Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Tesis de Licenciatura

El ataque MOV al problema del logaritmo discreto en curvas elípticas

Juan Francisco Piombo

Director: Nicolás Martín Sirolli

Junio de 2019

Agradecimientos

Puede que haya algunos agradecimientos que, en principio, no tengan nada que ver con la tesis. Seguro tienen algo que ver, aunque sea de un modo bastante indirecto. Me encantaría incluso agradecerles más, pero esta parte no puede ocupar lo mismo que toda la tesis. Seguramente elija un par de cositas de las más significativas que pasé con ustedes, pero sepan que hay mucho más. En algún momento las charlamos.

Los nombres no están en ningún orden particular. O sí, pero cómo saberlo. De todos modos, hay dos personas a las que quiero agradecer primero.

A mi mamá y a mi papá. Gracias por bancarme en todo esto, por alentarme, acompañarme, cuidarme, aconsejarme, interesarse (dentro de lo posible) por lo que hacía. Por siempre empujarme a dar un poquito más.

Ahora por separado: gracias ma por enseñarme a defender y cuestionar mis ideas. Por las charlas que tuvimos cuando era chiquito en el comedor de casa. Yo era un nenito y vos me preguntabas qué opinaba sobre un montón de cosas. Eso quedó marcado en mi para siempre.

Gracias pa por los jueguitos de dados y otras yerbas en el auto cuando volvíamos del colegio. Por mostrarme de chiquito que la matemática no es "hacer cuentas". Hay pocas cosas que recuerde y disfrute tanto como esos momentos.

A Bel, Ray, Male (casi digo tu apodo), Rami, Lu, Santi, y ahora también Ori, por todos esos domingos a la tarde en casa. Por sus mensajes de aliento cada vez que iba a rendir, por las cargadas cada vez que decía que no sabía cómo me había ido, por coparse a pensar algún juego para divertirnos un rato. Por estar conmigo, por abrazarme, por hacerme saber que siempre van a estar. Con ustedes jamás puedo sentirme solo. Gracias.

A Rochi, por ser la mejor amiga que podría haber imaginado. Por tooooodo lo que compartimos en estos años. Por hacerme ver tantas cosas desde otro punto de vista, cuestionarlas, replantearlas y aprender constantemente. Por la vez que me dijiste *"vamos a jugar un juego"*. Por ese abrazo en silencio en el subsuelo de FADU.

A Nico Murrone, por ser mi primer amigo de la Facultad. Por cruzar el continente para juntarnos a jugar un rato al fútbol o tomar unos mates. Por las charlas de matemática y de básquet, siempre esperando el artículo interesante del día. Y por las tardes de verano en el fondo de casa, que ya van a volver.

A Requi, por la compañía en los momentos en los que más perdido estuve, en ese cuatrimestre cursando Teoría de Álgebras. Por confiar en mí para cuidar a tus gatites. Por estar siempre ahí para darme una mano, incluso desde la otra punta del mundo, literalmente. Por haberme recomendado hablar con Nico para que fuera mi director. Una parte importante de esta tesis se debe a vos.

A Pota, por todos esos viajes de vuelta en tren y subte, charlando sobre series y fútbol para relajar un rato. Por haber hecho un esfuerzo gigante para acompañarme un ratito el día de la defensa.

A Seba, por encontrar un par de eñes que eran enes con tilde en la introducción. Por ayudarme a escribir algunas partes de la tesis, revisarlas y discutirlas conmigo. Por manijear con las preguntas. Por hacer acupunturismo de la palabra y pincharme siempre en los lugares justos. Por la vez que me dijiste *"hablame"* y me hiciste entender, un poco mejor, la importancia de las palabras. Sobre todo, por hacer crecer tanto esta amistad durante el último tiempo.

A Abese en conjunto, por todos los ratos que pasamos cursando, estudiando, jugando al truco, comiendo, divirtiéndonos. Su amistad es lo más importante que me llevo de todo esto.

A Celia, por estar conmigo para las cosas boludas del día a día tanto como para las cosas importantes. Por recomendarme escuchar Snarky. Por las charlas que tuvimos en el banco de la plaza y enfrente del río en Tigre. Por darme el lugar y la confianza para ser la versión más auténtica de mí mismo. Por el apoyo que me diste en este trabajo, por haberte bancado los días en los que estaba insoportable, enojado, frustrado. *Gracias, en especial por la compañía, que de verdad es algo que valoro mucho*.

A la gente de Futsal Exactas y de ABS, por bancarse la persona en la que me convierto adentro de una cancha de fútbol. Y, sobre todo, por confiar en mi para capitanear los equipos. Gracias a estos espacios tengo un poquito más de ganas de ir a la Facultad.

A Vicki, por haberme acompañado prácticamente desde mi primer día en la Facultad. Por cuidarme y darme amor siempre, por crecer conmigo. Por haberme ayudado a encontrar el camino cuando estaba totalmente desorientado.

A Adri, por haberme acompañado cuando "empezó" esto. Por aconsejarme sobre la elección de la carrera, por confiar en mi para el taller de OMA y por los chocolatitos cada vez que iba a rendir.

A mi madrina, por haber dejado en mí la huella de su amor. Esta tesis está dedicada especialmente a vos.

A mi padrino y mis primas, por hacerme parte de su familia. Por lograr que siempre espere con ganas fin de año para compartir un par de días.

A todas las personas de las que aprendí compartiendo un aula durante todo este tiempo. Como alumno, como docente, como compañero de cursada o de trabajo. Este agradecimiento engloba a una cantidad enorme de personas. Nombrarlas a todas me

resultaría imposible. Ustedes saben quiénes son. Gracias por todo lo que me enseñaron, no solo sobre matemática.

A Tincho, por haber confiado en mí para trabajar juntos y por todo lo que aprendí gracias a eso. Por las hamburguesas y las charlas en el auto. Ya volveremos a hacer equipo para algo.

A Nico Sirolli, por dirigir esta tesis. Por estar siempre atento al detalle, por guiarme y ayudarme a crecer como matemático. Por la buena onda cada vez que nos juntamos a charlar, y por odiar tanto la parte burocrática como yo. Por la birra que nos tomamos en Córdoba y por la que todavía te debo. Por todo lo que hiciste por mí en este tiempo: gracias.

A Teresa y Martín, por aceptar ser jurados de esta tesis. Por sus correcciones y sus preguntas. Pero sobre todo, por sus palabras el día de la defensa.

A mis amigos de toda la vida de La Chola. Decir que son mis amigos de toda la vida ya es suficiente motivo para agradecerles. Gracias por el fulbito de los domingos, por las vacaciones, por las salidas. Por estar ahí y ayudarme a desconectar.

A Nico Allo e Isa, por haberme bancado infinitamente durante este cuatrimestre. Isa: gracias por coser mi mochila. Nico: gracias por recordarme siempre que Isa cosió mi mochila. También por recomendarme para trabajar en Di Tella. Y gracias, sobre todo últimamente, por dejar la armadura y mostrar tu lado más sensible.

A Ser, por todo lo que compartimos de chicos en OMA. Como te dije, si no hubiese sido por vos, probablemente habría dejado de participar. Por esa despedida en nuestro último Nacional, que fue el final de una etapa hermosa y el principio de una mejor. Gracias por seguir conmigo después de tanto tiempo.

A las Pepus de Fueguito, por hacerme un lugar (bastante chico) en el asiento de atrás del auto. Por hacerme entender a la perfección la delegación de tareas. Por el equipito que fuimos formando. Por sus mensajes tirando buena onda y por haberse bancado mi desaparición durante este último tiempo.

A Iván, por haber sido un increíble compañero de estudio, de trabajo y, sobre todo, por además ser mi amigo.

A Fran Kordon, por esas charlas con un mate de por medio en Geometría Diferencial, que me ayudaron un montón en la visión a largo plazo de lo que quería hacer.

A la Olimpíada Matemática Argentina (y todas las personas que conocí gracias a ella), por haber sido el espacio donde terminé de convencerme de que esto era lo que quería hacer.

A la educación pública y a la Universidad de Buenos Aires. Me hubiese sido imposible alcanzar este lugar de haber tenido que pagar para estudiar.

Llegando a este punto, siento que estoy dejando sin mencionar a un montón de gente. Perdón, pero sepan que, en todo caso, prefiero agradecerles con un abrazo.

Índice general

Introducción

A lo largo de la historia de la humanidad, la necesidad de tener privacidad y seguridad en las comunicaciones y transacciones ha impulsado el desarrollo de diversas técnicas. La criptografía clásica estudia los métodos utilizados para enviar mensajes en secreto o cifrados, de manera tal que únicamente quien los recibe pueda descifrarlos. Aquello que comenzara como un arte en la antigüedad, se ha convertido en un objeto de estudio científico en la sociedad actual, en la cual la teoría de la información tiene una importancia cada vez mayor.

La aplicación criptográfica más simple consiste en transformar un mensaje en *texto plano* a un mensaje *cifrado*. Para poder hacerlo, se considera una función de encriptación

$$E : \mathcal{M} \longrightarrow \mathcal{C},$$

donde $\mathcal{M}$ es el conjunto de posibles mensajes de texto plano y $\mathcal{C}$ el conjunto de todos los mensajes cifrados. Por supuesto, para poder descifrar los mensajes, necesitamos que esta función sea inversible. A fines prácticos, también es deseable que la función de encriptación sea fácil de calcular, pero obtener su inversa (o incluso la preimagen de algún punto) sea computacionalmente inviable, para poder garantizar la seguridad del método. Para que el receptor del mensaje sea capaz de descifrarlo, el emisor debe proveerle de algún tipo de información extra, que se conoce como la *clave*. Por supuesto, quien posea la clave sería capaz de decodificar los mensajes, con lo cual es de especial interés que ésta solo sea conocida por quien emite y por quien recibe el mensaje. Este tipo de encriptación se conoce como *encriptación o cifrado de clave simétrica*, ya que ambas partes involucradas en el intercambio deben conocer la misma clave. Para poder hacer el intercambio de la clave, se requeriría un canal de comunicación seguro entre emisor y receptor, lo cual podría no ser posible si una tercera parte vigilase todas sus comunicaciones.

Hasta mediados la década de 1970, no se conocían métodos de encriptación que pudieran resistir al monitoreo de una tercera parte. En 1976, W. Diffie y M. Hellman publicaron su artículo [DH76], en el cual dieron a conocer el concepto de *criptografía de clave pública* o de *clave asimétrica*.[1] En este caso, la clave es en realidad un par de claves, una privada y la otra pública, con la particularidad de que es muy difícil obtener la

[1] El concepto de criptografía de clave pública ya había sido descubierto en 1969 por J. Ellis, quien trabajaba para el Departamento de Comunicaciones del Gobierno Británico. Sin embargo, su trabajo fue clasificado como material secreto, y recién fue desclasificado en 1997, luego del fallecimiento de Ellis.

clave privada si solo se conoce la clave pública. Se produjo entonces una revolución en el área de la criptografía.[2]

La implementación original de Diffie y Hellman consiste en seleccionar un primo p y trabajar en el grupo multiplicativo de unidades módulo p, es decir, el grupo $\mathbb{F}_p^\times$. Realizando la elección de un entero $g \in \mathbb{F}_p^\times$ cuyo orden sea un primo grande, cada parte elige de forma secreta un entero, digamos a y b, y calcula $A = g^a$ y $B = g^b$. Los valores de A y B son luego intercambiados públicamente. Por último, se calculan en privado $B^a = A^b = g^{ab}$, que es ahora la clave privada compartida.

Desde el punto de vista de la parte que vigila las comunicaciones, son conocidos los valores del primo p, el entero g y también de $A = g^a$ y $B = g^b$. Una forma de obtener la clave privada sería determinar los valores de a y b a partir de A y B. Este último problema se conoce como el *problema del logaritmo discreto (PLD)*.

Una característica interesante del procedimiento dado por Diffie y Hellman es que tiene sentido en cualquier grupo, con lo cual la búsqueda de grupos en los cuales resulte difícil atacarlo se convirtió en objeto de investigación. Dado que en cuerpos finitos existen ataques particulares al PLD que permiten resolverlo más rápidamente que en el caso general, esto impulsó la búsqueda de alternativas.

En 1985, N. Koblitz y V. Miller propusieron utilizar curvas elípticas en lugar de cuerpos finitos, argumentando que el PLD resulta más difícil de resolver en este contexto. Se conjeturaba que en las curvas elípticas no se podrían llevar a cabo ataques que funcionasen mejor que los conocidos para grupos arbitrarios, lo cual haría que las claves necesarias para obtener el mismo nivel de seguridad que en cuerpos finitos tuviesen menor tamaño. Más aun, muchas de las curvas que se proponían para llevar a cabo los procedimientos pertenecían a la familia de curvas *supersingulares*, en las cuales los cálculos podían realizarse de una manera muy eficiente. Sin embargo, esta conjetura se debía en gran parte a que el PLD en curvas elípticas no se había estudiado lo suficiente.

El uso de curvas supersingulares fue considerado como seguro hasta 1993, cuando A. Menezes, T. Okamoto y S. Vanstone desarrollaron en su artículo [MOV93] un algoritmo que las hacía vulnerables, ya que permitía trasladar el PLD en una curva elíptica a un cuerpo finito. Esto puso en jaque a la criptografía de curvas elípticas, ya que no se sabía si este ataque podía realizarse también en el caso general. Esta cuestión fue resuelta en 1998 por R. Balasubramanian y N. Koblitz. En su artículo [BK98], probaron que la proporción de curvas elípticas susceptibles a este ataque es muy pequeña, basándose principalmente en los resultados provistos por H. Lenstra en [LJ87], un trabajo en el que además se habían sentado las bases para la utilización de curvas elípticas en la factorización de enteros, otra de sus grandes implementaciones criptográficas. Este descubrimiento abrió nuevamente el panorama a la criptografía en curvas elípticas. En la actualidad, los protocolos que dependen de curvas elípticas son ampliamente utilizados y recomendados por entidades internacionales.

[2] De hecho, el artículo de Diffie y Hellman comienza con la frase "We stand today on the brink of a revolution in cryptography".

La estructura de este trabajo es la siguiente:

En el Capítulo 1 desarrollaremos la teoría clásica de curvas elípticas. En el Teorema 1.4.13 definiremos el emparejamiento de Weil, que será fundamental para atacar el problema del logaritmo discreto usando el algoritmo MOV.

En el Capítulo 2 estudiaremos formas cuadráticas y cuerpos de números cuadráticos. La conexión entre estas dos ramas estará dada por los números de clase. Aplicaremos esta teoría en el Teorema 2.3.20, para estimar la cantidad de curvas elípticas definidas sobre un cuerpo finito con orden prefijado, siguiendo las líneas de [LJ87].

En el Capítulo 3 abordaremos el problema del logaritmo discreto, y discutiremos algunos algoritmos para resolverlo en el caso general, y principalmente en cuerpos finitos y curvas elípticas. Estudiaremos en detalle el algoritmo MOV y su complejidad.

En el Capítulo 4 analizaremos el grado de inmersión, que permite comparar la dificultad entre resolver el problema del logaritmo discreto en una curva elíptica y trasladarlo a un cuerpo finito. Probaremos en el Corolario 4.1.5 que en las curvas supersingulares el grado de inmersión es pequeño, con lo cual el ataque MOV es altamente efectivo sobre ellas. Finalmente, aplicando los resultados del Capítulo 2, nos basaremos en [BK98] para acotar la probabilidad de que una curva elíptica seleccionada de forma aleatoria sea susceptible al ataque MOV en el Teorema 4.2.7.

Capítulo 1

Curvas elípticas

Este capítulo se basa principalmente en los textos [Sil09] y [Was03]. En [Sil09] se realiza un tratamiento más detallado y avanzado del tema, mientras que en [Was03] se hace énfasis en el punto de vista criptográfico.

1.1. Geometría de las curvas elípticas

Existen diferentes definiciones de lo que es una curva elíptica. Damos a continuación la que utilizaremos a lo largo del texto.

Definición 1.1.1. Sea K un cuerpo. Una *curva elíptica E definida sobre K* es una curva proyectiva plana no singular dada por la ecuación

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

donde $a_1, \ldots, a_6 \in K$. Esta ecuación se denomina *forma de Weierstrass generalizada*.

Notemos que la curva tiene un único punto en el infinito (es decir, con $Z = 0$), dado por $\mathcal{O} = [0 : 1 : 0]$, de modo que usando coordenadas no homogéneas $x = X/Z$ e $y = Y/Z$, los puntos de la curva serán las soluciones de la ecuación afín

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

junto con el punto $\mathcal{O}$ mencionado anteriormente. Esta forma de describir a la curva es mucho más cómoda, y es la que utilizaremos a partir de ahora.

Más aun, si la característica de K no es 2 ni 3, podemos simplificar la expresión completando cuadrados y cubos, y así obtenemos una ecuación del tipo

$$E: \quad y^2 = x^3 + Ax + B,$$

denominada *ecuación de Weierstrass*. Con esta descripción, la curva resultará no singular únicamente cuando la ecuación $x^3 + Ax + B = 0$ no tenga raíces múltiples, es decir, cuando el discriminante $-(4A^3 + 27B^2)$ sea no nulo.

Por comodidad, de ahora en más supondremos que la característica de K es distinta de 2 y 3, para poder utilizar la ecuación de Weierstrass. La teoría que desarrollaremos en este capítulo puede aplicarse a los casos que excluimos, pero muchas de las demostraciones requieren tratarlos aparte.

El principal objeto de estudio son los puntos de la curva, que pueden tener coordenadas en cualquier extensión de K.

Definición 1.1.2. Sea E una curva elíptica definida sobre K, dada por la ecuación de Weierstrass

$$E: \quad y^2 = x^3 + Ax + B.$$

Si L/K es una extensión de cuerpos, definimos el *conjunto de puntos L-racionales de E* como

$$E(L) = \{(x, y) \in L \times L : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

Decimos que los puntos de $E(L)$ están *definidos sobre L*.

Podemos ver a los puntos de $E(L)$ en coordenadas proyectivas como $[x : y : 1]$ en la ecuación de Weierstrass generalizada. De este modo, tiene sentido considerar que el punto $\mathcal{O}$ está definido sobre cualquier extensión de K, ya que sus coordenadas proyectivas son $[0 : 1 : 0]$. En general, cuando escribamos $P \in E$, sin especificar el cuerpo sobre el cual está definido, estaremos pensando a P con coordenadas en una clausura algebraica de K, que denotaremos $\bar{K}$.

Teniendo en cuenta el punto $\mathcal{O}$, podemos dotar a cualquier curva elíptica de una estructura de grupo abeliano. Este sorprendente hecho puede probarse a partir de las propiedades geométricas de la curva dentro del plano proyectivo. En efecto, sea E una curva elíptica definida sobre K. Dados $P_1, P_2 \in E$, consideramos la recta en $\mathbb{P}^2(\bar{K})$ que pasa por P_1 y P_2 (en el caso $P_1 = P_2$, tomamos la recta tangente a la curva por P_1; como la curva es no singular, siempre podemos hacer esto). Esta recta debe intersecar a la curva en tres puntos (contados con multiplicidad); llamamos $P_1 * P_2$ al tercer punto de intersección. Finalmente, consideramos la recta que pasa por $P_1 * P_2$ y por $\mathcal{O}$, que nuevamente debe intersecar a E en un tercer punto, el cual será denotado $P_1 + P_2$.

Damos a continuación las fórmulas que se desprenden de calcular explícitamente estas operaciones.

Definición 1.1.3. Sea E una curva elíptica dada por la ecuación de Weierstrass

$$E: \quad y^2 = x^3 + Ax + B.$$

Sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$, con $P_1, P_2 \neq \mathcal{O}$.

(1) Si $x_1 \neq x_2$, entonces $P_1 + P_2 = (x_3, y_3)$ con

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

(2) Si $x_1 = x_2$ pero $y_1 \neq y_2$, entonces $P_1 + P_2 = \mathcal{O}$.

(3) Si $P_1 = P_2$ con $y_1 \neq 0$, entonces $P_1 + P_2 = (x_3, y_3)$ con

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

(4) Si $P_1 = P_2$ con $y_1 = 0$, entonces $P_1 + P_2 = \mathcal{O}$.

Finalmente, definimos

$$P + \mathcal{O} = P$$

para todo $P \in E$.

Observación 1.1.4. Si los puntos P_1, P_2 y la curva elíptica E están definidos sobre un cuerpo L, entonces $P_1 + P_2$ también está definido sobre L. Esto puede verificarse inmediatamente a partir de las fórmulas dadas. Se sigue que $E(L)$ es cerrado para la suma.

Teorema 1.1.5. *Sea E una curva elíptica definida sobre K. Sea L/K una extensión de cuerpos. Entonces $E(L)$ es un grupo abeliano con elemento neutro $\mathcal{O}$.*

Demostración. Exceptuando la asociatividad, todas las propiedades se deducen inmediatamente de la Definición 1.1.3. La demostración puede verse en [Was03, Teorema 2.1] o [Sil09, Capítulo III, Teorema 3.6]. □

Observación 1.1.6. De la Definición 1.1.3 se desprende que, si la curva está dada por su ecuación de Weierstrass, entonces el inverso de $P = (x, y)$ es $-P = (x, -y)$. En la forma de Weierstrass generalizada, las fórmulas resultantes son distintas, y pueden verse en [Sil09, Capítulo III, páginas 53 y 54].

1.2. Isogenias

Como las curvas elípticas tienen un punto distinguido $\mathcal{O}$, tiene sentido considerar los morfismos (de curvas) entre ellas que preservan este punto. En general, un morfismo entre curvas está dado por funciones racionales en cada coordenada, si pensamos a las curvas como subconjuntos de $\mathbb{P}^2$. Como las curvas elípticas son, por definición, no singulares, las funciones racionales quedan definidas en todos los puntos (ver [Sil09, Capítulo II, Proposición 2.1]).

Definición 1.2.1. Sean E_1, E_2 curvas elípticas. Una *isogenia* de E_1 a E_2 es un morfismo de curvas $\phi : E_1 \to E_2$ tal que $\phi(\mathcal{O}) = \mathcal{O}$.

Decimos que las curvas E_1 y E_2 son *isógenas* si existe una isogenia no constante de E_1 a E_2.

Si existen isogenias $\phi : E_1 \to E_2$, $\psi : E_2 \to E_1$ tales que $\phi \circ \psi = \mathrm{id}_{E_2}$ y $\psi \circ \phi = \mathrm{id}_{E_1}$, decimos que las curvas E_1 y E_2 son *isomorfas*.

Ejemplo 1.2.2. Dado $m \in \mathbb{Z}$, la multiplicación por m dentro de la curva da lugar a una isogenia

$$[m] : E \to E.$$

Esto define efectivamente una isogenia porque las fórmulas para la suma de dos puntos sobre la curva están dadas por funciones racionales, y procediendo inductivamente se prueba para la multiplicación por cualquier entero.

Proposición 1.2.3. *Toda isogenia no constante es sobreyectiva.*

Demostración. Ver [Was03, Teorema 2.22]. □

En realidad, esta proposición también puede verse como un caso particular de un resultado más general. Lo enunciamos, ya que lo utilizaremos más adelante.

Proposición 1.2.4. *Sea $\phi : C_1 \to C_2$ un morfismo entre curvas proyectivas. Entonces ϕ es constante o es sobreyectivo.*

Demostración. Ver [Har13, Capítulo II, Proposición 6.8]. □

Podemos dar una idea intuitiva sobre la demostración de este resultado notando que, al estar trabajando sobre una clausura algebraica, es posible resolver las ecuaciones que provienen de las funciones racionales que definen a los morfismos.

Proposición 1.2.5. *Sea E/K una curva elíptica y sea $m \in \mathbb{Z}$ no nulo. Entonces la isogenia $[m] : E \to E$ no es constante.*

Demostración. Ver [Sil09, Capítulo III, Proposición 4.2]. La demostración se basa en las fórmulas para la suma de puntos en E dadas en la Definición 1.1.3. □

Como las curvas elípticas tienen estructura de grupo abeliano, las funciones entre ellas también forman un grupo. Denotamos $\mathrm{Hom}(E_1, E_2)$ al grupo de isogenias de E_1 a E_2, con la suma definida puntualmente. Si $E_1 = E_2$, también podemos componer isogenias. Denotaremos $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ al anillo de endomorfismos de la curva E, con la multiplicación dada por la composición.

Como consecuencia de lo anterior, tenemos un morfismo de grupos inyectivo

$$[\ \ ] : \mathbb{Z} \hookrightarrow \mathrm{End}(E),$$

ya que si $[m] = [n]$, entonces $[m - n]$ es constante, y por lo tanto debe ser $m = n$.

Aunque no daremos la demostración, se sabe que si K es un cuerpo finito, entonces $\mathrm{End}(E)$ siempre contiene estrictamente a $\mathbb{Z}$ (ver [Sil09, Capítulo 5, Sección 3]). Se dice en este caso que E tiene *multiplicación compleja*. Veamos un ejemplo.

Ejemplo 1.2.6. Sea K un cuerpo finito, y sea $i \in \bar{K}$ una raíz cuarta primitiva de la unidad, es decir, tal que $i^2 = -1$. Sea E la curva elíptica dada en forma de Weierstrass como

$$E : \quad y^2 = x^3 - x.$$

En este caso, tenemos un endomorfismo dado por

$$[i] : (x, y) \mapsto (-x, iy),$$

ya que si $(x, y) \in E$, entonces

$$(iy)^2 = -y^2 = -x^3 + x = (-x)^3 - (-x).$$

Tenemos que $[i] \notin \mathbb{Z}$, ya que

$$[i] \circ [i](x, y) = [i](-x, iy) = (x, -y) = -(x, y),$$

es decir, $[i]^2 = [-1]$.

El siguiente resultado dice que, además de ser un morfismo de curvas, toda isogenia es un morfismo de grupos abelianos.

Teorema 1.2.7. *Sea $\phi : E_1 \to E_2$ una isogenia. Entonces*

$$\phi(P + Q) = \phi(P) + \phi(Q) \quad \textit{para todos } P, Q \in E_1.$$

Más aun, si ϕ no es constante, entonces $\ker \phi$ es un grupo finito.

Demostración. Ver [Sil09, Capítulo III, Teorema 4.8]. □

Sean E_1 y E_2 curvas elípticas definidas sobre un cuerpo K. Toda isogenia no constante $\phi : E_1 \to E_2$ definida sobre K induce un morfismo entre los cuerpos de funciones

$$\phi^* : \bar{K}(E_2) \to \bar{K}(E_1), \quad \phi^*(f) = f \circ \phi.$$

En este contexto, $\bar{K}(E_1)$ resulta ser una extensión finita de $\phi^*\bar{K}(E_2)$. La demostración de este hecho puede verse en [Har13, Capítulo II, Proposición 6.8].

Definición 1.2.8. Sea $\phi : E_1 \to E_2$ una isogenia definida sobre K. Si ϕ es constante, decimos que ϕ tiene *grado* igual a 0. Si ϕ no es constante, definimos su *grado* como

$$\deg(\phi) = [\bar{K}(E_1) : \phi^*\bar{K}(E_2)].$$

Con esta definición, dadas $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ isogenias, se tiene que

$$\deg(\psi \circ \phi) = \deg(\psi) \deg(\phi).$$

Decimos también que ϕ es *separable*, *inseparable* o *puramente inseparable* si la extensión de cuerpos $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$ tiene la propiedad correspondiente. Definimos el *grado de separabilidad* $\deg_s \phi$ y el *grado de inseparabilidad* $\deg_i \phi$ de ϕ como los grados de separabilidad y de inseparabilidad de la extensión $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$, respectivamente.

Proposición 1.2.9. *Sea $\phi : E_1 \to E_2$ una isogenia no constante.*

(1) Para cada $Q \in E_2$,

$$\#\phi^{-1}(Q) = \deg_s \phi.$$

(2) La función

$$\ker \phi \to \mathrm{Aut}\left(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\right), \quad T \mapsto \tau_T^*,$$

es un isomorfismo, donde τ_T denota la traslación por T dentro de la curva, y τ_T^* es el automorfismo que induce.

(3) Si ϕ es separable, entonces

$$\#\ker \phi = \deg \phi,$$

y $\bar{K}(E_1)$ es una extensión de Galois de $\phi^*\bar{K}(E_2)$.

Demostración. Ver [Sil09, Capítulo III, Teorema 4.10]. □

De este resultado se deduce un corolario que permite factorizar isogenias bajo ciertas condiciones, que se asemejan a la propiedad universal del cociente. Lo enunciamos aquí, pero recién será utilizado en la última parte.

Corolario 1.2.10. *Sean*

$$\phi : E_1 \to E_2 \quad y \quad \psi : E_1 \to E_3$$

isogenias no constantes, y supongamos que ϕ es separable. Si $\ker(\phi) \subseteq \ker(\psi)$, entonces existe una única isogenia

$$\lambda : E_2 \to E_3$$

tal que $\psi = \lambda \circ \phi$.

Demostración. Ver [Sil09, Capítulo III, Corolario 4.11]. □

La condición de ser isógenas es una relación de equivalencia entre curvas elípticas. La simetría se deduce del siguiente resultado.

Teorema 1.2.11. *Sea $\phi : E_1 \to E_2$ una isogenia no constante de grado m. Existe una única isogenia*

$$\hat{\phi} : E_2 \to E_1 \quad \textit{tal que} \quad \hat{\phi} \circ \phi = [m].$$

Demostración. Ver [Sil09, Capítulo III, Teorema 6.1]. □

Definición 1.2.12. Sea $\phi : E_1 \to E_2$ una isogenia. La *isogenia dual* de ϕ es la isogenia

$$\hat{\phi} : E_2 \to E_1$$

dada por el Teorema 1.2.11. Si $\phi = [0]$, entonces definimos $\hat{\phi} = [0]$.

El siguiente teorema resume algunas propiedades básicas de la isogenia dual, que serán utilizadas más adelante.

Teorema 1.2.13. *Sea $\phi : E_1 \to E_2$ una isogenia.*

(a) Sea $m = \deg(\phi)$. Entonces

$$\hat{\phi} \circ \phi = [m] \quad \textit{en } E_1 \quad y \quad \phi \circ \hat{\phi} = [m] \quad \textit{en } E_2.$$

(b) Sea $\lambda : E_2 \to E_3$ otra isogenia. Entonces

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(c) Sea $\psi : E_1 \to E_2$ otra isogenia. Entonces

$$\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}.$$

(d) Para todo $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m] \quad y \quad \deg[m] = m^2.$$

(e) Se tiene que $\deg \hat{\phi} = \deg \phi$.

(f) Se tiene que $\hat{\hat{\phi}} = \phi$.

Demostración. Si ϕ es constante, no hay nada que probar. Del mismo modo, las partes (b) y (c) son inmediatas si λ o ψ son constantes. Podemos suponer entonces que todas las isogenias son no triviales.

(a) La primera igualdad es por la definición de $\hat{\phi}$. Para la segunda, tenemos

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi,$$

ya que la multiplicación por m conmuta con cualquier endomorfismo, por ser morfismos de grupos. Como ϕ es sobreyectiva, se sigue que $\phi \circ \hat{\phi} = [m]$.

(b) Si $\deg \lambda = n$, tenemos

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

Por la unicidad de la isogenia dual, se sigue que $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

(c) Ver [Sil09, Capítulo III, Teorema 6.2].

(d) Si $m = 0$ o $m = 1$, no hay nada que probar. Usando la parte (c) con $\phi = [m]$ y $\psi = [1]$ y procediendo inductivamente, se tiene que $\widehat{[m]} = [m]$ para todo $m \in \mathbb{Z}$. Supongamos ahora que $d = \deg[m]$. Entonces

$$[d] = \widehat{[m]} \circ [m]$$

por definición de la isogenia dual, y a su vez

$$\widehat{[m]} \circ [m] = [m] \circ [m] = [m^2],$$

ya que $\widehat{[m]} = [m]$. Por la Proposición 1.2.5, se sigue que $d = m^2$.

(e) Sea $m = \deg \phi$. Entonces, usando las partes (a) y (d), obtenemos

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg \phi)(\deg \hat{\phi}) = m(\deg \hat{\phi}),$$

así que $m = \deg \hat{\phi}$.

(f) Sea $m = \deg \phi$. Entonces, usando las partes (a), (b) y (d), resulta

$$\hat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\hat{\phi} \circ \phi} = \hat{\phi} \circ \hat{\hat{\phi}}.$$

Luego, se tiene que $\phi = \hat{\hat{\phi}}$, como queríamos. □

El grupo de automorfismos

En general, dada una curva elíptica E, se sabe cuáles son los posibles anillos que pueden aparecer como $\mathrm{End}(E)$. En particular, se conoce el grupo de unidades que puede tener el anillo de endomorfismos, al que denotaremos como $\mathrm{Aut}(E)$, el *grupo de automorfismos* de la curva elíptica E.

Ejemplo 1.2.14. El endomorfismo $[i] : E \to E$ dado en el Ejemplo 1.2.6 es un automorfismo de dicha curva, ya que $[i] \circ [i]^3 = [i]^3 \circ [i] = [1]$.

El grupo $\mathrm{Aut}(E)$ puede ser calculado explícitamente en términos de los coeficientes de la ecuación de Weierstrass de E. Esta caracterización será utilizada en el próximo capítulo, para poder estimar la cantidad de curvas elípticas definidas sobre un cuerpo finito.

Teorema 1.2.15. *Sea E una curva elíptica definida sobre K dada por la ecuación de Weierstrass*

$$E: \quad y^2 = x^3 + Ax + B.$$

Entonces $\mathrm{Aut}(E)$ es un grupo cíclico, y su orden es

$$|\mathrm{Aut}(E)| = \begin{cases} 2 & \text{si } AB \neq 0, \\ 4 & \text{si } B = 0, \\ 6 & \text{si } A = 0. \end{cases}$$

Demostración. Ver [Sil09, Capítulo III, Teorema 10.1]. □

El endomorfismo de Frobenius

Dado p primo y $q = p^r$, será de especial interés el caso en que $K = \mathbb{F}_q$, el cuerpo finito de q elementos. En este contexto, el morfismo de Frobenius juega un rol fundamental, al igual que en la Teoría de Galois.

Definición 1.2.16. Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Definimos el *endomorfismo de Frobenius* como

$$\phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), \quad \phi_q(x, y) = (x^q, y^q), \quad \phi_q(\mathcal{O}) = \mathcal{O}.$$

Algunas de sus propiedades básicas son las siguientes.

Lema 1.2.17. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Entonces ϕ_q es un endomorfismo puramente inseparable de E, de grado q.*

Además, dados $r, s \in \mathbb{Z}$, la isogenia

$$[r] + [s]\phi_q : E \to E$$

es separable si y solo si p no divide a r. En particular, la multiplicación por r es separable si y solo si p no divide a r.

Demostración. Ver [Sil09, Capítulo II, Proposición 2.11 y Capítulo III, Corolario 5.5]. □

Lema 1.2.18. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$, y sea $(x, y) \in E(\bar{\mathbb{F}}_q)$. Entonces*

$$(x, y) \in E(\mathbb{F}_q) \quad \textit{si y solo si} \quad \phi_q(x, y) = (x, y).$$

Demostración. La demostración es inmediata usando la forma de Weierstrass generalizada para la curva, y el hecho de que los coeficientes quedan fijos por el morfismo de Frobenius ya que pertenecen a $\mathbb{F}_q$. □

1.3. Puntos de torsión

Definición 1.3.1. Sea E una curva elíptica definida sobre K, y sea $n \in \mathbb{N}$. El *subgrupo de n-torsión de E*, que denotamos $E[n]$, es el núcleo de la multiplicación por n en E, esto es,

$$E[n] = \{P \in E(\bar{K}) : [n]P = \mathcal{O}\}.$$

Es importante notar que los puntos de torsión admiten coordenadas en $\bar{K}$, no solamente en el cuerpo K.

Usando la noción de isogenia dual, podemos caracterizar el grupo de puntos de n-torsión.

Proposición 1.3.2. *Sea E una curva elíptica definida sobre K y sea n un entero positivo. Si la característica de K no divide a n, entonces*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Si la característica de K es $p > 0$, entonces se cumple alguna de las siguientes:

1. *$E[p^e] = \{\mathcal{O}\}$ para todo $e \in \mathbb{N}$.*
2. *$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ para todo $e \in \mathbb{N}$.*

Demostración. Supongamos primero que la característica de K no divide a n. Como $\deg[n] = n^2$ por el Teorema 1.2.13, se sigue que $[n]$ es una isogenia separable, ya que

el grado de inseparabilidad es una potencia de la característica de K. Entonces, de la Proposición 1.2.9 se deduce

$$\#\ker[n] = \#E[n] = \deg[n] = n^2.$$

Más aun, para cada d divisor de n, se tiene

$$\#E[d] = d^2.$$

Utilizando el Teorema de Estructura para grupos abelianos finitos, obtenemos

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Ahora, si la característica de K divide a n, consideramos el morfismo de Frobenius ϕ_p. Entonces

$$\#E[p^e] = \deg_s[p^e] = (\deg_s[p])^e = (\deg_s[\hat{\phi}_p \circ \phi_p])^e = (\deg_s[\hat{\phi}_p])^e,$$

donde la última igualdad se debe a que ϕ_p es puramente inseparable. Por el Lema 1.2.17 y el Teorema 1.2.13,

$$p = \deg \phi_p = \deg \hat{\phi}_p.$$

Tenemos dos posibilidades. Si $\hat{\phi}_p$ es inseparable, entonces $\deg_s \hat{\phi}_p = 1$, y por lo tanto

$$\#E[p^e] = 1 \quad \text{para todo } e.$$

Por otro lado, si $\hat{\phi}_p$ es separable, resulta que $\deg_s \hat{\phi}_p = p$, así que

$$\#E[p^e] = p^e \quad \text{para todo } e.$$

Nuevamente, por el Teorema de Estructura para grupos abelianos, resulta que

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}.$$ □

1.4. El emparejamiento de Weil

El emparejamiento de Weil será fundamental para la parte criptográfica que desarrollaremos en el Capítulo 3. Además, será uno de los componentes que utilizaremos para probar el Teorema de Hasse, que se encuentra entre los resultados básicos más importantes sobre curvas elípticas definidas sobre cuerpos finitos. Esta debería ser suficiente motivación como para entender su importancia.

Para poder dar la definición, hablaremos en primer lugar sobre los divisores, que son uno de los ingredientes principales para su construcción. Esta teoría puede desarrollarse para curvas algebraicas en general, pero enunciaremos los resultados para el caso particular de curvas elípticas.

Divisores

Definición 1.4.1. Sea E una curva elíptica definida sobre K. El *grupo de divisores de la curva* E, que denotamos $\mathrm{Div}(E)$, es el grupo abeliano libre generado por los puntos en $E(\bar{K})$. Un *divisor* $D \in \mathrm{Div}(E)$ es una suma formal

$$D = \sum_{P \in E} n_P(P),$$

donde $n_P \in \mathbb{Z}$ y $n_P = 0$ salvo para finitos $P \in E$.

El *grado de D* se define como

$$\deg(D) = \sum_{P \in E} n_P \quad \in \mathbb{Z},$$

mientras que su *suma* se define como

$$\mathrm{sum}(D) = \sum_{P \in E} n_P P \quad \in E(\bar{K}).$$

Resultarán sumamente importantes los divisores de grado 0, que forman un subgrupo de $\mathrm{Div}(E)$, el cual denotaremos $\mathrm{Div}^0(E)$.

La función suma induce un morfismo sobreyectivo

$$\mathrm{sum} : \mathrm{Div}^0(E) \to E(\bar{K}),$$

ya que $\mathrm{sum}((P) - (\mathcal{O})) = P$. En lo que sigue, estudiaremos su núcleo.

Definición 1.4.2. Dado un punto P en una curva elíptica E, se puede probar que existe una función $u_P \in \bar{K}(E)$, llamada *uniformizador en* P, tal que toda función $f \in \bar{K}(E)$ puede escribirse como

$$f = u_P^r \cdot g,$$

donde $r \in \mathbb{Z}$ y $g \in \bar{K}(E)$ es una función racional que está definida y es no nula en P. En este caso, el *orden de* f *en* P se define como

$$\mathrm{ord}_P(f) = r.$$

Si E es una curva elíptica y consideramos un punto $P = (x_0, y_0) \in E$, $P \neq \mathcal{O}$, el uniformizador u_P puede tomarse como cualquier recta que pasa por P y no es tangente a E en P. Una elección posible es $u_P = x - x_0$ si $y_0 \neq 0$, y $u_P = y$ si $y_0 = 0$.

Para el punto en el infinito $\mathcal{O}$, puede tomarse como uniformizador $u_{\mathcal{O}} = x/y$.

Definición 1.4.3. Sea E una curva elíptica definida sobre K. Dada una función racional $f \in \bar{K}(E)$, diremos que f tiene un *cero de orden* r *en* P si $\mathrm{ord}_P(f) = r > 0$, y que tiene un *polo de orden* $-r$ *en* P si $\mathrm{ord}_P(f) = r < 0$. Para simplificar la notación, si f tiene un polo en P escribiremos $f(P) = \infty$.

Ejemplo 1.4.4. Consideremos la curva elíptica

$$E: \quad y^2 = x^3 - x.$$

Sea $f(x,y) = x/y \in \bar{K}(E)$. El uniformizador en $P = (0,0) \in E$ puede tomarse como $u_P = y$, y como en $\bar{K}(E)$ se tiene que

$$\frac{x}{y} = y\frac{1}{x^2-1},$$

resulta que $\mathrm{ord}_P(f) = 1$. De manera similar, la función y/x coincide con $y^{-1}(x^2-1)$ en $\bar{K}(E)$, con lo cual tiene un polo de orden 1 en P.

Ejemplo 1.4.5. Sea E la curva elíptica dada en forma de Weierstrass por

$$E: \quad y^2 = x^3 + 72.$$

Consideramos el punto $P = (-2,8) \in E$. El uniformizador para este punto puede tomarse como $u_P = x + 2$. La función $f(x,y) = x + y - 6$ se anula en P, veamos con qué orden. Podemos reescribir la ecuación para la curva como

$$(y+8)(y-8) = (x+2)^3 - 6(x+2)^2 + 12(x+2).$$

De este modo, obtenemos

$$f(x,y) = (x+2) + (y-8) = (x+2)\left(1 + \frac{(x+2)^2 - 6(x+2) + 12}{y+8}\right).$$

La función entre paréntesis está definida y no se anula en P, así que $\mathrm{ord}_P(f) = 1$.

Por otro lado, la función que proviene de la recta tangente a E en P está dada por

$$t(x,y) = \frac{3}{4}(x+2) - y + 8.$$

En este caso, tenemos

$$\begin{aligned} t(x,y) &= (x+2)\left(\frac{3}{4} - \frac{(x+2)^2 - 6(x+2) + 12}{y+8}\right) \\ &= \frac{(x+2)}{4(y+8)}(-4(x+2)^2 + 24(x+2) + 3(y-8)) \\ &= \frac{(x+2)^2}{4(y+8)}\left(-4(x+2) + 24 + 3\frac{(x+2)^2 - 6(x+2) + 12}{y+8}\right). \end{aligned}$$

Nuevamente, la función entre paréntesis no tiene un cero ni un polo en P, así que $\mathrm{ord}_P(t) = 2$. En el caso general, la ecuación de la recta tangente dará lugar a una función que tiene un cero de orden al menos 2: el orden será exactamente 2, a menos que el punto sea de 3-torsión, en cuyo caso el orden será 3.

Definición 1.4.6. Sea $f \in \bar{K}(E)^\times$ una función racional. Definimos el *divisor asociado a* f como

$$\mathrm{div}(f) = \sum_{P \in E(\bar{K})} \mathrm{ord}_P(f)(P) \quad \in \mathrm{Div}(E).$$

Un divisor $D \in \mathrm{Div}(E)$ es *principal* si existe $f \in \bar{K}(E)^\times$ tal que $D = \mathrm{div}(f)$.

Estudiaremos ahora cómo obtener una función con un divisor dado. En principio, no cualquier divisor es de la forma $\mathrm{div}(f)$ para alguna función racional $f \in \bar{K}(E)^\times$. El siguiente resultado da una condición necesaria, y además muestra que el divisor asociado a una función está bien definido.

Proposición 1.4.7. *Sea E una curva elíptica y sea $f \in \bar{K}(E)^\times$. Entonces*

(1) f tiene solo finitos ceros y polos;

(2) $\deg(\mathrm{div}(f)) = 0$*;*

(3) si f no tiene ceros ni polos (es decir, $\mathrm{div}(f) = 0$*), es constante.*

Demostración. La demostración de *(1)* puede verse en [Har13, Capítulo I, Lema 6.5].
Para *(2)* y *(3)*, ver [Ful89, Capítulo 8, Proposición 1]. □

Veremos a continuación que el núcleo de la función suma está dado por los divisores principales. Además, la demostración de este resultado es constructiva, es decir, nos proveerá de un algoritmo para obtener, dado un divisor D que cumpla ciertas hipótesis, una función f tal que $\mathrm{div}(f) = D$. Este resultado será fundamental para definir el emparejamiento de Weil.

Teorema 1.4.8. *Sea E una curva elíptica. Sea $D \in \mathrm{Div}(E)$. Entonces D es un divisor principal si y solo si*

$$\mathrm{sum}(D) = \mathcal{O} \quad y \quad \deg(D) = 0.$$

Demostración. Sea $D \in \mathrm{Div}(E)$. Escribamos a este divisor como

$$D = \sum_{n_P > 0} n_P(P) + \sum_{n_P < 0} n_P(P).$$

Mostraremos que es posible reescribir esta expresión en términos de los divisores asociados únicamente a tres puntos de E (uno de los cuales será el punto en el infinito) y el divisor asociado a una función racional en $\bar{K}(E)$.

Supongamos que P_1, P_2, P_3 son puntos de E que pertenecen a la recta $ax+by+c = 0$, de modo que la función

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

se anula en dichos puntos. Si $b \neq 0$, entonces podemos escribir

$$f(x, y) = \left(\frac{x}{y}\right)^{-3} \left(\frac{ax^4 + cx^3 + byx^3}{y(x^3 + Ax + B)}\right),$$

donde el último paréntesis no se anula en $\mathcal{O}$. Esto prueba que f tiene un polo de orden 3 en $\mathcal{O}$, ya que x/y es el uniformizador en este punto, lo cual implica que

$$\operatorname{div}(ax + by + c) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}).$$

Por otro lado, la recta que pasa por $P_3 = (x_3, y_3)$ y $-P_3 = (x_3, -y_3)$ es $x - x_3 = 0$. El divisor de la función $x - x_3$ es

$$\operatorname{div}(x - x_3) = (P_3) + (-P_3) - 2(\mathcal{O}), \tag{1.4.1}$$

y por lo tanto

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

Como $P_1 + P_2 = -P_3$, obtenemos

$$(P_1) + (P_2) = (P_1 + P_2) + (\mathcal{O}) + \operatorname{div}\left(\frac{ax + by + c}{x - x_3}\right). \tag{1.4.2}$$

Además, llamando g a la función dentro del divisor, tenemos que

$$\operatorname{sum}(\operatorname{div}(g)) = P_1 + P_2 - P_1 - P_2 - \mathcal{O} = -\mathcal{O} = \mathcal{O}.$$

Más aun, si $P_1 + P_2 = \mathcal{O}$, de (1.4.1) deducimos que $(P_1) + (P_2)$ es igual a $2(\mathcal{O})$ más el divisor de una función. Esto prueba que la suma de todos los términos en D con coeficientes positivos es igual a cierto divisor (P) más un múltiplo de $(\mathcal{O})$, sumado al divisor de una función, y se tiene una expresión análoga para la suma con coeficientes negativos. Con todo esto, tenemos que existen $P, Q \in E$, una función $g_1 \in \bar{K}(E)$ y un entero n tal que

$$D = (P) - (Q) + n(\mathcal{O}) + \operatorname{div}(g_1).$$

Además, como g_1 es un cociente de productos de funciones g tales que $\operatorname{sum}(\operatorname{div}(g)) = \mathcal{O}$, resulta que

$$\operatorname{sum}(\operatorname{div}(g_1)) = \mathcal{O}.$$

Por la Proposición 1.4.7, sabemos que $\deg(\operatorname{div}(g_1)) = 0$, así que

$$\deg(D) = 1 - 1 + n + 0 = n.$$

Esto prueba que, si $\deg(D) = 0$, entonces $D = (P) - (Q) + \operatorname{div}(g_1)$. Si además se cumple $\operatorname{sum}(D) = \mathcal{O}$, entonces

$$\mathcal{O} = \operatorname{sum}(D) = P - Q + \operatorname{sum}(\operatorname{div}(g)) = P - Q + \mathcal{O} = P - Q,$$

con lo cual $D = \operatorname{div}(g_1)$. Concluimos que D es un divisor principal.

Recíprocamente, si $D = \operatorname{div}(f)$ para cierta función f, entonces

$$\operatorname{div}(f/g_1) = (P) - (Q).$$

El siguiente lema implica que $P = Q$, y por lo tanto $\operatorname{sum}(D) = \mathcal{O}$. Como $\deg(\operatorname{div}(f)) = 0$ por la Proposición 1.4.7, el resultado está probado. □

No daremos la demostración de este último lema, ya que es bastante extensa y no aporta al entendimiento del tema.

Lema 1.4.9. *Sea E una curva elíptica definida sobre K. Sean $P, Q \in E$, y supongamos que existe una función $h \in \bar{K}(E)^\times$ tal que*

$$\operatorname{div}(h) = (P) - (Q).$$

Entonces $P = Q$.

Demostración. Ver [Was03, Lemas 11.3, 11.5 y 11.6]. □

Observación 1.4.10. Del resultado anterior se deduce que toda función racional h no constante tiene al menos dos polos contados con multiplicidad, ya que si tuviera solo uno, por la Proposición 1.4.7 también tendría un único cero, y por lo tanto su divisor sería de la forma $\operatorname{div}(h) = (P) - (Q)$, para ciertos $P, Q \in E$. Por el Lema 1.4.9 y la Proposición 1.4.7, h debe ser constante ya que no tiene ceros ni polos.

Ejemplo 1.4.11. Sea E la curva elíptica definida sobre $\mathbb{F}_{11}$ por la ecuación de Weierstrass

$$E: \quad y^2 = x^3 - x.$$

Consideramos el divisor en E dado por

$$D = 2((4,4)) + ((6,1)) - ((-1,0)) - 2(\mathcal{O}).$$

Es claro que D es de grado cero, y usando las fórmulas dadas en la Definición 1.1.3, resulta que $\operatorname{sum}(D) = \mathcal{O}$. Nos basaremos en la demostración del Teorema 1.4.8 para hallar una función $f \in \bar{K}(E)^\times$ tal que $\operatorname{div}(f) = D$.

La recta que pasa por $(4,4)$ y $(6,1)$ es $y = 4x - 1$. Como

$$(4,4) + (6,1) = (6,-1),$$

de (1.4.2) deducimos que

$$((4,4)) + ((6,1)) = ((6,-1)) + (\mathcal{O}) + \operatorname{div}\left(\frac{4x - y - 1}{x - 6}\right).$$

Reescribimos entonces

$$D = ((4,4)) + ((6,-1)) - ((-1,0)) - (\mathcal{O}) + \operatorname{div}\left(\frac{4x - y - 1}{x - 6}\right).$$

Repetimos este procedimiento con los puntos $(4,4)$ y $(6,-1)$. La recta que pasa por ellos es $y = 3x + 3$, mientras que

$$(4,4) + (6,-1) = (-1,0).$$

Así, obtenemos nuevamente de (1.4.2)

$$((4,4)) + ((6,-1)) = ((-1,0)) + (\mathcal{O}) + \operatorname{div}\left(\frac{3x-y+3}{x+1}\right),$$

y por lo tanto

$$\begin{aligned} D &= \operatorname{div}\left(\frac{3x-y+3}{x+1}\right) + \operatorname{div}\left(\frac{4x-y-1}{x-6}\right) \\ &= \operatorname{div}\left(\frac{(3x-y+3)(4x-y-1)}{(x+1)(x-6)}\right). \end{aligned}$$

Construcción del emparejamiento

A continuación, construiremos el emparejamiento de Weil y probaremos sus propiedades fundamentales. Recordemos que $E[n]$ denota al subgrupo de n-torsión de E (ver la Definición 1.3.1).

Notación 1.4.12. Denotaremos μ_n al grupo de raíces n-ésimas de la unidad en $\bar{K}$.

Teorema 1.4.13. *Sea E una curva elíptica definida sobre un cuerpo K y sea n un entero positivo. Supongamos que la característica de K no divide a n. Entonces existe una función*

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

el emparejamiento de Weil*, que satisface las siguientes propiedades:*

(1) Es bilineal en cada variable:

$$\begin{aligned} e_n(S_1 + S_2, T) &= e_n(S_1, T)e_n(S_2, T), \\ e_n(S, T_1 + T_2) &= e_n(S, T_1)e_n(S, T_2). \end{aligned}$$

(2) Es alternado:

$$e_n(T, T) = 1.$$

En particular, $e_n(S,T) = e_n(T,S)^{-1}$.

(3) Es no degenerado:

$$\text{Si } e_n(S,T) = 1 \text{ para todo } S \in E[n], \text{ entonces } T = \mathcal{O}.$$

(4) Para todo σ automorfismo de $\bar{K}$ que fija a los coeficientes de E,

$$e_n(\sigma(S), \sigma(T)) = \sigma(e_n(S,T)).$$

En particular, si $\sigma \in \operatorname{Gal}(\bar{K}/K)$, se cumple esta igualdad.

(5) *Para todo endomorfismo separable α de E,*

$$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}.$$

Más aun, si $K = \mathbb{F}_q$, la propiedad es válida para el endomorfismo de Frobenius ϕ_q.

(6) *Es compatible en el siguiente sentido:*

$$e_{nn'}(S, T) = e_n\left([n']S, T\right) \quad \textit{para todo } S \in E[nn'] \textit{ y } T \in E[n].$$

Demostración. Construiremos primero el emparejamiento y luego veremos que cumple las propiedades enunciadas.

Sea $T \in E[n]$. Por el Teorema 1.4.8, existe una función f tal que

$$\operatorname{div}(f) = n(T) - n(\mathcal{O}). \tag{1.4.3}$$

Tomemos ahora un punto $T' \in E$ tal que $[n]T' = T$, cuya existencia está garantizada por la Proposición 1.2.3. Nuevamente por el Teorema 1.4.8, existe una función g que cumple

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

En efecto, la suma de este divisor es $\mathcal{O}$ ya que hay n^2 puntos en $E[n]$, y $n^2T' = nT = \mathcal{O}$, mientras que los elementos R se cancelan. Notemos además que g es independiente de T', ya que cualquier otra elección difiere en un punto $R \in E[n]$. En consecuencia, podemos escribir

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

De (1.4.3), deducimos que

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

Por lo tanto, por la Proposición 1.4.7, g^n es un múltiplo de $f \circ [n]$. Multiplicando a f por una constante, podemos suponer entonces que $f \circ [n] = g^n$.

Sea ahora $S \in E[n]$. Dado $X \in E$ cualquiera, obtenemos

$$g(X + S)^n = f([n]X + [n]S) = f([n]X) = g(X)^n.$$

Luego, para cualquier $X \in E$ tal que $g(X + S)$ y $g(X)$ están definidos y son no nulos, tenemos que $g(X + S)/g(X) \in \mu_n$. Considerando el morfismo de curvas

$$E \to \mathbb{P}^1, \qquad S \mapsto g(X + S)/g(X),$$

de lo anterior tenemos que no es sobreyectivo, y por la Proposición 1.2.4 debe ser constante.

Esto nos permite definir el emparejamiento como

$$e_n(S,T) = \frac{g(X+S)}{g(X)}.$$

El valor de $e_n(S,T)$ está bien definido ya que la función g queda determinada por su divisor, salvo una constante.

Veamos ahora que el emparejamiento tiene las propiedades enunciadas.

(1) Para la linealidad en la primera coordenada, calculamos

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

Notar que aprovechamos el hecho de que, al calcular $e_n(S_2,T) = g(Y+S_2)/g(Y)$, podemos elegir el valor de Y arbitrariamente.

Para la segunda coordenada, sean $T_1, T_2, T_3 \in E[n]$ tales que $T_1+T_2 = T_3$. Para cada $1 \leq i \leq 3$, sean f_i, g_i las funciones utilizadas para definir $e_n(S,T_i)$. Por el Teorema 1.4.8, existe una función h tal que

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

Luego, de la ecuación (1.4.3) resulta que

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

y por lo tanto existe una constante $c \in \bar{K}^\times$ tal que

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

Componiendo con la multiplicación por n y usando que $f_i \circ [n] = g_i^n$, obtenemos

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

De este modo, siguiendo la definición del emparejamiento resulta

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

ya que $[n]S = \mathcal{O}$, así que $h([n](P+S)) = h([n]P)$.

(2) De la propiedad *(1)*, se deduce que

$$e_n(S+T,S+T) = e_n(S,S)e_n(S,T)e_n(T,S)e_n(T,T).$$

Dado $P \in E$, denotamos $\tau_P : E \to E$ a la traslación por P en la curva. Calculamos el siguiente divisor

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

lo cual implica que $\prod_{j=0}^{n-1} f \circ \tau_{[j]T}$ es constante. Eligiendo $T' \in E$ tal que $[n]T' = T$, resulta que

$$\prod_{j=0}^{n-1} g \circ \tau_{[j]T'}$$

también es constante, dado que su potencia n-ésima es el producto anterior. Evaluando este producto en P y en $P + T'$, se tiene la igualdad

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

Ahora bien, como P es arbitrario, podemos asumir que fue elegido de forma que todos los factores involucrados sean no nulos y finitos. Cancelando en la igualdad anterior, finalmente tenemos

$$g(P) = g(P + [n]T') = g(P + T),$$

ya que $[n]T' = T$. Esto dice que

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

como queríamos.

(3) Supongamos que $T \in E$ cumple que $e_n(S, T) = 1$ para todo $S \in E[n]$. Esto es lo mismo que decir que $g(P + S) = g(P)$ para todo $P \in E$, es decir, $g \circ \tau_S = g$. Tenemos entonces que g queda fijo por τ_S^* para todo $S \in \ker[n]$, de modo que por la Proposición 1.2.9 (1), existe una función h tal que $g = [n]^*h = h \circ [n]$. Pero entonces

$$h^n \circ [n] = (h \circ [n])^n = g^n = f \circ [n],$$

así que $h^n = f$ por la sobreyectividad de $[n]$. Luego,

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

y por lo tanto $\operatorname{div}(h) = (T) - (\mathcal{O})$. El Teorema 1.4.8 implica que $T = \mathcal{O}$.

(4) Sea $\sigma \in \operatorname{Aut}(\bar{K})$ que fija a los coeficientes de E. Denotando f^σ, g^σ a las funciones que surgen de aplicar σ a los coeficientes de las funciones racionales f, g respectivamente, resulta que f^σ, g^σ corresponden a la definición del emparejamiento comenzando con el punto $\sigma(T)$ en lugar de T al principio de la demostración. Por lo tanto,

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

(5) Sea $\alpha \in \mathrm{End}(E)$ separable. Sea $\{Q_1, \ldots, Q_k\} = \ker(\alpha)$. Por la Proposición 1.2.9, sabemos que $\deg(\alpha) = k$. Sean

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

y

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

Si τ_Q es la traslación por Q, obtenemos

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

Luego,

$$\begin{aligned}
\mathrm{div}(f_{\alpha(T)} \circ \alpha) &= n \sum_{\alpha(T'')=\alpha(T)} (T'') - n \sum_{\alpha(Q)=\mathcal{O}} (Q) \\
&= n \sum_{i=1}^{k} ((T + Q_i) - (Q_i)) \\
&= \mathrm{div}\left(\prod_{i=1}^{k} (f_T \circ \tau_{-Q_i}) \right).
\end{aligned}$$

Para cada $1 \leq i \leq k$, elegimos Q_i' con $[n]Q_i' = Q_i$. De este modo,

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

Por lo tanto, obtenemos una igualdad entre divisores

$$\begin{aligned}
\mathrm{div}\left(\prod_{i=1}^{k} (g_T \circ \tau_{-Q_i'})^n \right) &= \mathrm{div}\left(\prod_{i=1}^{k} (f_T \circ \tau_{-Q_i} \circ [n]) \right) \\
&= \mathrm{div}(f_{\alpha(T)} \circ \alpha \circ [n]) \\
&= \mathrm{div}(f_{\alpha(T)} \circ [n] \circ \alpha) \\
&= \mathrm{div}\left((g_{\alpha(T)} \circ \alpha)^n \right).
\end{aligned}$$

Esto último implica que $\prod_i g_T \circ \tau_{-Q_i'}$ y $g_{\alpha(T)} \circ \alpha$ difieren en una constante. Por definición del emparejamiento, obtenemos

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

donde la tercera igualdad se debe a que el valor de e_n es el mismo si tomamos P o $P - Q_i'$.

Cuando $K = \mathbb{F}_q$, tomando $\sigma = \phi_q$ y aplicando (4), obtenemos

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

Por el Lema 1.2.17, resulta que $\deg(\phi_q) = q$, y se cumple la propiedad.

(6) Tomando f, g como antes, obtenemos

$$\operatorname{div}(f^{n'}) = nn'(T) - nn'(\mathcal{O})$$

y también

$$(g \circ n')^{nn'} = (f \circ [n] \circ [n'])^{n'}.$$

De la definición del emparejamiento, se sigue que

$$e_{nn'}(S,T) = \frac{g([n']X + [n']S)}{g([n']X)} = \frac{g(Y + [n']S)}{g(Y)} = e_n([n']S, T). \qquad \square$$

A continuación, probaremos algunas consecuencias de este resultado, que serán aplicadas más adelante. Para las mismas, haremos uso de la estructura del grupo de puntos de n-torsión. Recordemos que, si la característica de K no divide a n, por la Proposición 1.3.2 tenemos que

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Esto implica que $E[n]$ es un $\mathbb{Z}/n\mathbb{Z}$-módulo libre de rango 2.

Corolario 1.4.14. *Sea $\{T_1, T_2\}$ una base de $E[n]$ como $\mathbb{Z}/n\mathbb{Z}$-módulo. Entonces $e_n(T_1, T_2)$ es una raíz n-ésima primitiva de la unidad.*

Demostración. Supongamos que $e_n(T_1, T_2) = \zeta$, donde ζ es raíz d-ésima primitiva de la unidad. Notar que, como $\zeta \in \mu_n$, sabemos que d divide a n. Bastará ver que n divide a d. Usando la propiedad *(1)* del emparejamiento, obtenemos

$$1 = \zeta^d = e_n(T_1, T_2)^d = e_n(T_1, [d]T_2).$$

A su vez, aplicando *(1)* y *(2)*, resulta que

$$e_n(T_2, [d]T_2) = e_n(T_2, T_2)^d = 1^d = 1.$$

Ahora, dado $S \in E[n]$ arbitrario, escribimos $S = aT_1 + bT_2$ para ciertos enteros a, b. De este modo,

$$e_n(S, [d]T_2) = e_n(T_1, [d]T_2)^a e_n(T_2, [d]T_2)^b = 1.$$

Como S era cualquiera, de la propiedad *(3)* deducimos que $[d]T_2 = \mathcal{O}$. Pero el orden de T_2 es n, de modo que n divide a d, y por lo tanto ζ es una raíz n-ésima primitiva de la unidad. $\square$

Observación 1.4.15. Del corolario anterior se deduce que el emparejamiento de Weil es sobreyectivo.

Corolario 1.4.16. *Si $E[n] \subseteq E(K)$, entonces $\mu_n \subseteq K^\times$.*

Demostración. Sea $\{T_1, T_2\}$ una base de $E[n]$ y sea $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Como T_1, T_2 tienen coordenadas en K, resulta que $\sigma(T_1) = T_1$ y $\sigma(T_2) = T_2$. Sea $\zeta = e_n(T_1, T_2)$. Así, por la propiedad *(4)* del emparejamiento, tenemos que

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

Por el Teorema fundamental de la teoría de Galois, resulta que $\zeta \in K$. Además, por el Corolario 1.4.14, resulta que ζ es una raíz n-ésima primitiva de la unidad, y por lo tanto $\mu_n \subseteq K$. Más aun, es un subgrupo de $K^\times$. □

Dada $\phi : E_1 \to E_2$ isogenia, su isogenia dual $\hat{\phi} : E_2 \to E_1$ es también dual respecto del emparejamiento de Weil.

Proposición 1.4.17. *Sea $\phi : E_1 \to E_2$ una isogenia. Entonces, para todo $S \in E_1[n]$ y $T \in E_2[n]$, se tiene*

$$e_n(\phi(S), T) = e_n(S, \hat{\phi}(T)).$$

Demostración. Ver [Sil09, Capítulo III, Proposición 8.2]. □

Usando la Proposición 1.3.2, podemos asociar a cada endomorfismo una matriz que representa su acción en los puntos de n-torsión. Dado n entero positivo no divisible por la característica de K, tomamos una base $\{T_1, T_2\}$ de $E[n]$. Si α es un endomorfismo de E, tenemos que $\alpha(E[n]) \subseteq E[n]$. Por lo tanto, existen $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ tales que

$$\alpha(T_1) = aT_1 + cT_2, \quad \alpha(T_2) = bT_1 + dT_2.$$

Así, cada $\alpha \in \mathrm{End}(E)$ admite una representación de la forma

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

El grado del endomorfismo tiene la siguiente relación con el determinante de esta matriz.

Proposición 1.4.18. *Sea α un endomorfismo separable de una curva elíptica E definida sobre un cuerpo K, o $\alpha = \phi_q$, el endomorfismo de Frobenius, si $K = \mathbb{F}_q$. Sea n un entero positivo no divisible por la característica de K. Entonces*

$$\det(\alpha_n) \equiv \deg(\alpha) \ (\textit{mód } n).$$

Demostración. Sea T_1, T_2 una base de $E[n]$ y sea $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ la matriz de α asociada a esta base. Por el Corolario 1.4.14, $\zeta = e_n(T_1, T_2)$ es una raíz n-ésima primitiva de la unidad. Aplicando las propiedades del emparejamiento de Weil, obtenemos

$$\begin{aligned} \zeta^{\deg(\alpha)} &= e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{bc} \\ &= \zeta^{ad-bc}. \end{aligned}$$

Por lo tanto, se tiene $\deg(\alpha) \equiv ad - bc$ (mód n), y la proposición sigue. □

1.5. El módulo de Tate

Dada E curva elíptica definida sobre K y $n \geq 2$ no divisible por la característica de K, el grupo $\mathrm{Gal}(\bar{K}/K)$ actúa sobre los puntos de n-torsión, ya que dados $P \in E[n]$ y $\sigma \in \mathrm{Gal}(\bar{K}/K)$, se tiene

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

De este modo, obtenemos una representación

$$\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

donde el isomorfismo depende de la elección de una base para $E[n]$. Para poder trabajar con estas representaciones simultáneamente, introducimos el concepto del *módulo de Tate*.

Definición 1.5.1. Sea E una curva elíptica y sea $\ell \in \mathbb{Z}$ primo. El *módulo de Tate (ℓ-ádico) de E* es el grupo

$$T_\ell(E) = \varprojlim_m E[\ell^m],$$

donde el límite inverso se toma respecto de las funciones

$$E[\ell^{m+1}] \xrightarrow{[\ell]} E[\ell^m].$$

Como $E[\ell^m]$ es un $\mathbb{Z}/\ell^m\mathbb{Z}$-módulo para cada $m \geq 1$, el módulo de Tate tiene una estructura natural de $\mathbb{Z}_\ell$-módulo, donde $\mathbb{Z}_\ell$ denota al *anillo de enteros ℓ-ádicos*.

Proposición 1.5.2. *El módulo de Tate tiene estructura de $\mathbb{Z}_\ell$-módulo dada por*

(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *si* $\ell \neq \mathrm{char}(K)$.

(b) $T_p(E) \cong \{0\}$ *o* $\mathbb{Z}_p$ *si* $p = \mathrm{char}(K) > 0$.

Demostración. Se sigue inmediatamente de la Proposición 1.3.2. □

El módulo de Tate nos permitirá estudiar algunas características de las isogenias. En efecto, toda isogenia

$$\phi : E_1 \to E_2$$

induce un morfismo entre los grupos de ℓ^m-torsión correspondientes, y por lo tanto induce una función $\mathbb{Z}_\ell$-lineal

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2).$$

Obtenemos así un morfismo

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)), \quad \phi \mapsto \phi_\ell,$$

que en el caso particular $E_1 = E_2 = E$ resulta ser

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(T_\ell(E)).$$

Si $\ell \neq \mathrm{char}(K)$, dada $\phi \in \mathrm{End}(E)$, eligiendo una base de $T_\ell(E)$ como $\mathbb{Z}_\ell$-módulo, podemos describir a $\phi_\ell \in \mathrm{End}(T_\ell(E))$ mediante una matriz de 2×2 con coeficientes en $\mathbb{Z}_\ell$. Esto nos permite calcular

$$\det(\phi_\ell) \in \mathbb{Z}_\ell \quad \text{y} \quad \mathrm{tr}(\phi_\ell) \in \mathbb{Z}_\ell.$$

El determinante y la traza de ϕ_ℓ guardan una conexión con el grado de ϕ. La demostración utiliza el *emparejamiento de Weil ℓ-ádico* en el módulo de Tate, que procedemos a construir.

De manera análoga a lo hecho para definir el módulo de Tate, podemos considerar para cada $m \geq 1$ el grupo

$$\mu_{\ell^m} \subseteq \bar{K}^\times.$$

En lugar de la multiplicación por ℓ, ahora tenemos

$$\mu_{\ell^{m+1}} \xrightarrow{\zeta \mapsto \zeta^m} \mu_{\ell^m},$$

y tomando límite inverso obtenemos el *módulo de Tate de $\bar{K}^\times$*,

$$T_\ell(\mu) = \varprojlim_m \mu_{\ell^m}.$$

Para ver que los emparejamientos

$$e_{\ell^m} : E[\ell^m] \times E[\ell^m] \to \mu_{\ell^m}$$

son compatibles con el límite inverso, bastará ver que

$$e_{\ell^{m+1}}(S,T)^\ell = e_{\ell^m}([\ell]S, [\ell]T) \quad \text{para todo } S, T \in E[\ell^{m+1}].$$

Utilizando la bilinealidad y la compatibilidad del emparejamiento de Weil, obtenemos

$$e_{\ell^{m+1}}(S,T)^\ell = e_{\ell^{m+1}}([\ell]S, T) = e_{\ell^m}([\ell]S, [\ell]T).$$

Esto prueba que el emparejamiento

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

está bien definido, y es el límite de los emparejamientos e_{l^m}. Además, preserva todas las propiedades del emparejamiento original, de lo cual se desprende el siguiente resultado.

Proposición 1.5.3. *Existe un emparejamiento bilineal, alternado, no degenerado y Galois invariante*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

Más aun, si $\phi : E_1 \to E_2$ es una isogenia, entonces

$$e(\phi_\ell(S), T) = e(S, \hat{\phi}_\ell(T)).$$

Veamos ahora cómo aplicar el emparejamiento ℓ-ádico para deducir la relación entre ϕ_ℓ y ϕ.

Proposición 1.5.4. *Sea $\phi \in \mathrm{End}(E)$ y sea $\phi_\ell : T_\ell(E) \to T_\ell(E)$ el morfismo inducido por ϕ en el módulo de Tate. Entonces*

$$\det(\phi_\ell) = \deg(\phi) \quad y \quad \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi).$$

En particular, $\det(\phi_\ell)$ y $\mathrm{tr}(\phi_\ell)$ son enteros que no dependen de ℓ.

Demostración. Sea $\{v_1, v_2\}$ una base de $T_\ell(E)$ como $\mathbb{Z}_\ell$-módulo, y supongamos que la matriz de ϕ_ℓ con respecto a esta base es

$$\phi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Aplicando las propiedades del emparejamiento, obtenemos

$$\begin{aligned}
e(v_1, v_2)^{\deg \phi} &= e([\deg \phi]v_1, v_2) && \text{por la bilinealidad de } e, \\
&= e(\hat{\phi}_\ell \phi_\ell(v_1), v_2) && \text{por 1.2.13}, \\
&= e(\phi_\ell(v_1), \phi_\ell(v_2)) && \text{por 1.2.13 y 1.5.3}, \\
&= e(av_1 + cv_2, bv_1 + dv_2) \\
&= e(v_1, v_2)^{ad-bc} && \text{porque } e \text{ es bilineal y alternado}, \\
&= e(v_1, v_2)^{\det \phi_\ell}.
\end{aligned}$$

Como e es no degenerado, se sigue que $\deg \phi = \det \phi_\ell$. La segunda igualdad se deduce de que

$$\mathrm{tr}(\phi_\ell) = a + d = 1 + (ad - bc) - ((1 - a)(1 - d) - bc) = 1 + \det(\phi_\ell) - \det(1 - \phi_\ell). \quad \square$$

1.6. El grupo de puntos racionales

En esta parte, veremos las propiedades fundamentales del grupo $E(\mathbb{F}_q)$. Empezaremos estudiando su orden, y luego analizaremos su estructura como grupo abstracto.

Dada una curva elíptica E definida sobre $\mathbb{F}_q$, cuya forma de Weierstrass es

$$E: \quad y^2 = x^3 + Ax + B,$$

un método ingenuo para hallar sus puntos definidos sobre $\mathbb{F}_q$ es tomar $x \in \mathbb{F}_q$ e intentar resolver la ecuación de Weierstrass para hallar el valor de y correspondiente. Cada valor de x nos proporciona a lo sumo dos valores para y, y junto con el punto en el infinito $\mathcal{O}$, esto nos da la cota

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

Ahora bien, si suponemos que los valores de $x^3 + Ax + B$ se distribuyen de una manera aproximadamente uniforme cuando x recorre $\mathbb{F}_q$, deberíamos esperar que la ecuación de Weierstrass nos proporcione dos puntos sobre la curva aproximadamente la mitad de las veces, ya que la mitad de los elementos de $\mathbb{F}_q^\times$ son cuadrados. Esto nos dice que el orden de $E(\mathbb{F}_q)$ debería ser aproximadamente $q + 1$. El siguiente resultado, probado por Hasse, acota el error cometido en esta aproximación.

Teorema 1.6.1 (Hasse). *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Entonces el orden de $E(\mathbb{F}_q)$ satisface la desigualdad*

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

Demostración. (a) Llamemos $a = q + 1 - \#E(\mathbb{F}_q)$. Por el Lema 1.2.18, resulta que

$$E(\mathbb{F}_q) = \ker(1 - \phi_q).$$

Aplicando la Proposición 1.2.9, obtenemos

$$\#E(\mathbb{F}_q) = \#\ker(1 - \phi_q) = \deg(1 - \phi_q),$$

con lo cual bastará ver que

$$|a| = |q + 1 - \deg(1 - \phi_q)| \leq 2\sqrt{q}.$$

Dados $r, s \in \mathbb{Z}$, donde r es coprimo con q, el endomorfismo $r - s\phi_q$ es separable por el Lema 1.2.17. Por la Proposición 1.4.18, dado n entero positivo coprimo con q, tenemos que

$$\deg(r - s\phi_q) \equiv \det((r - s\phi_q)_n) \text{ (mód } n).$$

Llamando $\phi = \phi_q$ y calculando este último determinante, se deduce la igualdad

$$\begin{aligned} \det((r - s\phi)_n) &= r^2 + \det(s\phi_n) - rs\,\mathrm{tr}(\phi_n) \\ &= r^2 + s^2 \det(\phi_n) - rs(1 + \det(\phi_n) - \det(1 - \phi_n)). \end{aligned}$$

Luego, obtenemos

$$\deg(r - s\phi) \equiv r^2 + s^2 \deg(\phi) - rs(1 + \deg(\phi) - \deg(1 - \phi)) \text{ (mód } n),$$

y como esto vale para infinitos valores de n, debe ser una igualdad. Ahora bien, por el Lema 1.2.17, sabemos que $\deg(\phi) = q$, de modo que

$$\deg(r - s\phi) = r^2 + s^2 q - rs(1 + q - \deg(1 - \phi)).$$

Como $\deg(r - s\phi) \geq 0$, dividiendo por $r^2 \neq 0$ deducimos que

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

Esta desigualdad vale para todos los números racionales s/r donde r es coprimo con q, y como este conjunto es denso en $\mathbb{R}$, el polinomio $qx^2 - ax + 1$ tiene a lo sumo una raíz real, es decir, su discriminante cumple

$$a^2 - 4q \leq 0.$$

Esto último implica que

$$|a| \leq 2\sqrt{q},$$

y la demostración está completa. □

A partir del orden de $E(\mathbb{F}_q)$, se puede determinar la cantidad de puntos definidos sobre $\mathbb{F}_{q^n}$ para todo $n \geq 1$.

Teorema 1.6.2. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Sea*

$$a = q + 1 - \#E(\mathbb{F}_q).$$

(a) Sean $\alpha, \beta \in \mathbb{C}$ las raíces del polinomio $X^2 - aX + q$. Entonces α, β son números complejos conjugados tales que $|\alpha| = |\beta| = \sqrt{q}$, y para todo $n \geq 1$,

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

(b) El endomorfismo de Frobenius ϕ_q satisface la ecuación

$$\phi_q^2 - a\phi_q + q = 0 \quad \textit{en } \operatorname{End}(E).$$

Demostración. (a) Denotaremos al endomorfismo de Frobenius como $\mathrm{Frob} = \phi_q$, para evitar ambigüedades con el morfismo ϕ_ℓ inducido en el módulo de Tate. Dado ℓ primo, llamamos Frob_ℓ al morfismo inducido por Frob en $T_\ell(E)$. Por la Proposición 1.5.4, obtenemos

$$\begin{aligned} \det(\mathrm{Frob}_\ell) &= \deg(\mathrm{Frob}) = q, \\ \operatorname{tr}(\mathrm{Frob}_\ell) &= 1 + \deg(\mathrm{Frob}) - \deg(1 - \mathrm{Frob}) = 1 + q - \#E(\mathbb{F}_q) = a. \end{aligned}$$

Luego, el polinomio característico de Frob_ℓ es

$$\det(T - \mathrm{Frob}_\ell) = T^2 - \mathrm{tr}(\mathrm{Frob}_\ell)T + \det(\mathrm{Frob}_\ell) = T^2 - aT + q \in \mathbb{Z}[T].$$

El discriminante de este polinomio es

$$a^2 - 4q \leq 0,$$

donde la desigualdad se deduce del Teorema de Hasse. Luego, si $\alpha, \beta \in \mathbb{C}$ son sus raíces, deben ser números complejos conjugados porque el polinomio tiene coeficientes enteros. Además, como

$$\alpha\beta = \det(\mathrm{Frob}_\ell) = q,$$

resulta que $|\alpha| = |\beta| = \sqrt{q}$. Como $\alpha + \beta = a$, deducimos que

$$\#E(\mathbb{F}_q) = q + 1 - \alpha - \beta.$$

Análogamente, dado $n \geq 1$, tenemos

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \mathrm{Frob}^n).$$

Para calcular el polinomio característico de Frob_ℓ^n, notemos que de lo hecho para Frob_ℓ se deduce que la forma de Jordan de su matriz asociada es

$$\begin{pmatrix} \alpha & 0 \\ * & \beta \end{pmatrix}.$$

Luego, la forma de Jordan de Frob_ℓ^n debe ser

$$\begin{pmatrix} \alpha^n & 0 \\ * & \beta^n \end{pmatrix},$$

de modo que su polinomio característico es

$$\det(T - \mathrm{Frob}_\ell^n) = (T - \alpha^n)(T - \beta^n).$$

Especializando en $T = 1$, por la Proposición 1.5.4 es

$$q^n + 1 - \alpha^n - \beta^n = \det(1 - \mathrm{Frob}_\ell^n) = \deg(1 - \mathrm{Frob}^n) = \#E(\mathbb{F}_{q^n}),$$

como queríamos.

(b) Por lo hecho en la parte anterior, aplicando el Teorema de Hamilton-Cayley a la matriz de Frob_ℓ, resulta que

$$\mathrm{Frob}_\ell^2 - a\,\mathrm{Frob}_\ell + q = 0.$$

Por la Proposición 1.5.4, deducimos que

$$0 = \det(\mathrm{Frob}_\ell^2 - a\,\mathrm{Frob}_\ell + q) = \deg(\mathrm{Frob}^2 - a\,\mathrm{Frob} + q),$$

con lo cual

$$\mathrm{Frob}^2 - a\,\mathrm{Frob} + q = \phi_q^2 - a\phi_q + q$$

es el endomorfismo nulo en E. □

Observación 1.6.3. Llamando $a_n = \alpha^n + \beta^n$, tenemos $a_0 = 2$, $a_1 = a = q + 1 - \#E(\mathbb{F}_q)$, y para todo $n \geq 1$,

$$a_{n+1} = a_1 a_n - q a_{n-1}.$$

Mediante esta recurrencia, podemos obtener rápidamente el orden de $E(\mathbb{F}_{q^n})$ a partir del valor de $\#E(\mathbb{F}_q)$.

Definición 1.6.4. El entero $a = q + 1 - \#E(\mathbb{F}_q)$ se llama la *traza de Frobenius*.

Observación 1.6.5. Notar que, en la demostración del Teorema 1.6.1, usamos que

$$a \equiv \mathrm{tr}(\phi_n) \text{ (mód } n) \quad \text{para todo } n \text{ coprimo con } q,$$

mientras que en la demostración del Teorema 1.6.2, dedujimos que

$$a = \mathrm{tr}(\phi_\ell) \quad \text{para todo } \ell \text{ primo.}$$

Es natural preguntarse cuáles son los enteros en el intervalo $[q+1-2\sqrt{q},\ q+1-2\sqrt{q}]$ (llamado *intervalo de Hasse*) para los cuales existe una curva con esa cantidad de puntos definidos sobre $\mathbb{F}_q$. El siguiente resultado da una caracterización completa.

Teorema 1.6.6. *Sea p primo y $q = p^r$. Existe una curva elíptica E tal que $\#E(\mathbb{F}_q) = q+1-a$ si y solo si $|a| \leq 2\sqrt{q}$, y se cumple alguna de las siguientes condiciones:*

(1) p no divide a a;

(2) r es par y $a = \pm 2\sqrt{q}$;

(3) r es par, $a = \pm\sqrt{q}$ y $p \not\equiv 1$ (mód 3);

(4) r es par, $a = 0$ y $p \not\equiv 1$ (mód 4);

(5) r es impar y $a = 0$;

(6) r es impar, $p = 2$ o $p = 3$ y $a = \pm\sqrt{pq}$.

Demostración. Ver [Wat69, Teorema 4.1]. □

Damos un cierre a este capítulo mostrando cuales son los grupos abelianos que aparecen como $E(\mathbb{F}_q)$, al considerar todas las posibles curvas elípticas E definidas sobre $\mathbb{F}_q$.

Teorema 1.6.7. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Entonces existen enteros n_1, n_2, donde n_1 divide a n_2, tales que*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}.$$

Más aun, n_1 divide a $q-1$.

Demostración. Como $E(\mathbb{F}_q)$ es un grupo abeliano finito, por el Teorema de estructura para grupos abelianos tenemos que

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z},$$

donde $n_i | n_{i+1}$ para todo $1 \leq i \leq r-1$. Ahora bien, para cada i, el grupo $\mathbb{Z}/n_i\mathbb{Z}$ tiene n_1 elementos de orden que divide a n_1, así que $E(\mathbb{F}_q)$ tiene n_1^r elementos de este tipo. Por la Proposicion 1.3.2, resulta que $r \leq 2$.

Veamos ahora que n_1 divide a $q-1$. Si p es la característica de $\mathbb{F}_q$, por la Proposición 1.3.2 sabemos que hay a lo sumo p puntos de p-torsión. Esto implica que p no puede dividir a n_1, ya que en ese caso también dividiría a n_2 y tendríamos al menos p^2 puntos de p-torsión. Luego, n_1 es coprimo con p, y por lo tanto

$$E[n_1] \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z}.$$

Como n_1 divide a n_2, resulta que

$$E[n_1] \subseteq E(\mathbb{F}_q),$$

y por el Corolario 1.4.16 tenemos que $\mu_{n_1} \subseteq \mathbb{F}_q^\times$. Esto implica que n_1 divide a $q-1$. □

A pesar de que no lo utilizaremos más adelante, el último resultado que daremos en esta sección tiene interés en si mismo, ya que caracteriza todos los posibles grupos que aparecen como $E(\mathbb{F}_q)$.

Teorema 1.6.8. *Sea $h = q+1-a$ uno de los posibles órdenes de $E(\mathbb{F}_q)$ dados por el Teorema 1.6.6. Escribimos $h = p^e n_1 n_2$, donde $\mathrm{mcd}(p, n_1 n_2) = 1$ y n_1 divide a n_2. Entonces existe una curva elíptica E definida sobre $\mathbb{F}_q$ tal que*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/p^e n_2\mathbb{Z}$$

si y solo si

(1) n_1 divide a $q-1$ en los casos (1), (3), (4), (5) y (6) del Teorema 1.6.6;

(2) $n_1 = n_2$ en el caso (2) del Teorema 1.6.6.

Demostración. Ver [Rüc87]. □

Capítulo 2

La conexión entre números de clase

Comenzaremos este capítulo estudiando la teoría básica de formas cuadráticas, para luego continuar con cuerpos de números cuadráticos. En ambos contextos, definiremos relaciones de equivalencia, y probaremos que existe un nexo entre las clases de equivalencia respectivas. Este vínculo nos permitirá terminar el capítulo aplicando los resultados obtenidos a la teoría de curvas elípticas desarrollada anteriormente.

2.1. Formas cuadráticas enteras

Definición 2.1.1. Una *forma cuadrática binaria entera (forma)* es un polinomio

$$f = ax^2 + bxy + cy^2,$$

con $a, b, c \in \mathbb{Z}$. Su *discriminante* es

$$\Delta(f) = b^2 - 4ac.$$

Una forma es *no degenerada* si su discriminante es no nulo. Si f es no degenerada, decimos que es *definida positiva* si $f(x, y) \geq 0$ para todo $(x, y) \in \mathbb{R}^2$, con igualdad si y solo si $(x, y) = (0, 0)$.

El *contenido de* f es el máximo común divisor de sus coeficientes. Si su contenido es igual a 1, diremos que f es *primitiva*.

A cada forma cuadrática $f = ax^2 + bxy + cy^2$ podemos asociarle una matriz

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in M_2(\mathbb{Q}),$$

de modo tal que $f(x, y) = (x, y) \cdot M_f \cdot (x, y)^t$.

Observación 2.1.2. Una forma f resulta definida positiva si y solo si M_f es una matriz definida positiva. Esta última condición es equivalente a que se cumplan simultáneamente

$$\Delta(f) < 0 \quad \text{y} \quad a > 0.$$

Observación 2.1.3. Si f es una forma, entonces

$$\Delta(f) = b^2 - 4ac \equiv b^2 \pmod 4.$$

Luego, se tiene que $\Delta(f) \equiv 0 \pmod 4$ o $\Delta(f) \equiv 1 \pmod 4$.

Notación 2.1.4. Denotaremos por $\mathrm{SL}_2(\mathbb{Z})$ al grupo de matrices $A \in \mathbb{Z}^{2\times 2}$ tales que $\det(A) = 1$.

Definición 2.1.5. Sea f una forma. Un *automorfismo* de f es una matriz $A \in \mathrm{SL}_2(\mathbb{Z})$ tal que $M_f = A^t \cdot M_f \cdot A$. Denotaremos $\mathrm{Aut}(f)$ al grupo de automorfismos de f.

Definición 2.1.6. Diremos que dos formas f y f' son *(propiamente) equivalentes* si existe $A \in \mathrm{SL}_2(\mathbb{Z})$ tal que $M_f = A^t \cdot M_{f'} \cdot A$.

Observación 2.1.7. Es inmediato que esta definición da lugar a una relación de equivalencia. Notemos que si f y f' son equivalentes, entonces

$$f(x, y) = f'(px + qy, rx + sy),$$

donde $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ es la matriz que da la equivalencia.

Los siguientes resultados muestran que el contenido y el discriminante son invariantes en cada clase de equivalencia.

Lema 2.1.8. *Dos formas equivalentes tienen el mismo discriminante.*

Demostración. Sean f y f' formas equivalentes. Tenemos que

$$\Delta(f) = -4 \cdot \det(M_f).$$

Tomando determinante en la igualdad

$$M_f = A^t \cdot M_{f'} \cdot A,$$

el resultado sigue ya que $\det(A) = 1$. □

Lema 2.1.9. *Dos formas equivalentes tienen el mismo contenido.*

Demostración. Sean $f = ax^2 + bxy + cy^2$ y $f' = a'x^2 + b'xy + c'y^2$ formas equivalentes. Por la definición de equivalencia, existe $A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tal que $M_f = A^t \cdot M_{f'} \cdot A$. Notemos que

$$\mathrm{mcd}(a, b, c) = \mathrm{mcd}(a, a + b + c, c),$$

así que el contenido de f es igual a $\mathrm{mcd}(f(1,0), f(1,1), f(0,1))$. De la Observación 2.1.7 se sigue que

$$\mathrm{mcd}(f(1,0), f(1,1), f(0,1)) = \mathrm{mcd}(f'(p,r), f'(p+q, r+s), f'(q,s)),$$

y el lado derecho de esta igualdad es divisible por el contenido de f'. Cambiando f por f', tenemos la igualdad buscada, ya que los contenidos se dividen mutuamente. □

Otra característica interesante a estudiar en las formas es la *representación de enteros.*

Definición 2.1.10. Decimos que la forma f *representa* al entero N si existe $(x, y) \in \mathbb{Z}^2$ tal que $f(x, y) = N$.

La representación de enteros también resulta un invariante de cada clase de equivalencia de formas. Explicitamos esto en el siguiente resultado.

Proposición 2.1.11. *Dos formas equivalentes representan los mismos enteros, contados con multiplicidad. Más precisamente, si f y f' son equivalentes, para todo $N \in \mathbb{Z}$ se tiene*

$$\#\{(x, y) \in \mathbb{Z}^2 : f(x, y) = N\} = \#\{(x, y) \in \mathbb{Z}^2 : f'(x, y) = N\}.$$

Demostración. Sean f y f' formas equivalentes y $N \in \mathbb{Z}$. Sea $A \in \mathrm{SL}_2(\mathbb{Z})$ tal que $M_{f'} = A^t \cdot M_f \cdot A$. Dado $(x, y) \in \mathbb{Z}^2$ tal que $f'(x, y) = N$, de la igualdad matricial deducimos que $f(A \cdot (x, y)^t) = N$. Como A es inversible, la asignación

$$(x, y) \mapsto A \cdot (x, y)^t$$

es una biyección entre los conjuntos $\{(x, y) \in \mathbb{Z}^2 : f'(x, y) = N\}$ y $\{(x, y) \in \mathbb{Z}^2 : f(x, y) = N\}$, lo cual prueba el resultado. □

Formas reducidas

Dado Δ entero negativo, nuestro objeto de estudio serán las clases de equivalencia de formas definidas positivas de discriminante Δ. El conjunto de tales clases es finito, como veremos a lo largo de esta sección. Para ello, primero necesitamos la noción de forma reducida.

Definición 2.1.12. Una forma primitiva, definida positiva $f = ax^2 + bxy + cy^2$ se dice *reducida* si

$$|b| \leq a \leq c, \quad \text{y} \quad b \geq 0 \text{ cuando } a = c \text{ o } |b| = a.$$

Proposición 2.1.13. *Existe una cantidad finita de formas reducidas de discriminante fijo.*

Demostración. Sea Δ entero negativo. Supongamos que $f = ax^2+bxy+cy^2$ es una forma reducida de discriminante Δ. Entonces $b^2 \leq a^2$ y $a \leq c$, de lo cual deducimos que

$$-\Delta = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2,$$

así que se tiene la desigualdad

$$0 \leq a \leq \sqrt{(-\Delta/3)}. \tag{2.1.1}$$

Luego, a solo puede tomar finitos valores, y como $|b| \leq a$, lo mismo vale para b. Además, de la igualdad $\Delta = b^2 - 4ac$ se desprende que hay a lo sumo un valor de c que cumple esta ecuación. Por lo tanto, solo existe una cantidad finita de formas reducidas de discriminante Δ. □

Teorema 2.1.14. *Toda forma primitiva, definida positiva es equivalente a una única forma reducida.*

Demostración. Sea f una forma primitiva, definida positiva. Veremos primero que existe una forma reducida equivalente a ella, y luego que es única. Dentro de la clase de equivalencia de f, tomamos $f' = ax^2 + bxy + cy^2$ tal que $|b|$ sea mínimo. En este caso, resulta que $a \geq |b|$. Si no fuese así, definimos

$$g(x, y) = f'(x + my, y) = ax^2 + (2am + b)xy + c'y^2,$$

que resulta ser equivalente a f. Además, podemos elegir $m \in \{\pm 1\}$ tal que $|2am + b| < |b|$. En efecto, si $b > 0$ basta tomar $m = -1$, ya que

$$-2a + b < b \quad \text{y} \quad 2a - b < b.$$

De forma análoga, vemos que podemos tomar $m = 1$ cuando $b < 0$. Repitiendo este argumento con $g(x, y) = f'(x, mx + y)$, se tiene que $c \geq |b|$. Por último, si $a > c$, cambiamos $f'(x, y)$ por la forma equivalente $f'(-y, x)$.

Lo hecho hasta ahora muestra que existe una forma equivalente a f, digamos $f_1 = ax^2+bxy+cy^2$, con $|b| \leq a \leq c$. Además, f_1 es reducida, excepto en el caso en que $b < 0$ y se cumple que $a = c$ o $b = -a$. De ser así, la forma $f_2(x, y) = ax^2-bxy+cy^2$ es reducida. Bastará ver que f_2 es equivalente a f_1. Si $a = c$, tenemos que $f_2(x, y) = f_1(-y, x)$; mientras que si $b = -a$, entonces $f_2(x, y) = f_1(x+y, y)$. Luego, f_2 y f_1 son equivalentes, con lo cual existe una forma reducida en la clase de f. Para probar que dicha forma es única, separamos en casos.

Caso 1: $a = b = c$. La primitividad implica que $a = b = c = 1$, y por lo tanto $f(x, y) = x^2 + xy + y^2$. Se sigue de (2.1.1) que es la única forma reducida con discriminante igual a -3.

Caso 2: $|b| < a = c$. En este caso, si $xy \neq 0$, tenemos que

$$f(x, y) \geq a - |b| + c > c = a.$$

Entonces f representa a a exactamente cuatro veces, cuando $(x, y) \in \{(\pm 1, 0), (0, \pm 1)\}$. Cualquier forma reducida equivalente a f es de la forma $f'(x, y) = ax^2 + b'xy + c'y^2$, ya que ambas formas representan los mismos enteros y a es el menor entero representado por f. Si $c' > a$, entonces $f'(0, \pm 1) > a$, y para cualesquiera $x, y \neq 0$, resulta que $f'(x, y) \geq a - |b'| + c' > a$. De lo anterior deducimos que f' solo representa a a dos veces, lo cual es absurdo por la Proposición 2.1.11. Esto muestra que $c' = a$, y como f' es reducida, debe ser $f'(x, y) = ax^2 + b'xy + cy^2$ con $b' \geq 0$. Como $\Delta(f) = \Delta(f')$ y $b, b' \geq 0$, se tiene que $f = f'$.

Caso 3: $a < c$. En este caso, el segundo menor entero no nulo representado por f es c. Si fijamos a, c y $\Delta(f) = b^2 - 4ac$, la única forma reducida que puede ser equivalente a f es $f'(x, y) = ax^2 - bxy + cy^2$. Separamos nuevamente en casos.

Caso 3(i): $|b| = a$. Por la definición de forma reducida, tenemos que $b \geq 0$ y no hay nada que probar.

Caso $3(ii)$: $|b| < a < c$. Entonces $f(x,y) = a$ si y solo si $(x,y) = (\pm 1, 0)$, y $f(x,y) = c$ si y solo si $(x,y) = (0, \pm 1)$. Veamos que, en este caso, las formas $f = ax^2 + bxy + cy^2$ y $f' = ax^2 - bxy + cy^2$ no son equivalentes si $b \neq 0$. En efecto, si lo fuesen, existirían enteros p, q, r, s tales que $ps - qr = 1$, y además

$$f'(x,y) = f(px + qy, rx + sy).$$

De este modo, resulta que $a = f'(1,0) = f(p,q)$ y a la vez $c = f'(0,1) = f(r,s)$. Pero entonces $(p,q) = (\pm 1, 0)$ y $(r,s) = (0, \pm 1)$, así que $q = r = 0$ y $p = s = 1$ o $p = s = -1$. Cualquiera de estas dos posibilidades implica que $f = f'$, lo cual es absurdo.

Como no hay otros casos posibles, esto concluye la demostración. □

Corolario 2.1.15. *Sea Δ un entero negativo. Entonces existe una cantidad finita de clases de equivalencia de formas primitivas, definidas positivas, de discriminante Δ. Más aun, están en correspondencia biyectiva con las formas reducidas de discriminante Δ.*

Definición 2.1.16. Sea Δ un entero negativo, $\Delta \equiv 0, 1 \pmod 4$. Definimos el *número de clase de formas reducidas* como

$$\widetilde{h}(\Delta) = \sum_f \frac{1}{|\operatorname{Aut}(f)|},$$

donde la suma (que es finita por la Proposición 2.1.13) recorre las formas reducidas de discriminante Δ.

Observación 2.1.17. Veremos más adelante que el grupo de automorfismos de una forma es finito.

Es importante notar que, por el Corolario 2.1.15, el número de clase de formas reducidas cuenta la cantidad de clases de equivalencia de formas primitivas, donde la clase de f tiene peso $|\operatorname{Aut}(f)|^{-1}$.

Observación 2.1.18. En la Observación 2.1.3 notamos que el discriminante de una forma siempre es 0 o 1 módulo 4. Recíprocamente, dado Δ entero tal que $\Delta \equiv 0, 1 \pmod 4$, existe una forma (reducida) con este discriminante. Si $\Delta \equiv 0 \pmod 4$, consideramos

$$f_\Delta(x,y) = x^2 - \frac{\Delta}{4} y^2,$$

mientras que si $\Delta \equiv 1 \pmod 4$, tomamos

$$f_\Delta(x,y) = x^2 + xy + \frac{1-\Delta}{4} y^2.$$

En ambos casos, f_Δ resulta una forma reducida de discriminante Δ, de modo que $\widetilde{h}(\Delta) > 0$.

El número de clase de Hurwitz-Kronecker

Terminaremos esta sección definiendo el número de clase de Hurwitz-Kronecker, el cual vinculará la teoría de formas cuadráticas y cuerpos de números con la de curvas elípticas.

Definición 2.1.19. Sea Δ un entero negativo, $\Delta \equiv 0, 1 \pmod 4$. El *número de clase de Hurwitz-Kronecker de* Δ, que denotaremos $H(\Delta)$, se define como

$$H(\Delta) = \sum_f \frac{1}{|\operatorname{Aut}(f)|},$$

donde la suma recorre un conjunto de representantes de las clases de equivalencia de formas definidas positivas de discriminante Δ.

Veremos más adelante que el orden del grupo de automorfismos es un invariante de la clase de equivalencia de una forma definida positiva, con lo cual el número de clase de Hurwitz-Kronecker resulta bien definido.

El número de clase de Hurwitz-Kronecker resulta ser finito, como muestra el siguiente resultado, junto con la Proposición 2.1.13.

Proposición 2.1.20. *Sea Δ un entero negativo, $\Delta \equiv 0, 1 \pmod 4$. Entonces*

$$H(\Delta) = \sum_d \widetilde{h}(\Delta/d^2),$$

donde la suma recorre los enteros positivos d tales que $\Delta/d^2 \in \mathbb{Z}$ y $\Delta/d^2 \equiv 0, 1 \pmod 4$.

Demostración. Sea $f = ax^2 + bxy + cy^2$ una forma definida positiva de discriminante Δ, y sea d su contenido. Luego, $\frac{1}{d}f$ es una forma primitiva y definida positiva, así que, por el Teorema 2.1.14, en su clase de equivalencia existe una única forma reducida, que llamaremos f_r. Además, si g es una forma equivalente a f, por el Lema 2.1.8 tenemos que $\frac{1}{d}g$ también es una forma primitiva y definida positiva equivalente a $\frac{1}{d}f$, de modo que $f_r = g_r$. Esto nos permite asignar a cada clase de formas f una forma reducida f_r. Calculando su discriminante, observamos que

$$\Delta(f_r) = \Delta\left(\frac{1}{d}f\right) = \frac{b^2 - 4ac}{d^2} = b'^2 - 4a'c',$$

y por lo tanto $\Delta/d^2 \equiv 0, 1 \pmod 4$.

Similarmente, dada una forma reducida f de discriminante Δ/d^2, podemos asignarle la clase $\overline{df}$ de formas de discriminante Δ. Estas dos funciones son claramente inversas.

Finalmente, como el grupo de automorfismos no cambia al multiplicar por una constante no nula, los pesos de las clases de equivalencia de f y f_r son los mismos, y por lo tanto tenemos la igualdad buscada. □

Definición 2.1.21. Sea Δ un entero negativo, $\Delta \equiv 0, 1 \pmod 4$. El mayor valor de d tal que $\Delta/d^2 \in \mathbb{Z}$ y $\Delta/d^2 \equiv 0, 1 \pmod 4$ es el *conductor* $\mathfrak{f}$ de Δ, y $\Delta_0 = \Delta/\mathfrak{f}^2$ es el *discriminante fundamental asociado a* Δ.

Observación 2.1.22. Los valores de d que aparecen en la Proposición 2.1.20 son exactamente los divisores positivos del conductor de Δ.

2.2. Cuerpos de números cuadráticos

Esta sección se basa principalmente en [Mar77]. A pesar de que desarrollaremos la teoría únicamente para el caso cuadrático, muchos de los resultados se extienden al caso general, es decir, a extensiones de los números racionales de grado finito arbitrario.

Existe también una noción de discriminante en este contexto. La teoría que desarrollaremos permitirá conectar esta nueva definición con el discriminante de formas cuadráticas, lo cual será clave para obtener los resultados finales de este capítulo.

Definición 2.2.1. Un *cuerpo de números cuadrático* es un subcuerpo de los números complejos, de dimensión 2 como $\mathbb{Q}$-espacio vectorial.

Todo cuerpo de números cuadrático es de la forma $\mathbb{Q}(\sqrt{d})$ para algún entero d libre de cuadrados. Si $d < 0$, diremos que es un *cuerpo cuadrático imaginario*, mientras que si $d > 0$, lo llamaremos *cuerpo cuadrático real*.

El grupo de Galois de $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ está dado por

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{1, \sigma\},$$

donde $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Denotaremos $\sigma(\alpha) = \overline{\alpha}$, llamado el *conjugado* de α.

Dado $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, su *norma* es

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2,$$

y su *traza* es

$$T(\alpha) = \alpha + \overline{\alpha} = 2a.$$

Un elemento de $\mathbb{Q}(\sqrt{d})$ se dice *entero (cuadrático)* si es raíz de un polinomio mónico con coeficientes enteros. El *anillo de enteros* de $\mathbb{Q}(\sqrt{d})$ consiste de todos los enteros cuadráticos en $\mathbb{Q}(\sqrt{d})$, y será denotado $\mathcal{O}_d$. También es usual denotarlo como $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.

Notar que $\alpha = a + b\sqrt{d}$ es raíz del polinomio

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + a^2 - db^2 \in \mathbb{Q}[x], \tag{2.2.1}$$

así que α es entero si este polinomio tiene coeficientes enteros. Esto es equivalente a que la norma y la traza de α sean números enteros.

Proposición 2.2.2. *El anillo de enteros $\mathcal{O}_d$ es un $\mathbb{Z}$-módulo libre de rango 2. Una base de enteros (esto es, una base como $\mathbb{Z}$-módulo) está dada por $\{1, \sqrt{d}\}$ si $d \equiv 2, 3 \pmod 4$, y por $\{1, (1 + \sqrt{d})/2\}$ si $d \equiv 1 \pmod 4$.*

Demostración. Ver [Mar77, Capítulo 1, Corolario 2]. □

Utilizando la norma, es posible determinar la cantidad de raíces de la unidad en $\mathbb{Q}(\sqrt{D})$. Haremos uso de este resultado más adelante.

Proposición 2.2.3. *Sea $D < 0$ un discriminante fundamental. Entonces la cantidad de raíces de la unidad contenidas en $\mathbb{Q}(\sqrt{D})$ está dada por*

$$w = \begin{cases} 2 & \text{si } D < -4, \\ 4 & \text{si } D = -4, \\ 6 & \text{si } D = -3. \end{cases}$$

Demostración. Sea α una raíz de la unidad contenida en $\mathbb{Q}(\sqrt{D})$. Sabemos que $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ para cierto entero d libre de cuadrados. Como $\alpha \in \mathcal{O}_d$, por la Proposición 2.2.2 podemos escribir

$$\alpha = \begin{cases} a + b\sqrt{d} & \text{si } d \equiv 2, 3 \text{ (mód } 4), \\ a + b\frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \text{ (mód } 4). \end{cases}$$

Como α es una unidad, tenemos que $N(\alpha) = 1$, y por lo tanto es

$$1 = N(\alpha) = \begin{cases} a^2 - b^2 d & \text{si } d \equiv 2, 3 \text{ (mód } 4), \\ a^2 + ab + b^2\frac{1-d}{4} & \text{si } d \equiv 1 \text{ (mód } 4). \end{cases}$$

Si $d = -1 \equiv 3$ (mód 4) (y, por lo tanto, $D = -4$), las únicas soluciones de esta ecuación son $\alpha \in \{\pm 1, \pm i\}$.

Si $d = D = -3$, las únicas soluciones son $\alpha \in \{\pm 1, \pm\frac{1+\sqrt{-3}}{2}, \pm\left(1 - \frac{1+\sqrt{-3}}{2}\right)\}$.

Finalmente, si $D < -4$, las únicas soluciones son $\alpha \in \{\pm 1\}$. □

Uno de los invariantes más importantes asociados a un cuerpo de números es su discriminante. Lo definiremos únicamente para el caso cuadrático, ya que este será nuestro objeto de estudio.

Definición 2.2.4. Sea $\mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático. Sea $\{\alpha_1, \alpha_2\}$ una base de $\mathcal{O}_d$ como $\mathbb{Z}$-módulo. El *discriminante* de $\mathbb{Q}(\sqrt{d})$ es

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \det\begin{pmatrix} \alpha_1 & \alpha_2 \\ \overline{\alpha_1} & \overline{\alpha_2} \end{pmatrix}^2.$$

El discriminante es independiente de la base de enteros elegida, ya que las matrices asociadas a dos bases distintas difieren en una matriz de cambio de base con coeficientes enteros. Por lo tanto, podemos calcularlo para las bases especificadas anteriormente. De este modo, obtenemos

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d & \text{si } d \equiv 1 \text{ (mód } 4), \\ 4d & \text{si } d \equiv 2, 3 \text{ (mód } 4). \end{cases}$$

Definición 2.2.5. Un *discriminante fundamental* es un entero que es el discriminante de algún cuerpo de números cuadrático.

En vistas de lo hecho anteriormente, D es un discriminante fundamental si y solo si $D \neq 1$, es libre de cuadrados y $D \equiv 1 \pmod 4$, o $D = 4d$, con $d \equiv 2, 3 \pmod 4$ y d es libre de cuadrados. En cualquiera de los dos casos, se tiene que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D})$.

Observación 2.2.6. Dado un entero negativo Δ, el discriminante fundamental Δ_0 asociado a Δ dado en la Definición 2.1.21 es efectivamente un discriminante fundamental con esta definición.

Las nociones de anillo de enteros y discriminante pueden generalizarse. Haremos uso de estas herramientas para demostrar el Teorema 2.3.2.

Definición 2.2.7. Sea K un cuerpo de números cuadrático. Un *orden (cuadrático)* en K es un subanillo $\mathcal{O} \subseteq \mathcal{O}_K$ que también es un $\mathbb{Z}$-módulo de rango 2.

El *discriminante* de un orden cuadrático se define de manera análoga a la Definición 2.2.4.

Se tiene una caracterización de todos los órdenes cuadráticos. Para dar esta descripción, notemos que por la Proposición 2.2.2, siempre podemos escribir al anillo de enteros como

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega_K, \quad \text{donde } \omega_K = \frac{\Delta_K + \sqrt{\Delta_K}}{2}. \tag{2.2.2}$$

Proposición 2.2.8. *Sea K un cuerpo de números cuadrático de discriminante Δ_K. Sea $\mathcal{O}$ un orden en K. Entonces $\mathcal{O}$ tiene índice finito en $\mathcal{O}_K$. Si llamamos $r = [\mathcal{O}_K : \mathcal{O}]$, entonces*

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}r\omega_K,$$

donde ω_K se define como en (2.2.2). El discriminante de $\mathcal{O}$ es $\Delta(\mathcal{O}) = r^2\Delta_K$.

Demostración. Ver [Cox11, Capítulo 7, Lema 7.2]. □

Definición 2.2.9. Dado un entero Δ, denotaremos por $\mathcal{O}(\Delta)$ al único orden cuadrático de discriminante Δ.

Observación 2.2.10. Los anillos de enteros se corresponden exactamente con los órdenes cuadráticos cuyo discriminante es un discriminante fundamental.

El grupo de clases

El anillo de enteros $\mathcal{O}_d$ de un cuerpo de números cuadrático no es, en general, un dominio de factorización única. Sin embargo, se recupera esta noción a nivel de ideales: todo ideal no nulo de $\mathcal{O}_d$ se escribe de forma única como producto de ideales primos. Este hecho se deduce esencialmente del siguiente resultado.

Proposición 2.2.11. *Sean I, J ideales de $\mathcal{O}_d$. Entonces existe un ideal J' tal que $JJ' = I$ si y solo si $I \subseteq J$.*

Demostración. Ver [Mar77, Capítulo 3, Corolario 3 y Teorema 14]. □

Los ideales primos de $\mathbb{Z}$ podrían no ser primos si los consideramos dentro del anillo de enteros cuadrático $\mathcal{O}_d$, pero se conoce su posible factorización.

Proposición 2.2.12. *Sea $p \in \mathbb{Z}$ primo y sea $\mathcal{O}_d$ un anillo de enteros cuadrático. Entonces la factorización en primos de $p\mathcal{O}_d$ está dada por alguna de las siguientes posibilidades:*

$$p\mathcal{O}_d = \begin{cases} \mathfrak{P}^2 & \text{para algún ideal primo } \mathfrak{P}, \\ \mathfrak{P} & \text{para algún ideal primo } \mathfrak{P}, \\ \mathfrak{P}_1\mathfrak{P}_2 & \text{para ciertos ideales primos } \mathfrak{P}_1, \mathfrak{P}_2. \end{cases}$$

Demostración. Ver [Mar77, Capítulo 3, Teorema 25]. □

Además de los ideales usuales, es interesante estudiar los *ideales fraccionarios*. En lo que sigue, llamaremos $K = \mathbb{Q}(\sqrt{d})$ para aligerar la notación.

Definición 2.2.13. Un *ideal fraccionario* de un cuerpo de números cuadrático K es un conjunto de la forma αI, donde I es un ideal no nulo de $\mathcal{O}_K$ y $\alpha \in K^\times$.

Como $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango 2, todo ideal I de $\mathcal{O}_K$ es un submódulo de rango a lo sumo 2, y por lo tanto todo ideal fraccionario es de la forma $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, con $\omega_1, \omega_2 \in K$.

Denotaremos por $\mathcal{I}_K$ al conjunto de todos los ideales fraccionarios de K.

Es un resultado clásico de la teoría de números algebraica que el conjunto $\mathcal{I}_K$ resulta ser un grupo; más aun, es el grupo abeliano libre generado por los ideales primos de $\mathcal{O}_K$.

Definición 2.2.14. El subgrupo de *ideales fraccionarios principales*, denotado $\mathcal{P}_K$, está dado por los ideales fraccionarios de la forma $\alpha\mathcal{O}_K$ para algún $\alpha \in K^\times$.

Se tiene una relación de equivalencia entre ideales fraccionarios: dados $I, J \in \mathcal{I}_K$, diremos que son equivalentes si y solo si existe $\alpha \in \mathcal{O}_K$ tal que $I = \alpha J$.

Definición 2.2.15. El *grupo de clases* de un cuerpo de números cuadrático K es el grupo cociente $\mathcal{I}_K/\mathcal{P}_K$, es decir, el cociente de los ideales fraccionarios por la relación de equivalencia anterior.

Uno de los resultados principales de la teoría algebraica de números es la finitud del grupo de clases. La demostración puede verse en [Mar77, Capítulo 5, Teorema 35, Corolarios 1 y 2].

Definición 2.2.16. Sea $K = \mathbb{Q}(\sqrt{d})$ un cuerpo de números cuadrático. El *número de clase de K* es el orden de su grupo de clases. Lo denotaremos como $h(d)$.

Se tiene también una noción de norma para los ideales.

Definición 2.2.17. Si I es un ideal de $\mathcal{O}_K$, su *norma (absoluta)* es

$$N(I) = [\mathcal{O}_K : I].$$

Dado I un ideal de $\mathcal{O}_K$, podemos escribir $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, $I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, donde $\omega_1, \omega_2 \in \mathcal{O}_K$. Luego, existen $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ tales que

$$\begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} = \begin{pmatrix} \omega_1 & \omega_2 \\ \overline{\omega}_1 & \overline{\omega}_2 \end{pmatrix}.$$

Así, la norma de I puede calcularse como

$$N(I) = \det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}. \tag{2.2.3}$$

Ejemplo 2.2.18. Si $I = (\alpha) = \alpha\mathcal{O}_K$, escribiendo $\alpha = a + b\omega$ se obtiene de la definición anterior que la norma del ideal generado por α coincide con la norma del elemento α.

Por ejemplo, si $d \equiv 2,\ 3 \pmod 4$, entonces $\omega = \sqrt{d}$ y por lo tanto

$$I = \mathbb{Z}\alpha + \mathbb{Z}\omega\alpha = \mathbb{Z}(a + b\omega) + \mathbb{Z}(bd + a\omega).$$

Así, resulta

$$\begin{pmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{pmatrix} \begin{pmatrix} a & bd \\ b & a \end{pmatrix} = \begin{pmatrix} \alpha & \alpha\omega \\ \overline{\alpha} & \overline{\alpha\omega} \end{pmatrix}.$$

Esto implica que $N(I) = N((\alpha)) = a^2 - db^2 = N(\alpha)$.

La norma resulta ser multiplicativa, es decir, $N(IJ) = N(I)N(J)$. Esta propiedad se deduce esencialmente del Teorema chino del resto. Usando la multiplicatividad, la norma se extiende a los ideales fraccionarios de $\mathcal{O}_K$.

Existe además una conexión entre las normas de los elementos de un ideal y la correspondiente al ideal.

Proposición 2.2.19. *Sea I un ideal de $\mathcal{O}_K$ y sea $\alpha \in I$. Entonces $N(I)$ divide a $N(\alpha)$.*

Demostración. Como $\alpha \in I$, tenemos que $(\alpha) \subseteq I$. Luego, por la unicidad de factorización en ideales primos, existe un ideal J tal que $(\alpha)J = I$, y el resultado sigue por la multiplicatividad de la norma. □

2.3. Conexión entre números de clase

En lo que sigue, estableceremos la conexión entre el número de clase de Hurwitz-Kronecker y el número de clase de un cuerpo de números cuadrático. Así como el grupo de clases se obtiene considerando los ideales fraccionarios módulo ideales fraccionarios principales, es de utilidad considerar un caso particular de esta relación de equivalencia.

Definición 2.3.1. Diremos que dos ideales I, J de $\mathcal{O}_d$ son *estrechamente equivalentes* si existe $\alpha \in \mathbb{Q}(\sqrt{d})$ tal que $I = \alpha J$, con $N(\alpha) > 0$.

Sea D un discriminante fundamental. Por definición, existe un entero d libre de cuadrados tal que $D = \Delta_{\mathbb{Q}(\sqrt{d})}$. Probaremos a continuación que existe una correspondencia biyectiva entre clases de equivalencia de formas de discriminante D y clases estrechas de ideales en el cuerpo de números cuadrático $\mathbb{Q}(\sqrt{d})$. En lo que sigue, $\sqrt{d}$ denotará al número complejo $i\sqrt{|d|}$ si $d < 0$. Para el caso $d > 0$, denotará a la raíz cuadrada usual.

Dado I ideal fraccionario de $\mathbb{Q}(\sqrt{d})$, podemos escribirlo como

$$I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2, \quad \text{donde } \omega_1, \omega_2 \in I, \quad \frac{\overline{\omega}_1\omega_2 - \omega_1\overline{\omega}_2}{\sqrt{d}} > 0.$$

Asociamos al ideal I (y ω_1, ω_2) la forma cuadrática

$$Q_I(x, y) = \frac{(x\omega_1 - y\omega_2)(x\overline{\omega}_1 - y\overline{\omega}_2)}{N(I)} = \frac{\omega_1\overline{\omega}_1 x^2 - (\omega_1\overline{\omega}_2 + \overline{\omega}_1\omega_2)xy + \omega_2\overline{\omega}_2 y^2}{N(I)}.$$

Resulta que Q_I tiene coeficientes enteros y discriminante D. En efecto, podemos suponer que I es un ideal entero, ya que la forma Q_I no cambia si tomamos nI en lugar de I, con base $\{n\omega_1, n\omega_2\}$, donde n es un entero positivo. Siempre es posible elegir $n \in \mathbb{Z}$ de modo que $n\omega_1, n\omega_2$ sean enteros, en vistas de (2.2.1). De esta forma, deducimos que ω_1, ω_2 y sus conjugados están en $\mathcal{O}_d$. Esto último, junto con la Proposición 2.2.19, implica que las normas de $\omega_1, \omega_2, \omega_1 + \omega_2$ son enteros divisibles por $N(I)$, es decir,

$$N(I) \mid \omega_1\overline{\omega}_1,\ \omega_2\overline{\omega}_2,\ (\omega_1 + \omega_2)(\overline{\omega}_1 + \overline{\omega}_2).$$

Luego, la forma Q_I tiene coeficientes enteros.

Veamos ahora que $\Delta(Q_I) = D$. Por la Proposición 2.2.2, sabemos que $\mathcal{O}_d = \mathbb{Z} + \mathbb{Z}\omega$, donde $\omega \in \{\sqrt{d}, (1 + \sqrt{d})/2\}$. Por (2.2.3), resulta que

$$\begin{vmatrix} \omega_1 & \overline{\omega}_1 \\ \omega_2 & \overline{\omega}_2 \end{vmatrix}^2 = N(I)^2 \begin{vmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{vmatrix}^2 = N(I)^2 D.$$

El discriminante de Q_I es

$$\Delta(Q_I) = \frac{(\omega_1\overline{\omega}_2 + \overline{\omega}_1\omega_2)^2 - 4\omega_1\overline{\omega}_1\omega_2\overline{\omega}_2}{N(I)^2} = \frac{(\omega_1\overline{\omega}_2 - \overline{\omega}_1\omega_2)^2}{N(I)^2},$$

así que $D = \Delta(Q_I)$, como queríamos probar.

Como el discriminante de Q_I es un discriminante fundamental, la forma Q_I es primitiva. Luego, por el Teorema 2.1.14, Q_I es equivalente a una única forma reducida

$$Q_i = a_i x^2 + b_i xy + c_i y^2 = a_i(x - z_i y)(x - \overline{z}_i y),$$

donde

$$a_i > 0, \qquad z_i = \frac{-b_i + \sqrt{D}}{2a_i}, \qquad \overline{z}_i = \frac{-b_i - \sqrt{D}}{2a_i}.$$

Probaremos ahora que el ideal I es estrechamente equivalente al ideal $I_i = \mathbb{Z} + \mathbb{Z}z_i$. Esto nos permitirá pasar de la asignación $I \mapsto Q_I$ a $I_i \mapsto Q_i$.

Por la definición de equivalencia de formas, existe $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ tal que

$$Q_I(px + qy, rx + sy) = Q_i(x, y).$$

Podemos reescribir esta última igualdad como

$$\frac{N(p\omega_1 - r\omega_2)}{N(I)}(x - zy)(x - \overline{z}y) = a_i(x - z_i y)(x - \overline{z}_i y), \tag{2.3.1}$$

donde

$$z = \frac{-q\omega_1 + s\omega_2}{p\omega_1 - r\omega_2}.$$

Comparando coeficientes de x^2 en (2.3.1), resulta que

$$N(p\omega_1 - r\omega_2) = a_i N(I) > 0.$$

Entonces tenemos

$$\frac{z - \overline{z}}{\sqrt{D}} = \frac{ps - qr}{N(p\omega_1 - r\omega_2)} \cdot \frac{\overline{\omega}_1\omega_2 - \omega_1\overline{\omega}_2}{\sqrt{D}} = \frac{1}{N(p\omega_1 - r\omega_2)} N(I) = \frac{1}{a_i},$$

y

$$\frac{z_i - \overline{z}_i}{\sqrt{D}} = \frac{1}{a_i}.$$

Además, comparando coeficientes de xy en (2.3.1), obtenemos

$$z + \overline{z} = z_i + \overline{z}_i,$$

de lo cual deducimos que $z = z_i$. De lo anterior se desprende que

$$I = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}(p\omega_1 - r\omega_2) + \mathbb{Z}(-q\omega_1 + s\omega_2)$$

es estrechamente equivalente a

$$\mathbb{Z} + \mathbb{Z}z = \mathbb{Z} + \mathbb{Z}z_i = I_i,$$

ya que $(p\omega_1 - r\omega_2)I_i = I$ con $N(p\omega_1 - r\omega_2) > 0$.

Para probar que la correspondencia es biyectiva, resta ver que los ideales I_i, I_j no son estrechamente equivalentes si $i \neq j$. Supongamos que sí lo son, es decir, existe $\mu \in \mathbb{Q}(\sqrt{d})$ con $N(\mu) > 0$ tal que

$$\mu(\mathbb{Z} + \mathbb{Z}z_i) = \mathbb{Z} + \mathbb{Z}z_j.$$

Debe existir entonces $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ tal que

$$\mu = p + qz_j, \qquad \mu z_i = r + sz_j.$$

Despejando,

$$z_i = \frac{r + sz_j}{p + qz_j} \qquad \text{con} \qquad N(p + qz_j) = N(\mu) > 0.$$

Al igual que antes, resulta que

$$\frac{1}{a_i} = \frac{z_i - \overline{z}_i}{\sqrt{D}} = \frac{ps - qr}{N(p + qz_j)} \cdot \frac{z_j - \overline{z}_j}{\sqrt{D}} = \frac{ps - qr}{N(p + qz_j)} \cdot \frac{1}{a_j},$$

y por lo tanto, dado que a_i, a_j son positivos, deducimos que

$$ps - qr = 1 \qquad \text{y} \qquad N(p + qz_j) = \frac{a_i}{a_j}.$$

De todo esto se desprende que

$$Q_i(x, y) = Q_j(px - ry, -qx + sy),$$

así que Q_i y Q_j son equivalentes. Concluímos que $i = j$.

Hemos probado el siguiente resultado.

Teorema 2.3.2. *Sea D un discriminante fundamental. Entonces existe una correspondencia biyectiva entre clases de equivalencia estrechas de ideales del anillo $\mathcal{O}_D$ y clases de equivalencia de formas de discriminante D.*

Ahora bien, en el caso cuadrático imaginario no existen unidades con norma negativa (equivalentemente, todos los elementos no nulos tienen norma positiva), de modo que la equivalencia estrecha no es otra que la equivalencia usual de ideales (es decir, considerando los ideales fraccionarios módulo ideales principales). Lo anterior prueba entonces que el grupo de clases de $\mathbb{Q}(\sqrt{D})$ está en correspondencia biyectiva con el conjunto de clases de equivalencia de formas de discriminante D.

Se tiene una expresión conocida para el orden del grupo de clases. Un teorema básico e importante de la teoría de números algebraica es la fórmula del número de clases, que relaciona invariantes asociados a un cuerpo de números con la cantidad de elementos en su grupo de clases. La utilizaremos solamente para el caso cuadrático imaginario. Antes de este resultado, haremos algunas definiciones que serán necesarias.

Definición 2.3.3. Sea p un primo impar. Dado un entero a, definimos el *símbolo de Legendre de a con respecto a p* como

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

El símbolo de Legendre puede calcularse explícitamente como

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (\text{mód } p).$$

Si $p = 2$, definimos el *símbolo de Kronecker de a con respecto a 2* como

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{si } 2 \mid a, \\ 1 & \text{si } a \equiv \pm 1 \text{ (mód } 8), \\ -1 & \text{si } a \equiv \pm 5 \text{ (mód } 8). \end{cases}$$

Definición 2.3.4. Sea $D < 0$ un discriminante fundamental. Definimos el *caracter cuadrático asociado a D* como $\chi : \mathbb{Z} \to \{0, 1, -1\}$,

$$\begin{cases} \chi(\ell) = \left(\frac{D}{\ell}\right) & \text{si } \ell \text{ es un primo impar,} \\ \chi(0) = 0,\ \chi(1) = 1,\ \chi(-1) = -1, & \\ \chi(2) = \left(\frac{D}{2}\right), & \\ \chi(nm) = \chi(n)\chi(m) & \text{para todo } n, m \in \mathbb{N}. \end{cases}$$

Definición 2.3.5. Sea D un discriminante fundamental y sea χ el caracter cuadrático asociado a D. Definimos la *L-serie asociada a χ* como

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

para $s \in \mathbb{C}$ con $\mathrm{Re}(s) > 0$.

Observación 2.3.6. En principio, la L-serie asociada a χ sólo está definida en el semiplano $\mathrm{Re}(s) > 1$. Sin embargo, puede probarse que la serie converge también en el semiplano $\mathrm{Re}(s) > 0$ utilizando herramientas del análisis complejo y de la teoría de caracteres. Más aun, como la convergencia es absoluta, se tiene la igualdad

$$L(s, \chi) = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Teorema 2.3.7 (Fórmula del número de clases cuadrático)**.** *Sea $D < 0$ un discriminante fundamental. Entonces*

$$h(D) = \frac{w\sqrt{|D|}}{2\pi} L(1, \chi),$$

donde w es la cantidad de raíces de la unidad contenidas en $\mathbb{Q}(\sqrt{D})$.

Demostración. Ver [Mar77, Capítulo 7]. □

Para probar el vínculo entre números de clases, introduciremos la *ecuación de Pell*.

Definición 2.3.8. Sea Δ un entero negativo. La *ecuación de Pell asociada a Δ* es

$$x^2 - \Delta y^2 = 4.$$

Teorema 2.3.9. *Sea $f = ax^2 + bxy + cy^2$ una forma reducida. La función que envía una solución $(x, y) \in \mathbb{Z}^2$ de la ecuación de Pell asociada a $\Delta = \Delta(f)$ a la matriz*

$$U(f, x, y) = \begin{pmatrix} (x - yb)/2 & -cy \\ ay & (x + yb)/2 \end{pmatrix}$$

es una biyección entre el conjunto de dichas soluciones y el grupo de automorfismos de f.

Demostración. Sea $(x, y) \in \mathbb{Z}^2$ una solución de la ecuación de Pell asociada a $\Delta(f)$. Veamos primero que $U = U(f, x, y)$ es un automorfismo de f. En efecto, como Δ y b tienen la misma paridad, reduciendo la ecuación de Pell módulo 2 obtenemos

$$x \equiv x^2 \equiv by^2 \equiv by \text{ (mód 2)},$$

así que U tiene coeficientes enteros. Además, su determinante es

$$\det U = \frac{x^2 - y^2b^2}{4} + acy^2 = \frac{x^2 - (b^2 - 4ac)y^2}{4} = \frac{x^2 - \Delta y^2}{4} = 1.$$

Reescribiendo $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ para simplificar la notación, resulta que

$$(U^t)^{-1} \cdot M_f = \frac{1}{2} \begin{pmatrix} 2as - br & -2cr + bs \\ -2aq + bp & 2cp - bq \end{pmatrix}, \tag{2.3.2}$$

mientras que

$$M_f \cdot U = \frac{1}{2} \begin{pmatrix} 2ap + br & 2aq + bs \\ 2cr + bp & 2cs + bq \end{pmatrix}. \tag{2.3.3}$$

Los coeficientes de estas matrices son iguales, así que $U \in \mathrm{Aut}(f)$.

Probemos ahora que la asignación $(x, y) \mapsto U(f, x, y)$ es biyectiva. La inyectividad se obtiene comparando coeficientes de $U(f, x, y)$ y $U(f, x', y')$. Veamos la sobreyectividad. Sea $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ un automorfismo de f. Entonces se tiene la igualdad

$$(U^t)^{-1} \cdot M_f = M_f \cdot U.$$

Igualando las expresiones en (2.3.2) y (2.3.3), tenemos que $aq = -cr$. Como la forma f es reducida, en particular $a \neq 0$, de modo que a divide a r por ser a y c coprimos. Definimos $(x, y) = (p + s, r/a)$, y así $U = U(f, x, y)$. Tomando determinante, obtenemos

$$4 = 4 \det(U) = x^2 - \Delta y^2,$$

con lo cual $(x, y) \in \mathbb{Z}^2$ es efectivamente una solución a la ecuación de Pell. □

Ahora estamos en condiciones de establecer la conexión deseada.

Proposición 2.3.10. *Dos formas reducidas con el mismo discriminante tienen el mismo grupo de automorfismos.*

Demostración. Sean f, g formas reducidas de discriminante Δ. Por el Teorema 2.3.9, la función que envía al automorfismo $U(f, x, y)$ de f al automorfismo $U(g, x, y)$ de g, donde (x, y) es una solución de la ecuación de Pell asociada, es una biyección.

Omitimos los detalles de que esta función es un morfismo de grupos, ya que nos interesará únicamente que los grupos de automorfismos tengan el mismo cardinal. La demostración puede verse en [BV07, Capítulo 2, Teorema 2.5.7] □

Proposición 2.3.11. *Sea f una forma reducida de discriminante $\Delta < 0$. Entonces el grupo de automorfismos de f tiene cardinal*

$$|\mathrm{Aut}(f)| = \begin{cases} 2 & si\ \Delta < -4, \\ 4 & si\ \Delta = -4, \\ 6 & si\ \Delta = -3. \end{cases}$$

Demostración. Por la Proposición 2.3.10, bastará probar esta igualdad para cualquier forma reducida f de discriminante $\Delta < 0$. Las únicas soluciones enteras de la ecuación de Pell asociada a Δ son $(\pm 2, 0)$ si $\Delta < -4$; $(\pm 2, 0)$ y $(0, \pm 1)$ si $\Delta = -4$; y $(\pm 2, 0)$, $(\pm 1, \pm 1)$ si $\Delta = -3$. Por el Teorema 2.3.9, el grupo de automorfismos de f tiene el orden correspondiente en cada caso. □

Observación 2.3.12. Este último resultado prueba que el número de clase de Hurwitz-Kronecker está bien definido.

De todo lo hecho anteriormente se deduce la siguiente proposición.

Proposición 2.3.13. *Sea $D < 0$ un discriminante fundamental. Entonces*

$$\widetilde{h}(D) = \frac{h(D)}{w},$$

donde w es la cantidad de raíces de la unidad contenidas en $\mathbb{Q}(\sqrt{D})$.

Podemos aplicar entonces la fórmula para el número de clases en el caso cuadrático dada en el Teorema 2.3.7. Como $\Delta < 0$, resulta que

$$\widetilde{h}(\Delta) = \frac{\sqrt{|\Delta|}}{2\pi} \cdot L(1, \chi),$$

donde $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ es la L-serie del caracter cuadrático χ asociado a Δ. Si $\mathfrak{f}$ es el conductor asociado a Δ y χ_0 es el caracter cuadrático asociado al discriminante fundamental Δ_0 (ver la Definición 2.1.21), se tiene que

$$L(1, \chi) = L(1, \chi_0) \cdot \prod_{\ell \mid \mathfrak{f}} \left(1 - \frac{\chi_0(\ell)}{\ell}\right),$$

donde ℓ recorre los primos que dividen a $\mathfrak{f}$. De estas dos últimas igualdades, junto con la Proposición 2.1.20, se desprende que

$$H(\Delta) = \frac{\sqrt{|\Delta|}}{2\pi} \cdot L(1, \chi_0) \cdot \psi(\mathfrak{f}), \tag{2.3.4}$$

donde la función $\psi : \mathbb{N} \to \mathbb{R}$ es multiplicativa y se define, para ℓ primo y $k \geq 1$, como

$$\psi(\ell^k) = \begin{cases} \frac{\ell - \ell^{-k}}{\ell - 1} & \text{si } \chi_0(\ell) = 0, \\ 1 & \text{si } \chi_0(\ell) = 1, \\ \frac{\ell + 1 - 2\ell^{-k}}{\ell - 1} & \text{si } \chi_0(\ell) = -1. \end{cases}$$

Observación 2.3.14. Dado $\ell \in \mathbb{Z}$ primo y $k \geq 1$, obtenemos la desigualdad

$$\psi(\ell^k) \leq \frac{\ell + 1 - 2\ell^{-k}}{\ell - 1}.$$

El objetivo es obtener cotas superiores e inferiores para $H(\Delta)$, ya que esto nos permitirá estimar más adelante la cantidad de curvas definidas sobre $\mathbb{F}_p$. Para eso, acotaremos el valor de la L-serie y de la función ψ. Introducimos la notación que usaremos para los órdenes, que es la que se utiliza habitualmente en este contexto.

Definición 2.3.15. Sean $f(x), g(x)$ funciones positivas. Diremos que

$$f(x) = O(g(x))$$

si existen constantes positivas c y C tales que

$$f(x) \leq cg(x) \quad \text{para todo } x \geq C.$$

Proposición 2.3.16. *Si φ es la función de Euler y $\mathfrak{f} \in \mathbb{N}$, se tiene que*

$$1 \leq \psi(\mathfrak{f}) \leq (\mathfrak{f}/\varphi(\mathfrak{f}))^2 = O\left((\log\log \mathfrak{f})^2\right).$$

Demostración. La primera desigualdad es inmediata de la definición de ψ y de la multiplicatividad. Para la segunda, como ambas funciones son multiplicativas, bastará probar el caso en que $\mathfrak{f} = \ell^k$ con ℓ primo. Se tiene que

$$\psi(\ell^k) \leq \frac{\ell + 1 - 2\ell^{-k}}{\ell - 1} \leq \frac{\ell + 1}{\ell - 1},$$

mientras que

$$\left(\frac{\ell^k}{\varphi(\ell^k)}\right)^2 = \frac{\ell^{2k}}{\ell^{2k-2}(\ell - 1)^2} = \frac{\ell^2}{(\ell - 1)^2}.$$

Como

$$\frac{\ell + 1}{\ell - 1} \leq \frac{\ell^2}{(\ell - 1)^2},$$

se sigue la desigualdad buscada.

El hecho de que

$$(\mathfrak{f}/\varphi(\mathfrak{f}))^2 = O\left((\log\log \mathfrak{f})^2\right)$$

se deduce de

$$\liminf_{n \to \infty} \frac{\varphi(n) \log\log n}{n} = e^{-\gamma},$$

y la demostración puede verse en [HW+79, Teorema 328]. □

Proposición 2.3.17. *Si Δ_0 es el discriminante fundamental asociado a Δ y χ_0 su caracter cuadrático correspondiente, entonces*

$$L(1, \chi_0) = O(\log |\Delta_0|).$$

Además, existe una constante efectivamente computable c tal que para todo entero $z \geq 2$, existe $\Delta^* < -4$ que cumple

$$L(1, \chi_0) \geq \frac{c}{\log z} \quad si \ |\Delta_0| \leq z, \ \Delta_0 \neq \Delta^*.$$

Demostración. Ver [Pra57, Capítulo 4]. □

Corolario 2.3.18. *Existen constantes positivas c_1, c_2 tales que, para cada entero $z \geq 2$, existe $\Delta^* = \Delta^*(z) < -4$ tal que*

$$c_1 \frac{\sqrt{|\Delta|}}{\log(z)} \leq H(\Delta) \leq c_2 \cdot (\log |\Delta|)(\log\log |\Delta|)^2 \sqrt{|\Delta|},$$

para todo $\Delta \in \mathbb{Z}$ con $-z \leq \Delta < 0$, $\Delta \equiv 0, 1$ (mód 4), excepto que la desigualdad de la izquierda puede no ser válida si $\Delta_0 = \Delta^*$.

Demostración. Usando la expresión para $H(\Delta)$ dada en (2.3.4), las desigualdades se siguen de las Proposiciones 2.3.16 y 2.3.17. □

El vínculo deseado entre formas cuadráticas y curvas elípticas está dado por el número de clase de Hurwitz-Kronecker. Específicamente, por el siguiente resultado.

Teorema 2.3.19. *Sea $p > 3$ un primo y a un entero tal que $|a| \leq 2\sqrt{p}$. Sea A_a el conjunto de clases de isomorfismo de curvas elípticas E definidas sobre $\mathbb{F}_p$ tales que $\#E(\mathbb{F}_p) = p + 1 - a$. Entonces*

$$\sum_{E \in A_a} \frac{1}{|\operatorname{Aut}(E)|} = H(a^2 - 4p).$$

Demostración. Ver [Deu41] o [Sch87]. □

Para terminar este capítulo, aplicaremos todo lo hecho para poder acotar la cantidad de clases de isomorfismo de curvas elípticas definidas sobre $\mathbb{F}_p$ con orden prefijado. Haremos uso del mismo en la última parte, como herramienta para obtener el resultado central de esta tesis.

Teorema 2.3.20. *Existen constantes efectivamente computables c_4 y c_5 tales que para cada primo $p > 3$ y cada subconjunto de enteros $\widetilde{S} \subseteq [p + 1 - 2\sqrt{p}, \ p + 1 + 2\sqrt{p}]$, la cantidad de clases de isomorfismo de curvas elípticas E definidas sobre $\mathbb{F}_p$ con $\#E(\mathbb{F}_p) \in \widetilde{S}$ es menor o igual que*

$$c_4 \cdot \#\widetilde{S} \cdot (\log p)(\log\log p)^2 \sqrt{p};$$

mientras que para cada conjunto de enteros $S \subseteq [p + 1 - \sqrt{p}, \ p + 1 + \sqrt{p}]$ con $\#S \geq 3$, la cantidad de clases de isomorfismo con $\#E(\mathbb{F}_p) \in S$ es mayor o igual que

$$c_5 \cdot (\#S - 2) \cdot \frac{\sqrt{p}}{\log p}.$$

Demostración. Sea a un entero tal que $p+1-a \in [p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$. Sea A_a el conjunto definido como en el Teorema 2.3.19.

Para la primera desigualdad, por el Teorema 1.2.15 sabemos que el grupo de automorfismos de una curva elíptica tiene a lo sumo seis elementos, así que del Teorema 2.3.19 se deduce que

$$\frac{\#A_a}{6} = \sum_{E \in A_a} \frac{1}{6} \leq H(a^2-4p).$$

Aplicando el Corolario 2.3.18 para $z = 4p$ y $\Delta = a^2 - 4p$, como $|\Delta| \leq 4p$ obtenemos

$$\#A_a \leq 6c_2\sqrt{4p} \cdot \log(4p) \cdot (\log\log(4p))^2 \leq c_4(\log p)(\log\log p)^2\sqrt{p},$$

para alguna constante positiva c_4. Sumando ahora sobre todos los enteros a tales que $p+1-a \in \widetilde{S}$, obtenemos la primera desigualdad.

Para la segunda desigualdad, como el grupo de automorfismos de cualquier curva elíptica tiene al menos un elemento resulta que

$$H(a^2-4p) \leq \sum_{E \in A_a} 1 = \#A_a.$$

Nuevamente, por el Corolario 2.3.18, tomando $z = 4p$ y $\Delta = a^2 - 4p$, tenemos que

$$c_1 \frac{\sqrt{|a^2-4p|}}{\log(4p)} \leq H(a^2-4p),$$

si el discriminante fundamental asociado a $a^2 - 4p$ no es igual a Δ^*. Como

$$p+1-\sqrt{p} \leq p+1-a \leq p+1+\sqrt{p},$$

tenemos que $|a| \leq \sqrt{p}$, y por lo tanto

$$|a^2-4p| = 4p - a^2 \geq 3p.$$

Esto prueba que existe una constante positiva c_5 tal que

$$c_5 \frac{\sqrt{p}}{\log(p)} \leq H(a^2-4p) \leq \#A_a. \tag{2.3.5}$$

Veamos ahora que existen a lo sumo dos valores enteros de a tales que el discriminante fundamental asociado a $a^2 - 4p$ es igual a Δ^*. Sea a un entero que cumpla con esta condición, y sea $K = \mathbb{Q}(\sqrt{\Delta^*})$. Consideramos el polinomio $x^2 - ax + p \in \mathbb{Z}[x]$. Entonces sus raíces complejas $\alpha, \overline{\alpha}$ deben pertenecer al anillo de enteros $\mathcal{O}_{\Delta^*}$. A su vez, como $\alpha\overline{\alpha} = p$, por la Proposición 2.2.12 resulta que los ideales generados por α y $\overline{\alpha}$ son primos. Luego, α está determinado salvo conjugación y producto por unidades. Pero, como $\Delta^* < -4$, por la Proposición 2.2.3 tenemos que el grupo de unidades de $\mathcal{O}_{\Delta^*}$ es $\{\pm 1\}$. Luego, α queda determinado salvo conjugación y signo, y por lo tanto $a = \alpha + \overline{\alpha}$ queda determinado, salvo un signo, por Δ^*, como queríamos.

Sumando las desigualdades (2.3.5) sobre todos los valores de a tales que $p+1-a \in S$ (que son todos salvo a lo sumo dos), se sigue la segunda desigualdad. □

Capítulo 3

El problema del logaritmo discreto

Definición 3.0.1. Sea $(G, \cdot)$ un grupo, y sean $g, h \in G$, tales que h pertenece al subgrupo generado por g. El *problema del logaritmo discreto (PLD)* consiste en hallar un entero k tal que

$$g^k = h.$$

La dificultad del PLD depende del grupo G considerado. Nos interesarán principalmente los casos en que G sea el grupo multiplicativo de unidades de un cuerpo finito, esto es, $G = \mathbb{F}_q^\times$, o el grupo de puntos definidos sobre un cuerpo finito de una curva elíptica E, esto es, $G = E(\mathbb{F}_q)$. A continuación, discutiremos algunos algoritmos para resolverlo en cada caso y su complejidad, es decir, la cantidad de operaciones o pasos necesarios para que el algoritmo funcione. Este último punto es de vital importancia, ya que no solo nos interesa encontrar una solución al problema, sino también hacerlo en una cantidad de tiempo que resulte razonable. Principalmente, nos interesará saber cuánto demora la resolución de un problema en función del tamaño de los datos ingresados. En el caso del problema del logaritmo discreto, esto dependerá del orden del grupo en el cual queremos resolverlo. En general, el tamaño de los datos suele medirse en cantidad de bits, ya que esto dice cuánta capacidad de almacenamiento se requiere para guardarlos.

Utilizaremos la notación de orden dada en la Definición 2.3.15.

Definición 3.0.2. Supongamos que tenemos un problema cuyos datos de entrada son de tamaño $O(k)$ bits.

* Si existe una constante $A \geq 0$ tal que la solución al problema puede encontrarse en $O(k^A)$ pasos, entonces decimos que puede resolverse en *tiempo polinomial*. Si $A = 1$, diremos que requiere de tiempo *lineal*.
* Si existe una constante $c > 0$ tal que la solución puede encontrarse en $O(\exp(ck))$ pasos, entonces decimos que el problema puede resolverse en *tiempo exponencial*.
* Por último, si para cada $\epsilon > 0$, la solución puede encontrarse en $O(\exp(\epsilon k))$ (donde las constantes c y C dependen de ϵ), entonces decimos que el problema puede resolverse en *tiempo subexponencial*.

En general, los problemas que pueden resolverse en tiempo polinomial se consideran fáciles, mientras que aquellos que requieren de tiempo exponencial se consideran difíciles. Los problemas resolubles en tiempo subexponencial se encuentran en un área intermedia.

Por supuesto, dependiendo del tamaño de los datos de entrada, la resolución de un problema que requiere de tiempo exponencial puede ser más simple que la de uno que puede resolverse en tiempo polinomial.

Otro hecho a tener en cuenta es la cantidad de almacenamiento requerida para resolver un problema, ya que se dispone únicamente de una cantidad finita del mismo. En la mayoría de los casos que estudiaremos a continuación, estaremos trabajando con grupos de orden N. En este contexto, los datos de entrada son de tamaño $O(\log(N))$ bits. Por ejemplo, en la sección siguiente analizaremos algoritmos que requieren almacenar $\sqrt{N} = \exp(\frac{1}{2}\log N)$ datos. Cuando el valor de N es muy grande, esto puede representar un obstáculo mayor que realizar los cálculos involucrados.

3.1. El caso general

Comenzamos analizando dos algoritmos que resuelven el PLD en cualquier grupo y requieren de tiempo exponencial. El primero es el algoritmo de *fuerza bruta*. Dado G un grupo y $g \in G$ de orden N, el problema del logaritmo discreto

$$g^k = h$$

puede resolverse en $O(N)$ pasos con $O(1)$ almacenamiento, donde cada paso consiste en la multiplicación por g. Simplemente calculamos sucesivamente las potencias de g, guardando únicamente el último valor hallado.

Este algoritmo ingenuo es claramente ineficiente, ya que los datos de entrada (el grupo G de orden N) son de tamaño $O(\log(N))$ bits y la cantidad de pasos requeridos es $O(N) = O(\exp(\log(N)))$, con lo cual resuelve el problema en tiempo exponencial. Aplicando técnicas de colisión, la complejidad puede reducirse bastante. La idea detrás de estos algoritmos es que, para realizar una búsqueda, es más fácil buscar una coincidencia entre objetos que buscar un objeto en particular.

Algoritmo 3.1.1 (Shanks, Algoritmo Babystep-Giantstep)**.** *Sea G un grupo y sea $g \in G$ un elemento de orden $N \geq 2$. El siguiente algoritmo resuelve el problema del logaritmo discreto $g^k = h$ en $O(\sqrt{N} \cdot \log N)$ pasos usando $O(\sqrt{N})$ almacenamiento.*

(1) Sea $n = 1 + \lfloor \sqrt{N} \rfloor$.

(2) Se crean dos listas, la primera dada por

$$e,\ g,\ g^2, \ldots,\ g^n,$$

donde e es el elemento neutro de G; y la segunda dada por

$$h,\ hg^{-n},\ hg^{-2n}, \ldots,\ hg^{-n^2}.$$

(3) *Se busca una coincidencia entre ambas listas, digamos* $g^i = hg^{-jn}$. *Entonces* $h = g^{i+jn}$, *así que* $k = i + jn$ *es una solución al problema del logaritmo discreto. Si no existe una coincidencia, entonces* h *no pertenece al subgrupo generado por* g.

Demostración. El armado de ambas listas requiere de aproximadamente $2n$ multiplicaciones en el grupo G. Para encontrar una coincidencia, podemos utilizar algoritmos de búsqueda, que requieren $O(n \log n)$ pasos. Por lo tanto, el algoritmo requiere de $O(\sqrt{N} \log N)$ pasos. Como ambas listas tienen longitud n, se necesita $O(\sqrt{N})$ almacenamiento.

Ahora veamos que el algoritmo efectivamente produce una solución al problema del logaritmo discreto, si esta existe. Supongamos que $g^k = h$, y escribamos

$$k = nq + r \quad \text{con } 0 \leq r < n.$$

Luego, tenemos

$$g^r = hg^{-nq},$$

y como $1 \leq k < N$, debe ser

$$q = \frac{k - r}{n} < \frac{N}{n} < n.$$

Esto nos dice que hg^{-nq} pertenece a la segunda lista, así que siempre se encuentra una coincidencia cuando h pertenece al subgrupo generado por g. □

Observación 3.1.2. En general, el factor $\log N$ se omite ya que su contribución a la complejidad es mucho menor comparada con $\sqrt{N}$. Podemos decir entonces que la complejidad del algoritmo anterior es de $O(\sqrt{N})$.

El algoritmo Babystep-Giantstep es el mejor algoritmo para resolver el PLD en un grupo arbitrario. Su principal desventaja es la cantidad de almacenamiento necesaria. Una alternativa que requiere aproximadamente la misma cantidad de pasos, pero utiliza almacenamiento prácticamente nulo, es el *algoritmo* ρ *de Pollard*, que puede verse en [Pol78].

3.2. El caso $G = \mathbb{F}_q^\times$

El algoritmo que describiremos a continuación, llamado *cálculo de índices*, permite resolver el PLD en el grupo de unidades de un cuerpo finito. Si $g \in \mathbb{F}_q^\times$ es un elemento primitivo, todo $h \in \mathbb{F}_q^\times$ puede escribirse como $h = g^k$ para un único $0 \leq k \leq q - 1$. A fines de simplificar la escritura, denotaremos al logaritmo discreto de h con respecto a g como

$$k = \log_g(h) \quad \in \mathbb{Z}/(q-1)\mathbb{Z}.$$

Introducimos primero una definición que resultará útil para describir el algoritmo.

Definición 3.2.1. Decimos que un entero n es B-suave si todos los primos que dividen a n son menores o iguales que B.

Consideremos el caso en que $q = p$ es un primo. Dado $g \in \mathbb{F}_p^\times$ elemento primitivo y $h \in \mathbb{F}_p^\times$, en lugar de intentar hallar $\log_g(h)$ directamente, elegimos un entero positivo B y resolvemos el PLD

$$g^k \equiv \ell \pmod{p} \quad \text{para todo primo } \ell \leq B.$$

Es decir, calculamos $\log_g(\ell)$ para todo primo $\ell \leq B$. Una vez hecho esto, computamos

$$h \cdot g^{-n} \quad \text{para } n \geq 1,$$

hasta encontrar un valor de n tal que $h \cdot g^{-n} \pmod{p}$ sea B-suave. Para este valor de n, se tiene

$$h \cdot g^{-n} \equiv \prod_{\ell \leq B} \ell^{e_\ell} \mod p,$$

para ciertos enteros e_ℓ. En términos de logaritmos discretos, esto puede reescribirse como

$$\log_g(h) \equiv n + \sum_{\ell \leq B} e_\ell \cdot \log_g(\ell) \mod (p-1).$$

Como ya conocemos $\log_g(\ell)$ para todo $\ell \leq B$, esto determina el valor de $\log_g(h)$.

Veamos ahora cómo obtener $\log_g(\ell)$ para los primos ℓ. Elegimos exponentes j al azar, y calculamos

$$g_j \equiv g^j \pmod{p} \quad \text{con } 0 < g_j < p.$$

Si g_j no es B-suave, lo descartamos, mientras que si g_j es B-suave, podemos factorizarlo como

$$g_j = \prod_{\ell \leq B} \ell^{u_\ell(j)}.$$

En términos de logaritmos discretos, esto nos proporciona la ecuación

$$j \equiv \log_g(g_j) \equiv \sum_{\ell \leq B} u_\ell(j) \cdot \log_g(\ell) \mod (p-1).$$

Si obtenemos suficientes relaciones de este tipo, podemos encontrar los valores de $\log_g(\ell)$ mediante álgebra lineal. Más precisamente, como las ecuaciones de congruencia son módulo $p-1$, las resolvemos módulo r para cada primo r que divide a $p-1$. Luego, si r^e aparece en la factorización en primos de $p-1$, obtenemos una solución en $\mathbb{Z}/r^e\mathbb{Z}$ a partir de la que tenemos en $\mathbb{Z}/r\mathbb{Z}$. Finalmente, el Teorema chino del resto nos permite combinar las soluciones para cada potencia de un primo y obtener una solución módulo $p-1$.

Un análisis de este algoritmo puede verse en el artículo de Adleman [Adl79], donde se conjetura que, bajo hipótesis razonables sobre la distribución de los números B-suaves, la cantidad esperada de pasos para el cálculo de índices en este caso es

$$O(\exp((\log p)^{1/2}(\log\log p)^{1/2}).$$

Existen muchas generalizaciones para adaptar lo hecho para el caso en que $q = p$ al caso general. El propio Adleman provee un algoritmo que utiliza cuerpos de funciones en [Adl94]. Este algoritmo tiene una complejidad conjeturada de

$$O(\exp(c(\log q)^{1/3}(\log\log q)^{2/3}),$$

para cierta constante $c > 0$, y puede aplicarse para el caso en que $q = p^m$ con $\log(p) \leq m^{g(m)}$, donde g es cualquier función tal que $0 < g(m) < 0{,}98$ y $\lim_{m\to\infty} g(m) = 0$.

Encontrar un algoritmo que funcione para todos los cuerpos finitos con esta cantidad de pasos esperados es un problema abierto.

El cálculo de índices es subexponencial, en contraste con los algoritmos vistos anteriormente. Al depender fuertemente de la factorización en primos, no puede extenderse a grupos arbitrarios.

3.3. El algoritmo MOV

Una buena estrategia a la hora de intentar resolver el PLD es transformarlo en un problema más fácil de abordar. Como vimos anteriormente, el cálculo de índices es mucho más veloz que los algoritmos que funcionan en el caso general. A continuación analizaremos el algoritmo MOV ([MOV93], Menezes - Okamoto - Vanstone), que permite trasladar el PLD en una curva elíptica a un cuerpo finito, mediante el emparejamiento de Weil.

Supongamos que queremos resolver el PLD en una curva elíptica E definida sobre $\mathbb{F}_q$. Sean $P,\ Q \in E(\mathbb{F}_q)$, y sea N el orden de P. Asumamos que N es coprimo con q. El objetivo es hallar k tal que $Q = kP$, en caso de que exista. Comenzaremos viendo una condición necesaria y suficiente para que esto suceda.

Lema 3.3.1. *Existe un entero k tal que $Q = kP$ si y solo si $NQ = \mathcal{O}$ y el emparejamiento de Weil entre P y Q es trivial, es decir, $e_N(P, Q) = 1$.*

Demostración. Supongamos primero que $Q = kP$. Entonces $NQ = kNP = \mathcal{O}$, ya que el orden de P es N. Además,

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

así que la condición es suficiente.

Recíprocamente, si $NQ = \mathcal{O}$, resulta que $Q \in E[N]$. Además, como $\mathrm{mcd}(N, q) = 1$, por la Proposición 1.3.2 tenemos que

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}.$$

Tomando R tal que $\{P,\ R\}$ sea una base de $E[N]$, podemos escribir

$$Q = aP + bR,$$

para ciertos enteros a, b. Bastará probar que $bR = \mathcal{O}$. Ahora bien, como $\{P,\ R\}$ es base, resulta que $\xi = e_N(P, R)$ es una raíz N-ésima primitiva de la unidad por el Corolario 1.4.14. Por lo tanto, como estamos asumiendo que $e_N(P, Q) = 1$, tenemos

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

Esto implica que N divide a b, así que $bR = \mathcal{O}$, como queríamos. □

Para poder llevar a cabo el algoritmo, necesitaremos trabajar con todos los puntos de N-torsión, que podrían no estar definidos sobre $\mathbb{F}_q$. Pero como todos los puntos de $E[N]$ tienen coordenadas en $\bar{\mathbb{F}}_q = \bigcup_{j\geq 1} \mathbb{F}_{q^j}$, existe $m \in \mathbb{N}$ tal que

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

Definición 3.3.2. En este contexto, el menor valor de m tal que $E[N] \subseteq E(\mathbb{F}_{q^m})$ es el *grado de inmersión de E con respecto a N*.

Por el Corolario 1.4.16, resulta que el grupo μ_N está contenido en $\mathbb{F}_{q^m}^\times$. Todos los cálculos necesarios para el procedimiento serán realizados sobre $\mathbb{F}_{q^m}$, ya que podemos considerar

$$e_N : E[N] \times E[N] \longrightarrow \mathbb{F}_{q^m}^\times.$$

Procedemos a continuación a detallar el algoritmo.

Algoritmo 3.3.3 (MOV). *Sea E una curva elíptica definida sobre $\mathbb{F}_q$, y sean $P, Q \in E(\mathbb{F}_q)$. Sea N el orden de P, y asumamos que N es coprimo con q. Sea m el grado de inmersión de E con respecto a N. Supongamos que existe un entero k tal que $Q = kP$. El siguiente algoritmo determina k módulo N.*

(1) Se elige un punto al azar $T \in E(\mathbb{F}_{q^m})$.

(2) Se calcula el orden de T, que llamaremos M.

(3) Sea $d = \mathrm{mcd}(M, N)$, y sea $T_1 = (M/d)T$. De este modo, T_1 tiene orden d, que divide a N, así que $T_1 \in E[N]$.

(4) Se calculan $\zeta_1 = e_N(P, T_1)$ y $\zeta_2 = e_N(Q, T_1)$.

(5) Usando que ζ_1 y ζ_2 están en $\mu_d \subseteq \mathbb{F}_{q^m}^\times$, se resuelve el problema del logaritmo discreto $\zeta_2 = \zeta_1^k$ en $\mathbb{F}_{q^m}^\times$ mediante cálculo de índices. Esto determina k (mód d'), donde d' divide a d.

(6) Se repite con puntos T elegidos al azar hasta que el mínimo común múltiplo de los distintos valores de d' obtenidos sea N. Así, se obtiene k (mód N).

Demostración. Es inmediato que el punto T_1 construido en el paso *(3)* tiene orden d. Además, como $Q = kP$, tenemos

$$\zeta_2 = e_N(Q, T_1) = e_N(kP, T_1) = e_N(P, T_1)^k = \zeta_1^k.$$

Además, como

$$\zeta_1^d = e_N(P, T_1)^d = e_N(P, dT_1) = e_N(P, \mathcal{O}) = 1,$$

el orden de ζ_1 es un divisor de d, digamos d', y por lo tanto k queda determinado módulo d'. □

Un posible inconveniente es que el valor de d sea pequeño y no aporte suficiente información. Pero, debido a la estructura de $E(\mathbb{F}_{q^m})$, ocurre lo contrario. En efecto, por el Teorema 1.6.7, tenemos

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

para ciertos enteros n_1, n_2 tales que $n_1 \mid n_2$ (donde posiblemente $n_1 = 1$, en cuyo caso el grupo es cíclico). Entonces, N divide a n_2, ya que n_2 es el exponente del grupo. Si T_1, T_2 son generadores de $E(\mathbb{F}_{q^m})$ de órdenes n_1 y n_2, respectivamente, existen enteros a_1, a_2 tales que

$$T = a_1T_1 + a_2T_2.$$

Sea ℓ^e una potencia de un primo que divide a N. Como N divide a n_2, resulta que

$$\ell^f \mid n_2 \quad \text{con } f \geq e.$$

Como T es de orden M, debe ser

$$Ma_2T_2 = \mathcal{O},$$

con lo cual n_2 divide a Ma_2. Si ℓ no divide a a_2, resulta que ℓ^f divide a M. Luego, ℓ^e divide a $d = \operatorname{mcd}(M, N)$. Como la probabilidad de que ℓ no divida a a_2 es $1 - 1/\ell$, tenemos una probabilidad aun mayor de que ℓ^e divida a d. Este análisis muestra que es muy probable que d sea igual a N. Luego de algunas iteraciones, el algoritmo debería recuperar el valor de k.

Complejidad del algoritmo MOV

Para terminar con esta parte, analizaremos la complejidad de cada uno de los pasos necesarios para llevar a cabo el algoritmo MOV. Para ello, probaremos que todos los métodos involucrados, exceptuando el cálculo de índices, requieren de tiempo polinomial. Esto implica que la dificultad del algoritmo se encuentra esencialmente en resolver el PLD en $\mathbb{F}_{q^m}^\times$.

En primer lugar, detallaremos un algoritmo auxiliar que nos permitirá calcular potencias de elementos dentro de un grupo. Este método es conocido con nombres como *exponenciación rápida* o algoritmo de *duplicar-y-sumar*, entre otros.

Algoritmo 3.3.4. *Sea G un grupo. Dados $g \in G$ y n un número natural, el siguiente algoritmo calcula g^n en menos de $2\log_2(n)$ operaciones en G.*

(1) Escribimos la expansión binaria de n como

$$n = \epsilon_0 + \epsilon_1 \cdot 2 + \epsilon_2 \cdot 2^2 + \ldots + \epsilon_r \cdot 2^r,$$

con $\epsilon_i \in \{0, 1\}$, donde asumimos que $\epsilon_r = 1$.

(2) Calculamos $g_i = g^{2^i}$ para $0 \leq i \leq r$, donde cada elemento se obtiene a partir del anterior elevando al cuadrado.

(3) Ponemos $h = 1$, $i = 0$.

(4) Ponemos $h = g_i^{\epsilon_i} \cdot h$ e $i = i + 1$.

(5) Si $i \leq r$, repetimos el paso (4). Si $i = r + 1$, devolvemos el valor de h, que es igual a g^n.

Demostración. En el paso *(2)*, realizamos $r = \log_2(n)$ operaciones en G. Luego, en el paso *(4)*, realizamos una operación si $\epsilon_i = 1$, y ninguna si $\epsilon_i = 0$. Más aun, en el caso $i = 0$ no hacemos ninguna operación, ya que el valor de g es conocido. Luego, a lo sumo estaremos haciendo r multiplicaciones en G, con lo cual el algoritmo requiere de a lo sumo $2r = 2\log_2(n)$ operaciones en el grupo.

Para ver que calcula el valor de g^n, simplemente notamos que el valor final de h es

$$\prod_{i=0}^{r} g_i^{\epsilon_i} = \prod_{i=0}^{r} g^{\epsilon_i 2^i} = g^{\epsilon_0 + \epsilon_1 \cdot 2 + \epsilon_2 \cdot 2^2 + \ldots + \epsilon_r \cdot 2^r} = g^n. \qquad \square$$

Regresando al algoritmo MOV, para comenzar debemos saber cómo calcular el orden de un elemento de $E(\mathbb{F}_q)$. El siguiente resultado de teoría de grupos proporciona un método para hallarlo.

Lema 3.3.5. *Sea G un grupo finito y $\alpha \in G$. Sea $\{p_1, p_2, \ldots, p_r\}$ el conjunto de primos que dividen al exponente de G. Entonces α tiene orden n si y solo si*

$$\alpha^n = 1 \quad y \quad \alpha^{n/p_i} \neq 1 \text{ para todo } 1 \leq i \leq r \text{ tal que } p_i \mid n.$$

Algoritmo 3.3.6. *Sea G un grupo finito de exponente $N = \prod_{i=1}^{r} p_i^{\beta_i}$, y sea $\alpha \in G$. El siguiente algoritmo calcula el orden de α.*

(1) Ponemos $n = 1$ e $i = 1$.

(2) Ponemos $b = \alpha^{N/p_i^{\beta_i}}$.

(3) Mientras $b \neq 1$, ponemos $n = n \cdot p_i$ y $b = b^{p_i}$.

(4) Cuando $b = 1$:

(5) Si $i \leq r - 1$, ponemos $i = i + 1$ y volvemos al paso (2).

(6) Si $i = r$, se devuelve el valor de n.

Demostración. Sea $n = \prod_{i=1}^{r} p_i^{\gamma_i}$ la factorización en primos del valor de n devuelto en el paso *(6)*. Llamando $b_i = \alpha^{N/p_i^{\beta_i}}$, por el Lema 3.3.5 tenemos que el orden de b_i es $p_i^{\gamma_i}$. Entonces

$$1 = b_i^{p_i^{\gamma_i}} = \alpha^{(N/p_i^{\beta_i}) \cdot p_i^{\gamma_i}},$$

con lo cual el orden de a divide a

$$s_i = p_i^{\gamma_i} \cdot (N/p_i^{\beta_i}) = p_i^{\gamma_i} \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{\beta_j}.$$

Luego, el orden de α divide al máximo común divisor de los s_i, que es n. Esto prueba que $\alpha^n = 1$. Ahora, si p_i divide a n, resulta

$$a^{N/p_i} = a^{(N/p_i^{\beta_i}) \cdot p_i^{\beta_i - 1}} = b_i^{p_i^{\beta_i - 1}} \neq 1,$$

así que por el Lema 3.3.5, el orden de α es n. □

Observación 3.3.7. El algoritmo anterior también funciona si N es un múltiplo del exponente del grupo, es decir, si únicamente pedimos que $g^N = 1$ para todo $g \in G$.

Proposición 3.3.8. *El Algoritmo 3.3.6 requiere de $O(\log^3(N))$ operaciones en el grupo G.*

Demostración. La cantidad de operaciones necesarias para calcular el valor de b en el paso *(2)* del algoritmo es $O(\log(N) - \beta_i \log(p_i))$ usando el Algoritmo 3.3.4. Para cada $1 \leq i \leq r$, el paso *(4)* se realiza a lo sumo β_i veces, y en cada iteración realizamos $O(\log(p_i))$ multiplicaciones, con lo cual en este paso se realizan $O(\log(N))$ multiplicaciones en G. Como la cantidad de primos que dividen a N es $O(\log(N))$, se sigue que la cantidad de operaciones realizadas en G es $O(\log^3(N))$. □

En el caso que estamos estudiando, para poder aplicar el Algoritmo 3.3.6 se requiere conocer el exponente de $E(\mathbb{F}_q)$. Por el Teorema 1.6.7, sabemos que

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z},$$

donde n_1 divide a n_2, con lo cual n_2 es el exponente buscado. Pero este teorema no nos provee de ningún método para calcular los enteros n_1 y n_2. Los siguientes algoritmos, debidos a R. Schoof [Sch85] y V. Miller [Mil04], nos permiten determinar la estructura de grupo de $E(\mathbb{F}_q)$ y, en particular, su exponente. El algoritmo de Miller determina dicha estructura a partir del orden del grupo, con lo cual nos concentraremos primero en resolver este problema, mediante el algoritmo de Schoof.

Supongamos que tenemos una curva elíptica E definida sobre $\mathbb{F}_q$ por la ecuación

$$E: \quad y^2 = x^3 + Ax + B.$$

Queremos hallar $\#E(\mathbb{F}_q) = q + 1 - a$, para lo cual buscamos determinar el valor de a. Sea $S = \{2, 3, 5, \ldots, L\}$ un conjunto de primos tales que

$$\prod_{\ell \in S} \ell > 4\sqrt{q}.$$

Como la longitud del intervalo de Hasse (es decir, el intervalo $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$) es $4\sqrt{q}$, si podemos determinar a módulo ℓ para todo $\ell \in S$, entonces conoceremos su valor por el teorema chino del resto.

Sea ℓ primo. Por simplicidad, asumimos que ℓ es coprimo con q, y que q es impar.

Para $\ell = 2$, si $x^3 + Ax + B$ tiene una raíz $e \in \mathbb{F}_q$, entonces $(e, 0) \in E(\mathbb{F}_q)$ y, por la Observación 1.1.6, resulta que $(e, 0) \in E[2]$, con lo cual $E(\mathbb{F}_q)$ tiene orden par. Esto implica que a es par. Por el contrario, si x^3+Ax+B no tiene raíces en $\mathbb{F}_q$, entonces $E(\mathbb{F}_q)$ no tiene elementos de orden 2, con lo cual a es impar. Observemos que, para decidir si x^3+Ax+B tiene raíces en $\mathbb{F}_q$, podemos hacer algo mejor que probar todos los elementos de $\mathbb{F}_q$. Como todo $\alpha \in \mathbb{F}_q$ es una raíz del polinomio $x^q - x \in \mathbb{F}_q[x]$, podemos utilizar el algoritmo de Euclides para decidir si el polinomio cúbico $x^3 + Ax + B$ tiene raíces en $\mathbb{F}_q$, simplemente calculando

$$\mathrm{mcd}(x^q - x, x^3 + Ax + B).$$

Más aun, para evitar trabajar con el polinomio x^q, cuyo grado puede ser demasiado grande, podemos calcular $x_q \equiv x^q \pmod{x^3 + Ax + B}$ aplicando el Algoritmo 3.3.4, y usar esto para obtener el máximo común divisor buscado, ya que

$$\mathrm{mcd}(x^q - x,\ x^3 + Ax + B) = \mathrm{mcd}(x_q - x,\ x^3 + Ax + B).$$

Para el caso $\ell > 2$, se utilizan los *polinomios de división*, que procedemos a definir.

Definición 3.3.9. Sea E una curva elíptica dada por la ecuación de Weierstrass

$$E: \quad y^2 = x^3 + Ax + B.$$

Definimos los *polinomios de división* $\psi_n \in \mathbb{Z}[x, y, A, B]$ como

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

La siguiente propiedad de los polinomios de división se deduce inductivamente de la definición.

Lema 3.3.10. *Si n es impar, entonces ψ_n es un polinomio en $\mathbb{Z}[x, y^2, A, B]$, mientras que si n es par, ψ_n es un polinomio en $2y\mathbb{Z}[x, y^2, A, B]$.*

Considerando a ψ_n como función en E, podemos reemplazar y^2 por $x^3 + Ax + B$, así que para n impar podemos ver a ψ_n como polinomio en $\mathbb{Z}[x, A, B]$. Cuando n es par, debemos considerar ψ_n^2 para que esta reescritura sea posible. En cualquiera de los dos casos, podemos escribir a ψ_n^2 como un polinomio en la variable x.

La principal propiedad del polinomio de división ψ_n es que caracteriza a los puntos de n-torsión, ya que dado $(x, y) \in E(\bar{\mathbb{F}}_q)$, se tiene

$$(x, y) \in E[n] \quad \text{si y solo si} \quad \psi_n^2(x) = 0.$$

Ahora veremos cómo se involucran los polinomios de división en el algoritmo de Schoof. Consideremos el endomorfismo de Frobenius $\phi_q(x, y) = (x^q, y^q)$. Por el Teorema 1.6.2, sabemos que se cumple la ecuación

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

Dado un punto (x_0, y_0) de orden ℓ, obtenemos

$$(x_0^{q^2}, y_0^{q^2}) + [q](x_0, y_0) = [a](x_0^q, y_0^q), \tag{3.3.1}$$

y podemos reescribir

$$[q](x_0, y_0) = [q_\ell](x_0, y_0) \quad \text{donde } q_\ell \equiv q \ (\text{mód } \ell),\ 0 \leq q_\ell < \ell.$$

De manera similar, podemos calcular $[a](x_0^q, y_0^q)$ reduciendo $a \equiv a_\ell \ (\text{mód } \ell)$. De este modo, es posible obtener todos los términos en (3.3.1), excepto el valor de a_ℓ. Como queremos resolver la ecuación (3.3.1) para todos los puntos de ℓ-torsión simultáneamente, utilizamos el polinomio de división $\psi_\ell(x) \in \mathbb{F}_q[x]$. La clave está en notar que la igualdad (3.3.1) se cumple para todos los puntos (x_0, y_0) de orden ℓ si y solo si se tiene la igualdad

$$(x^{q^2}, y^{q^2}) + [q_\ell](x, y) = [a_\ell](x^q, y^q), \tag{3.3.2}$$

donde todos los polinomios involucrados son reducidos en el anillo

$$R_\ell = \frac{\mathbb{F}_q[x, y]}{(\psi_\ell(x), y^2 - x^3 - Ax - B)}.$$

Más precisamente, podemos usar las fórmulas para la suma de puntos sobre la curva dadas en la Definición 1.1.3 para expresar el lado izquierdo de (3.3.2) en términos de funciones racionales en x e y, y luego reducir estas expresiones en el anillo R_ℓ. Así, cada vez que obtenamos una potencia de y, intercambiamos y^2 por $x^3 + Ax + B$. Además, $\psi_\ell(x)$ tiene grado $\frac{1}{2}(\ell^2 - 1)$, hecho que se deduce de las relaciones de recurrencia que cumple (recordemos que sus raíces son todas las posibles coordenadas x de los puntos de ℓ-torsión no nulos; esto implica que dichas raíces son simples). Así, cada vez que tengamos una potencia x^n con $n \geq \frac{1}{2}(\ell^2 - 1)$, podemos cambiarla por el resto en la división por $\psi_\ell(x)$.

Los polinomios de división pueden calcularse explícitamente utilizando la Definición 3.3.9, con lo cual no hay mayores dificultades en llevar a cabo el procedimiento anterior. Con las reducciones en el anillo R_ℓ, siempre trabajamos con polinomios de grado a lo sumo $\frac{1}{2}(\ell^2 - 3)$.

Utilizando las fórmulas para la operación de grupo en la curva, podemos verificar para qué valor de $0 \leq r \leq \ell - 1$ se cumple la ecuación

$$(x^{q^2}, y^{q^2}) + [q_\ell](x, y) = [r](x^q, y^q), \tag{3.3.3}$$

comparando las coordenadas resultantes (que serán funciones racionales) al hacer las operaciones a cada lado de la igualdad y reducir en R_ℓ. El valor de r que cumpla esta

ecuación será $r = a_\ell$. En efecto, si r hace que valga la igualdad, restando las ecuaciones (3.3.2) y (3.3.3), obtenemos

$$0 = [a_\ell - r](x^q, y^q).$$

Como (x^q, y^q) también es de ℓ-torsión si (x, y) lo es, esto implica que ℓ divide a $a_\ell - r$.

Resumimos a continuación el funcionamiento de este algoritmo.

Algoritmo 3.3.11 (Schoof). *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Sea p la característica de $\mathbb{F}_q$. El siguiente algoritmo calcula el valor de $\#E(\mathbb{F}_q) = q + 1 - a$.*

(1) Elegimos un conjunto de primos $S = \{2, 3, 5, \ldots, L\}$ tal que $p \notin S$ y además $\prod_{\ell \in S} \ell > 4\sqrt{q}$.

(2) Para $\ell = 2$, tenemos $a \equiv 0 \pmod 2$ si y solo si $\operatorname{mcd}(x^q - x,\ x^3 + Ax + B) \neq 1$. Llamamos $r_2 = a \pmod 2$.

(3) Para cada primo impar $\ell \in S$:

(I) Calculamos $q_\ell \equiv q \pmod \ell$.

(II) Ponemos $r = 0$.

(III) En el anillo R_ℓ, si

$$(x^{q^2}, y^{q^2}) + [q_\ell](x, y) = [r](x^q, y^q),$$

llamamos $r = r_\ell$ y pasamos al siguiente primo en S. Si no, ponemos $r = r + 1$ y repetimos este paso.

(4) Aplicamos el teorema chino del resto para encontrar el único entero a que satisface $|a| \leq 2\sqrt{q}$ y $a \equiv r_\ell \pmod \ell$, para todo $\ell \in S$. Así, $\#E(\mathbb{F}_q) = q + 1 - a$.

La complejidad del algoritmo de Schoof es polinomial, como veremos a continuación. Para probarlo, necesitaremos estimar el tamaño del conjunto de primos S. Esto puede hacerse gracias al Teorema de los números primos, el resultado central en la teoría de distribución de primos.

Teorema 3.3.12 (Teorema de los números primos). *Sea $\pi(x)$ la cantidad de primos positivos menores o iguales que x. Entonces*

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1.$$

Equivalentemente,

$$\lim_{x \to \infty} \frac{1}{x} \sum_{\ell \leq x} \log \ell = 1,$$

donde ℓ recorre los primos menores o iguales que x.

Demostración. Ver [Apo13, Capítulo 13]. La equivalencia de las dos formulaciones puede verse en [Apo13, Teorema 4.4]. □

Proposición 3.3.13 (Complejidad del algoritmo de Schoof)**.** *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. El algoritmo anterior calcula $\#E(\mathbb{F}_q)$ en $O((\log q)^8)$ pasos.*

Demostración. Verificamos que la complejidad es correcta calculando la cantidad de pasos necesaria para cada parte del algoritmo.

(a) El mayor primo ℓ utilizado en el algoritmo cumple $\ell = O(\log q)$: Por el Teorema de los números primos, obtenemos

$$\lim_{x\to\infty} \frac{1}{x} \sum_{\ell \leq x} \log \ell = 1,$$

y por lo tanto $\prod_{\ell<x} \ell \approx e^x$. Para que este producto sea mayor que $4\sqrt{q}$, basta con tomar $x \approx \log(4\sqrt{q}) = \frac{1}{2}\log(16q)$.

(b) Las multiplicaciones necesarias en el anillo R_ℓ requieren de $O(\ell^4(\log q)^2)$ operaciones: En el anillo R_ℓ, todas las operaciones serán entre polinomios de grado a lo sumo $\frac{1}{2}(\ell^2 - 3)$. Luego, los elementos de R_ℓ son polinomios de grado $O(\ell^2)$, y la multiplicación de dos de ellos y su reducción módulo $\psi_\ell(x)$ requiere de $O(\ell^4)$ operaciones elementales (sumas y multiplicaciones) sobre $\mathbb{F}_q$. Cada multiplicación en $\mathbb{F}_q$ consume $O((\log q)^2)$ operaciones, con lo cual los cálculos en R_ℓ requieren de $O(\ell^4(\log q)^2)$ pasos.

(c) Se requieren $O(\log q)$ operaciones de anillo en R_ℓ para reducir $x^q, y^q, x^{q^2}, y^{q^2}$: En general, el Algoritmo 3.3.4 nos permite calcular x^n, y^n realizando $O(\log n)$ multiplicaciones en R_ℓ.

De la parte *(a)*, obtenemos que la parte *(b)* requiere de $O((\log q)^6)$ operaciones. Además, el valor de $[n](x^q, y^q)$ puede obtenerse con $O(1)$ operaciones en R_ℓ a partir del valor de $[n-1](x^q, y^q)$. Esto prueba que el algoritmo de Schoof requiere de

$$O(\log q)O((\log q)^6)O(\log q) = O((\log q)^8)$$

operaciones. □

Una vez calculado el orden de $E(\mathbb{F}_q)$ mediante el algoritmo de Schoof, podemos determinar la estructura de dicho grupo con el algoritmo de Miller.

Algoritmo 3.3.14 (Miller)**.** *El siguiente algoritmo calcula la estructura de grupo de $E(\mathbb{F}_q)$, a partir de su orden.*

(1) Sea $N = \#E(\mathbb{F}_q)$. Se calcula $r = \mathrm{mcd}(N, q-1)$. Se descompone $N = N_0 N_1$, donde N_0 y N_1 son coprimos, y un primo divide a N_0 si y solo si divide a r.

(2) Se eligen $P, Q \in E(\mathbb{F}_q)$ de manera equiprobable e independiente. Se definen $P' = N_1 P$, $Q' = N_1 Q$.

(3) *Se encuentra el orden de P' y Q', digamos s y t respectivamente (en este paso se necesita la factorización de r).*

(4) *Llamando $m = \mathrm{mcm}(s,t)$, se calcula $\zeta = e_m(P', Q')$.*

(5) *Se calcula el orden de ζ, que llamaremos d. Si $md = N_0$, entonces la estructura del grupo es*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/(N/d)\mathbb{Z}.$$

Si no, se regresa al paso (2).

Antes de ver cómo llevar a cabo cada uno de los pasos, probaremos que este algoritmo efectivamente calcula la estructura del grupo de puntos $\mathbb{F}_q$-racionales.

Lema 3.3.15. *Sea G un grupo abeliano finito, y supongamos que*

$$G \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/e\mathbb{Z}.$$

Sean P, Q generadores independientes de G, de órdenes d y e respectivamente. Sea $M = \mathrm{mcm}(d,e)$ el exponente de G. Si m es un entero, entonces el subgrupo

$$G[m] = \{g \in G : m \cdot g = 0\}$$

está generado por $d'P$ y $e'Q$, donde

$$d' = \frac{d}{\mathrm{mcd}(d,m)}, \quad e' = \frac{e}{\mathrm{mcd}(e,m)}.$$

Proposición 3.3.16. *Supongamos que $G = E(\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/dd'\mathbb{Z}$. Sean $P, Q \in G$, de órdenes s y t, respectivamente. Llamamos $m = \mathrm{mcm}(s,t)$. Entonces $\mathrm{ord}(e_m(P,Q))$ divide a $\mathrm{mcd}(d,m)$, con igualdad si y solo si P y Q generan $G[m]$.*

Demostración. Sean P_0, Q_0 generadores independientes de G, de órdenes $\mathrm{ord}(P_0) = d$ y $\mathrm{ord}(Q_0) = dd'$. Llamamos

$$\eta = e_{dd'}(P_0, Q_0) = e_d(P_0, d'Q_0),$$

donde la última igualdad es por la compatibilidad del emparejamiento. Como P_0 y $d'Q_0$ son independientes, por la no-degeneración tenemos que $\mathrm{ord}(\eta) = d$. Por el Lema 3.3.15, el subgrupo $G[m]$ está generado por

$$P_1 = \frac{d}{\mathrm{mcd}(d,m)} P_0, \quad Q_1 = \frac{dd'}{\mathrm{mcd}(dd',m)} Q_0.$$

En este caso, como m es el mínimo común múltiplo de los órdenes de P y Q, debe dividir al exponente de G, que es dd'. Esto implica que $\mathrm{mcd}(dd', m) = m$. Así, nuevamente por la compatibilidad, obtenemos

$$\begin{aligned} \eta^{d/\mathrm{mcd}(d,m)} &= e_{dd'}(P_1, Q_0) \\ &= e_{\mathrm{mcd}(d,m)}\left(P_1, \frac{dd'}{\mathrm{mcd}(d,m)} Q_0\right) \\ &= e_{\mathrm{mcd}(d,m)}\left(P_1, \frac{m}{\mathrm{mcd}(d,m)} Q_1\right). \end{aligned}$$

Llamemos $\zeta = e_m(P_1, Q_1)$. Luego, por la compatibilidad deducimos

$$\zeta = e_{\mathrm{mcd}(d,m)}\left(P_1, \frac{m}{\mathrm{mcd}(d,m)}Q_1\right) = \eta^{d/\,\mathrm{mcd}(d,m)},$$

así que $\mathrm{ord}(\zeta) = \mathrm{mcd}(d, m)$.

Finalmente, si $P = a_1P_1 + b_1Q_1$ y $Q = a_2P_1 + b_2Q_1$, entonces

$$e_m(P, Q) = \zeta^{a_1b_2 - a_2b_1},$$

por la bilinealidad y antisimetría del emparejamiento. El orden de este elemento divide a $\mathrm{ord}(\zeta) = \mathrm{mcd}(d, m)$, y la igualdad se cumple si y solo si

$$\mathrm{mcd}(a_1b_2 - a_2b_1, \mathrm{mcd}(d, m)) = 1,$$

es decir, si P y Q generan $G[m]$. □

Proposición 3.3.17. *Sea E un curva elíptica definida sobre $\mathbb{F}_q$. Sea G un subgrupo de $E(\mathbb{F}_q)$, y sean $P, Q \in G$. Sea $m = \mathrm{mcd}(\mathrm{ord}(P), \mathrm{ord}(Q))$. Entonces P y Q son generadores de G si y solo si*

$$m\,\mathrm{ord}(e_m(P, Q)) = |G|.$$

En tal caso, llamando $d = \mathrm{ord}(e_m(P, Q))$ tenemos que

$$G \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Demostración. Supongamos que $G \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/dd'\mathbb{Z}$. Entonces m es un divisor de dd'. Luego, si

$$m\,\mathrm{ord}(e_m(P, Q)) = |G| = d^2d',$$

entonces $\mathrm{ord}(e_m(P, Q)) \geq d$. Pero, por la Proposición 3.3.16, se tiene que $\mathrm{ord}(e_m(P, Q))$ divide a $\mathrm{mcd}(d, m)$. Debemos tener entonces las igualdades

$$\mathrm{ord}(e_m(P, Q)) = d = \mathrm{mcd}(d, m),$$

y por lo tanto P y Q generan $G[m]$.

Recíprocamente, si P y Q generan G, entonces

$$m = \mathrm{mcm}(\mathrm{ord}(P), \mathrm{ord}(Q)) = dd',$$

ya que el lado izquierdo de la última igualdad es el orden del subgrupo generado por P y Q. Por la Proposición 3.3.16, tenemos

$$\mathrm{ord}(e_m(P, Q)) = \mathrm{ord}(e_{dd'}(P, Q)) = \mathrm{mcd}(d, m) = \mathrm{mcd}(d, dd') = d,$$

de modo que

$$m\,\mathrm{ord}(e_m(P, Q)) = d^2d' = |G|.$$ □

Este último resultado es la clave para el Algoritmo 3.3.14. Procedemos a probar que dicho algoritmo efectivamente calcula la estructura del grupo de puntos $\mathbb{F}_q$-racionales.

Proposición 3.3.18. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. El Algoritmo 3.3.14 calcula correctamente la estructura del grupo $E(\mathbb{F}_q)$.*

Demostración. Por el Teorema 1.6.7, tenemos que

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z},$$

donde n_1 divide a n_2 y a $q-1$. Bastará probar que $d = n_1$.

Siguiendo la notación del Algoritmo 3.3.14, consideramos el subgrupo

$$G = N_1 E(\mathbb{F}_q) \leqslant E(\mathbb{F}_q).$$

Como n_1 divide a $q-1$ y a $N = \#E(\mathbb{F}_q)$, resulta que n_1 divide a $r = \mathrm{mcd}(N, q-1)$. De esto se deduce que $\mathrm{mcd}(n_1, N_1) = 1$, y por lo tanto

$$G = N_1 E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/(n_2/N_1)\mathbb{Z}.$$

Por construcción, los puntos P', Q' son elementos de G, que tiene orden

$$|G| = n_1 \frac{n_2}{N_1} = \frac{N}{N_1} = N_0.$$

Luego, la Proposición 3.3.17 implica que P' y Q' son generadores de G, ya que

$$m \,\mathrm{ord}(e_m(P', Q')) = md = N_0.$$

Más aun, es

$$G \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z},$$

y por lo tanto $d = n_1$. □

Detallaremos ahora cómo llevar a cabo el Algoritmo 3.3.14. En primer lugar, debemos dar la descomposición de $N = \#E(\mathbb{F}_q)$.

Algoritmo 3.3.19. *Dados enteros $N, r \geq 1$, el siguiente algoritmo devuelve enteros $N_0, N_1 \geq 1$ tales que $N = N_0 N_1$, $\mathrm{mcd}(N_0, N_1) = \mathrm{mcd}(r, N_1) = 1$ y cualquier divisor primo de N_0 divide a r. Dicha descomposición es única.*

(1) Ponemos $N_0 = 1$ y $N_1 = N$.

(2) Calculamos $s = \mathrm{mcd}(r, N_1)$. Si $s = 1$, devolvemos N_0, N_1.

(3) Si $s \neq 1$, ponemos $N_0 = N_0 s$ y $N_1 = N_1/s$, y volvemos al paso (2).

Observación 3.3.20. La unicidad de la descomposición es independiente del algoritmo.

Demostración. Para probar que la descomposición es única, supongamos

$$N = N_0 N_1 = N_0' N_1'.$$

Podemos reescribir esta última igualdad como

$$\frac{N_0}{N_0'} = \frac{N_1'}{N_1}.$$

Si existe algún primo que divide al numerador o al denominador del lado izquierdo de la igualdad, entonces ese primo debe dividir a r. Pero dicho primo no puede dividir al denominador ni al denominador del lado derecho, ya que r es coprimo con N_1 y N_1'. Concluimos que ambos lados deben ser iguales a 1.

Es claro que el algoritmo devuelve enteros N_0, N_1 tales que $N_0 N_1 = N$. Además, si el algoritmo concluye en el paso *(2)*, entonces $\mathrm{mcd}(r, N_1) = 1$. Veamos que también se tiene $\mathrm{mcd}(N_0, N_1) = 1$. Si no fuese así, tomemos ℓ primo que divide a $\mathrm{mcd}(N_0, N_1)$. Luego, ℓ no puede dividir a r, ya que este es coprimo con N_1. Además, si N_0^e denota el valor de N_0 en el paso anterior del algoritmo, tenemos

$$N_0 = N_0^e \,\mathrm{mcd}(r, N_1^e).$$

Debemos tener entonces que ℓ divide a N_0^e ya que no puede dividir a $\mathrm{mcd}(r, N_1^e)$. Si repetimos este razonamiento, llegaremos a que ℓ divide al valor inicial de N_0, que es igual a 1.

Por último, si ℓ es un primo que divide a N_0, debe dividir a $\mathrm{mcd}(r, N_1)$ para alguno de los valores intermedios de N_1. Luego, ℓ divide a r. □

Proposición 3.3.21. *El Algoritmo 3.3.19 requiere de $O(\log_2 \mathrm{máx}(r, N) \log_2(N))$ pasos.*

Demostración. El algoritmo de Euclides para calcular el máximo común divisor requiere de $O(\log_2 \mathrm{máx}(r, N_1)) = O(\log_2 \mathrm{máx}(r, N))$ pasos. Además, en cada ejecución del paso *(3)*, existe algún primo que divide a N_1 cuya potencia se reduce en al menos uno. Luego, este último paso se realiza a lo sumo $\log_2 N_1 = O(\log_2(N))$ veces, y tenemos la complejidad estipulada. □

La elección de puntos en $E(\mathbb{F}_q)$ de manera equiprobable e independiente puede hacerse mediante el siguiente algoritmo.

Algoritmo 3.3.22. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$, dada por la ecuación de Weierstrass*

$$E: \quad y^2 = x^3 + Ax + B.$$

(1) Se elige $x_0 \in \mathbb{F}_q \cup \{\infty\}$ uniformemente.

(2) Si $x_0 = \infty$, con probabilidad $1/2$ se toma el punto $\mathcal{O} \in E(\mathbb{F}_q)$, y con probabilidad $1/2$ se regresa al paso (1).

(3) Si no existe $y_0 \in \mathbb{F}_q$ tal que $(x_0, y_0) \in E(\mathbb{F}_q)$, se regresa al paso (1).

(4) Si la ecuación cuadrática

$$y^2 = {x_0}^3 + Ax_0 + B$$

tiene dos raíces en $\mathbb{F}_q$, se elige una de ellas de manera equiprobable.

(5) Si $x_0^3 + Ax_0 + B = 0$, con probabilidad $1/2$ se toma el punto $(x_0, 0) \in E(\mathbb{F}_q)$, y con probabilidad $1/2$ se regresa al paso (1).

Por el Teorema de Hasse 1.6.1, se tiene que $\#E(\mathbb{F}_q) \geq q + 1 - 2\sqrt{q}$, con lo cual hay al menos

$$\frac{q + 1 - 2\sqrt{q}}{2}$$

valores de $x_0 \in \mathbb{F}_q \cup \{\infty\}$ que producirán un punto en $E(\mathbb{F}_q)$. De esto deducimos que la probabilidad de que el valor de x_0 elegido en el paso *(1)* produzca un punto en $E(\mathbb{F}_q)$ es al menos

$$\frac{q + 1 - 2\sqrt{q}}{2(q+1)} = \frac{1}{2} - \frac{\sqrt{q}}{q+1}.$$

Si el valor de q es grande, la probabilidad de hallar un punto mediante este procedimiento es aproximadamente $\frac{1}{2}$. Luego de algunas iteraciones, deberíamos obtener un punto de la curva definido sobre $\mathbb{F}_q$.

Para resolver la ecuación cuadrática en tiempo polinomial, podemos usar un algoritmo como el dado por Rabin en [Rab80]. A grandes rasgos, el algoritmo encuentra raíces de polinomios $f \in \mathbb{F}_q[x]$ calculando en primer lugar el máximo común divisor

$$f_1(x) = \operatorname{mcd}(f(x), x^{q-1} - 1),$$

para saber si f tiene efectivamente raíces en $\mathbb{F}_q$. Luego, se elige un elemento $\alpha \in \mathbb{F}_q$ al azar, y se calcula el máximo común divisor

$$f_\alpha(x) = \operatorname{mcd}(f_1(x), (x + \alpha)^{\frac{q-1}{2}} - 1).$$

Si $0 < \deg(f_\alpha) < \deg(f_1)$, se define $f_2 = f_\alpha$ o $f_2(x) = f_1/f_\alpha$, dependiendo de si $\deg(f_\alpha) \leq \frac{1}{2}\deg(f_1)$ o no, respectivamente. Si $f_\alpha = 1$ o $f_\alpha = f_1$, se elige un nuevo $\alpha \in \mathbb{F}_q$. Como el grado de los polinomios se reduce al menos a la mitad en cada paso, se necesitan a lo sumo $\log_2(\deg(f))$ pasos hasta encontrar un factor lineal de $f(x)$. En el caso que estamos analizando, el polinomio a factorizar es cuadrático, así que el algoritmo logra encontrar una raíz en el primer paso, si $f_\alpha \neq 1,\ f_\alpha \neq f_1$. Rabin muestra que la probabilidad de que esto ocurra es $\frac{1}{2}$, con lo cual la cantidad esperada hasta obtener una raíz con este algoritmo es de dos intentos.

Por último, necesitamos calcular el emparejamiento de Weil. Esto puede hacerse mediante un algoritmo que requiere de tiempo lineal, también dado por Miller [Mil04]. El método hace uso de una definición equivalente a la que dimos en el Teorema 1.4.13 para el emparejamiento.

Definición 3.3.23. Sean $P, Q \in E[n]$. Sean f_P, f_Q funciones racionales en E tales que

$$\operatorname{div}(f_P) = n(P) - n(\mathcal{O}) \quad \text{y} \quad \operatorname{div}(f_Q) = n(Q) - n(\mathcal{O}).$$

Entonces el emparejamiento de Weil entre P y Q puede calcularse como

$$e_n(P, Q) = \frac{f_P(Q + S) f_Q(-S)}{f_P(S) f_Q(P - S)},$$

donde $S \in E$ es cualquier punto de la curva que cumpla $S \notin \{\mathcal{O}, P, -Q, P - Q\}$ (esto garantiza que todos los valores involucrados para el cálculo estén definidos y sean no nulos).

La demostración de que las dos definiciones dadas para el emparejamiento son equivalentes es muy técnica, con lo cual no la daremos aquí. Los detalles pueden verse en [Was03, Sección 11.6].

Antes de explicar el algoritmo, damos un resultado auxiliar.

Proposición 3.3.24. *Sea E una curva elíptica definida sobre K y sean $P = (x_P, y_P), Q = (x_Q, y_Q) \in E(\bar{K})$, con $P, Q \neq \mathcal{O}$. Sea λ la pendiente de la recta que pasa por P y Q, o la pendiente de la recta tangente a E que pasa por P si $P = Q$ (si la recta es vertical, tomamos $\lambda = \infty$). Definimos una función $g_{P,Q}$ en E como*

$$g_{P,Q} = \begin{cases} \frac{y - y_P - \lambda(x - x_P)}{x + x_P + x_Q - \lambda^2} & \text{si } \lambda \neq \infty, \\ x - x_P & \text{si } \lambda = \infty. \end{cases}$$

Entonces

$$\operatorname{div}(g_{P,Q}) = (P) + (Q) - (P + Q) - (\mathcal{O}). \tag{3.3.4}$$

Demostración. Supongamos primero que $\lambda \neq \infty$ y sea $y = \lambda x + \nu$ la recta que pasa por P y Q, o la recta tangente a E que pasa por P si $P = Q$. Esta recta interseca a la curva en los puntos $P, Q, -P - Q$, así que

$$\operatorname{div}(y - \lambda x - \nu) = (P) + (Q) + (-P - Q) - 3(\mathcal{O}).$$

Por otra parte, las rectas verticales que intersecan a E lo hacen en puntos que son inversos entre sí, con lo cual

$$\operatorname{div}(x - x_{P+Q}) = (P + Q) + (-P - Q) - 2(\mathcal{O}).$$

Deducimos entonces que la función

$$g_{P,Q} = \frac{y - \lambda x - \nu}{x - x_{P+Q}}$$

tiene el divisor dado en (3.3.4). La fórmula para la suma de puntos dada en la Definición 1.1.3 nos dice que $x_{P+Q} = \lambda^2 - x_P - x_Q$, y usando que $\nu = y_P - \lambda x_P$ obtenemos la expresión dada para $g_{P,Q}$.

En el caso $\lambda = \infty$, tenemos $P + Q = \mathcal{O}$. La función $x - x_P$ tiene divisor

$$\operatorname{div}(x - x_P) = (P) + (-P) - 2(\mathcal{O}),$$

que es exactamente el divisor dado en (3.3.4). □

Procedemos ahora con el algoritmo de Miller que permite calcular las funciones racionales involucradas en la definición alternativa del emparejamiento de Weil.

Algoritmo 3.3.25. *Sea $n \geq 1$ y escribamos su expansión binaria como*

$$n = \epsilon_0 + \epsilon_1 \cdot 2 + \epsilon_2 \cdot 2^2 + \ldots + \epsilon_t \cdot 2^t \quad \text{con } \epsilon_i \in \{0, 1\} \text{ y } \epsilon_t \neq 0.$$

El siguiente algoritmo devuelve una función f_P con divisor

$$\operatorname{div}(f_P) = n(P) - ([n]P) - (n-1)(\mathcal{O}),$$

donde las funciones $g_{T,T}$ y $g_{T,P}$ utilizadas se corresponden con las dadas en la Proposición 3.3.24. En particular, si P es de n-torsión, obtenemos

$$\operatorname{div}(f_P) = n(P) - n(\mathcal{O}).$$

(1) Ponemos $T = P$ y $f = 1$.

(2) Para $i = t - 1$ hasta 0:

(3) Ponemos $f = f^2 \cdot g_{T,T}$ y $T = 2T$.

(4) Si $\epsilon_i = 1$, ponemos $f = f \cdot g_{T,P}$ y $T = T + P$. Si $\epsilon_i = 0$, ponemos $i = i - 1$.

(5) Cuando termina el ciclo iniciado en (2), se devuelve el valor de f.

Demostración. Analizaremos el efecto de realizar el ciclo en i en los pasos *(2)* y *(3)* del algoritmo. Llamemos T_i^s y f_i^s a los valores de las variables T y f al principio de este ciclo, y supongamos que los valores finales son T_i^e y f_i^e. Aplicando los pasos *(2)* y *(3)* al punto T, obtenemos

$$T_i^e = 2T_i^s + \epsilon_i \cdot P.$$

Similarmente, teniendo en cuenta que el valor de T es duplicado en el paso *(3)*, para f resulta

$$f_i^e = (f_i^s)^2 \cdot g_{T_i^s, T_i^s} \cdot g_{2T_i^s, P}^{\epsilon_i}.$$

Por lo tanto, los divisores de f_i^s y f_i^e cumplen la relación

$$\begin{aligned}
\operatorname{div}(f_i^e) &= 2\operatorname{div}(f_i^s) + \operatorname{div}(g_{T_i^s, T_i^s}) + \epsilon_i \operatorname{div}(g_{2T_i^s, P}) \\
&= 2\operatorname{div}(f_i^s) + \big(2(T_i^s) - (2T_i^s) - (\mathcal{O})\big) + \epsilon_i\big((2T_i^s) + (P) - (2T_i^s + P) - (\mathcal{O})\big) \\
&= 2\operatorname{div}(f_i^s) + 2(T_i^s) - (2T_i^s + \epsilon_i P) + \epsilon_i(P) - (1 + \epsilon_i)(\mathcal{O}) \\
&= 2\operatorname{div}(f_i^s) + 2(T_i^s) - (T_i^e) + \epsilon_i(P) - (1 + \epsilon_i)(\mathcal{O}).
\end{aligned}$$

Dado que $T_i^e = T_{i-1}^s$ y $f_i^e = f_{i-1}^s$, esto nos permite deducir relaciones de recurrencia para los valores de T_i y f_i, dadas por

$$\begin{aligned}
T_{i-1}^s - 2T_i^s &= \epsilon_i P \\
\operatorname{div}(f_{i-1}^s) - 2\operatorname{div}(f_i^s) &= 2(T_i^s) - (T_{i-1}^s) + \epsilon_i(P) - (1 + \epsilon_i)(\mathcal{O}).
\end{aligned}$$

Usando sumas telescópicas en estas relaciones, los valores finales resultan ser $T_0^e = nP$ y $\operatorname{div}(f_0^e) = n(P) - ([n]P) - (n-1)(\mathcal{O})$. □

Notar que, para cada valor de i, los pasos *(2)* y *(3)* requieren cada uno a lo sumo dos multiplicaciones de funciones, y una suma de puntos sobre la curva. La cantidad de pasos necesaria para llevar a cabo el algoritmo es entonces $O(\log_2(n))$, y por lo tanto requiere de tiempo lineal.

Capítulo 4

El grado de inmersión

El principal inconveniente a la hora de llevar a cabo el algoritmo MOV es que el grado de inmersión m sea demasiado grande, en cuyo caso el PLD en el grupo $\mathbb{F}_{q^m}^{\times}$ resulta tan difícil como en el grupo $E(\mathbb{F}_q)$. En este capítulo estudiaremos primero un caso particular en el cual el algoritmo MOV resulta altamente efectivo, y luego estimaremos la cantidad de curvas elípticas definidas sobre un cuerpo finito para las cuales este algoritmo resulta subexponencial.

4.1. El caso supersingular

Definición 4.1.1. Sea p primo y $q = p^r$. Sea E una curva elíptica definida sobre $\mathbb{F}_q$, con $\#E(\mathbb{F}_q) = q + 1 - a$. Decimos que E es *supersingular* si p divide a a.

Por el Teorema 1.6.6, una curva elíptica E definida sobre $\mathbb{F}_q$ es supersingular si y solo si $a^2 \in \{0, q, 2q, 3q, 4q\}$. La estructura de grupo de $E(\mathbb{F}_q)$ en estos casos está dada por el siguiente resultado.

Lema 4.1.2. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = q + 1 - a$.*

- *Si $a^2 = q, 2q$ o $3q$, entonces $E(\mathbb{F}_q)$ es cíclico.*
- *Si $a^2 = 4q$, entonces*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z},$$

  con signo positivo si $a = -2\sqrt{q}$, y negativo si $a = 2\sqrt{q}$.

- *Si $a = 0$ y $q \not\equiv 3$ (mód 4), entonces $E(\mathbb{F}_q)$ es cíclico. Si $a = 0$ y $q \equiv 3$ (mód 4), entonces $E(\mathbb{F}_q)$ es cíclico o $E(\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/((q+1)/2)\mathbb{Z}$.*

Demostración. Ver [Sch87, Lema 4.8] □

Veremos ahora una proposición que proporciona condiciones necesarias y suficientes para que todos los puntos de N-torsión estén definidos sobre $\mathbb{F}_q$. Establecemos primero un resultado que usaremos durante la demostración.

Lema 4.1.3. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$ y sea N coprimo con q. Entonces la aplicación*

$$\mathrm{End}_{\mathbb{F}_q}(E)/[N]\,\mathrm{End}_{\mathbb{F}_q}(E) \longrightarrow \mathrm{End}(E[N])$$

es inyectiva.

Demostración. La restricción de $\mathrm{End}_{\mathbb{F}_q}(E)$ en $\mathrm{End}(E[N])$ está bien definida, ya que dados $\phi \in \mathrm{End}(E)$ y $P \in E[N]$, tenemos que

$$[N]\phi(P) = \phi([N]P) = \phi(\mathcal{O}) = \mathcal{O}.$$

Es claro que si $\phi \in [N]\,\mathrm{End}(E)$, entonces su restricción es nula. Además, si la restricción de ϕ a $E[N]$ es el endomorfismo nulo, entonces

$$\ker[N] \subseteq \ker\phi,$$

con lo cual la aplicación

$$\mathrm{End}_{\mathbb{F}_q}(E)/[N]\,\mathrm{End}_{\mathbb{F}_q}(E) \longrightarrow \mathrm{End}(E[N])$$

resulta bien definida.

Por otra parte, como N es coprimo con q, por el Lema 1.2.17 sabemos que $[N]$ es separable, y aplicando el Corolario 1.2.10, deducimos que existe $\psi \in \mathrm{End}(E)$ tal que

$$\phi = \psi \circ [N].$$

Como ψ y $[N]$ conmutan, esto prueba que $\phi \in [N]\,\mathrm{End}(E)$, así que el núcleo de la restricción es exactamente $[N]\,\mathrm{End}(E)$, y el resultado sigue. □

Proposición 4.1.4. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$ y $N \in \mathbb{N}$ coprimo con q. Sea ϕ_q el endomorfismo de Frobenius de E y sea a su traza. Entonces $E[N] \subseteq E(\mathbb{F}_q)$ si y solo si se cumplen las siguientes condiciones:*

(1) $N^2 \mid \#E(\mathbb{F}_q)$,

(2) $N \mid q-1$,

(3) $\phi_q \in \mathbb{Z}$, *o bien*

$$\mathcal{O}\left(\frac{a^2-4q}{N^2}\right) \subseteq \mathrm{End}(E),$$

donde $\mathcal{O}\left(\frac{a^2-4q}{N^2}\right)$ denota al orden cuadrático de discriminante $\frac{a^2-4q}{N^2}$.

Demostración. Veamos primero que $E[N] \subseteq E(\mathbb{F}_q)$ si y solo si $\phi_q - 1 \in [N]\,\mathrm{End}(E)$. En efecto, si $E[N] \subseteq E(\mathbb{F}_q) = \ker(\phi_q - 1)$, por el Lema 4.1.3 resulta que $\phi_q - 1 \in [N]\,\mathrm{End}(E)$.

Recíprocamente, si $\phi_q - 1 = [N]\psi$ con $\psi \in \mathrm{End}(E)$, dado $P \in E[N]$ tenemos

$$[N]\psi(P) = \psi([N]P) = \psi(\mathcal{O}) = \mathcal{O},$$

con lo cual

$$E[N] \subseteq \ker([N]\psi) = \ker(\phi_q - 1) = E(\mathbb{F}_q).$$

Bastará ver entonces que $\phi_q - 1 \in [N]\operatorname{End}(E)$ si y solo si se cumplen las condiciones del enunciado.

Supongamos que $\phi_q - 1 = [N]\psi$. Tomando grado en esta igualdad y aplicando el Teorema 1.2.13, tenemos que N^2 divide a $\deg(\phi_q - 1) = \#E(\mathbb{F}_q)$. Además, por el Corolario 1.4.16, resulta que $\mu_N \subseteq \mathbb{F}_q^\times$, y por lo tanto N divide a $q-1$. Como

$$\phi_q^2 - a\phi_q + q = 0, \tag{4.1.1}$$

sabemos que

$$([N]\psi + 1)^2 - a([N]\psi + 1) + q = ([N]\psi)^2 + (2-a)[N]\psi + q + 1 - a = 0.$$

Pero $\#E(\mathbb{F}_q) = q + 1 - a$ es divisible por N^2, y a su vez

$$2 - a = \#E(\mathbb{F}_q) - (q-1),$$

así que N divide a $2-a$. De esto último deducimos la igualdad

$$\psi^2 + \frac{2-a}{N}\psi + \frac{q+1-a}{N^2} = 0.$$

Como el discriminante del polinomio $x^2 + \frac{2-a}{N}x + \frac{q+1-a}{N^2}$ es

$$\left(\frac{2-a}{N}\right)^2 - 4 \cdot \frac{q+1-a}{N^2} = \frac{a^2-4q}{N^2}.$$

Luego, si $\phi_q \notin \mathbb{Z}$, esto implica que $\mathcal{O}\left(\frac{a^2-4q}{N^2}\right) \subseteq \operatorname{End}(E)$.

Para la otra implicación, supongamos primero que $\phi_q \in \mathbb{Z}$. De la igualdad (4.1.1) deducimos que

$$2\phi_q = a \quad \text{y} \quad \phi_q^2 = q.$$

Entonces, por *(1)*, resulta que

$$N^2 \mid \#E(\mathbb{F}_q) = q + 1 - a = \phi_q^2 - 2\phi_q + 1 = (\phi_q - 1)^2,$$

y por lo tanto N divide a $\phi_q - 1$. Esto prueba que $\phi_q - 1 \in [N]\operatorname{End}(E)$.

Por último, si $\mathcal{O}\left(\frac{a^2-4q}{N^2}\right) \subseteq \operatorname{End}(E)$, como $\frac{\phi_q - 1}{N}$ es raíz del polinomio

$$x^2 + \frac{2-a}{N}x + \frac{q+1-a}{N^2},$$

cuyo discriminante es $\frac{a^2-4q}{N^2}$, la Proposición 2.2.8 implica que $\frac{\phi_q-1}{N} \in \operatorname{End}(E)$. □

Corolario 4.1.5. *Sea E una curva elíptica supersingular definida sobre $\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = q + 1 - a$. Sea N el exponente de $E(\mathbb{F}_q)$.*

1. *Si* $a^2 = q$, *entonces* $E[N] \subseteq E(\mathbb{F}_{q^3})$.
2. *Si* $a^2 = 2q$, *entonces* $E[N] \subseteq E(\mathbb{F}_{q^4})$.
3. *Si* $a^2 = 3q$, *entonces* $E[N] \subseteq E(\mathbb{F}_{q^6})$.
4. *Si* $a^2 = 4q$, *entonces* $E[N] \subseteq E(\mathbb{F}_q)$.
5. *Si* $a = 0$, *entonces* $E[N] \subseteq E(\mathbb{F}_{q^2})$.

En particular, el grado de inmersión de E *con respecto a* N *es menor o igual que* 6.

Demostración. En todos los casos, el exponente de $E(\mathbb{F}_q)$ está dado por el Lema 4.1.2, y mediante un cálculo directo se prueba que se cumplen las tres condiciones de la Proposición 4.1.4. El morfismo de Frobenius correspondiente siempre resulta ser entero, con lo cual no tenemos que verificar la condición sobre el orden cuadrático.

Desarrollaremos el caso $a^2 = q$ para ilustrar la situación, los demás son análogos. Supongamos entonces que $a = \mp\sqrt{q}$. Por el Lema 4.1.2, el grupo $E(\mathbb{F}_q)$ es cíclico, con

$$\#E(\mathbb{F}_q) = q + 1 \pm \sqrt{q},$$

así que el exponente del grupo es

$$N = q + 1 \pm \sqrt{q}.$$

Aplicando el Teorema 1.6.2, podemos calcular el orden de $E(\mathbb{F}_{q^3})$ como

$$\#E(\mathbb{F}_{q^3}) = q^3 + 1 - \alpha^3 - \beta^3,$$

donde

$$\alpha + \beta = a = \mp\sqrt{q} \quad \text{y} \quad \alpha\beta = q.$$

Como

$$\begin{aligned}\alpha^3 + \beta^3 &= (\alpha+\beta)^3 - 3\alpha\beta(\alpha+\beta) = (\pm\sqrt{q})^3 - 3q(\mp\sqrt{q}) \\ &= \pm\sqrt{q}^3 \pm 3\sqrt{q}^3 = \pm 2\sqrt{q}^3,\end{aligned}$$

resulta que

$$\#E(\mathbb{F}_{q^3}) = q^3 + 1 \mp 2\sqrt{q}^3 = (\sqrt{q}^3 \mp 1)^2.$$

Calculamos

$$N^2(\sqrt{q} \mp 1)^2 = (q + 1 \pm \sqrt{q})^2(\sqrt{q} \mp 1)^2 = (\sqrt{q}^3 \mp 1)^2,$$

y por lo tanto $N^2 \mid \#E(\mathbb{F}_{q^3})$. Además,

$$N(q^2 \mp \sqrt{q}^3 \pm \sqrt{q} - 1) = (q \pm \sqrt{q} + 1)(q^2 \mp \sqrt{q}^3 \pm \sqrt{q} - 1) = q^3 - 1,$$

de modo que $N \mid q^3 - 1$. Por último, del Teorema 1.6.2 resulta que

$$\phi_{q^3}^2 - (\pm 2\sqrt{q}^3)\phi_{q^3} + q^3 = (\phi_{q^3} \mp \sqrt{q}^3)^2 = 0.$$

Usando que el grado de los endomorfismos es multiplicativo, esta última igualdad implica que

$$\deg(\phi_{q^3} \mp \sqrt{q}^3) = 0,$$

y por lo tanto

$$\phi_{q^3} = \pm\sqrt{q}^3 \in \mathbb{Z}.$$

Esto prueba que se cumplen las tres condiciones, así que $E[N] \subseteq E(\mathbb{F}_{q^3})$. □

4.2. Condiciones para que MOV sea subexponencial

En la sección anterior, probamos que las curvas supersingulares tienen malas propiedades desde el punto de vista criptográfico, ya que el algoritmo MOV permite resolver el PLD en tiempo subexponencial. En el caso general, el algoritmo MOV traslada el problema del logaritmo discreto a $\mathbb{F}_{q^m}^\times$, donde vimos que el cálculo de índices funciona con una cantidad de pasos

$$O(\exp(c(\log q^m)^{1/3}(\log\log q^m)^{2/3}).$$

Para que el algoritmo MOV resulte subexponencial en este contexto, es suficiente que $m \leq \log^2 q$. Si este fuese el caso para una gran cantidad de curvas elípticas, estaríamos ante un problema desde el punto de vista criptográfico, ya que podría resultar difícil elegir una curva en la cual el PLD no pueda ser resuelto en la práctica.

En esta última parte, estudiaremos la probabilidad de que una curva elíptica seleccionada al azar cumpla con esta condición.

Recordemos que el emparejamiento de Weil nos permite trasladar el PLD de una curva elíptica al grupo de unidades de un cuerpo finito, siempre y cuando todos los puntos de torsión correspondientes estén definidos sobre dicho cuerpo. En la práctica, suelen utilizarse puntos de ℓ-torsión, donde ℓ es primo. Nos concentraremos especialmente en este caso.

Teorema 4.2.1. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$, y supongamos que ℓ es un primo que divide a $N = \#E(\mathbb{F}_q)$, pero ℓ no divide a $q-1$. Entonces $E[\ell] \subseteq E(\mathbb{F}_{q^k})$ si y solo si ℓ divide a $q^k - 1$.*

Demostración. Si $E[\ell] \subseteq E(\mathbb{F}_{q^k})$, resulta que $\mu_\ell \subseteq \mathbb{F}_{q^k}^\times$ por el Corolario 1.4.16; más aun, como es un subgrupo, deducimos que ℓ divide a $q^k - 1$.

Recíprocamente, si ℓ divide a $q^k - 1$, en particular ℓ no divide a q, así que por la Proposición 1.3.2, existen ℓ^2 puntos de ℓ-torsión en $E(\bar{\mathbb{F}}_q)$. Sea r tal que $E[\ell] \subseteq E(\mathbb{F}_{q^r})$ (podemos tomar a r como el grado de inmersión, pero no será necesario). Sea $P \in E(\mathbb{F}_q)$ un punto de orden ℓ, el cual existe ya que ℓ divide a $N = \#E(\mathbb{F}_q)$. Consideramos $Q \in E(\mathbb{F}_{q^r})$ tal que $\{P, Q\}$ sea una base de $E[\ell]$.

Si ϕ_q denota al endomorfismo de Frobenius en $E(\mathbb{F}_{q^r})$, tenemos que $\phi_q(P) = P$, ya que este punto está definido sobre $\mathbb{F}_q$. Resulta entonces que, en la base $\{P, Q\}$, la matriz

de ϕ_q es de la forma

$$[\phi_q] = \begin{pmatrix} 1 & * \\ 0 & q \end{pmatrix},$$

por el Lema 1.2.17 y la Proposición 1.4.18. Por hipótesis, $q \not\equiv 1 \pmod{\ell}$, así que esta matriz tiene dos autovalores distintos, y por lo tanto es diagonalizable. Por otro lado, la matriz de $\phi_{q^k} = \phi_q^k$ es de la forma

$$[\phi_{q^k}] = \begin{pmatrix} 1 & * \\ 0 & q^k \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

ya que $q^k \equiv 1 \pmod{\ell}$. Como $[\phi_{q^k}]$ también es diagonalizable, debe ser la identidad. Esto implica que $Q \in E(\mathbb{F}_{q^k})$ por el Lema 1.2.18. Como $P \in E(\mathbb{F}_q) \subseteq E(\mathbb{F}_{q^k})$, concluímos que todos los puntos de orden ℓ están definidos sobre $\mathbb{F}_{q^k}$. □

El teorema anterior muestra que, en la práctica, es necesario y suficiente que ℓ divida a $q^k - 1$ para que el grado de inmersión de E con respecto a ℓ sea menor o igual que k. ya que suele evitarse el caso en que ℓ divide a $q - 1$. Esto se debe a que, si así fuese, entonces $\mu_\ell \subseteq \mathbb{F}_q^\times$, con lo cual podríamos trasladar el PLD a $\mathbb{F}_q^\times$.

Ahora bien, ¿cuál es la probabilidad de que ℓ divida a $q^k - 1$? En lo que sigue, daremos una respuesta a esta pregunta para el caso en que la curva está definida sobre $\mathbb{F}_p$. De este modo, podremos aplicar los resultados vistos en el Capítulo 2 para estimar la cantidad total de curvas. Comenzamos con un lema auxiliar.

Lema 4.2.2. *Sean h un entero par no nulo y k un número natural. Entonces $h^k - 1$ tiene menos que $2\log(|h|^k)$ divisores primos distintos.*

Demostración. Factorizando en primos,

$$h^k - 1 = \pm \prod_{j=1}^{r} p_j^{\alpha_j}, \tag{4.2.1}$$

donde $p_1, \ldots, p_r$ son todos los primos positivos que dividen a $h^k - 1$. Aplicando módulo y logaritmo a ambos lados de esta igualdad, resulta que

$$\log(|h^k - 1|) = \sum_{j=1}^{r} \alpha_j \log(p_j) \geq \sum_{j=1}^{r} \log(p_j) > \sum_{j=1}^{r} 1 = r,$$

donde la última desigualdad se debe a que $h^k - 1$ es impar, de modo que $p_j \geq 3$ para todo $j = 1, \ldots, r$. Supongamos ahora que $r \geq \log(|h|^k)$, lo cual es equivalente a que $e^r \geq |h|^k$. De (4.2.1) se deduce inmediatamente que

$$|h^k - 1| \geq 3^r.$$

Entonces

$$|h^k - 1| \geq 3^r \geq e^r \geq |h|^k,$$

así que la única posibilidad es que $h^k < 0$ y $r = 1$. Pero esto implica que $k = 1$ y $h = -2$, y en este caso $h^k - 1 = -3$ tiene menos de $2\log(|h|^k) = 2\log(2)$ divisores primos distintos. □

Notación 4.2.3. Sean x, y enteros coprimos. Denotaremos al orden multiplicativo de x módulo y como $\mathrm{ord}_y(x)$.

En todos los resultados que siguen, M y K representan constantes positivas.

Lema 4.2.4. *Sea $A_{M,K}$ el conjunto de pares ordenados (p, ℓ) de primos impares tales que $|p - \ell| \leq 2\sqrt{M}$ y $\mathrm{ord}_\ell(p) \leq K$. Entonces*

$$\#A_{M,K} \leq 2K^2\sqrt{M}\log(4M).$$

Demostración. Sea $\mathcal{H}$ el conjunto de enteros pares no nulos h tales que $|h| \leq 2\sqrt{M}$. Para cada $h \in \mathcal{H}$, denotamos B_h al conjunto de primos que dividen a $h^k - 1$ para algún $k \leq K$. Por el Lema 4.2.2, se sigue que

$$\#B_h \leq 2\sum_{k=1}^{K} k\log|h| \leq K(K+1)\log(2\sqrt{M}) \leq K^2\log(4M).$$

Sumando sobre los elementos de $\mathcal{H}$, obtenemos

$$\sum_{h\in\mathcal{H}} \#B_h \leq 2K^2\sqrt{M}\log(4M).$$

Ahora, para cada $h \in \mathcal{H}$, consideramos el subconjunto de $A_{M,K}$ que consiste de los pares (p, y) con $p - \ell = h$. Como $(p, \ell) \in A_{M,K}$, existe $k \leq K$ tal que y divide a $p^k - 1$, lo cual implica que ℓ divide a $h^k - 1$, ya que

$$h^k - 1 = (p-\ell)^k - 1 = p^k - 1 + \sum_{i=0}^{k-1}\binom{k}{i}p^i(-\ell)^{k-i},$$

y esta última sumatoria es divisible por ℓ. Deducimos que $\ell \in B_h$, así que la cantidad de pares $(p, \ell) \in A_{M,K}$ con $p - \ell = h$ es menor o igual que $\#B_h$. Por lo tanto,

$$\#A_{M,K} \leq \sum_{h\in\mathcal{H}} \#B_h,$$

y se sigue la desigualdad buscada. □

Lema 4.2.5. *Sea S_M el conjunto de pares de primos (p, ℓ) tales que $M/2 \leq p \leq M$ y $|p + 1 - \ell| \leq \sqrt{p}$. Entonces, para una constante efectivamente computable c_1 y M suficientemente grande, se tiene*

$$\#S_M \geq c_1\frac{M^{3/2}}{\log^2(M)}.$$

Demostración. Supongamos primero que M es de la forma $M = 4m^2$, donde m es un entero positivo. Subdividimos el intervalo $(M/2, M]$ en $2m$ subintervalos de la forma $((i-1)m, im]$, con $2m < i \leq 4m$. Sea $A = \pi(M) - \pi(M/2)$, la cantidad de primos en el intervalo $(M/2, M]$, y sea A_i la cantidad de primos en el i-ésimo subintervalo. Por el Teorema de los números primos, si M es suficientemente grande, tenemos

$$\frac{M}{3\log(M)} < A.$$

Ahora bien, si p e ℓ son primos en el mismo subintervalo, entonces el par (p, ℓ) pertenece a S_M, ya que $|p - \ell|$ es un entero menor que m, y por lo tanto tenemos

$$|p + 1 - \ell| \leq |p - \ell| + 1 \leq m - 1 + 1 = m = \sqrt{M}/2 \leq \sqrt{p}.$$

En cada subintervalo podemos formar A_i^2 pares de primos, de modo que

$$\sum_{i=2m+1}^{4m} A_i^2 \leq \#S_M.$$

Además, el valor mínimo de $\sum A_i^2$, sujeto a la condición $\sum A_i = A$, se obtiene cuando todos los sumandos son iguales, esto es, cuando $A_i = \frac{A}{2m}$. De lo anterior se desprende la desigualdad buscada:

$$\#S_M \geq \sum_{i=2m+1}^{4m} A_i^2 \geq \sum_{i=2m+1}^{4m} \left(\frac{A}{2m}\right)^2 = \frac{A^2}{M} 2m = \frac{A^2}{\sqrt{M}} > \frac{M^{3/2}}{9\log^2(M)}.$$

Veamos ahora que basta probar el resultado para el caso $M = 4m^2$. En efecto, consideremos el mínimo entero positivo m tal que $4m^2 \geq M$. Entonces tenemos

$$\frac{(4m^2)^{3/2}}{\log^2(4m^2)} \geq \frac{M^{3/2}}{\log^2(M)}. \tag{4.2.2}$$

Por lo probado anteriormente,

$$\#S_{4m^2} \geq \frac{(4m^2)^{3/2}}{9\log^2(4m^2)}. \tag{4.2.3}$$

Demostraremos que existe una constante $C > 0$ tal que

$$\#S_M + CM \geq \#S_{4m^2}.$$

Sea $(p, \ell) \in S = S_{4m^2} \setminus S_M$. Se cumple entonces

$$4(m-1)^2 < M < p \leq 4m^2, \quad p - \sqrt{p} \leq \ell \leq p + \sqrt{p},$$

y por lo tanto hay a lo sumo

$$4m^2 - 4(m-1)^2 = 4m - 1$$

posibilidades para el valor de p, y para cada p hay como máximo

$$2\sqrt{p} \leq 4m$$

posibilidades para ℓ. Luego,

$$\#S \leq (4m-1)(4m) < (4m)^2 = 4M,$$

de lo cual deducimos

$$\#S_M + 4M \geq \#S_{4m^2}. \tag{4.2.4}$$

Combinando las desigualdades (4.2.2), (4.2.3) y (4.2.4) obtenemos

$$\#S_M \geq \frac{M^{3/2}}{\log^2(M)} - 4M.$$

Si M es suficientemente grande, entonces

$$\frac{M^{3/2}}{\log^2(M)} \geq 4M,$$

y por lo tanto existe una constante $c_1 > 0$ tal que

$$\#S_M \geq c_1 \frac{M^{3/2}}{\log^2(M)}. \qquad \square$$

Lema 4.2.6. *Sea S_M definido como en el Lema 4.2.5. Sea $\widetilde{S}_{M,K}$ el conjunto de pares ordenados de primos (p,ℓ) tales que $M/2 \leq p \leq M$, $|p+1-\ell| \leq 2\sqrt{p}$, y además $\mathrm{ord}_\ell(p) \leq K$. Entonces se cumple*

$$\frac{\#\widetilde{S}_{M,K}}{\#S_M} \leq c_2 \frac{K^2 \log^3(M)}{M},$$

para una constante efectivamente computable c_2.

Demostración. Sea $(p,\ell) \in \widetilde{S}_{M,K}$. Entonces $\sqrt{p} \leq \sqrt{M}$, y por lo tanto tenemos la desigualdad

$$|p+1-\ell| \leq 2\sqrt{p} \leq 2\sqrt{M}.$$

Si denotamos $A_{M,K}$ como en el Lema 4.2.4, resulta que $\widetilde{S}_{M,K} \subseteq A_{M,K} \cup B_{M,K}$, donde $B_{M,K}$ es el conjunto de pares de primos (p,ℓ) tales que $M/2 \leq p \leq M$, $\mathrm{ord}_\ell(p) \leq K$ y

$$|p+1-\ell| \leq 2\sqrt{p} \leq 2\sqrt{M} < |p-\ell|.$$

Se sigue que $\ell > p$, y por lo tanto

$$\ell - p - 1 \leq 2\sqrt{p} \leq 2\sqrt{M} < \ell - p,$$

de lo cual se deduce

$$2\sqrt{M} + p < \ell \leq 2\sqrt{M} + p + 1.$$

Luego, si el primo p está fijo, hay a lo sumo un primo ℓ que cumple la desigualdad anterior. Al igual que en el Lema 4.2.5, suponemos que $M = 4m^2$ para cierto entero m. Así, la desigualdad anterior es

$$4m + p < \ell \leq 4m + p + 1,$$

y como p es entero, la única posibilidad es que $\ell = 4m + p + 1$, que es par. Esto prueba que el conjunto $B_{M,K}$ es vacío, y por lo tanto $\#\widetilde{S}_{M,K} \leq \#A_{M,K}$. Luego, el resultado se sigue de los Lemas 4.2.4 y 4.2.5. □

Combinando los resultados anteriores y el Teorema 2.3.20, se obtiene el último resultado de este trabajo, probado por R. Balasubramanian y N. Koblitz en [BK98]. La cota obtenida muestra que es altamente improbable que la dificultad del PLD pueda reducirse utilizando el algoritmo MOV, con lo cual resulta seguro utilizarlas con fines criptográficos.

Teorema 4.2.7. *Sea (p, E) un par (elegido de forma aleatoria) que consiste de un primo p en el intervalo $[M/2, M]$ y una clase de isomorfismo de curvas elípticas E definida sobre $\mathbb{F}_p$ con un número primo ℓ de puntos racionales. La probabilidad de que el grado de inmersión de E con respecto a ℓ sea menor o igual que $\log^2(p)$ es menor que*

$$c_3 \frac{\log^9(M)(\log\log M)^2}{M},$$

para una constante c_3 efectivamente computable.

Demostración. Sea p un primo en el intervalo $[M/2, M]$. Denotamos $\widetilde{S}_p$ al conjunto de primos $\ell \in [p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$ tales que ℓ divide a $p^k - 1$ para algún $k \leq \log^2(p)$, y S_p al conjunto de primos $\ell \in [p+1-\sqrt{p},\ p+1+\sqrt{p}]$. Si p es suficientemente grande, el Teorema de los números primos garantiza que S_p tiene al menos tres elementos.

Por el Teorema 2.3.20, la cantidad de clases de isomorfismo de curvas elípticas E definidas sobre $\mathbb{F}_p$ con $\#E(\mathbb{F}_p) \in \widetilde{S}_p$ es menor o igual que

$$c_4 \cdot \#\widetilde{S}_p \cdot (\log p)(\log\log p)^2\sqrt{p},$$

mientras que la cantidad de clases de isomorfismo con $\#E(\mathbb{F}_p) \in S_p$ es mayor o igual que

$$c_5 \cdot (\#S_p - 2) \cdot \frac{\sqrt{p}}{\log p}.$$

Sumando sobre todos los primos $p \in [M/2, M]$, resulta que hay a lo sumo

$$\sum_{M/2 \leq p \leq M} c_4 \cdot \#\widetilde{S}_p \cdot (\log p)(\log\log p)^2\sqrt{p}$$

clases de isomorfismo de curvas tales que ℓ tiene grado de inmersión menor o igual que $\log^2(p)$, mientras que hay al menos

$$\sum_{M/2\leq p\leq M} c_5 \cdot (\#S_p - 2) \cdot \frac{\sqrt{p}}{\log p}$$

clases de isomorfismo de curvas con un número primo ℓ de puntos racionales. Acotando $M/2 \leq p \leq M$ en ambos casos, la probabilidad de que el grado de inmersión de E con respecto a ℓ sea menor que $\log^2(p)$ es a lo sumo

$$\frac{\left(\sum_{M/2\leq p\leq M} \#\widetilde{S}_p\right) \cdot c_4 \cdot (\log M)(\log\log M)^2\sqrt{M}}{\left(\sum_{M/2\leq p\leq M} \#S_p - 2\right) \cdot c_5 \cdot \frac{\sqrt{M}}{\log M}}. \tag{4.2.5}$$

Pero además sabemos que $\sum_{M/2\leq p\leq M} \#\widetilde{S}_p$ es exactamente la cantidad de pares de primos (p,ℓ) tales que $M/2 \leq p \leq M$ y ℓ divide a $p^k - 1$ para algún $k \leq \log^2(p) \leq \log^2(M)$. Deducimos entonces la desigualdad

$$\sum_{M/2\leq p\leq M} \#\widetilde{S}_p \leq \#\widetilde{S}_{M,\log^2 M}.$$

Por otro lado, tenemos

$$\sum_{M/2\leq p\leq M} (\#S_p - 2) = \sum_{M/2\leq p\leq M} \#S_p - 2(\pi(M) - \pi(M/2)) = \#S_M - 2(\pi(M) - \pi(M/2)).$$

Por el Teorema de los números primos y el Lema 4.2.5, existe una constante $c > 0$ tal que

$$\#S_M - 2(\pi(M) - \pi(M/2)) \geq \#S_M - 2\frac{M}{\log(M)} \geq c \cdot \#S_M.$$

Luego, la expresión (4.2.5) es menor o igual que

$$\frac{c_4 \cdot \#\widetilde{S}_{M,\log^2 M} \cdot (\log^2(M))(\log\log M)^2}{c \cdot c_5 \cdot \#S_M},$$

y el resultado se sigue del Lema 4.2.6 tomando $K = \log^2(M)$. □

Bibliografía

[Adl79] Leonard M. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *20th Annual Symposium on Foundations of Computer Science (SFCS 1979)*, pages 55–60. IEEE, 1979.

[Adl94] Leonard M. Adleman. The function field sieve. In *International Algorithmic Number Theory Symposium*, pages 108–121. Springer, 1994.

[Apo13] Tom M. Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 2013.

[BK98] Ramachandran Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *Journal of cryptology*, 11(2):141–145, 1998.

[BV07] Johannes Buchmann and Ulrich Vollmer. *Binary Quadratic Forms: An Algorithmic Approach (Algorithms and Computation in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2007.

[Cox11] David A. Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[Deu41] Max Deuring. Die typen der multiplikatorenringe elliptischer funktionenkörper. In *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*, volume 14, pages 197–272. Springer, 1941.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[Ful89] William E. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley Publishing Company Advanced Book Program, 1989.

[Har11] Gergely Harcos. Equidistribution on the modular surface and L-functions. *Homogeneous Flows, Moduli Spaces and Arithmetic*, pages 377–387, 2011.

[Har13] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[HPS08] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography*, volume 1. Springer, 2008.

[HW+79] Godfrey Harold Hardy, Edward Maitland Wright, et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

[Kob91] Neal Koblitz. Elliptic curve implementation of zero-knowledge blobs. *Journal of Cryptology*, 4(3):207–213, 1991.

[LJ87] Hendrik W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[Mar77] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York-Heidelberg, 1977. Universitext.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of cryptology*, 17(4):235–261, 2004.

[MOV93] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory*, 39(5):1639–1646, 1993.

[Pol78] John M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of computation*, 32(143):918–924, 1978.

[Pra57] K. Prachar. *Primzahlverteilung*. Grundlehren der mathematischen Wissenschaften. Springer, 1957.

[Rab80] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on computing*, 9(2):273–280, 1980.

[Rüc87] Hans-Georg Rück. A note on elliptic curves over finite fields. *Mathematics of Computation*, 49(179):301–304, 1987.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170):483–494, 1985.

[Sch87] René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of combinatorial theory, Series A*, 46(2):183–211, 1987.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Was03] Lawrence C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2003.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 2(4):521–560, 1969.