiedades de autenticación, integridad y no-repudio, todas ellas requeridas en el comercio electrónico, parecen requerir el uso de la criptografía de clave pública.

Ejemplo I.2.1. En este ejemplo presentamos una forma de generar mensajes firmados válidos, bajo el esquema de firma digital de ElGamal, veamos.

Supongamos que se usó el protocolo de firma digital de ElGamal para generar el mensaje firmado (m, R, s) (A lo largo de este ejemplo conservaremos la notación usada al describir dicho protocolo). Denotemos por h a un entero que cumpla $\text{mcd}(h, N) = 1$. Supongamos también que $\text{mcd}(f(R), N) = 1$. Sean

$$\begin{aligned} R' = hR \quad & s' \equiv sf(R')f(R)^{-1}h^{-1} && \pmod{N}. \\ & m' \equiv mf(R')f(R)^{-1} && \pmod{N}. \end{aligned}$$

Denotemos por V_1 y V_2 a los valores de verificación del mensaje original (m, R, s), se sigue que $V_1 = V_2$. Veamos que (m', R', s') es un mensaje firmado válido, ya que tenemos:

$$V_1{}' = f(R')B + s'R \quad \text{y} \quad V_2{}' = m'A,$$

notemos ahora que $V_1{}' = f(R')f(R)^{-1}V_1$ y que $V_2{}' = f(R')f(R)^{-1}V_2$, de donde se sigue que $V_1{}' = V_2{}'$, por lo que el mensaje firmado (m', R', s') sería aceptado como válido. Afortunadamente, es muy poco probable que el mensaje m' tenga sentido, por lo que la seguridad del protocolo no se ve amenazada.

Presentamos ahora otro esquema de firma digital, conocido como **DSA** o Estándar de Firma Digital, por sus siglas en ingles:

DSA Digital Signature Algorithm El DSA es una variante del esquema de firma digital de ElGamal, el cual presentaremos a continuación: supongamos que Alicia quiere firmar un documento m, el cual representaremos con un entero. Alicia escoje un grupo G, útil para propósitos criptográficos y tal que $\#G = rp$, donde p es un primo grande y r es un entero pequeño, usualmente $1, 2$ o 4 (r debe ser pequeño para que el algoritmo sea eficiente). Alicia escoge un punto base $B \in G$ de orden p. Finalmente, elige un entero a y calcula $Q = aB$. Además de todo esto necesita de una función $f : G \longrightarrow \mathbb{Z}$, justo como la usada en el protocolo de firma de ElGamal y debe hacer pública la siguiente información: G, p, B, Q, f. Para firmar un mensaje hace lo siguiente:

1. Escoge un entero k al azar con $1 \leq k < p$ y calcula $R = kG$.

2. Calcula $s = k^{-1}(m + af(R)) \pmod{p}$.

El mensaje firmado es (m, R, s). Para verificar la firma, Beto hace lo siguiente:

1. Calcula $u_1 = s^{-1}m \pmod{r}$ y $u_2 = s^{-1}f(R) \pmod{p}$.

2. Calcula $V = u_1B + u_2Q$.

3. Acepta la firma como valida si $V = R$.

Veamos cómo siempre que un mensaje es firmado correctamente la ecuación de verificación se cumple:

$$V = u_1B + u_2Q = (s^{-1}m)B + (s^{-1}f(R))Q = s^{-1}(mB + aB) = kB = R.$$

La principal diferencia entre la firma digital de ElGamal y la de DSA es al momento de la verificación, puesto que en el sistema de ElGamal la ecuación de verificación $f(R)B + sR = mA$ requiere de efectuar tres exponenciaciones en el grupo (ésta es la parte más lenta del algoritmo), mientras en DSA sólo dos exponenciaciones de grupo son necesarias. Si se deben verificar muchas firmas, entonces la eficiencia mejorada que se obtiene del DSA es valiosa.

Capítulo II

Curvas Elípticas

Se puede escribir indefinidamente sobre curvas elípticas, esto no es una amenaza...
Serge Lang

En este capítulo introducimos el concepto de curva elíptica y estudiamos algunas de sus propiedades básicas. Comenzamos demostrando que sus puntos pueden ser dotados de estructura de grupo abeliano de una forma natural, para después revisar la relación entre la estructura de grupo definida y las propiedades generales de las curvas. Una vez hecho esto discutimos brevemente la relación entre las curvas elípticas y la criptografía. Estudiamos también las funciones de una curva en si misma que están dadas por funciones racionales y que además respetan la estructura de grupo, a estas funciones las llamaremos endomorfismos. Daremos una forma estándar para los endomorfismos y demostraremos propiedades muy interesantes usando dicha forma estándar. Finalizamos el capítulo caracterizando las funciones racionales que van de una curva al campo base en términos de su divisor asociado.

II.1 Definición

Definimos una *curva elíptica* como el conjunto de puntos $(x : y : z)$ en el plano proyectivo $\mathbb{P}^2_K$ sobre el campo K, que satisfacen la ecuación

$$ZY^2 = X^3 + AZ^2X + BZ^3 \tag{1}$$

donde $A, B \in K$ y $4A^3+27B^2 \neq 0$. Notemos que esta definición no depende de la elección del representante, puesto que la ecuación es un polinomio homogeneo. La condición $4A^3 + 27B^2 \neq 0$ se pide para asegurar la suavidad de la curva. En la práctica lo que esta condición garantiza es que la curva tendrá una tangente bien definida en cada punto. La explicación de esto es que si $\{e_1, e_2, e_3\}$ son las raices del polinomio $X^3 + AX + B$, entonces no es difícil ver que $\prod_{i<j}(e_i - e_j)^2 = 4A^3 + 27B^2$.

Observemos que una curva elíptica tiene un sólo punto al infinito, ya que si $z = 0$ entonces $x = 0$ y como no todas las coordenadas pueden ser cero se sigue que, sin pérdida de generalidad, $y = 1$, es decir, el único punto al infinito de una curva es el que corresponde a la clase de equivalencia del $[0 : 1 : 0]$. Es por esta razón que frecuentemente consideraremos a una curva elíptica como las soluciones (x, y) en el plano afín $\mathbb{A}^2_K$ sobre K de

$$Y^2 = X^3 + AX + B \tag{2}$$

junto con un punto al cual denotaremos $\mathcal{O}$, que es el punto al infinito correspondiente a las rectas verticales de $\mathbb{A}^2_K$. Decimos que una curva está definida sobre un campo K si $A, B \in K$, en este caso denotaremos por

$$\mathbf{E}(K) = \{(x, y) | y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

a los puntos de la curva con coordenadas en K. Hemos introducido esta notación porque si una curva está definida sobre K, entonces también lo estará sobre $\overline{K}$, y entonces denotaremos por $\mathbf{E}(\overline{K})$ a las soluciones a la ecuación (2) con coordenadas en $\overline{K}$. Cuando el campo sobre el que estemos trabajando sea claro del contexto o no sea relevante para la exposición, denotaremos a una curva elíptica simplemente por $\mathbf{E}$.

Notemos ahora que si tenemos dos puntos $P, Q \in \mathbf{E}(K)$, entonces la linea por P y Q intersectará a $\mathbf{E}(K)$ en un tercer punto (no daremos ahora una demostración de esta afirmación porque más tarde encontraremos fórmulas explícitas para el cálculo de este tercer punto). Esta afirmación sobre un tercer punto de intersección debe ser interpretada con cuidado, ya que puede ser que la recta no intersecte a la curva en 3 puntos diferentes, pero entonces lo que pasa es que la recta es de hecho tangente a $\mathbf{E}$ en P o Q. Esto se puede interpretar como una intersección doble o triple, así que deberemos considerar dicho punto de tangencia como el tercer punto de intersección de la recta. Cabe además aclarar qué es lo que pasa con el punto $\mathcal{O}$. Si trabajamos sobre $\mathbb{P}^2_K$ entonces no hay nada que hacer, puesto que se puede

tratar como cualquier otro punto, pero si deseamos restringirnos a $\mathbf{A}^2_K$, sólo debemos tratarlo formalmente como un punto situado "al final "de las rectas verticales.

Si al tercer punto de intersección de la recta por P y Q con $\mathbf{E}(K)$ lo denotamos por $P * Q$, entonces podemos definir una operación binaria en $\mathbf{E}(K)$ de la siguiente manera:

$$+ : \mathbf{E}(K) \times \mathbf{E}(K) \longrightarrow \mathbf{E}(K) \tag{3}$$

$$P + Q \longmapsto (P * Q) * \mathcal{O} \tag{4}$$

Resulta que $(\mathbf{E}(K), +)$ es un grupo abeliano al equiparlo con esta operación binaria. Daremos ahora fórmulas para calcular $(x_1, y_1) + (x_2, y_2)$.

Si $x_1 \neq x_2$, entonces la recta por (x_1, y_1) y (x_2, y_2) tiene pendiente

$$m = \frac{y_1 - y_2}{x_1 - x_2}$$

por lo tanto la recta por estos puntos tiene ecuación

$$y = \frac{y_1 - y_2}{x_1 - x_2}(x - x_1) + y_1. \tag{5}$$

sustituyendo todo esto en la ecuación (2), obtenemos

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B, \tag{6}$$

lo que se puede reescribir como

$$0 = x^3 - m^2x^2 + \cdots \quad .$$

como este polinomio ya tiene dos raices sobre K (a saber, x_1 y x_2) , podemos calcular la tercera. Esto se debe a que sabemos que la suma de sus raices es m^2, por lo tanto podemos calcular x_3 como

$$x_3 = m^2 - x_1 - x_2. \tag{7}$$

Para calcular el valor de y_3 sólo usamos la ecuación (6) y recordamos que debemos reflejar sobre el eje X, así que

$$y_3 = m(x_1 - x_3) - y_1. \tag{8}$$

En el caso $P = Q = (x_1, y_1)$, la recta por ambos puntos es la recta tangente. Para encontrar su pendiente, podemos derivar implicitamente en la ecuación(2) para obtener

$$2y\frac{dy}{dx} = 3x^2 + A.$$

Si $y = 0$, entonces la recta tangente es vertical y por tanto el tercer punto de intersección sera $\mathcal{O}$, el cual al ser reflejado en el eje X se queda igual. Si $y \neq 0$, la tangente tiene pendiente

$$m = \frac{3x_1^2 + A}{2y_1},$$

por lo tanto la tangente tiene ecuación

$$y = m(x - x_1) + y_1,$$

lo cual al ser sustituido en (2) resulta en

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

Como en el caso anterior esto se puede reescribir como

$$0 = x^3 - m^2x2 + \cdots \quad .$$

y al conocer una raiz doble (a saber, x_1) del polinomio anterior podemos calcular la tercera como

$$x_2 = m^2 - 2x_1.$$

Usando la ecuación de la recta y recordando reflejar en el eje X, podemos encontrar y_2 como

$$y_2 = m(x_1 - x_2) - y_1.$$

Por último, en el caso $x_1 = x_2$ pero $y_1 = -y_2$, es claro que la recta por ambos puntos es vertical, y por lo tanto el tercer punto de intersección de esta recta con $\mathbf{E}(K)$ es $\mathcal{O}$, el cual al ser reflejado con respecto al eje X se queda fijo, por lo tanto en este caso definimos la suma $(x_1, y_1) + (x_2, y_2) = \mathcal{O}$.

Una vez dadas las fórmulas de suma en la curva, podemos enunciar el siguiente Teorema.

Teorema II.1.1. *Una curva elíptica* $\mathbf{E}(K)$ *equipada con la operación binaria* $+$ *resulta ser un grupo abeliano con neutro* $\mathcal{O}$.

De las observaciones anteriores es claro que $\mathcal{O}$ es neutro de la operación binaria. La existencia de inversos es también clara, tanto de la definición como de la observación hecha anteriormente, donde mencionamos que $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$. Sólo la asociatividad es difícil de demostrar, y para hacerlo tomaremos prestado el siguiente Teorema de la geometría proyectiva (ver el libro de Fulton [Ful]):

Teorema II.1.2. *Sea* $\mathbf{E}(K)$ *una curva elíptica,* C', C'' *cúbicas. Supongase que* $\mathbf{E}(K) \cap C' = \{P_i\}_{i=1}^{9}$. *Este conjunto consiste de los puntos en los que* $\mathbf{E}(K)$ *se intersecta con* C'. *Un punto* P *aparece en el conjunto tantas veces como la multiplicidad de la intersección de* $\mathbf{E}(K)$ *con* C' *en* P. *Supongase además que* $\mathbf{E}(K) \cap C'' = \{P_i\}_{i=1}^{8} \cup \{Q\}$. *Entonces* $Q = P_9$.

Usando el Teorema II.1.2 daremos una demostración de la asociatividad.

Demostración. Supongamos que $P, Q, R \in \mathbf{E}(K)$. Queremos demostrar que $(P+Q)+R = P+(Q+R)$. Sea L_1 la recta por los puntos P y Q. Llamemos S' a su tercer punto de intersección con $\mathbf{E}$. Sea M_1 la recta por los puntos $\mathcal{O}$ y S', la cual tiene a S como tercer punto de intersección con $\mathbf{E}$. Entonces $P + Q = S$. Sea L_2 la recta por S y R y T' el tercer punto de intersección de L_2 con $\mathbf{E}$.

Análogamente, sea M_2 la recta por Q y R, con U' como tercer punto de intersección, L_3 la recta por $\mathcal{O}, U', U$, donde $Q + R = U$, y por último M_3 la linea por P y U con tercer punto de intersección T''. Como $(P + Q) + R = \mathcal{O} * T'$, y $P + (Q + R) = \mathcal{O} * T''$, basta demostrar que $T' = T''$. Para esto, usemos el Teorema II.1.2con $C' = L_1L_2L_3$ y $C'' = M_1M_2M_3$.

Entonces tenemos que

$$\mathbf{E} \cap C' = \{\mathcal{O}, S, S', U, U', P, Q, R, T'\}$$
$$\mathbf{E} \cap C'' = \{\mathcal{O}, S, S', U, U', P, Q, R, T''\}$$

De aquí se sigue que $T' = T''$, con lo que queda demostrada la asociatividad de la operación binaria. □

II.2 Un Paréntesis Criptográfico

Una vez que hemos demostrado que a los puntos de una curva elíptica se les puede dotar de una estructura de grupo, es claro dónde surge la relación entre las curvas elípticas y la criptografía. Basta para esto recordar los esquemas presentados en el primer capítulo de este trabajo. Hay, sin embargo, un par de cosas que nos gustaría puntualizar.

Todos los algoritmos criptográficos presentados en el primer capítulo fueron originalemente descritos en términos de grupos de la forma $\mathbb{F}_q^*$. Sin embargo, si uno usa tales grupos, el valor de q deberá ser muy grande. Esto se debe al desarrollo durante la pasada década de métodos subexponenciales para resolver el **PLD** en $\mathbb{F}_q^*$. Fue esta situación la que llevó a Miller [Mil] y Koblitz [Kob] a proponer la técnica, común en la teoría de los números, de reemplazar un grupo $\mathbb{F}_q^*$ por el grupo de puntos de $\mathbf{E}(\mathbb{F}_q)$, una curva elíptica. Los argumentos que ellos dieron en favor del uso de tales grupos en los esquemas de clave pública son los siguientes:

1. Se tiene una mayor flexibilidad para la elección del grupo. Esto es porque dado q una potencia de un primo, existe un único grupo $\mathbb{F}_q^*$, pero muchas curvas $\mathbf{E}(\mathbb{F}_q)$.

2. No se conocen métodos subexponenciales de cálculo de logaritmos discretos en $\mathbf{E}$ si la curva es elegida cuidadosamente.

3. El cálculo de la operación de grupo está dada en términos de polinomios de grado menor o igual a dos. Es por esto muy fácil implementar criptosistemas basados en curvas elípticas en computadoras, incluso aquellas con una capacidad restringida.

Es natural entonces preguntarse porqué no usar tambien curvas elípticas sobre $\mathbb{Q}$ para los esquemas de clave pública. La principal razón es el rápido crecimiento de sus puntos, es decir, si para representar un punto P de una curva sobre $\mathbb{Q}$ se necesitan d dígitos, representar nP tomará aproximadamente $n^2 d$ dígitos. Esto las hace imprácticas para fines criptográficos, ya que todos los esquemas dependen de tomar potencias grandes de puntos en el grupo.

Otro de los beneficios de los sistemas de curva elíptica es el tamaño de llave requerido. Para obtener un nivel similar de seguridad en la encripción, los tamaños de las llaves requeridas es considerablemente menor al compararlos

con aquellos requeridos por algoritmos como RSA, por ejemplo, se estima en [BSS] que un tamaño de llave de 4096 bits para RSA ofrece el mismo nivel de seguridad que una llave de 313 bits en un sistema de curva elíptica. Daswani y Boneh efectuaron experimentos usando una PalmPilot de la compañia 3Com. Encontraron que generar una llave para RSA de 512 bits toma 3.4 minutos, mientras que generar una llave de 166 bits para un sistema de curva eliptica toma 0.597 segundos. A pesar de que ciertos procedimientos, como la verificación de firmas, fueron ligeramente más rápidos para RSA, los métodos de curva elíptica ofrecen ventajas en cuanto a velocidad se refiere en muchas situaciones.

Una vez que hemos discutido la relación entre curvas elípticas y criptografía, sigamos con nuestra exposición.

II.3 Funciones

Del contexto en el que estamos trabajando, es claro que estaremos interesados en estudiar las funciones polinomiales de nuestra curva $\mathbf{E}(K)$ al campo K, es decir, los polinomios

$$f : \mathbf{E}(K) \longrightarrow K \quad \text{tales que} \quad f \in K[X, Y].$$

Si nuestra curva está dada por el polinomio $y^2 - x^3 - Ax - B$, entonces es claro que dos polinomios que difieran por un múltiplo de dicho polinomio tomarán los mismos valores al evaluarlos en puntos de nuestra curva. Por eso introducimos el siguiente concepto

Definición II.3.1. Sea $K[\mathbf{E}] = K[X, Y]/I$, donde

$$I = \{(y^2 - x^3 - Ax - B)f | f \in K[X, Y]\}$$

es el ideal generado por el polinomio que define a nuestra curva. Decimos que $K[\mathbf{E}]$ es el *anillo de coordenadas* de $\mathbf{E}$. Como describimos anteriormente, éste se puede considerar como el anillo de polinomios en $\mathbf{E}$. Como $\mathbf{E}$ es una curva irreducible, $K[\mathbf{E}]$ es un dominio entero.

Definición II.3.2. Al campo de cocientes de $K[\mathbf{E}]$, al cual denotaremos por $K(\mathbf{E})$, lo llamaremos el *campo de funciones* de $\mathbf{E}$.

Queremos ahora hacer notar que las funciones $h \in K(\mathbf{E})$ no tienen porqué estar bien definidas para todos los puntos de $\mathbf{E}$, sin embargo, en un momento veremos que sólo no están definidas para un número finito de puntos de $\mathbf{E}$.

Una vez hechas estas observaciones, es importante mencionar el siguiente Teorema, cuya demostración se puede encontrar en el libro de Fulton [Ful]:

Teorema II.3.3. *Sea f una función en $K[\mathbf{E}]$ y P un punto de $\mathbf{E}$, entonces existe una función $t_P \in K[\mathbf{E}]$ llamada* parámetro de uniformización de $\mathbf{E}$ en P, *tal que $f = t_P^d f'$ donde $f' \in K[\mathbf{E}]$ es una función que cumple $f'(P) \neq 0$. Además, cualquier recta por P que no sea tangente a $\mathbf{E}$ funciona como parámetro de uniformización. Al número d, el cual no depende de la elección del parametro de uniformización, se le llama el* orden *de f en P, y lo denotaremos por* $\mathrm{ord}(f)$

Ya que $K(\mathbf{E})$ es el campo de cocientes de $K[\mathbf{E}]$, si tomamos $h \in K(\mathbf{E})$ tal que $h = f/g$, entonces podemos definir el orden de h en P como

$$\mathrm{ord}(h) = \mathrm{ord}(f) - \mathrm{ord}(g).$$

Es claro del teorema anterior que dada esta definición del orden se tiene $h = t_P^{\mathrm{ord}(h)} h'$, donde h' es una función que está bien definida en P y $h'(P) \neq 0$. Hemos extendido así la definición de orden a todo $K(\mathbf{E})$. Es claro que esta definición es el análogo del orden de un cero o un polo de las funciones meromorfas, dependiendo de si el orden es positivo o negativo.

Cuando definimos las curvas elípticas, lo hicimos sobre el plano proyectivo completo. Sin embargo, hemos dejado de lado el proyectivo en favor del plano afín desde entonces. Es momento ahora de regresar al plano proyectivo por las importantes propiedades de "completud "que tiene. Para esto, debemos decir primero cómo extender nuestras funciones al punto al infinito.

Pensemos en la inclusión $i : \mathbb{A}^2 \hookrightarrow \mathbb{P}^2$ dada por $(x, y) \mapsto [x : y : 1]$. Es claro que si a la función racional $h(x, y) = f(x, y)/g(x, y)$ le asociamos la función

$$h^*[x : y : z] = \frac{f(\frac{x}{z}, \frac{y}{z})}{g(\frac{x}{z}, \frac{y}{z})},$$

entonces $h = h^* \circ i$ en los puntos de $\mathbb{A}^2$. Notemos además que tanto $f(\frac{x}{z}, \frac{y}{z})$ como $g(\frac{x}{z}, \frac{y}{z})$ son combinaciones algebraicas de $\frac{x}{z}$ y $\frac{y}{z}$, los cuales tienen grado cero. Se sigue entonces que h^* es un cociente de polinomios homogeneos de grado cero, por lo cual es una función bien definida en el proyectivo al no

depender de la elección del representante. Es ahora claro cómo definir el valor de una función en el punto $\mathcal{O}$ de una curva elíptica.

El objetivo de las anteriores observaciones es aclarar que, aunque durante el resto del capítulo al hacer cálculos explícitos trabajaremos con la *parte afín* de las curvas, en verdad no hay ambiguedad alguna al decir que evaluamos funciones polinomiales en el punto $\mathcal{O}$.

Definición II.3.4. Sean $\mathbf{E}_1$ y $\mathbf{E}_2$ curvas elípticas (vistas como subconjuntos de $\mathbb{P}^2$). Una *aplicación racional* de $\mathbf{E}_1$ a $\mathbf{E}_2$ es una aplicación de la forma

$$\begin{aligned} \phi &: \mathbf{E}_1 \longrightarrow \mathbf{E}_2 \\ \phi &= [f_1 : f_2 : f_3], \end{aligned}$$

donde $f_1, f_2, f_3 \in K(\mathbf{E}_1)$ son tales que para todo punto $P \in \mathbf{E}_1$ en el cual estén todas definidas,

$$\phi(P) = [f_1(P) : f_2(P) : f_3(P)] \in \mathbf{E}_2.$$

Puesto que puede que no todas las funciones estén definidas para todos los puntos de nuestra curva $\mathbf{E}_1$, es importante dar la siguiente defineión.

Definición II.3.5. Una aplicación racional

$$\phi = [f_1 : f_2 : f_3] : \mathbf{E}_1 \longrightarrow \mathbf{E}_2$$

es *regular* en $P \in \mathbf{E}_1$ si existe una función $g \in K(\mathbf{E}_1)$ tal que:

1. gf_i está definida en P para todo i.
2. Para algún i se tiene que $(gf_i)(P) \neq 0$.

De existir tal g, hacemos

$$\phi(P) = [gf_1(P) : gf_2(P) : gf_3(P)].$$

Puede ser necesario tomar distintas funciones g para distintos puntos. A una aplicación racional que es regular en todo punto le llamamos un *morfismo*.

En geometría algebraica, las aplicaciones regulares no tienen, en general, porque ser morfismos. Sin embargo, esto no es problema con las curvas, como nos dice el siguiente Teorema.

Teorema II.3.6. *Sean* $\mathbf{E}_1, \mathbf{E}_2$ *curvas elípticas y* $\phi : \mathbf{E}_1 \longrightarrow \mathbf{E}_2$ *una aplicación racional entre ellas. Entonces* ϕ *es un morfismo.*

Demostración. Escribamos $\phi = [f_1 : f_2 : f_3]$ como antes. Dado un punto $P \in \mathbf{E}_1$, elijamos un parámetro de uniformización t en P. Denotemos por

$$n = \min\{\mathrm{ord}_P f_i\}.$$

Entonces $\mathrm{ord}_P(t^{-n} f_i) \geq 0$ para todo i, y $\mathrm{ord}_P(t^{-n} f_j) = 0$ para alguna j, así que toda $t^{-n} f_i$ está definida en P y $(t^{-n} f_j)(P) \neq 0$. Por lo tanto ϕ es regular en P, de donde se sigue el Teorema. □

Ejemplo II.3.7. Sea $\mathbf{E}$ una curva elíptica, y sea $f \in K(\mathbf{E})$ una función. Entonces f define una aplicación racional, la cual denotaremos también por f,

$$\begin{aligned} f : \mathbf{E} &\longrightarrow \mathbb{P}^1 \\ P &\longmapsto [f(P) : 1]. \end{aligned}$$

Por un argumento idéntico al del Teorema II.3.6, esta aplicación es de hecho un morfismo. Está dado explícitamente por

$$f(P) = \begin{cases} [f(P) : 1] & \text{si } f \text{ está definida en } P \\ [1 : 0] & \text{si } f \text{ no está definida en } P. \end{cases}$$

Mencionamos ahora algunos resultados que usaremos más adelante en la exposición de este trabajo, cabe mencionar que los enunciamos para curvas elípticas, pero son válidos para cualquier curva algebraica.

Teorema II.3.8. *Sea* $\mathbf{E}(K)$ *una curva elíptica definida sobre el campo* K *y* $h \in K(\mathbf{E})$ *una función racional. Entonces hay sólo un número finito de puntos* $P \in \mathbf{E}[\overline{K}]$ *con* $\mathrm{ord}(h) \neq 0$.

Teorema II.3.9. *Dada* $h \in K(\mathbf{E})$ *una función racional en la curva* $\mathbf{E}(K)$. *Entonces se cumple que*

$$\sum_{P \in \mathbf{E}[\overline{K}]} \mathrm{ord}(h) = 0.$$

La suma anterior está bien definida por el Teorema anterior. Además, si h *es una función racional tal que* $\mathrm{ord}(h) = 0$ *para todo* $P \in \mathbf{E}[\overline{K}]$, *se sigue que* $h \in K^{\times}$.

Las demostraciones de los dos Teoremas anteriores se pueden encontrar en el libro de Fulton [Ful] o Silverman [Sil].

II.4 Endomorfismos

En esta sección introducimos el concepto de endomorfismo de una curva elíptica. Éste resulta ser una función de una curva elíptica en si misma que conserva sus dos características más importantes: el ser una curva algebraica y que posee una estructura de grupo. Damos también una forma estándar para los endomorfismos y la usamos para demostrar teoremas muy interesantes. Cabe resaltar que los métodos utilizados en la demostración de los resultados de este capítulo son elementales, lo que contrasta con la literatura, donde generalmente se usan resultados muy avanzados de geometría algebraica en su demostración (ver por ejemplo [Sil]).

Por un **endomorfismo** en $\mathbf{E}$, nos referiremos a un homomorfismo $\alpha : \mathbf{E}[\overline{K}] \longrightarrow \mathbf{E}[\overline{K}]$ que está dado por funciones racionales. En otras palabras , $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, y además existen funciones racionales $R_1(x, y)$ y $R_2(x, y)$ con coeficientes en $\overline{K}$ tales que

$$\alpha(x, y) = (R_1(x, y), R_2(x, y))$$

para todo $(x, y) \in \mathbf{E}[\overline{K}]$. Puesto que α es un homomorfismo, es claro que $\alpha(\mathcal{O}) = \mathcal{O}$. En general, supondremos que los endomorfismos con los que trabajamos no son triviales, es decir, existe un (x, y) para el que $\alpha(x, y) \neq \mathcal{O}$. El endomorfismo constante, que aplica a cada punto a $\mathcal{O}$ será denotado en esta sección por 0.

En adelante, nos será útil tener una forma estándar para las funciones racionales que describen nuestro endomorfismo. Sea $R(x, y)$ cualquier función racional. Puesto que $y^2 = x^3 + Ax + B$ para todo $(x, y) \in \mathbf{E}(\overline{K})$, podemos reemplazar cualquier potencia par de $\mathbf{y}$ por un polinomio en $\mathbf{x}$, y reemplazar cualquier potencia impar de $\mathbf{y}$ por $\mathbf{y}$ multiplicado por un polinomio en $\mathbf{x}$, y obtener una función racional que toma el mismo valor en los puntos de $\mathbf{E}(\overline{K})$. Podemos, por lo tanto, suponer que

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Si racionalizamos multiplicando el numerador y denominador por $p_3(x) - p_4(x)y$ y reemplazamos de nuevo y^2 por $x^3 + Ax + B$ obtenemos

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{9}$$

Consideremos un endomorfismo dado por

$$\alpha(x,y) = (R_1(x,y),\ R_2(x,y)),$$

como antes. Puesto que α es un endomorfismo tenemos que

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

Esto se traduce en

$$R_1(x,-y) = R_1(x,y) \quad \text{y} \quad R_2(x,-y) = -R_2(x,y).$$

Así que si escribimos a R_1 en la forma (9), entonces $q_2(x) = 0$, y si R_2 es escrita en la forma (9), entonces el correspondiente $q_1(x) = 0$. Por lo tanto, podemos suponer que

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

para r_1, r_2 funciones racionales.

Con la ayuda del siguiente Lema, podremos decir qué pasa cuando las funciones racionales antes mencionadas no están definidas:

Lema II.4.1. *Sea $\alpha : \mathbf{E} \longrightarrow \mathbf{E}$ un endomorfismo de una curva $\mathbf{E}$ dada por el polinomio $y^2 = x^3 + Ax + B$, donde $\alpha(x,y) = (p(x)/q(x), ys(x)/t(x))$. Si $q(x) \neq 0$, entonces $t(x) \neq 0$.*

Demostración. Podemos suponer que p, q y s, t no tienen raices comunes. Ahora, como para $(x,y) \in \mathbf{E}$ sabemos que $\alpha(x,y) \in \mathbf{E}$, tenemos que al pensar en las curvas con coordenadas proyectivas,

$$\alpha[x:y:1] = [p(\tfrac{x}{z},\tfrac{y}{z})t(\tfrac{x}{z},\tfrac{y}{z}) : \tfrac{y}{z}s(\tfrac{x}{z},\tfrac{y}{z})q(\tfrac{x}{z},\tfrac{y}{z}) : q(\tfrac{x}{z},\tfrac{y}{z})t(\tfrac{x}{z},\tfrac{y}{z})].$$

Podemos deducir entonces que si $q(\frac{x}{z},\frac{y}{z}) = 0$, más nos vale que $p(\frac{x}{z},\frac{y}{z})t(\frac{x}{z},\frac{y}{z}) = 0$, puesto que de otra forma tendríamos que $\alpha[x:y:1] = [1:0:0]$, un punto que no pertence a la curva $\mathbf{E}$. Pero hemos supuesto que q y p no tienen raices comunes, así que podemos deducir que $t(\frac{x}{z},\frac{y}{z}) = 0$. En todo caso, como estamos tratando con puntos finitos, hemos demostrado que si $q(x,y) = 0$ entonces necesariamente $t(x,y) = 0$, que era el resultado buscado. □

Ahora, si escribimos $r_1(x) = p(x)/q(x)$ para $p(x), q(x)$ polinomios sin raices comunes, definimos $\alpha(x, y) = \mathcal{O}$ cuando $q(x) = 0$. Esta definición está justificada por el Lema anterior.

Definimos el **grado** de α como

$$\text{grad}(\alpha) = \text{Max}\{\text{grad}\, p(x), \text{grad}\, q(x)\}$$

si α es no trivial. Para el endomorfismo trivial $\alpha = 0$, definimos $\text{grad}\, \alpha = 0$. Decimos que $\alpha \neq 0$ es un endomorfismo separable si la derivada r_1' no es identicamente cero. Esto es equivalente a decir que uno de p' y q' no es identicamente cero.

Un endomorfismo muy importante es la **aplicación de Frobenius**. Supongamos que $\mathbf{E}$ está definida sobre $\mathbb{F}_q$. Definamos

$$\phi_q(x, y) = (x^q, y^q).$$

La aplicación de Frobenius ϕ_q juega un papel muy importante en la teoría de curvas elípticas sobre campos finitos.

Lema II.4.2. *Sea* $\mathbf{E}$ *definida sobre* $\mathbb{F}_q$. *Entonces* ϕ_q *es un endomorfismo en* $\mathbf{E}$ *de grado* q, *y* ϕ_q *no es separable.*

Demostración. Puesto que $\phi_q(x, y) = (x^q, y^q)$, la aplicación está dada por funciones racionales y su grado es claramente q. Lo que es importante es que $\phi_q : \mathbf{E}(\overline{F}_q) \longrightarrow \mathbf{E}(\overline{F}_q)$ es un homomorfismo. Sean $(x_1, y_1), (x_2, y_2) \in \mathbf{E}(\overline{F}_q)$ con $x_1 \neq x_2$. La suma es (x_3, y_3) dada por:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{donde} \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

Al elevar todo a la q-ésima potencia, obtenemos

$$x_3^q = m'^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q \quad \text{donde } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q}.$$

De aquí deducimos que

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2).$$

Claramente, $\phi_q(P+(-P)) = \phi_q(P)+\phi_q(-P)$. Sin embargo, vale la pena hacer el caso cuando sumamos un punto consigo mismo. La fórmula dice que $2(x_1, y_1) = (x_3, y_3)$, con

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{para } m' = \frac{3x_1^2 + A}{2y_1}.$$

Cuando elevamos esto a la q-ésima potencia obtenemos

$$x_3^q = m'^2 - 2^q x_1^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{para } m' = \frac{3^q (x_1^q)^2 + A^q}{2^q y_1^q}.$$

Ahora, puesto que $2, 3, A \in \mathbb{F}_q$, se cumple que $2^q = 2, 3^q = 3, A^q = A$. Esto quiere decir que obtenemos de nuevo la forma para duplicar el punto (x_1^q, y_1^q) en $\mathbf{E}$, probando así que ϕ_q es un homomorfismo. Como ϕ_q está dado en términos de funciones racionales, podemos concluir que es un endomorfismo. Además $q = 0$ en $\mathbb{F}_q$, así que la derivada de x^q es identicamente cero, por lo que ϕ_q no es separable.

□

Proposición II.4.3. *Sea $\alpha \neq 0$ un endomorfismo separable de una curva elíptica* $\mathbf{E}$. *Entonces*

$$\operatorname{grad} \alpha = \#\operatorname{Ker}(\alpha),$$

donde $\operatorname{Ker}(\alpha)$ *es el nucleo del homomorfismo* $\alpha : \mathbf{E}[\overline{K}] \longrightarrow \mathbf{E}[\overline{K}]$. *Si $\alpha \neq 0$ no es separable, entonces*

$$\operatorname{grad} \alpha > \#\operatorname{Ker}(\alpha).$$

Demostración. Hagamos como antes, $\alpha(x, y) = (r_1(x), r_2(x))$ con $r_1(x) = p(x)/q(x)$. Como α es separable, tenemos que $p'q - pq'$ no es el polinomio constante cero. Sea S el conjunto de los $x \in \overline{K}$ tales que $(p'q - pq')(x) = 0$. Encontraremos $(a, b) \in \mathbf{E}[\overline{K}]$ un punto que cumpla con las siguientes condiciones

1. $a \neq 0$, $b \neq 0$, $(a, b) \neq \mathcal{O}$,
2. $\operatorname{grad}(p(x) - aq(x)) = \operatorname{Max}\{\operatorname{grad}(p), \operatorname{grad}(q)\} = \operatorname{grad}(\alpha)$,

3. $a \notin r_1(S)$, y

4. $(a, b) \in \alpha(\mathbf{E}[\overline{K}])$.

Para demostrar que existe un punto que cumple con las condiciones anteriores notemos que como $p'q - pq'$ no es el polinomio cero, el conjunto S es finito, por lo tanto su imagen bajo α es finita. Notemos tambien que la función $r_1(x)$ toma un número infinito de valores distintos. Para esto, basta ver que puede tomar cualquier valor a lo más un número finito de veces. Sea $x_0 \in \overline{K}$ (donde como antes, $\overline{K}$ denota a la cerradura algebraica de K y es, por lo tanto, un campo infinito) cualquier valor, si resolvemos $r_1(x) = x_0$, nos damos cuenta que esto es equivalente a que $p(x) - x_0 q(x) = 0$ (pidiendo además que $q(x) \neq 0$), pero la ecuación anterior tiene un número finito de soluciones, así que hay un número finito de x tales que $r_1(x) = x_0$. Por lo tanto la función racional $r_1(x)$ toma una cantidad infinita de valores mientras x corre por $\overline{K}$. Además, para cada x_0 hay al menos un punto $(x_0, y) \in \mathbf{E}[\overline{K}]$, de donde se sigue que $\alpha(\mathbf{E}[\overline{K}])$ es un conjunto infinito. De estas observaciones, junto con el hecho de que sólo un número finito de puntos es elimindado por las condiciones (1), (2) y (3), concluimos que existe un punto (a, b) con las propiedades pedidas.

Afirmamos ahora que hay exactamente $\text{grad}(\alpha)$ puntos $(x_1, y_1) \in \mathbf{E}[\overline{K}]$ tales que $\alpha(x_1, y_1) = (a, b)$. Para dichos puntos tenemos que

$$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b.$$

Como $(a, b) \neq \mathcal{O}$, entonces $q(x_1) \neq 0$. Por el Lema II.4.1, $r_2(x)$ está definido. Además $b \neq 0$ y $y_1 r_2(x_1) = b$, así que $y_1 = b/r_2(x_1)$. Por lo tanto, el valor de x_1 determina el de y_1, así que sólo tenemos que contar los valores de x_1.

Por nuestra suposición (2), $p(x) - aq(x) = 0$ tiene $\text{grad}(\alpha)$ raices contando multiplicidad, así que lo que debemos hacer es mostrar que $p - aq$ no tiene raices múltiples. Para esto supongamos que x_0 es una raiz múltiple, entonces

$$p(x_0) - aq(x_0) = 0 \quad \text{y} \quad p'(x_0) - aq'(x_0) = 0.$$

Multiplicando obtenemos la siguiente relación

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Como $a \neq 0$, esto implicaría que x_0 es una raiz de $pq' - p'q$, así que $x_0 \in S$. Entonces $a = r_1(x_0) \in S$, contradiciendo así nuestras hipótesis. Se sigue que $p - aq$ no tiene raices multiples, y por lo tanto tiene $\text{grad}(\alpha)$ raices distintas.

Como α es un homomorfismo, y existen exactamente $\text{grad}(\alpha)$ puntos cuya imagen es (a, b), podemos deducir entonces que $\#\,\text{Ker}(\alpha) = \text{grad}(\alpha)$, que es lo que se quería demostrar.

Cuando α no es separable, la prueba anterior permanece válida casi en su totalidad, con la excepción de que $p' - aq'$ es siempre el polinomio cero, así que $p(x) - aq(x)$ siempre tiene raices múltiples y por lo tanto admite menos de $\text{grad}(\alpha)$ soluciones. □

El siguiente es un ejemplo de un endomorfismo separable, el cual será muy importante para las siguientes secciones de este capítulo.

Ejemplo II.4.4. Consideremos $\mathbf{E}(\overline{\mathbb{F}_q})$ una curva definida sobre $\mathbb{F}_q$. Pensemos ahora en $\phi_q - 1 : \mathbf{E} \longrightarrow \mathbf{E}$, esta función es un endomorfismo. Veremos que es separable. Si $P = (x, y)$ es un punto de $\mathbf{E}$, denotemos por $(\phi_q - 1)(P) = (x_1, x_2)$ a la imagen de P. De la definición se sigue que

$$(\phi_q - 1)(x, y) = (x^q, y^q) - (x, y).$$

Y usando nuestras fórmulas de suma de puntos podemos afirmar:

$$\begin{aligned} x_1 &= \left(\frac{y^q - y}{x^q - x}\right)^2 - x - x^p \\ &= \frac{y^2(y^{q-1} - 1)^2 - (x^q - x)^2(x^q - x)}{(x^q - x)^2}. \end{aligned}$$

Para demostrar que es separable basta notar lo siguiente:

$$\begin{aligned} \frac{d}{dy}(x^q - x)^2 &= 2(x^q - x)(qx^{q-1} - 1) \\ &= -2(x^q - x) \neq 0. \qquad \text{(puesto que } q = 0 \text{ en } \mathbb{F}_q) \end{aligned}$$

Con lo que concluimos que $\phi_q - 1$ es un endomorfismo separable, puesto que hemos demostrado que la derivada del denominador es distinta de cero. Lo cual es una condición suficiente para garantizar la separabilidad.

Teorema II.4.5. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre un campo* K. *Sea* $\alpha \neq 0$ *un endomorfismo de* $\mathbf{E}$. *Entonces* $\alpha : \mathbf{E}(\overline{K}) \longrightarrow \mathbf{E}(\overline{K})$ *es suprayectiva.*

Demostración. Sea $(a, b) \in \mathbf{E}(\overline{K})$. Queremos demostrar que hay P con $\alpha(P) = (a, b)$. Puesto que $\alpha(\mathcal{O}) = \mathcal{O}$, podemos suponer que $(a, b) \neq \mathcal{O}$. Sea $r_1(x) = p(x)/q(x)$ la primera función coordenada. Si $p(x) - aq(x)$ no es un polinomio constante, entonces tiene una raiz x_0. Como $p(x)$ y $q(x)$ no tienen raices comunes, se sigue que $q(x_0) \neq 0$. Elijamos $y_0 \in \overline{K}$ una de las raices cuadradas de $x_0^3 + Ax_0 + B$. Entonces, por nuestro Lema II.4.1, sabemos que $\alpha(x_0, y_0)$ está definido y es igual a (a, b') para $b' = \pm b$. Si $b' = b$ ya acabamos, de otro modo, tendríamos que $\alpha(x_0, y_0) = (a, -b)$, por lo tanto $\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = (a, b)$.

Necesitamos ahora considerar el caso cuando $p - aq$ es constante. Como $\mathbf{E}(\overline{K})$ es infinito y el núcleo de α es finito, sólo un número finito de puntos de $\mathbf{E}(\overline{K})$ se pueden aplicar a un punto con una coordenada en x dada. Por lo tanto, o bien $p(x)$ o $q(x)$ no es constante. De aquí se sigue que existe a lo más una constante a tal que $p - aq$ es constante. Así que hay a lo más 2 puntos (a, b) y $(a, -b)$ que no están en la imagen de α. Elijamos cualquier otro punto (a_1, b_1). Sabemos que existe P_1 tal que $\alpha(P_1) = (a_1, b_1)$. Podemos incluso elegir un punto (a_1, b_1) tal que $(a_1, b_1) + (a, b) \neq (a, \pm b)$, así que existe P_2 tal que $\alpha(P_2) = (a_1, b_1) + (a, b)$. Por lo tanto $\alpha(P_2 - P_1) = (a, b)$ y $\alpha(P_1 - P_2) = (a, -b)$, probando así que α es suprayectiva. □

II.5 El Grupo de Torsión

Sea $\mathbf{E}$ una curva elíptica definida sobre un campo K. Para un entero positivo n definimos el grupo de n-torsión, el cual denotaremos por $\mathbf{E}[n]$, como

$$\mathbf{E}[n] = \{P \in \mathbf{E}(\overline{K}) | nP = \mathcal{O}\}.$$

Es decir, todos aquellos puntos cuyo orden es divisible entre n. En esta sección estudiaremos la estructura de este subgrupo de una curva elíptica. Nos parece importante recalcar que buscamos los puntos con coordenadas en $\overline{K}$, no sólo en K. Notemos además que este conjunto es un subgrupo de $\mathbf{E}(\overline{K})$, puesto que es el núcleo del morfismo *multiplicar por* n:

$$\begin{aligned} \phi_n : \mathbf{E}(\overline{K}) &\longrightarrow \mathbf{E}(\overline{K}) \\ P &\longmapsto nP \end{aligned}$$

La estructura del grupo $\mathbf{E}[n]$ está dada por el siguente Teorema:

Teorema II.5.1. *Sea* $\mathbf{E}$ *una curva elíptica sobre un campo* K *y* n *un entero positivo. Si la característica de* K *no divide a* n *o es* 0, *entonces*

$$\mathbf{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

Si la característica de K *es* $p > 0$ *y* $p|n$ *y si* $n = p^r n'$ *con* $\text{mcd}(p, n') = 1$, *entonces*

$$\mathbf{E}[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad o \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

No daremos la demostración de este Teorema, pero indicaremos un esquema de prueba. Como hemos indicado anteriormente, dada una curva elíptica $\mathbf{E}$, la multiplicación por n es un endomorfismo, y en particular está dada por funciones racionales. Además, como era de esperarse, estas se pueden calcular de manera recursiva. Para esto, definamos los *polinomios de división* $\psi_m \in \mathbb{Z}[x, y, A, B]$ por

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{para} \quad m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{para} \quad m \geq 2.
\end{aligned}$$

Si definimos además los polinomios

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),
\end{aligned}$$

se puede demostrar por diversos métodos el siguiente Teorema:

Teorema II.5.2. *Sea* $P = (x, y)$ *un punto en la curva* $y^2 = x^3 + Ax + B$ *(sobre un campo de característica distinta de* 2*)* y n *un entero positivo. Entonces*

$$nP = \left(\frac{\phi_n(x, y)}{\psi_n^2(x, y)}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3} \right).$$

Basta mencionar ahora que se puede demostrar que la fracción $\phi_n(x,y)/\psi_n^2(x,y)$ es irreducible, que el grado del Endomorfismo "multiplicar por n "es n^2, y que éste es separable si y solamente si la característica de K no divide a n. Usando todas estas observaciones, concluiremos el Teorema II.5.1.

Demostración. Consideremos primero el caso cuando n no es divisible por la característica de K. Por las observaciones hechas anteriormente y la Proposición II.4.3, $\mathbf{E}[n]$, que es precisamente el núcleo de la multiplicación por n, tiene orden n^2. El Teorema de estructura para grupos abelianos finitos nos dice que entonces

$$\mathbf{E}[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k},$$

para enteros $n_1, n_2, \ldots, n_k$ con la propiedad de $n_i | n_{i+1}$ para todo i. Sea l un primo que divide a n_1. Entonces $l | n_i$ para todo i. Esto implica que $\mathbf{E}[l] \subseteq \mathbf{E}[n]$ tiene orden l^k. Como acabamos de demostrar que hay l^2 puntos en $\mathbf{E}[l]$, se sigue que $k = 2$. Además, multiplicar por n anula a todo $\mathbf{E}[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, así que necesariamente $n_2 | n$. Como además $n^2 = n_1 n_2$, podemos concluir que $n = n_1 = n_2$. Por lo tanto,

$$\mathbf{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Consideremos ahora el caso cuando $p | n$. Para esto, estudiemos el grupo de p^k-torsión. Por las observaciones hechas anteriormente y la Proposición II.4.3, hay estrictamente menos de p^2 puntos de orden p. Puesto que todo elemento de $\mathbf{E}[p]$ tiene orden 1 o p, el orden de $\mathbf{E}[p]$ es una potencia de p, y por tanto es 1 o p. Si $\mathbf{E}[p]$ es trivial, entonces $\mathbf{E}[p^k]$ es trivial para toda k. Podemos suponer entonces que $\mathbf{E}[p]$ tiene p puntos, nosotros aseguramos que de ser así, entonces $\mathbf{E}[p^k]$ tiene p^k puntos para toda k, lo cual demostraremos a continuación. Supongamos que existe un punto P de orden p^j. Entonces por nuestro Teorema II.4.5, la multiplicación por p es suprayectiva, y por tanto existe un punto Q con $pQ = P$. De aquí tenemos $p^j Q = p^{j-1} P \neq \mathcal{O}$.

Sin embargo,$p^{j+1} Q = p^j P = \mathcal{O}$, por lo tanto el orden de Q es p^{j+1}. Se sigue ahora por inducción, que para todo k $\mathbf{E}[p^k]$ tiene orden p^k. Además, acabamos de demostrar que hay puntos de orden p^k, por lo tanto $\mathbf{E}[p^k] \simeq \mathbb{Z}_{p^k}$. Podemos ahora concluir. Si escribimos $n = p^k n'$ con $k \geq 0$ y $\mathrm{mcd}(k, n') = 1$, entonces

$$\mathbf{E}[n] \simeq \mathbf{E}[n'] \oplus \mathbf{E}[p^k].$$

Sabemos además que $\mathbf{E}[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$, y demostramos que $\mathbf{E}[p^k] \simeq \mathbb{Z}_{p^k}$ o $\mathbf{E}[p^k] \simeq 0$. Además como

$$\mathbb{Z}_{n'} \oplus \mathbb{Z}_p^r \simeq \mathbb{Z}_{n'p^k} \simeq \mathbb{Z}_n,$$

resulta que

$$\mathbf{E}[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{o} \quad \mathbf{E}[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_n.$$

Con lo que concluimos la demostración del Teorema II.5.1. □

Sea n un entero no divisible por la característica del campo K. Acabamos de demostrar que $\mathbf{E}[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Elijamos ahora una base $\{\beta_1, \beta_2\}$ de $\mathbf{E}[n]$. Esto quiere decir que cualquier elemento de $\mathbf{E}[n]$ se puede expresar como $m_1\beta_1 + m_2\beta_2$, con m_1 y m_2 enteros determinados unívocamente (mod n). Pensemos ahora en un endomorfismo $\alpha : \mathbf{E}[\overline{K}] \longrightarrow \mathbf{E}[\overline{K}]$. Éste induce un morfismo de $\mathbf{E}[n]$ en $\mathbf{E}[n]$. Por lo tanto, existen enteros $a, b, c, d \in \mathbb{Z}_n$ tales que

$$\alpha(\beta_1) = a\beta_1 + c\beta_2 \quad \text{y} \quad \alpha(\beta_2) = b\beta_1 + d\beta_2.$$

Así que a cada endomorfismo $\alpha : \mathbf{E}[\overline{K}] \longrightarrow \mathbf{E}[\overline{K}]$, le podemos asociar una matriz de 2×2

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

donde a la composición de homomorfismos le corresponde la multiplicación de matrices.

Ejemplo II.5.3. Consideremos la curva $y^2 = x^2 - x$ sobre $\mathbb{C}$. Entonces es claro que los puntos de 2-torsión son aquellos con coordenada **y** igual a 0, por lo tanto tenemos

$$\mathbf{E}[2] = \{\mathcal{O}, (1,0), (-1,0), (0,0)\}.$$

Además, tenemos que $(1,0) + (-1,0) = (0,0)$, por lo tanto el conjunto $\{(1,0), (-1,0)\}$ genera $\mathbf{E}[2]$. Si nos preguntamos por $\mathbf{E}[4]$, entonces es fácil ver que además de los puntos de $\mathbf{E}[2]$, contiene a los siguientes puntos:

$$\{ \pm (i, -1+i), \pm(-i, 1+i), \pm(1-\sqrt{2}, \sqrt{2}-2), \pm(1+\sqrt{2}, \sqrt{2}+2),$$
$$\pm(-1-\sqrt{2}, i(\sqrt{2}+2)), \pm(-1+\sqrt{2}, i(2-\sqrt{2})), \}$$

Hemos encontrado entonces a los 16 puntos de 4-torsión en $\mathbf{E}$. Una base para $\mathbf{E}[4]$ está dada por $\{(i, 1+i), (1+\sqrt{2}, 2+\sqrt{2})\}$. Notemos que ya que los coeficientes de la curva son números reales, la conjugación compleja induce un automorfismo de la curva en si misma. Esto sucede para cualquier curva, es decir, si una curva está definida sobre un campo K, entonces cualquier automorfismo de $\overline{K}$ que fije a K induce un morfismo de la curva en si misma, y como comentamos anteriormente, le podemos asociar una matriz. Veamos la matriz que le corresponde a la conjugación compleja en esta base:

$$\sigma(i, -1+i) = (-i, -1-i)$$
$$\sigma(1+\sqrt{2}, 2+\sqrt{2}) = (1+\sqrt{2}, 2+\sqrt{2})$$

Por lo tanto, la matriz que le corresponde es

$$\begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}$$

Una vez que sabemos cómo es la estructura del grupo de torsión de una curva elíptica, podemos enunciar y probar un Teorema referente a la estructura de $\mathbf{E}$. Éste es el siguiente.

Teorema II.5.4. *Sea* $\mathbf{E}$ *una curva elíptica sobre un campo finito* $\mathbb{F}_q$. *Entonces*

$$\mathbf{E}(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad o \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

para algún entero $n \geq 1$, *o para un par de enteros* $n_1, n_2 \geq 1$ *tales que* n_1 *divide a* n_2.

Demostración. El Teorema de estructura para grupos abelianos finitos nos asegura que cada uno de estos grupos es isomorfo a una suma directa de grupos cíclicos

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k},$$

tales que $n_i | n_{i+1}$ para $i \geq 1$. Puesto que para todo i, el grupo $\mathbb{Z}_{n_i}$ tiene n_1 elementos cuyo orden divide a n_1, encontramos que $\mathbf{E}(\mathbb{F}_q)$ tiene n_1^r elementos cuyo orden divide a n_1. Por el Teorema II.5.1, hay a lo más n_1^2 puntos con dicha característica (aún si admitimos puntos con coordenadas en la cerradura algebraica de $\mathbb{F}_q$). Por lo tanto $k \leq 2$. Con esto concluimos el Teorema. □

II.6 Divisores

El *grupo de divisores de una curva elíptica* $\mathbf{E}$, denotado por $\mathrm{Div}(\mathbf{E})$, es el grupo libre abeliano generado por los puntos de $\mathbf{E}$. Es decir, un divisor $D \in \mathrm{Div}(\mathbf{E})$ es una suma formal

$$D = \sum_{P \in \mathbf{E}} n_P [P]$$

con $n_P \in \mathbb{Z}$ y $n_P = 0$ para todos excepto un número finito de $P \in \mathbf{E}$. Definimos el *grado* de D como

$$\mathrm{grad}\, D = \sum_{P \in \mathbf{E}} n_P.$$

Los divisores de grado 0 forman un subgrupo de $\mathrm{Div}(\mathbf{E})$, el cual denotamos por

$$\mathrm{Div}^0(\mathbf{E}) = \{D \in \mathrm{Div}(\mathbf{E}) | \, \mathrm{grad}\, D = 0\}.$$

Sea $f : \mathbf{E} \longrightarrow K$ una función racional en $\mathbf{E}$, la cual no es la función constante cero. Entonces le podemos asociar el divisor $\mathrm{div}(f)$ dado por

$$\mathrm{div}(f) = \sum_{P \in \mathbf{E}} \mathrm{ord}_P(f)[P].$$

Éste es un divisor bien definido por el Teorema II.3.8. Puesto que ord_P cumple con:

1. $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$ para f, g funciones en $\overline{K}(C)^*$.

2. $\mathrm{ord}_P(c) = 0$ para $c \in \overline{K}^*$ una constante.

Nos damos cuenta que la aplicación

$$\mathrm{div} : \overline{K}(C)^* \longrightarrow \mathrm{Div}(\mathbf{E})$$

es un homomorfismo de grupos abelianos, que resulta ser el análogo de la aplicación que envía a cada elemento de una extensión finita de $\mathbb{Q}$ a su correspondiente ideal fraccional. Esto motiva la siguiente definición:

Definición II.6.1. Un divisor $D \in \mathrm{Div}(\mathbf{E})$ es *principal* si tiene la forma $D = \mathrm{div}(f)$ para alguna función $f \in \overline{K}(C)^*$. Dos divisores D_1 y D_2 son *linealmente equivalentes*, lo cual denotaremos por $D_1 \sim D_2$, si $D_1 - D_2$ es principal. El *grupo de clases de divisores* (o *grupo de Picard*) de $\mathbf{E}$, el cual denotaremos por $\mathrm{Pic}(\mathbf{E})$, es el cociente de $\mathrm{Div}(\mathbf{E})$ módulo el grupo de divisores principales.

Proposición II.6.2. *Sea* $\mathbf{E}$ *una curva elíptica y* $f \in \overline{K}(\mathbf{E})^*$. *Entonces se cumple que*

1. $\mathrm{div}(f) = 0$ *si y solamente si* $f \in \overline{K}^*$.
2. $\mathrm{grad}(\mathrm{div}(f)) = 0$.

Demostración. (1) Si $\mathrm{div}(f) = 0$, entonces f no tiene polos, así que la aplicación correspondiente $f : \mathbf{E} \longrightarrow \mathbb{P}^1$ no es suprayectiva. Por lo tanto es constante, así que $f \in \overline{K}(\mathbf{E})^*$. El recíproco es claro.

(2) Éste es simplemente el Teorema II.3.9. □

Definición II.6.3. La *parte cero del grupo de clases de divisores de* $\mathbf{E}$, la cual denotaremos por $\mathrm{Pic}^0(\mathbf{E})$, es el cociente de $\mathrm{Div}^0(\mathbf{E})$, módulo el subgrupo de divisores principales.

Definición II.6.4. Un divisor $D = \sum n_P[P] \in \mathrm{Div}(\mathbf{E})$ es *positivo*, lo cual denotaremos por $D \geq 0$, si $n_P \geq 0$ para todo $P \in \mathbf{E}$. De manera análoga, si $D_1, D_2 \in \mathrm{Div}(\mathbf{E})$, entonces escribimos $D_1 \geq D_2$ para indicar que $D_1 - D_2$ es positivo.

Ejemplo II.6.5. Sea $f \in \overline{K}(\mathbf{E})^*$ una función que es regular en todos lados excepto en un punto $P \in \mathbf{E}$, y tal que tiene un polo de orden a lo más n en P. Estas condiciones en f se pueden especificar simplemente por la desigualdad

$$\mathrm{div}(f) \geq -n[P].$$

De manera análoga,

$$\operatorname{div}(f) \geq [Q] - n[P]$$

dice que además f tiene un cero en Q. De esta manera, las desigualdades de divisores son una herramienta práctica para describir los ceros y polos de una función.

Definición II.6.6. Sea $D \in \operatorname{Div}(\mathbf{E})$. Le asociaremos a D el conjunto de funciones

$$\mathcal{L}(D) = \{f \in \overline{K}(\mathbf{E})^* \mid \operatorname{div}(f) \geq -D\} \bigcup \{0\}.$$

$\mathcal{L}(D)$ es un $\overline{K}$ espacio vectorial de dimension finita (ver [Sil]). Denotaremos su dimensión por

$$l(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

La siguiente proposición relaciona $l(D)$ con $\operatorname{grad}(D)$.

Proposición II.6.7. *Si* $\mathbf{E}$ *es una curva elíptica, y* $D \in \operatorname{Div}(\mathbf{E})$ *es un divisor para el cual* $\operatorname{grad} D > 0$, *entonces* $l(D) = \operatorname{grad} D$.

Demostración. Esta proposición es solamente un Corolario del Teorema de Riemann-Roch, consultar [Sil] . □

Usaremos ahora la herramienta desarrollada hasta el momento para relacionar el grupo de puntos de $\mathbf{E}$ con el grupo $\operatorname{Div}(\mathbf{E})$.

Lema II.6.8. *Sea* $\mathbf{E}$ *una curva elíptica, y sean* $P, Q \in \mathbf{E}$. *Entonces*

$$[P] \sim [Q] \quad \textit{si y solamente si} \quad P = Q.$$

Demostración. Supongamos $[P] \sim [Q]$, y elijamos una función $f \in \overline{K}(\mathbf{E})$ tal que

$$\operatorname{div}(f) = [P] - [Q].$$

Entonces $f \in \mathcal{L}([Q])$, y, por nuestra Proposición II.6.7

$$\dim \mathcal{L}([Q]) = 1.$$

Pero $\mathcal{L}([Q])$ ya contiene a las funciones constantes, así que $f \in \overline{K}$ y $P = Q$. □

Proposición II.6.9. *Sea* $\mathbf{E}$ *una curva elíptica. Entonces*

1. *Para todo divisor* $D \in \mathrm{Div}^0(\mathbf{E})$, *existe un único punto* $P \in \mathbf{E}$ *tal que*

$$D \sim [P] - [\mathcal{O}].$$

Si además denotamos por $\sigma : \mathrm{Div}^0(\mathbf{E}) \longrightarrow \mathbf{E}$ *a la aplicación que resulta de esta asociación, tenemos que:*

2. *La aplicación* σ *es suprayectiva.*

3. *Sean* $D_1, D_2 \in \mathrm{Div}^0(\mathbf{E})$. *Entonces*

$$\sigma(D_1) = \sigma(D_2) \quad \textit{si y solamente si} \quad D_1 \sim D_2.$$

Así σ *induce una biyección de conjuntos (que, abusando de la notación, también escribiremos como* σ*),*

$$\sigma : \mathrm{Pic}^0(\mathbf{E}) \longrightarrow \mathbf{E}.$$

4. *La inversa de* σ *está dada por*

$$\begin{aligned} \kappa : \mathbf{E} &\longrightarrow \mathrm{Pic}^0(\mathbf{E}) \\ P &\longmapsto \textit{clase de } [P] - [\mathcal{O}]. \end{aligned}$$

5. *La "ley geométrica de grupo"y la estructura de grupo inducida en* $\mathbf{E}$ *por* $\mathrm{Pic}^0(\mathbf{E})$ *vía* σ *coinciden.*

Demostración. (1) Como $\operatorname{grad} D = 0$, nuestra Proposición II.6.7 dice que

$$\dim \mathcal{L}(D + [\mathcal{O}]) = 1.$$

Sea $f \in K(\mathbf{E})$ un generador de $\mathcal{L}(D + [\mathcal{O}])$. Como

$$\operatorname{div}(f) \geq -D - [\mathcal{O}] \quad \text{y} \quad \operatorname{grad}(\operatorname{div}(f)) = 0,$$

podemos concluir que

$$\operatorname{div}(f) = -D - [\mathcal{O}] + [P]$$

para algún $P \in \mathbf{E}$. Por lo tanto,

$$D \sim [P] - [\mathcal{O}],$$

lo que demuestra la existencia de un punto con la propiedad deseada. Para ver que éste es único, supongamos que $P' \in \mathbf{E}$ tiene la misma propiedad. Entonces

$$[P] \sim D + [\mathcal{O}] \sim [P'],$$

y usando el Lema II.6.8 deducimos que $P = P'$, lo que demuestra la unicidad de P.

(2) Para todo punto $P \in \mathbf{E}$, se cumple

$$\sigma([P] - [\mathcal{O}]) = P.$$

(3) Sean $D_1, D_2 \in \mathrm{Div}^0(\mathbf{E})$ y hagamos $P_i = \sigma(D_i)$. Entonces de la definición de σ,

$$[P_1] - [P_2] \sim D_1 - D_2$$

Por lo tanto es claro que $P_1 = P_2$ implica que $D_1 \sim D_2$. De igual manera, si $D_1 \sim D_2$, entonces $P_1 \sim P_2$, lo que, usando el Lema II.6.8 implica $P_1 = P_2$.

(4) Basta notar en la demostración de (2) que $\sigma([P] - [\mathcal{O}]) = P$.

(5) Sean $P, Q \in \mathbf{E}$. Para demostrar la afirmación es suficiente probar que

$$\kappa(P + Q) = \kappa(P) + \kappa(Q).$$

Sea $f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ la línea L en $\mathbb{P}^2$ que pasa por P y Q. Denotemos por R al tercer punto de intersección de esta línea L con $\mathbf{E}$, y denotemos por $f'(X, Y, Z) = \alpha X' + \beta' Y + \gamma' Z = 0$ a la línea L' que pasa por R y $\mathcal{O}$. Entonces, por la definición de la suma en $\mathbf{E}$ y que la línea $Z = 0$ intersecta a $\mathbf{E}$ en $\mathcal{O}$ con multiplicidad 3 tenemos que

$$\mathrm{div}(f/Z) = [P] + [Q] + [R] - 3[\mathcal{O}],$$

y

$$\mathrm{div}(f'/Z) = [R] + [P + Q] - 2[\mathcal{O}].$$

De donde se sigue que

$$[P+Q]-[P]-[Q]+[\mathcal{O}] = \operatorname{div}(f'/f) \sim 0,$$

así que

$$\kappa(P+Q)-\kappa(P)-\kappa(Q)=0,$$

con lo que concluimos la demostración.

□

Corolario II.6.10. *Sea* $\mathbf{E}$ *una curva elíptica y* $D=\sum n_P[P] \in \operatorname{Div}(\mathbf{E})$. *Entonces* D *es principal si y solamente si* $\sum n_P = 0$ *y* $\sum n_P P = 0$ *(Cabe recalcar que la primera suma es una suma de enteros y la segunda es la suma en* $\mathbf{E}$*.)*

Demostración. De nuestra Proposición II.6.2, todo divisor principal tiene grado cero. Si suponemos ahora que $D \in \operatorname{Div}^0(\mathbf{E})$, la Proposición II.6.9 nos dice que

$$D \sim 0 \Leftrightarrow \sigma(D)=0 \Leftrightarrow \sum(n_P)\sigma([P]-[\mathcal{O}]=0,$$

lo que nos da el resultado buscado puesto que $\sigma([P]-[\mathcal{O}])=P$. □

LLegamos ahora a la siguiente pregunta: *Dado un divisor* $D=\sum n_P[P]$, *tal que* $\sum n_P[P]=0$ *y* $\sum n_P P=0$, *¿Cómo podemos encontrar una función* f *que cumpla* $\operatorname{div}(f)=D$ *?*. Para responderla notemos lo siguiente:

Supongamos que P_1, P_2 y P_3 son tres puntos en $\mathbf{E}$ que caen en la línea $ax+by+c=0$. Entonces la función

$$f(x,y)=ax+by+c$$

tiene ceros en P_1, P_2 y P_3. Además, si $b \neq 0$, entonces f tiene un polo de orden tres en $\mathcal{O}$. Tenemos entonces:

$$\operatorname{div}(f)=[P_1]+[P_2]+[P_3]-3[\mathcal{O}].$$

La línea por $P_3=(x_3,y_3)$ y $-P_3$ es $x-x_3=0$. El divisor de la función $x-x_3$ es

$$\operatorname{div}(x-x_3)=[P_3]+[-P_3]-2[\mathcal{O}].$$

Por lo tanto,

$$\operatorname{div}\left(\frac{ax+by+c}{x-x_3}\right) = \operatorname{div}(ax+by+c) - \operatorname{div}(x-x_3) = [P_1]+[P_2]-[-P_3]-[\mathcal{O}].$$

Puesto que $P_1 + P_2 = -P_3$ en $\mathbf{E}$, podemos reescribir esto como

$$[P_1] + [P_2] = [P_1 + P_2] + [\mathcal{O}] + \operatorname{div}\left(\frac{ax+by+c}{x-x_3}\right).$$

Usando esto podemos ahora calcular funciones cuyos divisores sean dados. Para hacerlo sólo necesitamos repetir el procedimiento anteriormente descrito varias veces. Esto se muestra en el siguiente ejemplo:

Ejemplo II.6.11. Consideremos la curva dada por $y^2 = x^3 + 5x + 3$ sobre $\mathbb{F}_{523}$. Ésta es isomorfa a $\mathbb{Z}_{507}$ y el punto $(1, 3)$ es generador. Nos preguntamos por una función f que cumpla:

$$\operatorname{div}(f) = [(239,302)]+[(326,394)]+[(274,411)]-[(343,301)]-[(22,469)]-[\mathcal{O}].$$

Es fácil ver que la suma del lado derecho en verdad es $\mathcal{O}$ en $\mathbf{E}$, así que tal función existe. Usemos la discusión anterior para encontrarla. Primero veamos que

$$[(239,302)] + [(326,394)] = [276,248] + [\mathcal{O}] + \operatorname{div}\left(\frac{494x-y-84}{x+275}\right).$$

Efectuando el mismo proceso de nuevo obtenemos

$$[(276,248)] + [(274,411)] = [(470,396)] + [\mathcal{O}] + \operatorname{div}\left(\frac{180x-y+253}{x+127}\right).$$

Por lo tanto

$$[(239,302)]+[(326,394)] + [(274,411)] = \\ [(470,396)] + 2[\mathcal{O}] + \operatorname{div}\left(\frac{(494x-y-84)(180x-y+253)}{(x+275)(x+127)}\right).$$

Análogamente encontramos que

$$[(343,301)]+[(22,469)]+[\mathcal{O}]=[(470,396)]+2[\mathcal{O}]+\operatorname{div}\left(\frac{151x-y+285}{x+127}\right).$$

Podemos entonces concluir que la función buscada es

$$f=\left(\frac{(494x-y-84)(180x-y+253)}{(x+275)(151x-y+285)}\right).$$

Capítulo III

El Apareo de Weil y el MOV

En este capítulo construimos el apareo de Weil, una función bilineal de $\mathbf{E}[n] \times \mathbf{E}[n]$ en μ_n, el grupo de raices n-ésimas de la unidad. Para hacerlo usamos toda la teoría desarrollada en el capítulo anterior, en especial la caracterización de una función en una curva en términos del divisor asociado. Posteriormente usaremos el apareo de Weil para demostrar el teorema de Hasse-Weil, el cual dice que el orden de una curva elíptica $\mathbf{E}$ sobre un campo finito $\mathbb{F}_q$ pertence al intervalo $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. Para terminar el capítulo describimos el algoritmo **MOV**, que reduce el problema del cálculo de logaritmos discretos en una curva elíptica sobre un campo $\mathbb{F}_q$ al del cálculo de logaritmos discretos en una extensión $\mathbb{F}_{q^n}$ del campo base. Esto resulta particularmente útil si el grado de la extensión no es muy grande, pues el método de cálculo de índices nos permite calcular logaritmos discretos en campos finitos mucho más rápido que si usaramos los algoritmos generales para grupos arbitrarios (ver el apéndice sobre algoritmos).

III.1 El Apareo de Weil

El objetivo de esta sección es construir el apareo de Weil y demostrar sus principales propiedades. A lo largo de esta sección, n denotará un entero no divisible por la característica del campo K, y $\mathbf{E}$ será una curva elíptica tal que

$$\mathbf{E}[n] \subset \mathbf{E}(K).$$

Queremos construir una función binaria

$$e_n : \mathbf{E}[n] \times \mathbf{E}[n] \longrightarrow \mu_n,$$

donde μ_n es el conjunto de raices n-ésimas de la unidad en $\overline{K}$.

Sea $T \in \mathbf{E}[n]$. Por el Corolario II.6.10, existe una función f tal que

$$\operatorname{div}(f) = n[T] - n[\mathcal{O}]. \tag{1}$$

Elijamos un $T' \in \mathbf{E}[n^2]$ tal que $nT' = T$. Usaremos el Corolario II.6.10 para probar que existe una función g tal que

$$\operatorname{div}(g) = \sum_{R \in \mathbf{E}[n]} ([T' + R] - [R]).$$

Necesitamos verificar que la suma de los puntos en el divisor es $\mathcal{O}$. Esto se sigue de que hay n^2 puntos R en $\mathbf{E}[n]$. Los puntos R en $\sum[T' + R]$ y $\sum[R]$ se cancelan, así que la suma es $n^2T' = nT = \mathcal{O}$. Notemos además que g no depende de la elección de T', puesto que cualesquiera dos elecciones de T' difieren por un elemento $R \in \mathbf{E}[n]$. Así que pudimos haber escrito

$$\operatorname{div}(g) = \sum_{nT''=T} [T''] - \sum_{nR=\mathcal{O}} [R].$$

Denotemos por $f \circ n$ a la función que toma un punto, lo multiplica por n, y después le aplica f. Los puntos $P = T' + R$ con $R \in \mathbf{E}[n]$ son aquellos puntos P que cumplen $nP = T$. Se sigue de (1) que

$$\operatorname{div}(f \circ n) = n\left(\sum_R [T' + R]\right) - n\left(\sum_R [R]\right) = \operatorname{div}(g^n).$$

Por lo tanto $f \circ n$ es igual a g^n multiplicado por una constante. Multiplicando f por una constante apropiada, podemos suponer que

$$f \circ n = g^n.$$

Sea $S \in \mathbf{E}[n]$ y hagamos $P \in \mathbf{E}(\overline{K})$. Entonces

$$g(P + S)^n = f(n(P + S)) = f(nP) = g(P)^n.$$

Así que $g(P + S)/g(P) \in \mu_n$. Lo que es más, el valor de $g(P + S)/g(P)$ es independiente de P.

Definamos el **apareo de Weil** por

$$e_n(S,T) = \frac{g(P+S)}{g(P)}. \tag{2}$$

Puesto que g está definido salvo un múltiplo escalar por su divisor, esta definición es independiente de la elección de g. Notemos tambien que (2) es independiente de la elección del punto auxiliar P. Las propiedades básicas de e_n están dadas por el siguiente teorema:

Teorema III.1.1. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre un campo* K, *y sea* n *un entero positivo. Supongamos que la característica de* K *no divide a* n. *Entonces el apareo de Weil*

$$e_n : \mathbf{E}[n] \times \mathbf{E}[n] \longrightarrow \mu_n$$

tiene las siguientes propiedades:

1. e_n *es bilineal. Esto quiere decir que*

$$e_n(S_1+S_2,T) = e_n(S_1,T)e_n(S_2,T)$$

y que

$$e_n(S,T_1+T_2) = e_n(S,T_1)e_n(S,T_2)$$

para cualesquiera $S, S_1, S_2, T, T_1, T_2 \in \mathbf{E}[n]$.

2. e_n *es no degenerado en cada variable. Esto quiere decir que si* $e_n(S,T) = 1$ *para todo* $T \in \mathbf{E}[n]$, *entonces* $S = \mathcal{O}$, *y también que si* $e_n(S,T) = 1$ *para todo* $S \in \mathbf{E}[n]$, *entonces* $T = \mathcal{O}$.

3. $e_n(T,T) = 1$ *para todo* $T \in \mathbf{E}[n]$.

4. $e_n(T,S) = e_n(S,T)^{-1}$ *para todo* $S, T \in \mathbf{E}[n]$.

5. $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$ *para todo automorfismo* σ *de* $\overline{K}$ *tal que* σ *sea la identidad en los coeficientes de* $\mathbf{E}$.

6. $e_n(\alpha(S),\alpha(T)) = e_n(S,T)^{\deg(\alpha)}$ *para todos los endomorfismos separables de* $\mathbf{E}$. *Si los coeficientes de* $\mathbf{E}$ *están en un campo finito* $\mathbb{F}_q$, *entonces esta propiedad también es válida cuando* α *es el endomorfismo de Frobenius* ϕ_q. *(Esta última propiedad es de hecho cierta para todos los endomorfismos* α, *separables o no. Ver [Eng].)*

Demostración. (1) Puesto que e_n es independiente de la elección de P, usamos la ecuación (2) con P y $P + S_1$ para obtener

$$\begin{aligned} e_n(S_1, T)e_n(S_2, T) &= \frac{g(P + S_1)}{g(P)} \frac{g(P + S_1 + S_2)}{g(P + S_1)} \\ &= \frac{g(P + S_1 + S_2)}{g(P)} \\ &= e_n(S_1 + S_2, T). \end{aligned}$$

Esto prueba la linealidad en la primera variable.
Supongamos que $T_1, T_2, T_3 \in \mathbf{E}[n]$ con $T_1 + T_2 = T_3$. Para $1 \leq i \leq 3$, denotemos por f_i, g_i a las funciones usadas para definir $e_n(S, T_i)$. Por el Corolario II.6.10, existe una función h tal que

$$\operatorname{div}(h) = [T_3] - [T_1] - [T_2] + [\mathcal{O}].$$

Usando la ecuación (1) obtenemos

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = n \operatorname{div}(h) = \operatorname{div}(h^n).$$

Por lo tanto, existe una constante $c \in \overline{K}^\times$ tal que

$$f_3 = c f_1 f_2 h^n.$$

Esto implica que

$$g_3 = c^{1/n}(g_1)(g_2)(h \circ n).$$

La definición de e_n resulta en

$$\begin{aligned} e_n(S, T_1 + T_2) &= \frac{g_3(P + S)}{g_3(P)} = \frac{g_1(P + S)}{g_1(P)} \frac{g_2(P + S)}{g_2(P)} \frac{h(n(P + S))}{h(n(P))} \\ &= e_n(S, T_1)e_n(S, T_2), \end{aligned}$$

puesto que $nS = \mathcal{O}$, así que $h(n(P + S)) = h(nP)$. Esto prueba la linealidad en la segunda variable.

(2) Supongamos que $T \in \mathbf{E}[n]$ es tal que $e_n(S, T) = 1$ para todo $S \in \mathbf{E}[n]$. Esto quiere decir que $g(P + S) = g(P)$ para todo P y para todo $S \in \mathbf{E}[n]$.

Por la Proposición 9.32 de [Was], existe una función h tal que $g = h \circ n$. Entonces

$$(h \circ n)^n = g^n = f \circ n.$$

Puesto que la multiplicación por n es suprayectiva en $\mathbf{E}[\overline{K}]$, tenemos que $h^n = f$. Por lo tanto,

$$n \operatorname{div}(h) = \operatorname{div}(f) = n[T] - n[\mathcal{O}],$$

así que $\operatorname{div}(h) = [T] - [\mathcal{O}]$. Por el Lema II.6.8, tenemos que $T = \mathcal{O}$. Esto prueba la primera mitad de (2). Para demostrar que es no degenerada en S, basta usar (4) y la no degeneración en T.

(3) Denotemos por τ_{jT} a la función que consiste en sumar jT, así $f \circ \tau_{jT}$ denota a la función $P \mapsto f(P+jT)$. El divisor de $f \circ \tau_{jT}$ es $n[T-jT]-n[-jT]$. Por lo tanto,

$$\operatorname{div}\left(\prod_{j=0}^{n-1} f \circ \tau_{jT}\right) = \sum_{j=0}^{n-1} (n[(1-j)T] - n[-jT]) = 0.$$

Esto quiere decir que $\prod_{j=0}^{n-1} f \circ \tau_{jT}$ es constante. La n-ésima potencia de la función $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ es el producto anterior de las f compuesto con la multiplicación por n, y es por lo tanto constante, ya que

$$\begin{aligned}\left(\prod_{j=0}^{n-1} g \circ \tau_{jT'}\right)^n &= \prod_{j=0}^{n-1} f \circ n \circ \tau_{jT} \\ &= \prod_{j=0}^{n-1} f \circ \tau_{jT} \qquad \text{(puesto que } nT' = T \text{).}\end{aligned}$$

Ya que que hemos probado que este último producto es constante, se sigue que $\prod_{j=0}^{n-1} g \circ \tau_{jT'}$ es constante . Por lo tanto tiene el mismo valor en P y $P + T'$, así que

$$\prod_{j=0}^{n-1} g(P + T' + jT') = \prod_{j=0}^{n-1} g(P + jT').$$

Cancelando términos comunes (suponemos que P es tal que todos los términos son finitos y distintos de cero), obtenemos

$$g(P + nT') = g(P).$$

Puesto que $nT' = T$, esto quiere decir que

$$e_n(T, T) = \frac{g(P+T)}{g(P)} = 1.$$

(4) Se sigue de las propiedades (1) y (3),

$$\begin{aligned} 1 = e_n(S+T, S+T) &= e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T) \\ &= e_n(S,T)e_n(T,S). \end{aligned}$$

Por lo tanto, $e_n(S,T) = e_n(T,S)^{-1}$.

(5) Sea σ un automorfismo de $\overline{K}$ que sea la identidad aplicado a los coeficientes de $\mathbf{E}$. Apliquemos σ a todos los elementos de la construcción de e_n. Entonces

$$\operatorname{div}(f^\sigma) = n[\sigma T] - n[\mathcal{O}],$$

y de manera similar para g^σ, donde f^σ y g^σ denotan las funciones obtenidas de aplicarle σ a los coeficientes de las funciones racionales que definen f y g. Por lo tanto,

$$\sigma(e_n(S,T)) = \sigma\left(\frac{g(P+S)}{g(P)}\right) = \frac{g^\sigma(\sigma P + \sigma)S}{g^\sigma(\sigma P)} = e_n(\sigma S, \sigma P).$$

(6) Sea $\{Q_1, \ldots, Q_k\} = \operatorname{Ker}(\alpha)$. Puesto que α es un morfismo separable, tenemos que $k = \operatorname{grad}(\alpha)$ por la Proposición II.4.3. Sea

$$\operatorname{div}(f_T) = n[T] - n[\mathcal{O}], \quad \operatorname{div}(f_{\alpha(T)}) = n[\alpha(T)] - n[\mathcal{O}],$$

y

$$g_T^n = f_T \circ n, \quad g_{\alpha(T)}^n = f_{\alpha(T)} \circ n.$$

Como en (3), denotemos por τ_Q a sumar Q. Tenemos que

$$\operatorname{div}(f_T \circ \tau_{-Q_i}) = n[T + Q_i] - n[Q_i].$$

Por lo tanto,

$$\begin{aligned}\operatorname{div}(f_{\alpha(T)} \circ \alpha) &= n \sum_{\alpha(T'')=\alpha(T)} [T''] - n \sum_{\alpha(Q)=\mathcal{O}} [Q] \\ &= n \sum_i ([T + Q_i] - [Q_i]) \\ &= \operatorname{div}(\prod_i (f_T \circ \tau_{-Q_i})).\end{aligned}$$

Para cada i, elijamos un Q_i' que cumpla $nQ_i' = Q_i$. Entonces

$$g_T(P - Q_i')^n = f_T(nP - Q_i).$$

Lo que implica que

$$\begin{aligned}\operatorname{div}\left(\prod_i (g_T \circ \tau_{-Q_i'})^n\right) &= \operatorname{div}\left(\prod_i f_T \circ \tau_{-Q_i} \circ n\right) \\ &= \operatorname{div}(f_{\alpha(T)} \circ \alpha \circ n) \\ &= \operatorname{div}(f_{\alpha(T)} \circ n \circ \alpha) \\ &= \operatorname{div}(g_{\alpha(T)} \circ \alpha)^n.\end{aligned}$$

Por lo tanto, $\prod_i g_T \circ \tau_{Q'_i}$ y $g_{\alpha(T)} \circ \alpha$ tienen el mismo divisor, y por lo tanto difieren por una constante C.

La definición de e_n nos da

$$\begin{aligned}e_n(\alpha(S), \alpha(T)) &= \frac{g_{\alpha(T)}(\alpha(P + S))}{g_{\alpha(T)}(\alpha(P))} \\ &= \prod_i \frac{g_T(P + S - Q'_i)}{g_T(P - Q'_i)} \\ &= \prod_i e_n(S, T) \\ &= e_n(S, T)^k = e_n(S, T)^{\operatorname{grad}(\alpha)}\end{aligned}$$

Cuando $\alpha = \phi_q$ es el endomorfismo de Frobenius, entonces (6) implica que

$$e_n(\phi_q(S), \phi_q(T)) = \phi_q(e_n(S, T)) = e_n(S, T)^q,$$

puesto que ϕ_q es la aplicación que eleva a la q-ésima potencia a los elementos de $\overline{\mathbb{F}_q}$. Además, es claro que $q = \text{grad}(\phi_q)$, lo que prueba (6) cuando $\alpha = \phi_q$. Con esto terminamos la prueba del Teorema III.1.1. □

Corolario III.1.2. *Sea* $\{T_1, T_2\}$ *una base de* $\mathbf{E}[n]$. *Entonces* $e_n(T_1, T_2)$ *es una raiz* n*-ésima primitiva de la unidad.*

Demostración. Supongase $e_n(T_1, T_2) = \zeta$ con $\zeta^d = 1$. Entonces $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$. Sea $S \in \mathbf{E}[n]$. Entonces $S = aT_1 + bT_2$ para dos enteros a y b. Por lo tanto,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

Puesto que esta relación se da para cada S, entonces la propiedad (2) implica que $dT_2 = \mathcal{O}$. Como $dT_2 = \mathcal{O}$ si y solamente si $n|d$, se sigue que ζ es una raiz n-ésima primitiva de la unidad. □

Corolario III.1.3. *Si* $\mathbf{E}[n] \subseteq \mathbf{E}(K)$, *entonces* $\mu_n \subset K$.

Demostración. Sea σ un automorfismo de $\overline{K}$ tal que σ restringido a K es la identidad. Sea $\{T_1, T_2\}$ una base de $\mathbf{E}[n]$. Puesto que estamos suponiendo que T_1, T_2 tienen coordenadas en K, tenemos que $\sigma(T_1) = T_1$ y $\sigma(T_2) = T_2$. Por la propiedad (5) del apareo de Weil,

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

Entonces del Teorema Fundamental de la Teoría de Galois se sigue que $\zeta \in K$. Como por el Corolario III.1.2, ζ es una raiz n-ésima primitiva de la unidad, se sigue que $\mu_n \subset K$. □

Observación III.1.4. Notemos ahora que el Corolario anterior implica que si $\mathbf{E}[n] \subset \mathbf{E}(K)$, y K es un campo finito, entonces $n|\#(K^*)$.

Corolario III.1.5. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre* $\mathbb{Q}$. *Entonces* $\mathbf{E}[n] \not\subseteq \mathbf{E}[\mathbb{Q}]$ *para* $n \geq 3$.

El siguiente resultado relaciona el grado de un endomorfismo con su acción sobre $\mathbf{E}[n]$. Recordemos que si α es un endomorfismo de $\mathbf{E}$, entonces obtenemos una matriz $\alpha_n = \begin{pmatrix} a & b \\ c & b \end{pmatrix}$ con entradas en $\mathbb{Z}_n$, que describe la acción de α en una base $\{T_1, T_2\}$ de $\mathbf{E}[n]$.

Proposición III.1.6. *Sea α un endomorfismo de una curva elíptica* $\mathbf{E}$ *definida sobre un campo K. Sea n un entero no divisible por la característica de K. Entonces* $\det(\alpha_n) \equiv \operatorname{grad}(\alpha) \pmod{n}$.

Demostración. Por el Corolario III.1.2, $\zeta = e_n(T_1, T_2)$ es una raiz primitiva n-ésima de la unidad. Por el inciso (6) del Teorema III.1.1, tenemos que

$$\begin{aligned}\zeta^{\operatorname{grad}(\alpha)} &= e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} \\ &= \zeta^{ad-bc}\end{aligned}$$

Puesto que ζ es una raiz n-ésima primitiva de la unidad, se sigue que $\det(\alpha_n) \equiv \operatorname{grad}(\alpha) \pmod{n}$.

□

Sean α y β endomorfismos de $\mathbf{E}$ y a, b enteros. El endomorfismo $a\alpha + b\beta$ está definido por

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Puesto que todas las operaciones están dadas en términos de funciones racionales, tenemos que entonces $a\alpha + b\beta$ también está dado por funciones racionales y es, por lo tanto, un endomorfismo de $\mathbf{E}$. Para este endomorfismo demostraremos la siguiente proposición.

Proposición III.1.7.

$$\operatorname{grad}(a\alpha + b\beta) = a^2 \operatorname{grad}\alpha + b^2 \operatorname{grad}\beta + ab(\operatorname{grad}(\alpha + \beta) - \operatorname{grad}\alpha - \operatorname{grad}\beta).$$

Demostración. Sea n un entero no divisible por la característica de K. Representemos α y β por matrices α_n y β_n, con respecto a una base de $\mathbf{E}[n]$. Entonces $a\alpha_n + b\beta_n$ nos da la acción de $a\alpha + b\beta$ en $\mathbf{E}[n]$, obtenemos:

$$\det(a\alpha_n + b\beta_n) = a^2 \det\alpha_n + b^2 \det\beta_n + ab(\det(\alpha_n + \beta_n) - \det\alpha_n - \det\beta_n)$$

para cualesquiera dos matrices de 2×2, por lo tanto, usando la Proposición anterior, tenemos:

$$\text{grad}(a\alpha+b\beta) \equiv a^2 \det \alpha_n + b^2 \det \beta_n ab(\det(\alpha_n+\beta_n)-\det \alpha_n-\det \beta_n) \pmod{n}.$$

Como esta ecuación se cumple para todo primo p, salvo a lo más uno, se sigue la igualdad buscada. □

Usando la herramienta que hemos desarrollado en los capítulos anteriores, sabemos cómo expresar un divisor de grado cero y cuya suma en $\mathbf{E}$ sea igual a $\mathcal{O}$ como divisor de una función. Este método es suficiente para calcular el apareo de Weil para ejemplos pequeños. Sin embargo, en ejemplos más grandes, se debe tener cuidado para no caer en enormes cálculos. Además de que la definición del apareo de Weil usa una función g cuyo divisor incluye a los n^2 puntos de $\mathbf{E}[n]$. Cuando n es muy grande, esto puede causar dificultades. El siguiente Teorema describe una manera alternativa de calcular el apareo de Weil e_n.

Teorema III.1.8. *Sean $S, T \in \mathbf{E}[n]$. Sean D_S y D_T divisores de grado 0 tales que*

$$\sigma(D_S) = S \quad y \quad \sigma(D_T) = T$$

donde σ es la función definida en la Proposición II.6.9. Supongamos además que D_S y D_T no tienen puntos en comun. Sean f_S y f_T funciones tales que

$$\text{div}(f_S) = nD_S \quad y \quad \text{div}(f_T) = nD_T \ ,$$

Entonces el apareo de Weil está dado por

$$e_n(S,T) = \frac{f_T(D_S)}{f_S(D_T)},$$

donde definimos $f\left(\sum a_i[P_i]\right) = \prod_i f\,(P_i)^{a_i}$.

Para una demostración de que esta operación coincide con el apareo de Weil consultar [How].

Una elección natural de divisores es

$$D_S = [S] - [\mathcal{O}], \quad D_T = [T+R] - [R],$$

para algún punto R elejido al azar. Esto resulta en

$$e_n(S,T) = \frac{f_S(R) f_T(S)}{f_S(T+R) f_T(\mathcal{O})}.$$

Ejemplo III.1.9. Consideremos la curva $y^2 = x^3 - 2x$ definida sobre $\mathbb{F}_{13}$. Esta curva tiene 18 puntos y como grupo es isomorfa a $\mathbb{Z}_3 \oplus \mathbb{Z}_6$. Es claro entonces que contiene a $\mathbf{E}[3]$ Supongamos que queremos calcular el apareo de Weil e_3 de los puntos $(1,5)$ y $(4,2)$ (sobra decir que ambos son puntos de 3-torsión). Para hacer esto, usemos el Teorema anterior. Como divisores asociados al $(1,5)$ y al $(4,2)$ tomamos:

$$D_{(1,5)} = [(1,5)] - [\mathcal{O}] \quad \text{y} \quad D_{(4,2)} = [(12,12)] - [(9,3)],$$

respectivamente, donde $(9,3) + (4,2) = (12,12)$ y todos son puntos de 3-torsión. Esto nos será útil puesto que es claro que un punto P es de 3-torsión si y solamente si la tangente a $\mathbf{E}$ por P intersecta a $\mathbf{E}$ con orden 3, así que para calcular $f_{(1,5)}$ y $f_{(4,2)}$ sólo debemos calcular las tangentes, que además tendrán un polo de orden 3 en $\mathcal{O}$. Veamos:

$$f_{(1,5)} = y + 9x + 12 \quad \text{y} \quad f_{(4,2)} = \frac{y + 7x + 8}{y + x + 1},$$

y entonces sabemos que

$$\begin{aligned} e_3((1,5),(4,2)) &= \frac{f_{(4,2)}(D_{(1,5)})}{f_{(1,5)}(D_{(4,2)})} \\ &= \frac{f_{(4,2)}([(1,5)] - [\mathcal{O}])}{f_{(1,5)}([(12,12)] - [(9,3)])} \\ &= \frac{f_{(4,2)}(1,5) f_{(1,5)}(9,3)}{f_{(4,2)}(\mathcal{O}) f_{(1,5)}(12,12)}. \end{aligned}$$

Para evaluar $f_{(4,2)}(\mathcal{O})$ lo que hacemos es tomar coordenadas homogeneas para $\mathcal{O}$ y homogeneizar a $f_{(4,2)}$. De este modo tenemos que evaluar la función

$$\begin{aligned} f_{(4,2)}(x : y : z) &= \frac{y + 7x + 8z}{y + x + z} \\ f_{(4,2)}(\mathcal{O}) &= f_{(4,2)}(0 : 1 : 0) = 1. \end{aligned}$$

sustituyendo, tenemos entonces que

$$e_3((1,5),(4,2)) = \frac{1 \cdot 5}{1 \cdot 2} \equiv 9 \pmod{13}$$

y ahora sólo falta notar que 9 es en efecto una raiz cúbica de la unidad en $\mathbb{Z}_{13}$, con lo que hemos calculado el valor del apareo de Weil para un par de puntos sin recurrir al grupo de n^2 torsión (en este caso, el grupo de 9-torsión).

III.2 La Aplicación de Frobenius

Sea $\mathbb{F}_q$ un campo finito, cuya cerradura algebraica denotaremos por $\overline{\mathbb{F}}_q$, y hagamos que la aplicación

$$\begin{aligned} \phi_q : \overline{\mathbb{F}}_q &\longrightarrow \overline{\mathbb{F}}_q \\ x &\longmapsto x^q \end{aligned}$$

denote a la *Aplicación de Frobenius* para $\mathbb{F}_q$. Sea $\mathbf{E}$ una curva elíptica definida sobre $\mathbb{F}_q$. Entonces ϕ_q actua sobre las coordenadas de los puntos de $\mathbf{E}$ de la siguiente manera:

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\mathcal{O}) = \mathcal{O}.$$

El siguiente Lema indica una relación profunda entre ϕ_q y los puntos de $\mathbf{E}$ con coordenadas en $\mathbb{F}_q$.

Lema III.2.1. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre* $\mathbb{F}_q$, *y sea* $(x, y) \in \mathbf{E}(\overline{\mathbb{F}}_q)$. *Entonces*

1. $\phi_q(x, y) \in \mathbf{E}(\overline{\mathbb{F}}_q)$.
2. $(x, y) \in \mathbf{E}(\mathbb{F}_q)$ *si y solamente si* $\phi_q(x, y) = (x, y)$

Demostración. Recordemos que si q es una potencia de la característica del campo, entonces $(a + b)^q = a^q + b^q$, y además, se sabe que $a \in \mathbb{F}_q$ si y solamente si $a^q = a$. Daremos la prueba para una curva cuya ecuación tiene la forma

$$y^2 = x^3 + Ax + B,$$

con $A, B \in \mathbb{F}_q$. Si elevamos ambos lados de la ecuación a la q-ésima potencia obtenemos

$$(y^q)^2 = (x^q)^3 + A(x^q) + B,$$

lo que quiere decir que (x^q, y^q) es un punto de $\mathbf{E}$, probando así (1).

Para demostrar (2), veamos que

$$\begin{aligned}(x,y) \in \mathbf{E}(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x \text{ y } \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x,y) = (x,y).\end{aligned}$$

□

El resultado que sigue es clave para contar puntos en curvas elípticas sobre campos finitos. Antes de enunciarlo cabe hacer notar que como ϕ_q es un endomorfismo de $\mathbf{E}$, también lo es $\phi_{q^n} = \phi_q^n = \phi_q \circ \phi_q \circ \ldots \circ \phi_q$ para todo $n \geq 1$. Como la multiplicación por -1 también es un endomorfismo, entonces $\phi_q^n - 1$ es un endomorfismo de $\mathbf{E}$.

Proposición III.2.2. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre* $\mathbb{F}_q$ *y* $n \geq 1$, *entonces*

1. $\mathrm{Ker}(\phi_q^n - 1) = \mathbf{E}(\mathbb{F}_{q^n})$.
2. $\phi_q^n - 1$ *es un endomorfismo separable, por lo tanto* $\#\mathbf{E}(\mathbb{F}_{q^n}) = \mathrm{grad}(\phi_q^n - 1)$.

Demostración. Puesto que ϕ_q^n es sólo la aplicación de Frobenius para el campo $\mathbb{F}_{q^n}$, la parte (1) solo es el Lema III.2.1. Demostramos en el ejemplo II.4.4 que $\phi_q^n - 1$ es separable, así que (2) se sigue del la Proposición II.4.3. □

El objetivo de esta sección es probar el Teorema de Hasse, que nos dice el intervalo en el que puede estar el orden de una curva elíptica sobre un campo finito. Para dar la demostración de dicho Teorema necesitamos el siguiente:

Lema III.2.3. *Sean* r, s *enteros con* $\mathrm{mcd}(s,q) = 1$. *Entonces* $\mathrm{grad}(r\phi_q - s) = r^2 q + s^2 - rsa$.

Demostración. Por la Proposición III.1.7 tenemos que

$$\begin{aligned}\mathrm{grad}(r\phi_q - s) = r^2 \,&\mathrm{grad}(\phi_q) + s^2 \,\mathrm{grad}(-1) \\ &+ rs(\mathrm{grad}(\phi_q - 1) - \mathrm{grad}(\phi_q) - \mathrm{grad}(-1)).\end{aligned}$$

Puesto que $\mathrm{grad}(\phi_q) = q$ y $\mathrm{grad}(-1) = 1$, hemos probado el Lema. □

Teorema III.2.4. *Sea* $\mathbf{E}$ *una curva elíptica sobre el campo finito* F_q. *Entonces el orden de* $\mathbf{E}(\mathbb{F}_q)$ *satisface la siguiente desigualdad*

$$|q + 1 - \#\mathbf{E}(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Demostración. Sea $a = q + 1 - \#\mathbf{E}(\mathbb{F}_q) = q + 1 - \text{grad}(\phi_q - 1)$. Lo que buscamos demostrar es que $|a| \leq 2\sqrt{q}$. Para esto notemos que $\text{grad}(r\phi_q - s) \geq 0$, y el Lema anterior implica que

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

para todo r, s tales que $\text{mcd}(s, q) = 1$. Además, el conjunto de los números racionales r/s tales que $\text{mcd}(s, q) = 1$ es denso en $\mathbb{R}$, por lo tanto,

$$qx^2 - ax + 1 \geq 0$$

para todo número real x. Concluimos entonces que el discriminante del polinomio es negativo o 0, lo que se traduce en $a^2 - 4q \leq 0$. Por lo tanto, $|a| \leq 2\sqrt{q}$. Con esto concluimos la demostración del Teorema de Hasse. □

Usando la misma técnica que aplicamos para probar este Teorema obtendremos el orden de una curva elíptica sobre un campo finito a partir de su orden sobre un subcampo. Para esto necesitamos el siguiente:

Teorema III.2.5. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre* $\mathbb{F}_q$ *y* a *como en el Teorema anterior. Entonces*

$$\phi_q^2 - a\phi_q + q = 0,$$

como endomorfismo de $\mathbf{E}$, *y además* a *es el único entero* k *tal que*

$$\phi_q^2 - k\phi_q + q = 0.$$

Demostración. Si $\phi_q^2 - a\phi_q + q$ no es el endomorfismo 0, entonces, por la Proposición II.4.3, su núcleo es finito. Mostraremos que el núcleo es infinito, y por lo tanto que es el endomorfismo 0.

Sea $m \geq 1$ un entero con $\text{mcd}(m, q) = 1$. Recordemos que ϕ_q induce una matriz $(\phi_q)_m$ que describe la acción de ϕ_q en $\mathbf{E}[m]$. Sea

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

Puesto que $\phi_q - 1$ es separable , la Proposición II.4.3 y la Proposición III.1.6 implican que

$$\begin{aligned} \#\operatorname{Ker}(\phi_q - 1) &= \operatorname{grad}(\phi_q - 1) \equiv \det((\phi_q)_m - I) \\ &= sv - tu - (s+v) + 1 \pmod{m}. \end{aligned}$$

Por la Proposición III.1.6, $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Además, por definición, $\#\operatorname{Ker}(\phi_q - 1) = q + 1 - a$. Por lo tanto,

$$\operatorname{Tr}((\phi_q)_m) = s + v \equiv a \pmod{m}.$$

Puesto que $X^2 - aX + q$ es el polinomio característico de $(\phi_q)_m$, por el Teorema de Cayley-Hamilton tenemos que

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \pmod{m}.$$

donde I es la matriz identidad de 2×2. Esto quiere decir que el endomorfismo $\phi_q^2 - a\phi_q + q$ es identicamente cero en los elementos de $\mathbf{E}[m]$. Como hay una infinidad de posibles elecciones de m, tenemos que el núcleo de este endomorfismo es infinito, así que debe ser el endomorfismo 0.

Para demostrar la unicidad, supongamos que $a_1 \neq a$ es tal que $\phi_q^2 - a_1\phi_q + q = 0$. Entonces

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0$$

Por el Teorema II.4.5, $\phi_q : \mathbf{E}(\overline{\mathbb{F}}_q) \longrightarrow \mathbf{E}(\overline{\mathbb{F}}_q)$ es un endomorfismo suprayectivo. Por lo tanto, $(a - a_1)$ anula a todo $\mathbf{E}(\overline{\mathbb{F}}_q)$, en particular, $(a - a_1)$ anula a $\mathbf{E}[m]$ para todo $m \geq 1$. Puesto que si $\operatorname{mcd}(m, q) = 1$, entonces $\mathbf{E}[m]$ tiene m^2 puntos. Esto implica que $a - a_1 \equiv 0 \pmod{m}$ para tal m. Como m fue arbitrario, podemos concluir que $a - a_1 = 0$, así que a es único. □

Al polinomio $X^2 - aX + q$ se le conoce también como el **polinomio característico de Frobenius.**

Hay veces en las que uno tiene una curva elíptica $\mathbf{E}$ definida sobre un campo finito pequeño $\mathbb{F}_q$ y desea conocer el orden de $\mathbf{E}(\mathbb{F}_{q^n})$ para algún n. Podemos determinar el orden de $\mathbf{E}(\mathbb{F}_q)$ de alguna manera elemental, como un cálculo exhaustivo con todos los elementos de $\mathbb{F}_q$. Lo sorprendente es que esto basta para determinar el orden de $\mathbf{E}(\mathbb{F}_{q^n})$ para todo n.

Teorema III.2.6. *Sea* $\#\mathbf{E}(\mathbb{F}_q) = q + 1 - a$. *Hagamos* $X^2 - aX + q = (X - \alpha)(X - \beta)$. *Entonces*

$$\#\mathbf{E}(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

para todo $n \geq 1$.

Demostración. Antes que nada, notemos que $\alpha^n + \beta^n$ es un entero, puesto que es un entero algebraico y un número racional. Sea

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Entonces $X^2 - aX + q = (X - \alpha)(X - \beta)$ divide a $f(X)$. Se sigue que el cociente es un polinomio $Q(X)$ con coeficientes enteros. Por lo tanto

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0,$$

como endomorfismos de $\mathbf{E}$, por el Teorema III.2.5. Notemos también que $\phi_q^n = \phi_{q^n}$ y de nuevo por el Teorema III.2.5, existe un único entero k tal que $(\phi_{q^n})^2 - k(\phi_{q^n}) + q^n = 0$, y tal k es igual a $k = q^n + 1 - \#\mathbf{E}(\mathbb{F}_{q^n})$. Por lo tanto,

$$\alpha^n + \beta^n = q^n + 1 - \#\mathbf{E}(\mathbb{F}_{q^n}),$$

con lo que concluimos la demostración del Teorema. □

Ejemplo III.2.7. Consideremos la curva $y^2 = x^3 - 2x + 6$ sobre $\mathbb{F}_{11}$. Calculando simplemente elemento por elemento obtenemos que $\#\mathbf{E}(\mathbb{F}_{11}) = 10$. En la notación de esta sección, tenemos que $a = q + 1 - \#\mathbf{E}(\mathbb{F}_{11}) = 11 + 1 - 10 = 2$, así que el polinomio característico de Frobenius es

$$X^2 - 2X + 11 = (X - (1 + \sqrt{-10}))(X - (1 - \sqrt{-10})),$$

y por el Teorema anterior obtenemos entonces que

$$\#\mathbf{E}(\mathbb{F}_{11^{10}}) = 11^{10} + 1 - (1 + \sqrt{-10})^{10} - (1 - \sqrt{-10})^{10}.$$

De aquí, es fácil ver que

$$(1 + \sqrt{-10})^{10} + (1 - \sqrt{-10})^{10} = 321102$$

y por lo tanto

$$\begin{aligned}\#\mathbf{E}(\mathbb{F}_{11^{10}}) &= 11^{10} + 1 - 321102 \\ &= 25937424601 + 1 - 321102 \\ &= 25937103500.\end{aligned}$$

Lo cual nos muestra la profundidad del anterior teorema, al encontrar el orden de una curva sobre un campo muy grande conociendo sólo su orden sobre $\mathbb{F}_{11}$, el cual es un campo pequeño.

Este último teorema es escencial en la demostración de las conjeturas de Weil para curvas elípticas, para ver esto consúltese el apéndice B.

III.3 El MOV

El ataque **MOV** llamado así por sus creadores Menezes, Okamoto y Vanstone, usa el apareo de Weil para convertir un problema del logaritmo discreto en $\mathbf{E}(\mathbb{F}_q)$ a uno en $\mathbb{F}_{q^m}^{\times}$. Puesto que un problema de logaritmo discreto en un campo finito puede ser atacado vía metodos de *cálculo de índices*, puede ser resuelto mucho más rápidamente que un problema de logaritmo discreto en una curva elíptica, siempre y cuando el campo $\mathbb{F}_{q^m}$ no sea mucho más grande que $\mathbb{F}_q$. Precisaremos qué quiere decir *mucho más grande* en el siguiente capítulo.

Recordemos que para una curva eliptica $\mathbf{E}$ definida sobre $\mathbb{F}_q$, denotamos por $\mathbf{E}[N]$ al conjunto de puntos con coordenadas en la cerradura de $\mathbb{F}_q$ y cuyo orden divide a N. Si $\mathrm{mcd}(q, N) = 1$ y $S, T \in \mathbf{E}[N]$, entonces el apareo de Weil $e_N(S, T)$ es una raiz N-ésima de la unidad. Para todo S, $e_N(S, S) = 1$. La lista completa de las propiedades básicas del apareo de Weil está dada en III.1.1.

Sea $\mathbf{E}$ una curva elíptica sobre $\mathbb{F}_q$. Sean $P, Q \in \mathbf{E}(\mathbb{F}_q)$. Denotemos por N el orden de P. Supongamos además que

$$\mathrm{mcd}(N, q) = 1.$$

Queremos encontrar k tal que $Q = kP$. Antes que nada, valdría la pena verificar que dicho k existe. Para eso usaremos el siguiente:

Lema III.3.1. *Existe k tal que $Q = kP$ si y solamente si $NQ = \mathcal{O}$ y el apareo de Weil $e_N(P,Q) = 1$.*

Demostración. Si $Q = kP$, entonces $NQ = kNP = \mathcal{O}$. Además,

$$e_N(P,Q) = e_N(P,P)^k = 1^k = 1.$$

Inversamente, si $NQ = \mathcal{O}$, entonces $Q \in \mathbf{E}[N]$. Puesto que $\mathrm{mcd}(N,q) = 1$, tenemos que $\mathbf{E}[N] \simeq \mathbb{Z}_N \oplus \mathbb{Z}_N$, por el Teorema II.5.1. Elijamos un punto R tal que $\{P,R\}$ sea una base de $\mathbf{E}[N]$. Entonces

$$Q = aP + bR$$

para a y b enteros. Por nuestro Corolario III.1.2, $e_N(P,R) = \zeta$ es una raiz N-ésima primitiva de la unidad. Por lo tanto, si $e_N(P,Q) = 1$, tenemos que

$$1 = e_N(P,Q) = e_N(P,P)^a e_N(P,R)^b = \zeta^b.$$

Esto implica que $b \equiv 0 \pmod{N}$, así que $bR = \mathcal{O}$. Por lo tanto $Q = aP$, como deseabamos demostrar. □

La idea para demostrar el Lema anterior es la que nos lleva al ataque **MOV** para logaritmos discretos en curvas elípticas, el cual describiremos a continuación. Elegimos m tal que

$$\mathbf{E}[N] \subseteq \mathbf{E}(\mathbb{F}_{q^m}).$$

Por el Corolario III.1.3, el grupo μ_N de raices N-ésimas de la unidad está contenido en $\mathbb{F}_{q^m}$. Haremos todos nuestros cálculos en $\mathbb{F}_{q^m}$. El algoritmo es el siguiente:

1. Elegir un punto $T \in \mathbf{E}(\mathbb{F}_{q^m})$ al azar.
2. Calcular el orden M de T.
3. Sea $d = \mathrm{mcd}(M,N)$, y denotemos por $T_1 = (M/d)T$. Entonces T_1 tiene orden d, el cual divide a N, así que $T_1 \in \mathbf{E}[N]$.
4. Calcular $\zeta_1 = e_N(P,T_1)$ y $\zeta_2 = e_N(Q,T_1)$. Tanto ζ_1 como ζ_2 son elementos de $\mu_d \subseteq \mathbb{F}_{q^m}^{\times}$.
5. Resolver el problema del logaritmo discreto $\zeta_2 = \zeta_1^k$ en $\mathbb{F}_{q^m}^{\times}$. Esto nos dara el valor de $k \pmod{d}$.

6. Repetir el proceso anterior hasta que el mínimo común múltiplo de los diversos d's sea N. Esto determina $k \pmod{N}$.

Observación III.3.2. Parecería en un principio que frecuentemente obtendremos $d = 1$. Sin embargo, sucede al revés, gracias a la estructura de $\mathbf{E}(\mathbb{F}_{q^m})$. Recordemos que

$$\mathbf{E}(\mathbb{F}_{q^m}) \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

para un par de enteros n_1, n_2 con $n_1 | n_2$. Entonces $N | n_2$, ya que n_2 es el mayor orden posible de un elemento del grupo. Sean B_1, B_2 puntos de orden n_1 y n_2 respectivamente, tales que B_1, B_2 generan a $\mathbf{E}(\mathbb{F}_{q^m})$. Entonces $T = a_1 B_1 + a_2 B_2$. Sea l^e una potencia de un primo que divida a N. Entonces $l^f | n_2$ con $f \geq e$. Si $l \nmid a_2$, entonces l^f divide a M, el orden de T. Por lo tanto, $l^e | d = \text{mcd}(M, N)$. Ya que la probabilidad de que $l \nmid a_2$ es $1 - 1/l$, la probabilidad de que la mayor potencia l^e esté en d es al menos $1 - 1/l$. Después de pocas elecciones de T, éste debería ser el caso. Por lo tanto, sólo unas cuantas iteraciones del algoritmo deberán ser necesarias para encontrar k.

Observación III.3.3. Notemos que por la observación III.1.4, una condición necesaria para poder efectuar el **MOV** en $\mathbb{F}_{q^m}^{\times}$, y resolver el problema de logaritmo discreto $Q = xP$, es que el orden de P divida a $\#(\mathbb{F}_{q^m}) - 1$. Este hecho será explotado a lo largo del siguiente capítulo.

Capítulo IV

La Probabilidad de Éxito del MOV

IV.1 Introducción

Sea $\mathbf{E}$ una curva elíptica definida sobre un campo finito $\mathbb{F}_p$ con p elementos, donde p es primo. Denotemos por $\mathbf{E}(\mathbb{F}_p)$ al conjunto de puntos $\mathbb{F}_p$-racionales en $\mathbf{E}$ (incluyendo el punto al infinito $\mathcal{O}$). Recordemos que $\mathbf{E}(\mathbb{F}_p)$ forma un grupo abeliano (con $\mathcal{O}$ como el elemento identidad). En el Teorema III.2.4 demostramos que su cardinalidad $N = \#\mathbf{E}(\mathbb{F}_p)$ pertenece al intervalo de *Hasse-Weil* , $N \in \mathcal{I}_p$, donde

$$\mathcal{I}_p = [p + 1 - 2p^{1/2}, p + 1 + 2p^{1/2}].$$

Con el Teorema II.5.4 demostramos que el grupo $\mathbf{E}(\mathbb{F}_p)$ tiene la forma $\mathbb{Z}_L \times \mathbb{Z}_M$, donde los enteros L y M están únicamente determinados y además cumplen que $M \mid L$. Para aplicaciones criptográficas la curva $\mathbf{E}$ es típicamente elejida de tal manera que $\mathbf{E}(\mathbb{F}_p)$ sea un múltiplo pequeño de un número primo. Al implementar un criptosistema usando una curva eliptica, es claro que su seguridad depende de la supuesta dificultad de resolver el problema del logaritmo discreto en un subgrupo cíclico maximal de $\mathbf{E}(\mathbb{F}_p)$ con orden primo, el cual denotaremos por Q. Entre los algoritmos que calculan logaritmos discretos en grupos arbitrarios, los más rápidos tomarían un tiempo de alrededor de $Q^{1/2}$ para calcular un logaritmo discreto en $\mathbf{E}(\mathbb{F}_p)$. Tanto como tardarían en cualquier otro grupo con el mismo orden N.

Un algoritmo diferente, que se ha desarrollado para calcular logaritmos

discretos en curvas elípticas es el conocido algoritmo de *Menezes-Okamoto-Vanstone*, o bien el **MOV** (ver [MOV1]). Este algoritmo construye una inyección de un subgrupo fijo de $\mathbf{E}(\mathbb{F}_p)$ con orden L, en el grupo multiplicativo $\mathbb{F}_{p^k}^*$ de una extensión apropiada de $\mathbb{F}_p$. Heurísticamnete, usando cálculo de índices, se pueden encontrar logaritmos discretos en $\mathbb{F}_{p^k}^*$ en un tiempo de $\mathcal{L}_{p^k}\left(1/3, (64/9)^{1/3}\right)$ (ver [CP, Schi, SWD]), donde, como es usual, $\mathcal{L}_m(\alpha, \beta)$ denota un número de la forma

$$\mathcal{L}_m(\alpha, \beta) = \exp\left((\beta + o(1))(\log m)^{\alpha}(\log\log m)^{1-\alpha}\right).$$

En particular, se sigue que para que el tiempo que le toma al **MOV** (combinado con el cálculo de índices) sea subexponencial, se necesita que $k \leq \log^2 p$. Se puede, sin embargo, presuponer ciertos avances en los algoritmos de cálculo de logaritmos discretos en campos finitos, lo que nos obligaría a considerar valores mayores de k. Es por eso que consideramos una situación más general donde todos los valores de k menores que una cota K lo suficientemente grande son manejados como aceptables.

Se sabe que dos condiciones necesarias y suficientes para que el **MOV** se pueda efectuar en $\mathbb{F}_{p^k}$ es que $L \mid (p^k - 1)$, y que haya L^2 puntos de orden divisor de L en $\mathbf{E}(\mathbb{F}_{p^k})$ (ver la observación III.3.3).

También es bien sabido que la segunda condición implica la primera, Balasubramanian y Koblitz (ver [BK]) mostraron, inversamente, que la primera condición también implica a la segunda, siempre y cuando $\mathbf{E}(\mathbb{F}_p)$ sea cíclico de orden N, un primo que no divida a $p - 1$.

En el mismo artículo [BK], Balasubramanian y Koblitz calculan una cota superior a la probabilidad de que una pareja arbitraria $(p, \mathbf{E})$, la cual consiste de un primo p en el intervalo $[x/2, x]$ y una curva elíptica $\mathbf{E}$ sobre $\mathbb{F}_p$ que tenga un número primo de puntos (entonces $\#\mathbf{E}(\mathbb{F}_p) = N = L = Q$), satisfaga que $N \mid (p^k - 1)$ para algún $k \leq \log^2 p$. Se muestra entonces que para x suficientemente grande,la probabilidad es $O\left(x^{-1}\log^9 x \log\log^2 x\right)$. Esto quiere decir que para una curva elíptica arbitraria con un número primo de puntos, el **MOV** es efectivo con una probabilidad despreciable.

Sin embargo es también interesante analizar la efectividad del **MOV** en otros casos que pueden ocurrir durante aplicaciones específicas de curvas elípticas.

Es decir, aquí estimamos la posibilidad de que el **MOV** resulte efectivo en:

- el grupo de todos los puntos de $\mathbf{E}(\mathbb{F}_p)$;

- el subgrupo cíclico más grande de $\mathbf{E}(\mathbb{F}_p)$;
- el subrupo cíclico más grande de $\mathbf{E}(\mathbb{F}_p)$ que tenga orden primo.

Mostramos que en todos estos casos la probabilidad de éxito del **MOV** es exponencialmente pequeña. Nuestros resultados son válidos para cualquier primo p y una curva $\mathbf{E}$ elegida al azar sobre $\mathbb{F}_p$, mientras que para el resultado de [BK], es esencial que p tambien ser elegido al azar.

En particular, tambien extendemos el resultado arriba mencionado de [BK] en el que $\mathbf{E}(\mathbb{F}_p)$ es cíclico, con la salvedad de que no requerimos que su número de puntos sea primo, e incluso nuestros resultados se extienden al caso general, en el que no imponemos restricción alguna en la estructura del grupo $\mathbf{E}(\mathbb{F}_p)$.

Como en [BK], una de las herramientas básicas que usamos es un resultado de Lenstra publicado en [Len], que escencialmente dice que cualquier entero $N \in \mathcal{I}_p$ representa la cardinalidad $\#\mathbf{E}(\mathbb{F}_p)$ para aproximadamente el mismo número de curvas elípticas $\mathbf{E}$ sobre $\mathbb{F}_p$. Este teorema nos da una relación entre nuestro problema y el problema de teoría de números consistente en estudiar enteros pertenecientes a pequeños intervalos que dividan a $p^k - 1$ para algún k pequeño, problema que es interesante de manera independiente y que es además la base de nuestro resultado.

IV.2 Preliminares

Usamos $\omega(n)$ para denotar el número de factores primos distintos de un entero positivo n y usamos $P(n)$ para denotar el mayor divisor primo de n, definimos $\omega(1) = 0$ y $P(1) = 1$. Denotamos por $\mathrm{rad}(n)$ al radical de n, es decir, el mayor divisor libre de cuadrados de n.

Para un número real positivo x y un entero positivo k, usamos $\log_k x$ como la función definida recursivamente dada por $\log_k x = \max\{\log(\log_{k-1} x),\ 1\}$, donde log es el logaritmo natural. Cuando $k = 1$ omitimos el subíndice, y entonces entendemos que todos los logaritmos que aparecen son ≥ 1.

En este capítulo usaremos la notación de Landau, la cual describiremos a continuación:

Sea $g(x)$ una función positiva, definida para todo x real. Sea $f(x)$ una función real o compleja.

1. Si en una vecindad de un $a \in \mathbb{R} \cup \{\infty\}$ tenemos que $\frac{|f(x)|}{g(x)} \leq K$ para una constante K, entonces escribimos

$$f(x) = O(g(x)) \quad (x \to a) \quad \text{o bien} \quad f(x) \ll g(x) \quad (x \to a).$$

   Entenderemos $A \ll B$ y $B \gg A$ como equivalentes a $A = O(B)$

2. Si para $a \in \mathbb{R} \cup \{\infty\}$ tenemos que $\lim_{x \to a} \frac{f(x)}{g(x)} = 0$, entonces escribimos

$$f(x) = o(g(x)) \quad (x \to a).$$

3. Si se cumplen simultaneamente $A \gg B$ y $A \ll B$ escribiremos entonces $A \asymp B$

Cuando la notación de Landau se usa sin un $a \in \mathbb{R} \cup \{\infty\}$, entonces debe entenderse que $a = \infty$

En esta notación, podemos enunciar un conocido Teorema debido a Mertens como sigue:

$$\sum_{p \leq n} \frac{1}{p} = \log_2 n + O(1).$$

Donde la suma se toma sobre los números primos menores o iguales a n.

Usaremos también el hecho de que hay $2p + O(1)$ clases de curvas no isomorfas sobre $\mathbb{F}_p$ (ver Sección 1.4 de [Len]). La Proposición 1.9 de [Len] asegura además que sus cardinalidades están distribuidas de manera casi uniforme, salvo ciertos factores logarítmicos. Esta distribución está garantizada por el siguiente Lema.

Lema IV.2.1. *Para cualquier entero $N \in \mathcal{I}_p$ el número de clases de isomorfismo de curvas elípticas $\mathbf{E}$ sobre $\mathbb{F}_p$ con $N = \#\mathbf{E}(\mathbb{F}_p)$ es $O\left(p^{1/2} \log p \log_2^2 p\right)$.*

A lo largo de este capítulo usaremos repitidamente la siguiente fórmula debida a Stirling:

$$\lim_{n \to \infty} \frac{n!}{(n/e)^n \sqrt{2\pi n}} = 1.$$

De aquí en adelante usaremos que la desigualdad $\omega(n) < \log n$ se da para todos los enteros n suficientemente grandes, lo que se sigue de la desigualdad trivial $\omega(n)! \leq n$ y la formula de Stirling.

IV.3 Primeros Resultados

Para los números reales $H \geq h \geq 1$ y un entero $K \geq 1$, denotaremos por $\mathcal{N}(p, K, H, h)$ al conjunto de enteros positivos N en el intervalo $[H-h, H+h]$ tales que existe un entero positivo $k \leq K$ para el que se cumple $N \mid (p^k - 1)$.

Dado un entero $w \leq 1$, denotamos por $\mathcal{N}_1(p, K, H, h, w)$ y $\mathcal{N}_2(p, K, H, h, w)$ a los subconjuntos de $\mathcal{N}(p, K, H, h)$ que consisten de los $N \in \mathcal{N}(p, K, H, h)$ tales que $\omega(N) \leq w$ y $\omega(N) > w$ respectivamente.

Las siguientes dos proposiciones dan cotas superiores para $\#\mathcal{N}_1(p, K, H, h, w)$ y $\#\mathcal{N}_2(p, K, H, h, w)$,que más adelante usaremos para estimar

$$\#\mathcal{N}(p, K, H, h) = \#\mathcal{N}_1(p, K, H, h, w) + \#\mathcal{N}_2(p, K, H, h, w)$$

usando un valor optimo de w.

Lema IV.3.1. *Existe una constante $C_1 > 0$ tal que para todo entero $w \to \infty$ de forma tal que $w \leq 0.5K \log p$, la desigualdad*

$$\#\mathcal{N}_1(p, K, H, h, w) \ll K \left(\frac{C_1 K \log H \log p}{w} \right)^w$$

se cumple.

Demostración. Sea

$$N = \prod_{q \mid (p^k - 1)} q^{a_q}$$

la factorización en primos de $N \in \mathcal{N}_1(p, K, H, h, w)$ con $N \mid (p^k - 1)$ para algún $k \leq K$. Entonces N tiene en su soporte a lo más w primos $q \mid (p^k - 1)$ y para estos primos tenemos que $2^{a_q} \leq q^{a_q} \leq N \leq 2H$. Entonces $a_q \leq 2 \log H / \log 2 < 3 \log H$, y vemos que

$$\begin{aligned} \#\mathcal{N}_1(p, K, H, h, w) &\leq \sum_{k=1}^{K} \sum_{s=0}^{w} \binom{\omega(p^k - 1)}{s} (3 \log H)^s \\ &\leq (3 \log H)^w \sum_{k=1}^{K} \sum_{s=0}^{w} \binom{\omega(p^k - 1)}{s}. \end{aligned}$$

Claramente, la desigualdad $\omega(p^k - 1) \leq k \log p$ se da para valores de p suficientemente grandes. Concluimos entonces gracias a que $w < 1/2K \log p$ lo

siguiente

$$\begin{aligned}\#\mathcal{N}_1(p,K,H,h,w) &\leq Kw\binom{\lfloor K\log p\rfloor}{w}(3\log H)^w\\ &\leq \frac{wK}{(w)!}(3K\log H\log p)^w\end{aligned}$$

y aplicando la *fórmula de Stirling* en $(w)!$ concluimos la demostración. Veamos

$$\begin{aligned}\#\mathcal{N}_1(p,K,H,h,w) &\leq \frac{wK}{(w)!}(3K\log H\log p)^w\\ &\ll \frac{wK}{(w/e)^w\sqrt{2\pi w}}\\ &\ll K\sqrt{w}\left(\frac{C_0K\log H\log p}{w}\right)^w\\ &\ll K\left(\frac{C_1K\log H\log p}{w}\right)^w.\end{aligned}$$

Con lo que concluimos la demostración.

□

Lema IV.3.2. *Existe una constante $C_2 > 0$ tal que para todo $w \to \infty$ y $H \geq h$ se cumple la desigualdad*

$$\#\mathcal{N}_2(p,K,H,h,w) \leq h\left(\frac{C_2\log_2(K^2\log p)}{w}\right)^{w/2} + K\left(\frac{C_2K\log p}{w}\right)^{w/2}$$

para valores lo suficientemente grandes del primo p.

Demostración. Para todo $N \in \mathcal{N}_2(p,K,H,h,w)$, hacemos $N = m\ell$, donde m es el producto de los primeros (es decir, los más pequeños) $v = \lfloor w/2\rfloor$ factores primos distintos de N. Notemos que $\ell \geq m$ porque N tiene al menos w factores primos distintos. Se sigue entonces que $H/m - h/m \leq \ell \leq H/m + h/m$. Así, para un m fijo , hay a lo más $O(h/m) + 1$ valores de ℓ.

Sea $\mathcal{Q}_k$ el conjunto de todos los divisores primos de $p^k - 1$, y $\mathcal{M}_k$ el conjunto de todos los enteros m libres de cuadrados con todos sus factores

primos en $\mathcal{Q}_k$ y con $\omega(m) = v$. Hacemos también

$$\mathcal{M} = \bigcup_{k=1}^{K} \mathcal{M}_k \qquad \text{y} \qquad \mathcal{Q} = \bigcup_{k=1}^{K} \mathcal{Q}_k.$$

Tenemos así

$$\begin{aligned} \#\mathcal{N}_2(p, K, H, h, w) &\ll \sum_{m \in \mathcal{M}} \left(O\left(\frac{h}{m}\right) + 1 \right) \\ &\ll h \sum_{m \in \mathcal{M}} \frac{1}{m} + \#\mathcal{M} \\ &\leq \frac{h}{v!} \left(\sum_{q \in \mathcal{Q}} \frac{1}{q} \right)^v + \sum_{k=1}^{K} \binom{\omega(p^k - 1)}{v}. \end{aligned}$$

Reemplazando la suma sobre los primos en $\mathcal{Q}$ por la suma sobre los primeros $t = \#\mathcal{Q}$ primos, usando el *Teorema de Mertens* (ver el Teorema 427 en [HW]), obtenemos

$$\#\mathcal{N}_2(p, K, H, h, w) \ll \frac{h}{v!} \left(\log_2 t + O(1) \right)^v + \sum_{k=1}^{K} \frac{\omega(p^k - 1)^v}{v!}.$$

Remarcamos como antes que la desigualdad $\omega(p^k - 1) \leq k \log p$ se da para todos los primos p lo suficientemente grandes, por lo cual la desigualdad $t \leq K^2 \log p$ también se cumple para todo p lo suficientemente grande. Usando la fórmula de Stirling para $v!$ concluimos la prueba. □

Lema IV.3.3. *Sea $H \geq h$, $\log H \asymp \log h \asymp \log p$ y $\log K = O(\log_2 p)$. Entonces, la desigualdad*

$$\#\mathcal{N}(p, K, H, h) \leq h^{1 - 1/(2\kappa + 3) + o(1)}$$

se cumple, donde

$$\kappa = \frac{\log K}{\log_2 p}.$$

Demostración. Elijamos

$$w = \left\lfloor \frac{2 \log h}{2 \log K + 2 \log_2 p + \log_2 H} \right\rfloor,$$

para balancear (asintóticamente) los estimados de los Lemas IV.3.1 y IV.3.2, tomando en cuenta que $\log H \asymp \log h$ obtenemos

$$\log\left(\frac{K \log H \log p}{w}\right) \sim \log K + \log p.$$

Recalcamos que $\log_2 H \sim \log_2 h$. Entonces, como las hipótesis del Lema IV.3.1 se satisfacen, llegamos a

$$\#\mathcal{N}_1(p, K, H, h, w) \leq h^{\vartheta + o(1)},$$

donde

$$\vartheta = \frac{2\log K + 2\log_2 p}{2\log K + 2\log_2 p + \log_2 H} = \frac{2\log K + 2\log_2 p}{2\log K + 3\log_2 p} + o(1) = \frac{2\kappa + 2}{2\kappa + 3} + o(1).$$

Hacemos notar también que

$$\log w \sim \log_2 h \sim \log_2 p.$$

Como $\log K = O(\log_2 p)$, tenemos que $\log_2(K^2 \log p) = w^{o(1)}$. Así,

$$\begin{aligned}\left(\frac{\log_2(K^2 \log p)}{w}\right)^{w/2 + o(w)} &= \exp(-(0.5 + o(1))w \log w) \\ &= \exp\left(-(0.5 + o(1))\frac{2\log h \log_2 p}{2\log K + 2\log_2 p + \log_2 H}\right) \\ &= h^{-1/(2\kappa+3)+o(1)}.\end{aligned}$$

Tenemos también que

$$\begin{aligned}K\left(\frac{C_2 K \log p}{w}\right)^{w/2} &= \exp\left((0.5 + o(1))\, w \log K\right) \\ &= \exp\left((1 + o(1))\,\frac{\log h \log K}{2\log K + 2\log_2 p + \log_2 H}\right) \\ &= h^{\kappa/(2\kappa+3)+o(1)} < h^{\vartheta + o(1)},\end{aligned}$$

de donde se concluye el resultado. □

Dados dos números reales $H \geq h \geq 1$, y un entero $K \geq 1$, denotamos por $\mathcal{T}(p, K, H, h)$ al conjunto de enteros positivos N en el intervalo $[H - h, H + h]$

tales que todos sus factores primos dividen a $p^k - 1$ para algún entero positivo $k \leq K$; es decir,

$$\mathrm{rad}(N) \mid \prod_{k \leq K} (p^k - 1).$$

De igual manera, para un entero $w \geq 1$, denotamos por $\mathcal{T}_1(p, K, H, h, w)$ y $\mathcal{T}_2(p, K, H, h, w)$ a los subconjuntos de $N \in \mathcal{T}(p, K, H, h)$ con $\omega(N) \leq w$ y con $\omega(N) > w$, respectivamente. Usando los mismos argumentos que en las pruebas de los Lemas IV.3.1 y IV.3.2, y recordando que

$$\omega\left(\prod_{k=1}^{K} (p^k - 1)\right) \leq K^2 \log p,$$

obtenemos las siguientes proposiciones.

Lema IV.3.4. *Existe una constante $C_3 > 0$ tal que para todo entero $w \to \infty$ de tal manera que $w \leq 0.5K \log p$, la desigualdad*

$$\#\mathcal{T}_1(p, K, H, h, w) \ll \left(\frac{C_3 K^2 \log H \log p}{w}\right)^w$$

se cumple.

Demostración. Como en el Lema IV.3.1, si escribimos a un $N \in \mathcal{T}_1(p, K, H, h, w)$ como $N \prod_{q \in \mathcal{Q}} q^{a_q}$, entonces se sigue que $a \leq (3 \log H)$. Vemos entonces que

$$\begin{aligned}
\#\mathcal{T}_1(p, K, H, h, w) &\leq \sum_{s=1}^{w} \binom{\#\mathcal{Q}}{s} (3 \log H)^s \\
&\leq (3 \log H)^w \sum_{s=1}^{w} \binom{\#\mathcal{Q}}{s} (3 \log H)^s \\
&\leq w (3 \log H)^w \frac{(K^2 \log p)^w}{w!}
\end{aligned}$$

La última desigualdad se debe a que $w \leq 1/2K \log p$. Aplicando ahora la fórmula de Stirling concluimos la demostración. □

Lema IV.3.5. *Existe una constante $C_4 > 0$ tal que para todo $w \to \infty$ y $H \geq h$, la desigualdad*

$$\#\mathcal{T}_2(p, K, H, h, w) \leq h \left(\frac{C_4 \log_2(K^2 \log p)}{w} \right)^{w/2} + \left(\frac{C_4 K \log p}{w} \right)^{w/2}$$

se da para valores grandes del primo p.

Demostración. La demostración de este Lema es precisamente la demostración del Lema IV.3.2. □

Entonces, una combinación de los Lemas IV.3.4 y IV.3.5, nos lleva un análogo del Lema IV.3.6 .

Lema IV.3.6. *Sean $H \geq h$, $\log H \asymp \log h \asymp \log p$ y $\log K = O(\log_2 p)$. Entonces la desigualdad*

$$\#\mathcal{T}(p, K, H, h) \leq h^{1-1/(4\kappa+3)+o(1)}$$

se da, donde

$$\kappa = \frac{\log K}{\log_2 p}.$$

Demostración. Escojamos

$$w = \left\lfloor \frac{2 \log h}{2 \log K + 2 \log_2 p + \log_2 H} \right\rfloor,$$

para balancear (asintoticamente) los estimados de los Lemas IV.3.4 y IV.3.5, tomando en cuenta que $\log H \asymp \log h$, llegamos a

$$\log \left(\frac{K^2 \log H \log p}{w} \right) \sim 2 \log K + \log p.$$

Recalcamos que $\log_2 H \sim \log_2 h$. Entonces

$$\#\mathcal{T}_1(p, K, H, h, w) \leq h^{\vartheta + o(1)}.$$

donde

$$\vartheta = \frac{4 \log K + 2 \log_2 p}{4 \log K + 2 \log_2 p + \log_2 H} = \frac{4 \log K + 2 \log_2 p}{4 \log K + 3 \log_2 p} + o(1) = \frac{4\kappa + 2}{4\kappa + 3} + o(1).$$

También hacemos notar que

$$\log w \sim \log_2 h \sim \log_2 p.$$

Puesto que $\log K = O(\log_2 p)$, tenemos que $\log_2(K^2 \log p) = w^{o(1)}$. Así,

$$\begin{aligned}\left(\frac{\log_2(K^2 \log p)}{w}\right)^{w/2+o(w)} &= \exp(-(0.5+o(1))w \log w) \\ &= \exp\left(-(0.5+o(1))\frac{2\log h \log_2 p}{4\log K + 2\log_2 p + \log_2 H}\right) \\ &= h^{-1/(4\kappa+3)+o(1)}.\end{aligned}$$

También tenemos que

$$\begin{aligned}\left(\frac{C_4 K^2 \log p}{w}\right)^{w/2} &= \exp\left((0.5+o(1))\, w \log K\right) \\ &= \exp\left((1+o(1))\,\frac{\log h \log K}{4\log K + 2\log_2 p + \log_2 H}\right) \\ &= h^{\kappa/(4\kappa+3)+o(1)} < h^{\vartheta+o(1)},\end{aligned}$$

de donde concluimos el resultado.

□

IV.4 Resultados Principales

Teorema IV.4.1. *Sea p un número primo lo suficientemente grande, y sea K un entero positivo que cumpla $\log K = O(\log_2 p)$. Supongamos que $\mathbf{E}$ es una curva elíptica sobre $\mathbb{F}_p$ escogida al azar. Sea $N = \#\mathbf{E}(\mathbb{F}_p)$. La probabilidad de que $N \mid (p^k - 1)$ se de para algún entero positivo $k \leq K$ es a lo más $p^{-1/(4\kappa+6)+o(1)}$ donde*

$$\kappa = \frac{\log K}{\log_2 p}.$$

Demostración. El resultado se sigue de manera inmediata de los Lemas IV.2.1 y IV.3.3 haciendo $H = p$ y $h = 2p^{1/2}$ y usando además que para un primo dado hay $2p + O(1)$ clases de curvas no isomorfas sobre $\mathbb{F}_p$ □

En particular, para $K = \lceil \log^2 p \rceil$, la probabilidad estimada para el Teorema IV.4.1 se convierte en $p^{-1/14+o(1)}$.

Si $R = \mathrm{rad}\,(\#\mathbf{E}(\mathbb{F}_p))$ y L es el exponente de $\mathbf{E}(\mathbb{F}_p)$, entonces es claro que $R|L$.De esta manera es suficiente estimar la probabilidad de que $R \mid (p^k - 1)$ para un valor pequeño de k.

Teorema IV.4.2. *Sea p un número primo lo suficientemente grande, y sea K un entero positivo que cumpla $\log K = O(\log_2 p)$. Supongamos que $\mathbf{E}$ es una curva elíptica sobre $\mathbb{F}_p$ elegida al azar. Sea $R = \mathrm{rad}\,(\#\mathbf{E}(\mathbb{F}_p))$. La probabilidad de que $R \mid (p^k - 1)$ para algún entero positivo $k \leq K$ es a lo más $p^{-1/(4\kappa+8)+o(1)}$ donde*

$$\kappa = \frac{\log K}{\log_2 p}.$$

Demostración. Dado un entero $r \geq 1$, denotamos por $S(p, K, r)$ al número de enteros $N \in \mathcal{I}_p$ tales que $N = r^2 m$ con $m \mid (p^k - 1)$ para algún entero positivo $k \leq K$. Claramente, para $r \geq 2p^{1/3}$ tenemos que $m \leq p^{1/3}$ siempre que p sea lo suficientemente grande. Recalcamos que para todo entero $m \geq 1$ hay solamente $O(1)$ enteros libres de cuadrados en el intervalo $[(p+1)/m - 2p^{1/2}/m, (p+1)/m + 2p^{1/2}/m]$, así que

$$\sum_{r \geq 2p^{1/3}} S(p, K, r) \ll \sum_{m \leq p^{1/3}} 1 \ll p^{1/3}.$$

Tenemos también que

$$\begin{aligned}\sum_{p^{1/6} \leq r \leq 2p^{1/3}} S(p, K, r) &\leq \sum_{p^{1/6} \leq r \leq 2p^{1/3}} \left(\frac{4p^{1/2}}{r^2} + 1 \right) \\ &\leq 4p^{1/2} \sum_{r \geq p^{1/6}} \frac{1}{r^2} + \sum_{p^{1/6} \leq r \leq 2p^{1/3}} 1 \ll p^{1/3}.\end{aligned}$$

Para $r < p^{1/6}$, usamos la desigualdad trivial

$$S(p, K, r) \leq \#\mathcal{N}(p, K, (p+1)/r^2, 2p^{1/2}/r^2).$$

Por lo tanto, usando el Lema IV.3.3, tenemos que

$$\sum_{r < p^{1/6}} S(p, K, r) \leq \sum_{r < p^{1/6}} (p^{1/2}/r^2)^{1-1/(2\kappa+3)+o(1)} \leq p^{1/2-1/(4\kappa+6)+o(1)}.$$

Aplicando el Lema IV.2.1, concluimos la demostración.

□

Al calcular logaritmos discretos podemos combinar el **MOV** con un ataque del tipo Pohling-Hellman (ver [CP, MOV2]). Dicho esto de manera más precisa, uno puede factorizar

$$N = \#\mathbf{E}(\mathbb{F}_p) = \prod_{i=1}^{s} p_i^{\alpha_i},$$

y entonces resolver varios problemas de logaritmo discreto en los subgrupos de $\mathbf{E}(\mathbb{F}_p)$ de orden p_i para $i = 1, \ldots, s$.

Esto nos lleva a preguntarnos si los divisores primos de N están entre la unión de los divisores primos de $p^k - 1$, $k = 1, \ldots, K$, para alguna K razonablemente pequeña.

Para esto, usando el Lema IV.3.6 en lugar del Lema IV.3.3 en la demostración del Teorema IV.4.2, obtenemos el siguiente resultado.

Teorema IV.4.3. *Sea p un número primo lo suficientemente grande, y sea K un entero positivo que cumpla $\log K = O(\log_2 p)$. Supongamos que $\mathbf{E}$ es una curva elíptica sobre $\mathbb{F}_p$ elejida al azar. Sea $R = \mathrm{rad}\,(\#\mathbf{E}(\mathbb{F}_p))$. La probabilidad de que*

$$R \;\Big|\; \prod_{k \le K} (p^k - 1).$$

es a lo más $p^{-1/(8\kappa+6)+o(1)}$ donde

$$\kappa = \frac{\log K}{\log_2 p}.$$

Demostración. Dado un entero $r \ge 1$, denotamos por $\widetilde{S}(p, K, r)$ al número de enteros $N \in \mathcal{I}_p$ tales que $N = r^2 m$ con

$$m \;\Big|\; \prod_{k \le K} (p^k - 1).$$

Como en la demostraci'on del Teorema IV.4.2, obtenemos que

$$\sum_{r \ge p^{1/6}} \widetilde{S}(p, K, r) \ll p^{1/3} < p^{3/8}.$$

Para $r < p^{1/6}$, usamos la desigualdad trivial

$$\widetilde{S}(p, K, r) \leq \#\mathcal{T}(p, K, (p+1)/r^2, 2p^{1/2}/r^2).$$

Por lo tanto, gracias al Lema IV.3.6, obtenemos

$$\sum_{r<p^{1/6}} \widetilde{S}(p, K, r) \leq \sum_{r<p^{1/6}} (p^{1/2}/r^2)^{1-1/(4\kappa+3)+o(1)} \leq p^{1/2-1/(8\kappa+6)+o(1)}.$$

Usando el Lema IV.2.1, concluimos nuestra demostración. □

En particular, para $K = \lceil \log^2 p \rceil$ la probabilidad estimada en el Teorema IV.4.2 se vuelve $p^{-1/22+o(1)}$.

Teorema IV.4.4. *Sea p un primo lo suficientemente grande, y sea K un entero positivo con $\log K = O(\log_2 p)$. Supongamos que $\mathbf{E}$ es una curva elíptica sobre $\mathbb{F}_p$ elejida al azar. Hagamos $Q = P(\#\mathbf{E}(\mathbb{F}_p))$. La probabilidad de que $Q \mid (p^k - 1)$ con $k \leq K$ un entero positivo es a lo más* $\exp\left(-0.2(\log p \log_2 p)^{1/2}\right)$.

Demostración. Sea $u \geq 1$ un número real, y denotemos por

$$y = p^{1/2u}.$$

Se sigue, usando resultados conocidos sobre números suaves en intervalos pequeños (ver, por ejemplo [Hil]), que para $u \to \infty$ el número de valores de $N \in \mathcal{I}_p$ tales que $P(N) \leq y$ es a lo más $p^{1/2} \exp\left(-(1+o(1))u \log u\right)$.

Por otro lado, el número de valores N que satisfacen ambos $P(N) > y$ y $P(N) \mid (p^k - 1)$ para algún entero positivo $k \leq K$, es a lo más

$$\sum_{k=1}^{K} \omega(p^k - 1)\left(\frac{4p^{1/2}}{y} + 1\right) \ll p^{1/2} y^{-1} K^2 \log p.$$

Por lo tanto, el número total de $N \in \mathcal{I}_p$ para los cuales $P(N) \mid (p^k - 1)$ se da con algún entero positivo $k \leq K$ es

$$O\left(p^{1/2}\left(\exp\left(-(1+o(1))u \log u\right) + y^{-1} K^2 \log p\right)\right).$$

Si elegimos

$$u = \left(\frac{\log p}{5 \log_2 p}\right)^{1/2},$$

deducimos que la desigualdad

$$u \leq \frac{\log p}{8 \log K}$$

se da, siempre y cuando p sea suficientemente grande. Deducimos, por lo tanto, que la desigualdad

$$\exp\left(-(1+o(1))u \log u\right) \geq p^{-1/4u} \geq p^{-1/2u} K^2 = y^{-1} K^2$$

se da para valores de p suficientemente grandes. Usando el Lema IV.2.1y efectuando unos cuantos cálculos, concluimos la demostración. □

En particular, el estimado del Teorema IV.4.4 es valida cuando $K = \lceil \log^2 p \rceil$. Es facil ver que la constante 0.2 en los exponentes de la cota Teorema IV.4.4 se puede reducir.

Estas técnicas pueden ser usadas también para obtener cotas no triviales, de las probabilidades arriba mencionadas, en un rango mucho mayor que $\log K = O(\log_2 p)$, el cual usamos en nuestros resultados.

Apéndice A

Algoritmos

En este apéndice presentamos varios algoritmos que fueron mencionados a lo largo de la exposición hecha en este trabajo. Comenzamos con varios algoritmos de cálculo de logaritmos discretos que funcionan para grupos arbitrarios, como la reducción de Pohlig-Hellman y el método ρ de Pollard. Enfocado también al **PLD** presentamos el método del cálculo de índices, un algoritmo de cálculo de logaritmos discretos para grupos finitos. Finalmente presentamos el algoritmo de Schoof para calcular el orden de una curva elíptica sobre un campo finito, este algoritmo es muy eficiente y ha sido usado para determinar el orden de curvas elípticas sobre campos del orden de $\mathbb{F}_{2^{1999}}$.

A.1 El Problema del Logaritmo Discreto

La Reducción de Pohlig-Hellman

En esta sección presentamos la reducción de Pohlig-Hellman, la cual básicamente dice que la dificultad de calcular el logaritmo discreto $Q = kP$ reside en la dificultad de calcular logaritmos discretos en un grupo cíclico cuyo orden sea el primo más grande que divida al orden de P.

Sean P, Q elementos de un grupo G, para los cuales queremos encontrar un entero k que cumpla $Q = kP$. Supondremos que conocemos el orden N de P y la factorización en primos

$$N = \prod_i q_i^{e_i}$$

de N. La idea de Pohlig-Hellman es encontrar $k \pmod{q_i^{e_i}}$ para todo i, y

usar esta información junto con el Teorema Chino del Residuo para calcular el valor de $k \pmod N$. Sea q un primo y q^e la mayor potencia de q que divida a N. Escribamos a k con su expansión en base q como

$$k = k_0 + k_1 q + k_2 q^2 + \ldots$$

con $0 \leq k_i < q$. Calcularemos $k \pmod{q^e}$ determinando sucesivamente los valores de $k_0, k_1, \ldots, k_{e-1}$. El procedimiento es el siguiente:

1. Calcular $T = \{j \left(\frac{N}{q}P\right) | 0 \leq j \leq q-1\}$.
2. Calcular $\frac{N}{q}Q$. Éste será un elemento de la forma $k_0 \left(\frac{N}{q}P\right)$ y por lo tanto un miembro de T.
3. Parar si $e = 1$, de otro modo, continuar.
4. Sea $Q_1 = Q - k_0 P$.
5. Calcular $\frac{N}{q^2}Q_1$. Éste será de nuevo un elemento de la forma $k_1 \left(\frac{N}{q}P\right)$, y por lo tanto un miembro de T.
6. Parar si $e = 2$, de otro modo, continuar.
7. Supongamos que hemos calculado $k_0, k_1, \ldots, k_{r-1}$, y $Q_1, Q_2, \ldots, Q_{r-1}$.
8. Sea $Q_r = Q_{r-1} - k_{r-1} q^{r-1} P$.
9. Determinar k_r tal que $\frac{N}{q^{r+1}}Q_r = k_r \left(\frac{N}{q}P\right)$.
10. Parar si $r = e - 1$, de otro modo, volver al paso (7).

Entonces tenemos que

$$k \equiv k_0 + k_1 q + \ldots + k_{e-1} q^{e-1} \pmod{q^e}$$

Pero, ¿porqué funciona?, veamos

$$\begin{aligned} \frac{N}{q}Q &= \frac{N}{q}(k_0 + k_1 q + \ldots)P \\ &= k_0 \frac{N}{q}P + (k_1 + k_2 q + \ldots)NP = k_0 \frac{N}{q}P, \end{aligned}$$

ya que $NP = \mathcal{O}$ (estamos denotando por $\mathcal{O}$ a la identidad del grupo G). Por lo tanto, el paso (2) en verdad calcula k_0, así

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + \ldots)P,$$

entonces

$$\begin{aligned}\frac{N}{q^2}Q_1 &= (k_1 + k_2 q + \ldots)\frac{N}{q}P \\ &= k_1\frac{N}{q}P + (k_2 + k_3 q + \ldots)NP = K_1\frac{N}{q}P.\end{aligned}$$

Por lo tanto, así encontramos k_1. De manera similar, el método encuentra $k_2, k_3, \ldots$. Debemos parar después de que $r = e - 1$ ya que N/q^{e+1} no es un entero, y no podemos multiplicar Q_e por el número no entero N/q^{e+1}, además de que no es necesario continuar, puesto que ya conocemos el valor de $k \pmod{q^e}$.

El método de Pohlig-Hellman es muy efectivo si todos los primos que dividen a N son pequeños. Sin embargo, si q es un primo muy grande que divida a N, entonces es difícil dar la lista de elementos de T, que contiene q elementos. Podríamos intentar encontrar los k_i sin hacer la lista de los elementos de T; sin embargo, encontrar los k_i de esta manera se convierte en un problema de logaritmo discreto en el grupo generado por $(N/q)P$, el cual tiene orden q. Si q es del mismo orden de magnitud de N, entonces el metodo de Pohlig-Helman no es muy práctico. Por esta razón, si un sistema criptográfico está basado en logaritmos discretos, entonces el orden del grupo debe ser elegido de tal manera que contenga un factor primo grande.

Si N contiene factores primos pequeños, entonces el método de Pohlig-Hellman puede ser usado para obtener información parcial en el valor de k, obteniendo una congruencia módulo el producto de estos primos pequeños. En ciertas situaciones criptográficas, esto se debe evitar. Por lo tanto, el grupo G es usualmente elegido para tener un orden primo y grande. Esto se puede lograr iniciando con un grupo que tiene un factor primo grande en su orden. Elegimos un elemento P_1 al azar y calculamos su orden. Con una muy alta probabilidad (al menos $1 - 1/q$), el orden de P_1 es divisible por q, así que en pocos intentos debemos encontrar un tal P_1. Escribamos el orden de P_1 como qm. Entonces $P = mP_1$ tendrá orden q. Mientras q sea lo suficientemente grande, el problema del logaritmo discreto en el grupo generado por P resistirá el ataque de Pohlig-Hellman.

A.2 El Método rho de Pollard

En esta sección describimos un algoritmo probabilistico para calcular logaritmos discretos, que puede ser aplicado en un grupo finito G arbitrario, y cuyo tiempo esperado es $O(\sqrt{N})$, donde N denota el orden de G. Primero discutiremos la idea de Pollard y después haremos explicito el algoritmo.

La idea de Pollard es usar una función $f : G \longrightarrow G$ que aplique al grupo en si mismo de manera arbitraria. Entonces se inicia con P_0 un elemento abitrario y se calculan las iteraciones $P_{i+1} = f(P_i)$. Como G es un grupo finito, existen índices $i_0 < j_0$ tales que $P_{i_0} = P_{j_0}$, y entonces es claro que $P_{i_0+l} = P_{j_0+l}$ para toda $l \geq 0$. Por lo tanto la secuencia es periódica. Si logramos encontrar una función de la cual podamos extraer información una vez que encontremos la repetición, razonando como en la paradoja del cumpleaños, podríamos esperar que este método funcionara en $O(\sqrt{N})$. Propondremos ahora una función que nos de información en el cálculo de logaritmos discretos:

Dividamos G en s subconjuntos ajenos $S_1, S_2, \ldots, S_s$ de aproximadamente el mismo tamaño. Elijanse $2s$ enteros arbitrarios $a_i, b_i \bmod N$. Si el logaritmo discreto que queremos calcular es $Q = kP$ (denotaremos por N el orden de P) definamos

$$M_i = a_i P + b_i Q.$$

Definimos entonces $f(g) = g + M_i$ si $g \in S_i$. Una forma de entender esta función es como una caminata aleatoria en G con los posibles pasos siendo los elementos M_i.

Finalmente elegimos enteros arbitrarios a_0, b_0 y hacemos $P_0 = a_0 P + b_0 Q$ el punto inicial para nuestra caminata aleatoria. Mientras calculamos los puntos P_j guardamos también cómo se expresan estos puntos en términos de P y Q, escribamos para esto $P_j = u_j P + v_j Q$. Cuando tengamos una coincidencia $P_{j_0} = P_{i_0}$ resulta que

$u_{j_0} P + v_{j_0} Q = u_{i_0} P + v_{i_0} Q$, por lo tanto $(u_{i_0} - u_{j_0})P = (v_{i_0} - v_{j_0})Q$.
Si $\mathrm{mcd}(v_{j_0} - v_{i_0}, N) = d$, tenemos que

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \pmod{N/d}.$$

Esto nos da d posibles valores para k. Usualmente d será pequeño, así que podemos intentar todas las posibilidades hasta encontrar el valor que resuelve $Q = kP$.

Ejemplo A.2.1. Sea $G = \mathbf{E}(\mathbb{F}_{1093})$, donde $\mathbf{E}$ es la curva elíptica dada por $y^2 = x^3 + x + 1$. Usaremos $s = 3$. Sea $P = (0, 1)$ y $Q = (413, 959)$. Se puede mostrar que el orden de P es 1067. Queremos encontrar k tal que $kP = Q$. Sean
$P_0 = 3P + 5Q$, $M_0 = 4P + 3Q$, $M_1 = 9P + 17Q$, $M_2 = 19P + 6Q$.
Definimos $f : \mathbf{E}(\mathbb{F}_{1093}) \longrightarrow \mathbf{E}(\mathbb{F}_{1093})$ como

$$f(x, y) = (x, y) + M_i \quad \text{si } x \equiv i \pmod 3.$$

Consideramos a x como un entero entre 0 y 1992. Calculando obtenemos

$$P_0 = (326, 699), P_1 = (727, 589), P_2 = (560, 365), \ldots$$

y obtenemos que la primera coincidencia se da en $P_5 = (1006, 951) = P_{58}$. Al llevar registro de los coeficientes de P y Q en la sucesión observamos que

$$P_5 = 88P + 46Q \quad \text{y} \quad P_{58} = 685P + 620Q.$$

Por lo tanto $\mathcal{O} = P_{58} - P_5 = 597P + 574Q$. Como P tiene orden 1067, calculamos

$$(-574)^{-1}597 \equiv 499 \pmod{1067}.$$

Por lo tanto $Q = 499P$, o bien $k = 499$.

A.3 El Cálculo de Índices

Describiremos brevemente uno de los métodos subexponenciales de cálculo de logaritmos discretos para campos finitos, cabe mencionar que no haremos el análisis de su complejidad y en este respecto nos limitaremos a mencionar resultados conocidos.

Para facilitar la exposición describiremos primero la manera en que el algoritmo funcionaría sobre $\mathbb{F}_p$, p un número primo, y después mencionaremos cómo adaptarlo para un campo finito cualquiera.

La observación fundamental en el cálculo de índices es que al intentar resolver un **PLD** en $\mathbb{F}_p$, donde dados g y t se nos pide encontrar un entero l tal que $g^l = t$, podemos pensar en g y t como enteros y no sólo como elementos abstractos de un grupo, así que en lugar de resolver $g^l = t$ en $\mathbb{F}_p$, podemos pensar en resolver $g^l \equiv t \pmod p$. Notemos además que el entero l está bien definido módulo $(p-1)$, así que escribiremos $l \equiv \log_g t \pmod{p-1}$.

El primer paso en el cálculo de índices consiste en elegir un número B (diremos como elegirlo al final) y encontrar todos los primos $p_1, p_2, \ldots, p_k$ en el intervalo $[1, B]$. Una vez hecho esto, eligiremos al azar un número r entre 1 y $p-1$, calcularemos $g^r \pmod p$ (es decir el único número congruente a g^r en el intervalo $[1, p]$) e intentaremos calcular $r_1, \ldots, r_k$ tales que $g^r \equiv p_1^{r_1} \cdots p_k^{r_k} \pmod p$ de ser posible. Si esto no se puede (es decir, si g^r no es B-suave [1]), simplemente desechamos el valor de r y buscamos otro.
Notemos que esta congruencia nos da una congruencia de logaritmos discretos:

$$\log_g t \equiv r_1 \log_g p_1 + \cdots + r_k \log_g p_k \pmod{p-1}$$

Si tuvieramos suficientes de estas relaciones podríamos usar álgebra lineal para obtener los valores de $\log_g p_i$. Si entonces logramos encontrar R tal que $g^R t \equiv p_1^{r_1} \cdots p_k^{r_k} \pmod p$ entonces tenemos que

$$\log_g t \equiv -R + r_1 p_1 + \cdots + r_k p_k \pmod{p-1}.$$

Un primer análisis de este algoritmo nos indica que su éxito depende entre otras cosas de la probabilidad de que g^r sea B-suave, mientras mayor sea esta probabilidad, más rapido obtendremos las relaciones necesarias para pasar a la etapa del álgebra lineal, es así que desde esta perspectiva, un valor grande de B sería apropiado; pero por otro lado, durante el paso del álgebra lineal nos damos cuenta de que un valor muy grande de B (y por tanto de k) nos obligará a trabajar con vectores extremadamente grandes. Es así que se requiere un balance entre ambas partes para que el algoritmo sea efectivo. Crandall y Pomerance sugieren en [CP] un valor de B dado por $L(p)^c$, donde $L(n) = \exp\left(\sqrt{\ln n \ln\ln n}\right)$ y $c = 1/\sqrt{2}$. Usando este valor de B, la complejidad del algoritmo resulta ser $L(p)^{\sqrt{2}+o(1)}$. Esto quiere decir que el anterior es el número de operaciones necesarias para resolver la instancia del **PLD** planteado.

Veamos ahora cómo proceder para el caso de un **PLD** en $\mathbb{F}_{p^n}$. La vía que nos permitió usar el cálculo de índices en $\mathbb{F}_p$ es identificarlo con $\mathbb{Z}_p$, lo que debemos hacer en el caso de $\mathbb{F}_{p^n}$ es identificarlo con $\mathbb{Z}_p[x]/(f(x))$, para $f(x)$ un polinomio irreducible de grado n. Debemos también pensar en los elementos del campo no como si estuvieran dentro de un grupo abstracto,

[1] Decimos que un número natural n es B-suave si todos sus factores primos son menores o iguales a B.

sino como elementos de $\mathbb{Z}_p[x]$ de grado menor que n. Es también afortunado que podemos definir un concepto de *"suavidad"* para polinomios, decimos que un polinomio es b-suave si todos sus factores irreducibles tienen grado a lo más b (recordemos que $\mathbb{Z}_p[x]$ es un dominio de factorización única). Es entonces claro cómo proceder para obtener un algoritmo de cálculo de logaritmos discretos para $\mathbb{F}_{p^n}$ análogo al de $\mathbb{F}_p$: se establece una cota b de "suavidad", se calculan los polinomios irreducibles de grado menor o igual a b y se efectuan el resto de los pasos del algoritmo anterior de manera idéntica. Análisis heurísticos de este algoritmo arrojan una complejidad dada por $\exp\left(c(\log p^d)^{1/3}(\log\log p^d)^{2/3}\right)$.

A.4 El Algoritmo de Schoof

En 1985, René Schoof publicó un algoritmo para calcular el número de puntos en una curva elíptica sobre un campo finito $\mathbb{F}_q$, que es mucho más rápido que los demás algoritmos existentes, por lo menos para valores grandes de q. En particular, requiere de sólo un múltiplo constane de $\log^8 q$ operaciones, mientras su más cercano competidor, el método del "paso pequeño, paso grande" requiere de $q^{1/4}$ operaciones.

Sea $\mathbf{E}$ una curva dada por la ecuación $y^2 = x^3+Ax+B$ sobre $\mathbb{F}_q$. Sabemos por el Teorema III.2.4 que:

$$\#\mathbf{E}(\mathbb{F}_q) = q + 1 - a, \quad \text{con} |a| \leq 2\sqrt{q}.$$

Denotemos por $S = \{2, 3, 5, \ldots, L\}$ a un conjunto de primos tales que

$$\prod_{l \in S} l > 4\sqrt{q}.$$

Si podemos determinar el valor de $a \pmod{l}$ para cada primo $l \in S$, entonces usando el teorema chino del residuo podemos determinar el valor de $a \pmod{\prod l}$ y así determinar el valor de a.

Sea l un primo, supondremos que $l \neq p$ donde p es la característica de $\mathbb{F}_q$, diremos ahora cómo calcular $a \pmod{l}$.

Si $l = 2$ esto es muy fácil, puesto que el orden de $\mathbf{E}(\mathbb{F}_q)$ es par si y solamente si este grupo tiene un elemento de orden 2, lo cual sabemos que sucede si y solamente si $x^3 + Ax + B$ tiene una raíz en $\mathbb{F}_q$. Podríamos intentar con todos los elementos de $\mathbb{F}_q$ para ver si esto sucede, pero hay una manera

más facil de hacerlo. Sabemos que los miembros de $\mathbb{F}_q$ son exactamente las soluciones del polinomio $x^q - x$. Por lo tanto, $x^3 + Ax + B$ tiene raices en $\mathbb{F}_q$ si y solamente si tiene una raíz en común con el polinomio $x^q - x$. El algoritmo de Euclides, aplicado a los dos polinomios nos da su máximo común divisor. Si éste es 1, entonces el valor de a es impar, de otro modo a es par. Con esto concluimos el caso $l = 2$.

En la sección 5 del capítulo 2 definimos los polinomios de división ψ_n. Cuando n es impar, ψ_n es un polinomio en x, y para $(x, y) \in \mathbf{E}(\overline{\mathbb{F}}_q)$, tenemos:

$$(x, y) \in \mathbf{E}[n] \quad \text{si y solamente si} \quad \psi_n(x) = 0.$$

Estos polinomios jugarán un papel crucial en el algoritmo de Schoof.

Sea ϕ_q el endomorfismo de Frobenius, es decir $\phi_q(x, y) = (x^q, y^q)$. Tenemos por el Teorema III.2.5, $\phi_q^2 - a\phi_q + q = 0$. Sea (x, y) un punto de orden l. Entonces (x^q, y^q) es también un punto de orden l, y la relación:

$$\left(x^{q^2}, y^{q^2}\right) + q(x, y) = a(x^q, y^q),$$

determina el valor de $a \pmod{l}$. La idea ahora es calcular todos los elementos de la anterior relación salvo el valor de a y luego determinar el valor de a para el cual la anterior relación se cumple. Notemos que si hemos encontrado un valor de a que cumple la relación para un punto, entonces este mismo valor de a sirve para todos los puntos de $\mathbf{E}[l]$.

Supongamos primero que $(x^{q^2}, y^{q^2}) \neq \pm q(x, y)$ para algún (x, y) en $\mathbf{E}[l]$. Si definimos entonces

$$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q(x, y) \neq \mathcal{O}.$$

Sabemos entonces que $a \neq 0 \pmod{l}$. En este caso las coordenadas en x de los puntos $\left(x^{q^2}, y^{q^2}\right)$ y (x, y) son diferentes, por lo que podemos calcular su suma usando la línea que pasa por ambos puntos. Dado un entero j denotaremos al punto $j(x, y)$ por (x_j, y_j). Podemos calcular los valores de x_j y y_j usando los polinomios de división como se explicó en la sección 5 de capítulo 2. Escribamos además como en la página 24 $x_j = r_{1,j}(x)$ y $y_j = y r_{2,j}(x)$. Regresando a (x', y') tenemos:

$$x' = \left(\frac{y^{q^2} - y_q}{x^{q^2} - x_q}\right)^2 - x^{q^2} - x_q.$$

Si escribimos

$$\begin{aligned}\left(y^{q^2}-y_q\right)^2 &= y^2\left(y^{q^2-1}-r_{2,q}(x)\right)^2 \\ &= (x^3+Ax+B)\left((x^3+Ax+B)^{(q^2-1)/2}-r_{2,q}(x)\right)^2.\end{aligned}$$

y nos damos cuenta que x_q es una función de x, podemos escribir a x' como una función de x. Queremos encontrar un j tal que

$$(x',y') = (x_j^q, x_j^q).$$

Para hacer esto nos fijaremos primero en la primera coordenada. Dado un $(x,y) \in \mathbf{E}[l]$, tenemos que $(x',y') = \pm(x_j^q, y_j^q)$ si y solamente si $x' = x_j^q$. Como mencionamos antes, si esto sucede para un punto, entonces sucederá para todos los puntos (finitos) de $\mathbf{E}[l]$. Como las raices del polinomio ψ_l son las x-coordenadas de los puntos de $\mathbf{E}[l]$, esto implica que

$$x' - x_l^q \equiv 0 \pmod{\psi_l}, \tag{1}$$

es decir, que ψ_l divide al numerador de $x' - x_l^q$ (estamos usando que las raices de ψ_l son simples).

Supongamos ahora que hemos encontrado un j para el cual 1 se cumple. Entonces

$$(x',y') = \pm(x_j^q, y_j^q) = (x_j^q, \pm y_j^q).$$

Para determinar el signo, debemos observar las segundas coordenadas. Tanto y'/y como y_j^q/y se pueden escribir como funciones de x. Si

$$(y' - y_j^q)/y \equiv 0 \pmod{\psi_l},$$

entonces $a \equiv j \pmod{l}$. De otro modo, $a \equiv -j \pmod{\psi_l}$.

Falta considerar el caso cuando $\left(x^{q^2}, y^{q^2}\right) = \pm q(x,y)$ para todo $(x,y) \in \mathbf{E}[l]$. Si

$$\phi_q^2(x,y) = \left(x^{q^2}, y^{q^2}\right) = q(x,y),$$

entonces

$$a\phi_q(x,y) = \phi_q^2(x,y) + q(x,y) = 2q(x,y),$$

por lo tanto

$$a^2 q(x,y) = a^2\phi_q^2(x,y) = (2q)^2(x,y).$$

Por lo tanto, $a^2 q \equiv 4q^2 \pmod{l}$, así que q es un cuadrado mod l. Sea w tal que $q \equiv w^2 \pmod{l}$. Tenemos que

$$(\phi_q + w)(\phi_q - w)(x,y) = (\phi_q^2 - q)(x,y) = \mathcal{O}$$

para todo $(x,y) \in \mathbf{E}[l]$. Sea P cualquier punto de $\mathbf{E}[l]$. Entonces o bien $(\phi_q - w)P = \mathcal{O}$, es decir $\phi_q P = wP$, o $P' = (\phi_q - w)P$ es un punto finito con $(\phi_q + w)P' = \mathcal{O}$. En cualquier caso tenemos un punto $P \in \mathbf{E}[l]$ con $\phi_q P = \pm wP$.

Supongamos que existe un punto $P \in \mathbf{E}[l]$ tal que $\phi_q P = wP$. Entonces

$$\mathcal{O} = (\phi_q^2 - a\phi_q + q)P = (q - aw + q)P.$$

así que $aw \equiv 2q \equiv 2w^2 \pmod{l}$. Por lo tanto, $a \equiv 2w \pmod{l}$. De igual manera, si existe P tal que $\phi_q P = -wP$, entonces $a \equiv -2w \pmod{l}$. Para saber si estamos en este caso, necesitamos saber si

$$(x^q, y^q) = \pm w(x,y) = \pm(x_w, y_w) = (x_w, \pm y_w)$$

para algún $(x,y) \in \mathbf{E}[l]$. Para esto calculamos $x^q - x_w$, la cual es una función racional de x. Si

$$\text{mcd}(\text{numerador}(x^q - x_w), \psi_l) \neq 1,$$

entonces hay $(x,y) \in \mathbf{E}[l]$ tal que $\phi_q(x,y) = \pm w(x,y)$. Si esto sucede usamos la coordenada en y para determinar el signo.

Si tenemos que $\text{mcd}(\text{numerador}(x^q - x_w), \psi_l) = 1$, entonces no podemos estar en el caso

$$\left(x^{q^2}, y^{q^2}\right) = q(x,y)$$

así que el único caso restante es

$$\left(x^{q^2}, y^{q^2}\right) = -q(x,y).$$

En este caso, $aP = (\phi_q^2 + q)P = \mathcal{O}$ para todo $P \in \mathbf{E}[l]$. Por lo tanto, $a \equiv 0 \pmod{l}$.

Resumimos el algoritmo de Schoof como sigue: iniciamos con una curva elíptica $\mathbf{E}$ sobre $\mathbb{F}_p$ dada por $y^2 = x^3 + Ax + B$. Queremos calcular $\#\mathbf{E}(\mathbb{F}_q) = q + 1 - a$.

1. Elegimos un conjunto de primos $S = \{2, 3, \ldots, L\}$ (donde $p \notin S$) tal que $\prod_{l \in S} l > 4\sqrt{q}$.

2. Si $l = 2$, tenemos $a \equiv 0 \pmod{2}$ si y solamente si $\mathrm{mcd}(x^q - x, x^3 + Ax + B) \neq 1$.

3. Para cada primo impar $l \in S$, hacemos lo siguiente:

   (a) Calcular x', la coordenada en x de

   $$(x', y') = \left(x^{q^2}, y^{q^2}\right) + q(x, y) \pmod{\psi_l}.$$

   (b) Para $j = 1, 2, \ldots, (l-1)/2$, hacemos lo siguiene.

      i. Calcular x_j, la coordenada en x de $(x_j, y_j) = j(x, y)$.

      ii. Si $x' - x_j^q \equiv 0 \pmod{\psi_l}$, ir al paso (iii). De otro modo, intentar el siguiente valor de j (en el paso (c)). Si todos los valores $1 \leq j \leq (l-1)/2$ se han intentado, vamos al paso (d).

      iii. Calculamos y' y y_j. Si $(y' - y_j)/y) \equiv 0 \pmod{\psi_l}$, entonces $a \equiv j \pmod{l}$. De otro modo, $a \equiv -j \pmod{l}$.

   (c) Si se han intentado todos los valores $1 \leq j \leq (l-1)/2$ sin éxito, denotemos por $w^2 \equiv q \pmod{l}$. Si tal w no existe, entonces $a \equiv 0 \pmod{l}$. En otro caso, calculamos $\mathrm{mcd}(\mathrm{numerador}((y^q - y_w)/y), \psi_l)$. Si este mcd no es 1, entonces $a \equiv 2w \pmod{l}$. De otro modo, $a \equiv -2w \pmod{l}$.

4. Usar el valor de $a \pmod{l}$ para todo $l \in S$ para calcular $a \pmod{\prod l}$. Elegir el valor de a que satisface dicha conguruencia y tal que $|a| \leq 2\sqrt{q}$. El número de puntos en $\mathbf{E}(\mathbb{F}_q)$es $q + 1 - a$.

Apéndice B

Las Conjeturas de Weil para Curvas Elípticas

El objetivo de este apéndice es demostrar las conjeturas de Weil en el caso particular de una curva elíptica, esto se hace gracias a que el teorema III.2.6 relaciona el orden de una curva elíptica en $\mathbb{F}_q$ con el orden de la curva en $\mathbb{F}_{q^n}$. Esto es suficiente para calcular explícitamente la función zeta asociada a una curva y con ella demostrar una serie de propiedades semejantes a las que cumple la función zeta de Riemann. Definimos a continuación la función zeta asociada a una curva elíptica.

Sea $\mathbf{E}$ una curva elíptica sobre un campo $\mathbb{F}_q$. Sea

$$N_n = \#\mathbf{E}(\mathbb{F}_{q^n})$$

el número de puntos de $\mathbf{E}$ sobre el campo $\mathbb{F}_{q^n}$. La función Z de $\mathbf{E}$ está definida como

$$Z_{\mathbf{E}}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right),$$

donde $\exp(t) = \sum t^n/n!$ es la función exponencial usual. La función Z codifica cierta información aritmética de $\mathbf{E}$. A pesar de su apariencia complicada, la función Z puede ser calculada de una manera mucho más simple, como nos dice la siguiente proposición:

Proposición B.0.1. *Sea* $\mathbf{E}$ *una curva elíptica definida sobre* $\mathbb{F}_q$, *y sea* $\#\mathbf{E}(\mathbb{F}_q) = q + 1 - a$. *Entonces se cumple*

$$Z_{\mathbf{E}}(T) = \frac{qT^2 - aT + 1}{(1-T)(1-qT)}.$$

Demostración. Escribamos $X^2 - aX + q = (X-\alpha)(X-\beta)$. El teorema III.2.6 dice que

$$N_n = q^n + 1 - \alpha^n - \beta^n.$$

Por lo tanto, usando la expansión $-\log(1-t) = \sum t^n/n$, tenemos

$$\begin{aligned} Z_{\mathbf{E}}(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right) \\ &= \exp\left(\sum_{n=1}^{\infty} (q^n + 1 - \alpha^n - \beta^n)\frac{T^n}{n}\right) \\ &= \exp(-\log(1-qT) - \log(1-T) + \log(1-\alpha T) + \log(1-\beta T)) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \\ &= \frac{qT^2 - aT + 1}{(1-T)(1-qT)}. \end{aligned}$$

□

Notemos que el numerador de $Z_{\mathbf{E}}(T)$ es el polinomio característico del endomorfismo de Frobenius, con los coeficientes en orden invertido. La *función zeta* de $\mathbf{E}$ está definida como

$$\zeta_{\mathbf{E}}(s) = Z_{\mathbf{E}}(q^{-s}),$$

donde s es una variable compleja. Como demostraremos más adelante, $\zeta_{\mathbf{E}}(s)$ puede ser considerada como un análogo de la clásica función zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\text{primo}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathcal{R}(s) > 1.$$

Una de las propiedades más importantes de la función zeta de Riemann es que satisface una ecuación funcional que relaciona los valores de la función en s y $1-s$:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).$$

Una conjetura para $\zeta(s)$ es la Hipótesis de Riemann, la cual predice que si $\zeta(s) = 0$ con $0 \leq \mathcal{R}(s) \leq 1$, entonces $\mathcal{R}(s) = 1/2$ (no olvidemos que la función zeta tiene ceros triviales en los enteros negativos pares). La función zeta asociada a una curva elíptica $\zeta_{\mathbf{E}}(s)$ también satisface una ecuación funcional, y el análogo de la Hipótesis de Riemann se satisface, como demuestra el siguiente teorema:

Teorema B.0.2. *Sea* $\mathbf{E}$ *una curva elíptica sobre un campo finito, entonces se cumple lo siguiente:*

1. $\zeta_{\mathbf{E}}(s) = \zeta_{\mathbf{E}}(1-s)$
2. *Si* $\zeta_{\mathbf{E}}(s) = 0$, *entonces* $\mathcal{R}(s) = 1/2$.

Demostración. La demostración de la primera afirmación se sigue fácilmente de la proposición B.0.1:

$$\begin{aligned}\zeta_{\mathbf{E}}(s) &= \frac{q^{1-2s} - aq^{-s} + 1}{(1-q^{-s})(1-q^{1-s})} \\ &= \frac{1 - aq^{s-1} + q^{-1+2s}}{(q^s - 1)(q^{s-1} - 1)} \\ &= \zeta_{\mathbf{E}}(1-s).\end{aligned}$$

Puesto que el numerador de $Z_{\mathbf{E}}(T)$ es $(1-\alpha T)(1-\beta T)$, tenemos que

$$\zeta_{\mathbf{E}}(s) = 0 \quad \text{si y solamente si} \quad q^s = \alpha \text{ o } \beta.$$

Usando la fórmula cuadrática tenemos,

$$\alpha, \beta = \frac{a \pm \sqrt{a^2 - 4q}}{2}.$$

El teorema de Hasse III.2.4 dice que

$$|a| \leq 2\sqrt{q},$$

por lo tanto $a^2 - 4q \leq 0$. Podemos entonces decir que α y β son conjugados complejos y

$$|\alpha| = |\beta| = \sqrt{q}.$$

Si $q^s = \alpha$ o β, entonces

$$q^{\mathcal{R}(s)} = |q^s| = \sqrt{q}.$$

De donde se sigue que $\mathcal{R}(s) = 1/2$. □

Mostraremos finalmente cómo es que $\zeta_{\mathbf{E}}(s)$ puede ser definida en una manera similar a la función zeta de Riemann. Recordemos que la función zeta de Riemann puede ser escrita como el producto de Euler

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

cuando $\mathcal{R}(s) > 1$. Obtendremos $\zeta_{\mathbf{E}}(s)$ si reemplazamos los primos p por los puntos en $\mathbf{E}$. Consideremos un punto $P \in \mathbf{E}\left(\overline{\mathbb{F}_q}\right)$. Definimos el grado de P como el menor n tal que $P \in \mathbf{E}(\mathbb{F}_{q^n})$ y lo denotaremos por $\text{grad}(P)$. La aplicación de Frobenius ϕ_q actua en P, y es fácil demostrar que el conjunto

$$S_P = \{P, \phi_q(P), {\phi_q}^2(P), \ldots, {\phi_q}^{n-1}(P)\}$$

tiene exactamente $n = \text{grad}(P)$ elementos y que ${\phi_q}^n(P) = P$. Cada uno de los puntos en S_P también tiene grado n. Una vez hechas las anteriores definiciones demostremos el siguiente teorema:

Teorema B.0.3. *Sea* $\mathbf{E}$ *una curva elíptica sobre* $\mathbb{F}_q$. *Entonces*

$$\zeta_{\mathbf{E}}(s) = \prod_{S_P} \left(1 - \frac{1}{q^{s\,\text{grad}(P)}}\right)^{-1},$$

donde el producto es sobre todos los puntos $P \in \mathbf{E}\left(\overline{\mathbb{F}_q}\right)$, *pero tomando sólo un punto de cada conjunto* S_P.

Demostración. Si $\text{grad}(P) = m$, entonces P y todos los demás puntos de S_P tienen coordenadas en $\mathbb{F}_{q^m}$. Puesto que $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ si y solamente si $m|n$, podemos observar que S_P contribuye con m puntos para $N_n = \#\mathbf{E}(\mathbb{F}_{q^n})$ si y solamente si $m|n$, y no contribuye con nigún punto de otra manera. Entonces,

$$N_n = \sum_{m|n} \sum_{\substack{S_P \\ \text{grad}(P)=m}} m.$$

Si sustituimos esto en la definición de $Z(T)$ obtenemos

$$\begin{aligned}
\log Z(T) &= \sum_{n=1}^{\infty} \frac{N_n}{n} T^n \\
&= \sum_{n=1}^{\infty} \frac{1}{n} T^n \sum_{m|n} \sum_{\substack{S_P \\ \text{grad}(P)=m}} m \\
&= \sum_{j=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{jm} \sum_{\substack{S_P \\ \text{grad}(P)=m}} m T^{jm} \qquad \text{(donde } jm = n\text{)} \\
&= \sum_{j=1}^{\infty} \sum_{S_P} \frac{1}{j} T^{j \,\text{grad}(P)} \\
&= -\sum_{s_P} \log(1 - T^{\text{grad}(P)}).
\end{aligned}$$

Haciendo $T = q^{-s}$ y exponenciando obtenemos el resultado buscado. □

Si tomamos V una variedad sobre un campo finito, podemos definir una función $Z_V(T)$ de manera análoga a la función $Z_{\mathbf{E}}(T)$. Ésta resulta ser siempre una función racional, lo cual fue demostrado por E. Artin y F. K. Schmidt para curvas y por Dwork para variedades. Se cumple también el análogo del Teorema B.0.2. Para curvas, la existencia de la ecuación funcional fue demostrada por E. Artin y F. K. Schmidt, y la hipótesis de Riemann fue demostrada por Weil en los 1940s. En 1949 Weil anunció lo que se conoce como las conjeturas de Weil, las cuales predecían que análogos a la Proposición B.0.1 y al Teorema B.0.2 se cumplen para variedades sobre campos finitos. La ecuación funcional fue demostrada en los 1960s por M. Artin, Grothendieck, y Verdier, y el análogo de la hipótesis de Riemann fue demostrado por Deligne en 1973. Una buena parte de la geometría algebraica desarrollada por Grothendieck tenía como objetivo demostrar estos teoremas.

Bibliografía

[BK] R. Balasubramanian y N. Koblitz, 'The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm', *J. Cryptology*, **11** (1998), 141–145.

[BSS] I. F. Blake, G. Seroussi y N. P. Smart, *Elliptic Curves in Cryptography*, volumen 265 de la serie *London Mathematical Society Lecture Notes Series*. Cambridge University Press, Cambridge, 2000.

[BD] D. Boneh y N. Daswani, Experimenting with electronic commerce on the PalmPilot. En *Financial Cryptography '99*, volumen 1648 de la serie *Lecture Notes in Computer Science*, paginas 1-16. Springer-Verlag, Berlin, 1999.

[CP] R. Crandall y C. Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, New York, 2001.

[DH] W. Diffie, M.E. Hellman, 'New Directions in Cryptography.', *IEEE Trans. Info. Theory*, **22** (1976), 644-654.

[ElG] T. ElGamal, 'A public key cryptosystem and a signature scheme based on discrete logarithms.', *IEEE Trans. Info. Theory*, **31** (1985), 469-472.

[Eng] A. Enge, *Elliptic curves and their application to cryptography. An introduction*. Kluwer Academic Publisher, Dodrecht, 1999.

[Ful] W. Fulton. *Curvas Algebraicas*. Advanced Book Classics. Addison-Wesley Publishing Company, Red Wood City, CA, 1989.

[HW] G. H. Hardy y E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford, 1979.

[Hil] A. J. Hildebrand, 'Integers free of large prime divisors in short intervals', *Quart. J. Math.*, **36** (1985), 57–69.

[How] E. W. Howe, 'The Weil pairing and the Hilbert symbol'. *Math. Ann.*, **305** (1996), 387-392.

[Kob] N. Koblitz, 'Elliptic Curve Crypotsystems', *Math. Comp.* **48**, 203-209, 1987.

[Len] H. W. Lenstra, 'Factoring integers with elliptic curves', *Ann. Math.*, **126** (1987), 649–673.

[LMS] F. Luca, D. Mireles e I. Shparlinski, 'MOV attacks on subgroups of Elliptic Curves', *Illinois Journal of Mathematics*, por aparecer.

[Mau] U. M. Mauer, 'Towards the equivalence og breaking the Diffie-Hellman protocol and computing discrete logarithms'. En *Advances in Cryptology, CRYPTO 94. Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **839** ,1994

[MW] U. M. Mauer, S. Wolf. Diffie-Hellman oracles. En *Advances in Cryptology, CRYPTO 96. Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** ,1996

[Mil] V. Miller, 'Uses of Elliptic Curves in Cryptography', *Advances in Cryptology-Crypto '85*, Springer-Verlag, 1985.

[MOV1] A. Menezes, T. Okamoto y S. A. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Transactions on Information Theory*, **39** (1993), 16139–1646.

[MOV2] A. J. Menezes, P. C. van Oorschot y S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1996.

[Schi] O. Schirokauer, 'Discrete logarithms and local units,' *Philos. Trans. Roy. Soc. London, Ser. A*, **345** (1993), 409–423.

[SWD] O. Schirokauer, D. Weber y T. Denny, 'Discrete logarithms: The effectiveness of the index calculus method,' *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1122** (1996), 337–362.

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, volumen 106 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Was] L. C. Washington *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, FL, 1996.

Índice Alfabético