UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

CSIDH: Criptografía Postcuántica Basada en Isogenias de Curvas Elípticas

Autora: Blanca Gil Rosell

Director: Dr. Xavier Guitart Morales
Realitzat a: Departament de Matemàtiques i Informàtica

Barcelona, 21 de juny de 2020

Abstract

The aim of this project is to explain, as detailed as possible, how the isogeny-based cryptosystem Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) works from a mathematical point of view. In order to do so, we need to introduce the concept of elliptic curve and give some of their properties, which allow us to establish the basis of this cryptosystem. Furthermore, we also present some notions of Algebraic Number Theory, particularly those that are related to elliptic curves.

Once this theoretical basis is built, we proceed to describe the algorithm, paying special attention to the mathematical components. Finally, using SageMath– a mathematical software which includes elliptic curves implementations– we program the algorithm and check its efficiency by doing several tests.

Resumen

El objetivo de este proyecto es explicar de la forma más detallada posible cómo funciona, desde un punto de vista matemático, el criptosistema basado en isogenias llamado Commutative Supersingular Isogeny Diffie-Hellman (CSIDH). Para llevar a cabo tal propósito necesitamos introducir el concepto de curva elíptica y dar algunas de sus propiedades, cosa que nos permitirá establecer la base de este criptosistema. Además, también presentamos algunos aspectos de Teoría Algebraica de Números, particularmente aquellos que están relacionados con las curvas elípticas.

Una vez la base teórica está construida, procedemos a describir el algoritmo prestando especial atención a los componentes matemáticos. Para acabar, usando SageMath (un software matemático que incluye implementaciones específicas para curvas elípticas) programamos el algoritmo y probamos su eficiencia haciendo varios tests.

2010 Mathematics Subject Classification. 14H52, 14G50, 11T71

Agradecimientos

Para empezar, quiero dar las gracias a mi tutor, el Doctor Xevi Guitart, por su dedicación y atención durante estos últimos meses. Soy consciente que las circunstancias actuales, con la crisis del Covid-19, no han sido las mejores para realizar un trabajo de esta magnitud, pero aún y así ha hecho todo lo posible para ir guiándome mientras ha durado el proceso de investigación y escritura. Por supuesto, también quiero agradecerle haberme hablado del algoritmo CSIDH y toda la "revolución" postcuántica que está sucediendo actualmente; sin esto, y sin sus aclaraciones de aquellos conceptos que no acababa de comprender, este proyecto no hubiese sido posible.

También me gustaría agradecer a mis padres y a mis hermanas el apoyo que me han dado, no solamente durante la ejecución del Trabajo de Fin de Grado sino a lo largo de la carrera.

Finalmente, quiero dar gracias a Johan P Hansen, profesor de la Universidad de Aarhus (Dinamarca), por haberme introducido en el campo de las curvas elípticas y la criptografía. Me gustaría haber podido compartir con él lo que he aprendido durante estos últimos meses. *Tusind tak.*

Índice

1. Introducción **1**

1.1. Un poco de historia 1

1.2. La computación cuántica 2

1.3. Diffie-Hellman 4

1.4. Contexto actual de la criptografía postcuántica 5

1.5. Estructura del trabajo 7

2. Curvas Elípticas **8**

2.1. La Ley de Grupo 8

2.2. Endomorfismos 11

2.3. El invariante j 13

2.4. Puntos de n-torsión 14

2.5. Curvas elípticas sobre cuerpos finitos 15

2.5.1. El endomorfismo de Frobenius 15

2.6. Isogenias 19

3. Teoría algebraica de números **21**

3.1. Cuerpos de números 21

3.2. Enteros algebraicos 22

3.3. Ideales 22

3.4. Factorización de primos 24

4. CSIDH **25**

4.1. Curvas de Montgomery 25

4.2. El algoritmo de intercambio de claves 26

4.3. Verificar que una curva es supersingular 29

4.4. Cómo calcular la acción de un ideal en una curva elíptica 30

4.5. Implementación de los algoritmos 34

5. Conclusiones **37**

A. El código **38**

Referencias **41**

1. Introducción

1.1. Un poco de historia

La **criptografía** es el estudio de las técnicas que permiten comunicarse de forma segura, transformando un mensaje para que alguien no deseado (conocido como **adversario**) no pueda entenderlo.

Actualmente la criptografía juega un papel importante en nuestras vidas, ya que a raíz de la expansión de la informática y las telecomunicaciones han ido surgiendo problemas de seguridad; por ejemplo, al hacer una transacción a través de Internet, nuestros datos pueden ser interceptados por una tercera persona y ser usados de forma fraudulenta. Pero de hecho los orígenes de la criptografía se remontan a tiempos muy antiguos, pues la necesidad de comunicarse sin que los enemigos puedan enterarse ha sido siempre, al parecer, una preocupación de la humanidad. Se han encontrado evidencias de que en el Antiguo Egipto ya se empleaban técnicas criptográficas para ocultar mensajes disponiendo jeroglíficos de una forma distinta a la habitual; también hay indicios del uso de sistemas de encriptación en India, Mesopotamia, la Antigua Grecia y por parte de los romanos.

A estos últimos se les atribuye la invención (por lo menos parecen haber sido los primeros en usarlo) del **cifrado César**, consistente en reemplazar cada letra de un mensaje por otra que se encuentra un número fijo de posiciones más adelante en el alfabeto. El problema de esta técnica, que pertenece al tipo de cifrado conocido como **sustitución monoalfabética**, es que es relativamente fácil de descifrar y en consecuencia no se puede considerar un método muy seguro.

A raíz de este inconveniente, a partir de la Edad Media empezaron a aparecer los métodos de codificación polialfabéticos, más sofisticados y entre los que destaca el **cifrado de Vigenère** (descrito en 1553 por Giovan Battista Bellaso); este en concreto se basa en el uso de una *tabula recta*, una cuadrícula que contiene el alfabeto escrito en todas las filas, cada vez corrido una posición (es decir, en la primera fila se tiene el alfabeto escrito de la A a la Z; en la segunda empezamos por la B, llegamos hasta la Z y al final añadimos la A; para la tercera empezamos por la C y al final añadimos A y B, y así sucesivamente).

Poco a poco la criptografía fue desarrollándose y a principios del siglo XX se inventaron las máquinas de cifrado, que fueron ampliamente usadas durante la Segunda Guerra Mundial y entre las que se encuentra la famosa máquina **Enigma**. Este dispositivo electromecánico consistía en un teclado (como el de una máquina de escribir), un panel luminoso con las letras del alfabeto y tres rotores en paralelo, conectados entre sí y al teclado y al panel. De este modo, cuando el usuario apretaba una tecla, instantáneamente otra letra se iluminaba y así se obtenía el mensaje cifrado. El funcionamiento consistía en lo siguiente: para empezar se fijaban los rotores en una posición previamente establecida y a continuación, cada vez que se apretaba una tecla, el rotor de la derecha se movía una posición, generando así un circuito eléctrico que iluminaba la letra cifrada correspondiente; cuando el cilindro de la derecha había dado ya una vuelta completa, entonces el rotor del medio se movía una posición, y cuando éste había girado ya 360 grados entonces el tercer rotor avanzaba también una posición. Gracias a este ingenioso sistema se consiguió un sofisticado cifrado polialfabético, lo que permitió a los alemanes comunicarse secretamente de forma eficiente.

Con la aparición de los ordenadores la criptografía sufrió un gran cambio: anteriormente se usaba principalmente en ámbitos lingüísticos y lexicográficos, como bien hemos visto,

pero en la era de la información empezó a usarse también para encriptar datos numéricos combinando herramientas matemáticas más avanzadas, informática e ingeniería. En la actualidad podemos clasificar los sistemas criptográficos en dos tipos: los de clave privada y los de clave pública.

La **criptografía de clave privada** (también conocida como criptografía de clave simétrica) usa la misma clave para cifrar y descifrar el mensaje, de modo que emisor y receptor acuerdan una clave de antemano, el remitente encripta el texto que quiere transmitir y lo envía al destinatario, que puede desencriptarlo. El problema de estos métodos es que dependen de la seguridad del canal de transmisión de claves, pues si alguien consiguiese interceptar la clave el mensaje queda al descubierto. El cifrado de César, el de Vigenère y la máquina Enigma son ejemplos de criptosistemas de clave privada.

La **criptografía de clave pública** (o criptografía de clave asimétrica) se basa en el uso de dos claves: una pública, conocida por todo el mundo y que permite a cualquier emisor encriptar un mensaje, y una privada, solamente conocida por el propietario de este par de claves y que permite descifrar todo mensaje codificado usando su clave pública.

Este segundo tipo de criptosistemas son mucho más seguros debido a que no hay necesidad de intercambiar claves y se basan en problemas matemáticos complejos como por ejemplo la factorización de números enteros o el logaritmo discreto[2] pero, precisamente por ser más sofisticados, también son más lentos de calcular.

1.2. La computación cuántica

Los ordenadores clásicos almacenan la información en **bits**, y cada bit tiene únicamente dos valores (o estados) posibles: 0 y 1, de modo que el estado de un ordenador con n bits es una tira de n ceros y unos. Generalmente un bit representa la presencia o ausencia de voltaje eléctrico. Por otro lado, en computación cuántica la unidad mínima de información son los **qubits**, partículas subatómicas como los electrones o los fotones, cuya generación y manejo es mucho más complicada que la de los bits y que está suponiendo un gran reto científico. Los qubits, además, poseen algunas propiedades cuánticas y poco convencionales que permiten que un conjunto de n qubits proporcione una mayor capacidad computacional que un conjunto del mismo tamaño de bits. Dos de estas propiedades son la superposición y el entrelazamiento.

La primera propiedad, la **superposición**, es un principio de la mecánica cuántica que sostiene que un sistema físico puede estar en más de un estado simultáneamente (de hecho, dice que puede estar en todos sus teóricamente posibles estados a la vez). En el caso de los qubits esto se traduce en que sus posibles estados están representados por una combinación lineal del valor 0 y el valor 1 con coeficientes complejos tales que sus cuadrados suman 1; es decir, un único qubit $|\psi\rangle$ viene dado por

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1, \quad \alpha, \beta \in \mathbb{C}$$

donde $\{|0\rangle, |1\rangle\}$ forman la llamada "base computacional" (simplemente es una representación para los valores 0 y 1). Por tanto, podemos pensar en los coeficientes α y β como la "cantidad" de estado 0 y 1 que tiene cada qubit de modo que, si tenemos un

[2]El problema del **logaritmo discreto** consiste en, dado un grupo G y dos enteros $a, b \in G$, hallar k tal que $a = b^k$. Es un problema difícil de resolver computacionalmente si el orden de G es grande, pues en general no existen algoritmos clásicos para encontrar la solución.

ordenador con n qubits, un estado de la máquina vendrá representado por una combinación de todas las posibles colecciones de 0s y 1s, cada una de ellas con un coeficiente asignado que indica cuánto hay de cada combinación. Ilustrémoslo con un ejemplo. Supongamos que tenemos un ordenador (clásico) con 3 bits; entonces, un estado es cualquier combinación de 3 caracteres que pueden ser 1 o 0, como podría ser 001 o 010 o 111, entre los 8 casos posibles, pero sólo se puede estar en un estado a la vez. En un ordenador cuántico de 3 qubits, por lo contrario, un estado viene dado por $a_1000+a_2001+a_3010+a_4011+a_5100+a_6101+a_7110+a_8111$ con $a_i \in \mathbb{C}$ para $i = 1, \ldots, 8$ y $\sum_{i=1}^{8} |a_i|^2 = 1$. De este modo los qubits representan los 8 estados al mismo tiempo: sería como tener 8 ordenadores funcionando uno al lado del otro; en consecuencia, para describir un sistema con n componentes, en el escenario clásico se requieren únicamente n bits mientras que en el caso cuántico se necesitan 2^n números complejos. Debemos remarcar, pero, que en cuanto "medimos" o "miramos" un qubit, éste colapsa en uno de los dos estados base, cada uno de ellos con probabilidad $|\alpha|^2$ y $|\beta|^2$, respectivamente.

Para pasar de un estado a otro, en el caso de los ordenadores clásicos, se aplica una operación lógica (llamada **puerta lógica**) sobre los bits que definen el estado en ese momento; encadenando varias operaciones lógicas formamos un algoritmo, que es lo que nos permite llegar al nuevo estado y hallar la solución del problema que hayamos planteado. En el caso de los ordenadores cuánticos el sistema es parecido: vamos pasando de un estado a otro por medio de operaciones lógicas cuánticas (o **puertas cuánticas**[3]), que también se encadenan creando algoritmos. La clave de todo esto es que cuando hacemos una transformación sobre n qubits de hecho estamos haciendo 2^n operaciones a la vez (una por cada posible combinación de n bits), cosa que aumenta muchísimo la velocidad de cálculo.

La segunda propiedad, el **entrelazamiento**, es un fenómeno cuántico en el cual los estados (cuánticos) de dos o más objetos no pueden describirse independientemente; es decir, un conjunto de objetos entrelazados comparten la misma información y, pese a estar separados físicamente (incluso por millones de kilómetros), si uno de los objetos es modificado los demás sufren la misma alteración. En el caso de los qubits esto significa que cambiar el estado de uno de ellos implica cambiar el estado de otro qubit de una forma predecible, por muy lejos que estén. En consecuencia, gracias a este fenómeno, añadir qubits extra a un ordenador cuántico produce un aumento exponencial en su capacidad de cálculo mientras que en el caso de los ordenadores convencionales duplicar el número de bits "únicamente" supone duplicar su capacidad de procesamiento.

Pero todavía estamos lejos de la computación cuántica. Para producir un qubit primero se necesita un objeto que pueda soportar un estado de superposición cuántica entre dos estados, como por ejemplo el núcleo de un átomo (pues su espín[4]– el momento angular intrínseco, no asociado con giro o movimiento– puede apuntar en diferentes direcciones). Luego hay que crear la superposición, esto es, hay que conseguir que el qubit alcance un equilibrio entre estados; podríamos establecer un paralelismo entre la dificultad de lograr esto y la de conseguir que una moneda se sostenga de canto. Aparte de esto, hay que tener en cuenta que el estado cuántico de los qubits es extremadamente frágil: la más mínima vibración o cambio de temperatura pueden romper esta superposición y es por eso que los qubits deben mantenerse en cámaras frigoríficas con temperaturas rozando el cero absoluto y al vacío.

[3]De hecho, las puertas cuánticas son matrices unitarias con coeficientes complejos.

[4]Para información más detallada, ver [11].

Pese a todo esto, en los últimos años se están invirtiendo muchos esfuerzos y dinero en el desarrollo de la computación cuántica. Algunas de sus prometedoras aplicaciones comprenden desde la simulación del comportamiento de la materia hasta el ya mencionado aumento de la capacidad de cálculo, cosa que pondría en riesgo la seguridad y privacidad electrónica tal y como la conocemos actualmente. Aquí es, pues, donde entra en juego la criptografía postcuántica.

1.3. Diffie-Hellman

El intercambio de claves Diffie-Hellman (inventado por Whitfield Diffie y Martin Hellman en 1976– ver [20]) fue uno de los primeros métodos de encriptación de clave pública y que sigue usándose con frecuencia hoy en día. La motivación de este protocolo surgió a raíz de la necesidad de encontrar una forma segura de que dos personas, sin necesidad de haber tenido un encuentro físico previo, puedan establecer una clave secreta para codificar sus comunicaciones. Debemos remarcar que, debido al coste computacional de este algoritmo, su uso se restringe a generar una clave compartida por los dos usuarios para luego encriptar sus mensajes usando un cifrado de clave simétrica, que es mucho más rápido.

El método empieza con dos usuarios, llamémosles Alice y Bob, que eligen de forma conjunta un número primo p suficientemente grande (para garantizar una mínima seguridad se requiere que p tenga una longitud de 2048 bits por lo menos, lo que equivale a un número de 617 cifras en el sistema decimal). Con este número obtienen el grupo multiplicativo de los enteros módulo p, $\mathbb{Z}/p\mathbb{Z}$, y entonces eligen otro número $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ que sea una raíz primitiva módulo p (en particular g genera un grupo cíclico $\langle g \rangle$, cuyos elementos son las potencias de g). La pareja $\{p, g\}$ es, pues, la clave pública a la que todo el mundo puede tener acceso (en el sentido de que no es secreta). A continuación Alice y Bob eligen, cada uno independientemente y sin compartirlo con nadie, un número entero que será su clave secreta; pongamos a para la de Alice y b para la de Bob.

Llegados a este punto, Alice calcula $A = g^a \pmod p$ y se lo envía a Bob que, a su vez, calcula $B = g^b \pmod p$ y se lo manda a Alice. Entonces Alice, que conoce B, calcula $B^a \pmod p = (g^b)^a \pmod p$ y Bob, cuando ha recibido A, calcula $A^b \pmod p = (g^a)^b \pmod p$. Puesto que $\langle g \rangle$ es conmutativo (pues es cíclico) entonces

$$(g^b)^a \pmod p \equiv g^{ba} \pmod p \equiv g^{ab} \pmod p \equiv (g^a)^b \pmod p$$

y en consecuencia, como ambos Alice y Bob (y nadie más) conocen el número $g^{ab} \pmod p$, podemos tomarlo como su secreto compartido. Esta será, pues, su clave para mandarse mensajes a través de un canal de comunicaciones abierto (es decir, no necesariamente seguro).

La seguridad de este intercambio de claves radica, principalmente, en la dificultad de resolver el problema del logaritmo discreto definido anteriormente. En efecto, conociendo g, $A = g^a$ y $B = g^b$ no hay manera posible de encontrar a y b en un tiempo razonable con las herramientas computacionales actuales siempre y cuando, tal y como ya se ha dicho antes, p sea lo suficientemente grande.

Podemos definir una variante del algoritmo de Diffie-Hellman tomando un grupo abeliano G y un conjunto C cualesquiera y una acción $*$ de G en C. Es decir, consideramos la aplicación

$$\begin{aligned} * : G \times C &\longrightarrow C \\ (g, c) &\longmapsto g * c \end{aligned}$$

que cumple:

1. Para todo $c \in C$, $1_G * c = c$ donde 1_G es el elemento neutro de G.
2. Para todo $c \in C$ y $g_1, g_2 \in G$, $(g_1 g_2) * c = g_1 * (g_2 * c)$.

En este caso, para llevar a cabo el intercambio de claves, Alice y Bob deben acordar una clave pública $c_0 \in C$. Por un lado, Alice elige secretamente su clave privada $a \in G$ y calcula $a * c_0$ mientras que Bob, por su parte, escoge $b \in G$ y calcula $b * c_0$. A continuación intercambian los resultados obtenidos y entonces Alice calcula $a * (b * c_0)$ y Bob $b * (a * c_0)$. Por la propiedad 2 tenemos que $a * (b * c_0) = (ab) * c$ y $b * (a * c_0) = (ba) * c$ y, puesto que el grupo G es conmutativo, $(ab) * c = (ba) * c$. En consecuencia, esta es la clave secreta que comparten y que únicamente ellos dos conocen.

Observemos que en el caso de Diffie-Hellman original, se toma $G = \mathbb{Z}$ y $C = \langle g \rangle$ donde g es una raíz primitiva módulo un primo p acordado previamente y la acción considerada es la exponenciación módulo p.

Un ejemplo de variante de Diffie-Hellman es el protocolo llamado Elliptic-Curve Diffie–Hellman (ECDH– ver [23]), que aprovecha la estructura algebraica de las curvas elípticas y cuya implementación permite obtener resultados con niveles de seguridad similares al del caso de Diffie-Hellman tradicional usando claves de menor tamaño. En este caso C es el conjunto de puntos de una curva elíptica y $G = \mathbb{Z}$.

Actualmente el intercambio de claves de Diffie-Hellman sigue usándose para enviar datos por Internet de forma segura, tomando claves más grandes y complementándolo con un método de autenticación para garantizar la total seguridad, pero parece que la aparición de los ordenadores cuánticos supondría una amenaza para este protocolo gracias a su capacidad de resolver el problema del logaritmo discreto. De hecho, ya en 1994 el matemático Peter Shor inventó un algoritmo (el **algoritmo de Shor**– ver [17]) que permite factorizar números enteros en tiempo polinomial usando un ordenador cuántico. Como consecuencia de esto, y viendo la llegada de las computadoras cuánticas cada vez más cerca, la comunidad científica empezó a investigar para conseguir nuevos métodos de encriptación, resistentes a ataques cuánticos, que puedan sustituir Diffie-Hellman (entre otros). El Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) es uno de los propuestos.

1.4. Contexto actual de la criptografía postcuántica

Tal y como ya hemos comentado anteriormente, la investigación en el campo de la computación cuántica está en auge. Esto implica que, si en algún momento se llegan a construir ordenadores cuánticos a gran escala, muchos de los sistemas criptográficos de clave pública dejarían de ser seguros a causa de la enorme capacidad computacional de estas máquinas del futuro. Por este motivo, muchos científicos empezaron a investigar en la criptografía postcuántica con el objetivo de desarrollar algoritmos criptográficos capaces de resistir ataques tanto de ordenadores convencionales como de ordenadores cuánticos. Con este pretexto, el National Institute of Standards and Technology (NIST) inició, en 2016, un proceso para desarrollar y estandarizar uno o más algoritmos criptográficos de clave pública para reemplazar los actuales que quedarían obsoletos en un futuro con ordenadores cuánticos.

El proceso de selección consta de tres fases, durante las cuales se evalúan los métodos

propuestos y se descartan los que resultan ser menos potentes. Inicialmente se consideraron 69 protocolos, que comprendían criptosistemas basados en retículos, criptosistemas basados en códigos correctores, criptosistemas multivariables, criptosistemas basados en funciones hash y criptosistemas basados en curvas elípticas, entre otros, de los que solamente 26 pasaron a la segunda ronda. Todavía está por saber cuáles quedarán finalmente, aunque está prevista la publicación del resultado final entre 2022 y 2024.

Uno de los protocolos criptográficos basado en isogenias de curvas elípticas propuesto en el NIST es SIKE (Supersingular Isogeny Key Encapsulation), que es una alternativa más sofisticada del esquema SIDH (Supersingular Isogeny Diffie-Hellman). La criptografía basada en isogenias es un tipo de criptografía basado en curvas elípticas relativamente nuevo, cuya seguridad se fundamenta en la dificultad de calcular explícitamente una isogenia entre dos curvas elípticas sobre un cuerpo finito $\mathbb{F}_q$. El hecho de que los ordenadores cuánticos no parecen ser capaces de facilitar la resolución de este problema comporta que este tipo de criptosistemas se encuentren actualmente en el punto de mira (en lo que al campo de la criptografía se refiere).

La primera propuesta de criptosistema basado en isogenias data de 1997 y fue realizada por Jean-Marc Couveignes. En este protocolo de intercambio de claves el espacio de claves públicas es el conjunto de clases de $\mathbb{F}_q$-isomorfismos de curvas elípticas ordinarias definidas sobre $\mathbb{F}_q$, cuyo anillo de endomorfismos es un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario. El hecho de que el grupo de clases de ideales $\mathrm{cl}(\mathcal{O})$ actúa libre y transitivamente sobre este conjunto de clases de $\mathbb{F}_q$-isomorfismos, y gracias a que $\mathrm{cl}(\mathcal{O})$ es conmutativo, permitió a Couveignes definir un intercambio de claves del estilo de Diffie-Hellman. Cabe remarcar, sin embargo, que el trabajo de Couveignes no fue publicado hasta 2006 (ver [9]) y su método fue "redescubierto" independientemente por Alexander Rostovtsev y Anton Stolbunov, que también publicaron su hallazgo ese mismo año. El problema es que en 2010 Andrew M. Childs, David Jao y Vladimir Soukharev demostraron que romper este protocolo criptográfico es equivalente a resolver un caso particular del "abelian hidden-shift problem"[5], para el cual existen algoritmos cuánticos con complejidad temporal de orden subexponencial; aunque todavía está por ver hasta qué punto esto supone una amenaza, hay otro inconveniente y es que el método de Couveignes es extremadamente lento. No obstante, la simplicidad de su algoritmo ha resultado atractiva para la comunidad científica y es por eso que se han intentado desarrollar otros métodos partiendo de la idea de Couveignes.

El ataque propuesto por Childs, Jao y Soukharev se sustenta principalmente en el hecho de que $\mathrm{cl}(\mathcal{O})$ es conmutativo (y, de forma indirecta, en que $\mathcal{O}$ también lo es). Para sortear este obstáculo, a Luca De Feo, David Jao y Jérôme Plût se les ocurrió utilizar curvas elípticas supersingulares, cuyo anillo de endomorfismos es un orden en un álgebra de cuaterniones que, en particular, es no conmutativo. Esto dio lugar al intercambio de claves SIDH, y una variante suya, SIKE, fue presentada a NIST y pasó a la segunda fase.

Debemos remarcar, pero, que SIDH no es una adaptación del método de Couveignes reemplazando curvas ordinarias por curvas supersingulares. Este ajuste, sin embargo, es posible y queda demostrado con la introducción de CSIDH, protocolo descrito en 2018 por Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny y Joost Renes. La idea clave de este método, para sacar partido de la propiedad conmutativa, es considerar las curvas elípticas supersingulares y el subanillo de endomorfismos definidos únicamente

[5]El "abelian hidden-shift problem" consiste en, dado un grupo abeliano G y dos funciones inyectivas $f_0, f_1 : G \to X$ (donde X es un conjunto arbitrario) tales que $f_1(x) = f_0(x+s)$ para todo $x \in G$, encontrar este $s \in G$. Para más detalles, ver [6].

sobre $\mathbb{F}_p$ (y no su clausura algebraica). La ventaja de tal elección es que este (sub)anillo de endomorfismos es isomorfo a un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario, que en particular es conmutativo. Entonces, igual que propuso Couveignes, se tiene que $\mathrm{cl}(\mathcal{O})$ actúa via isogenias sobre el conjunto de clases de $\mathbb{F}_p$-isomorfismos de curvas elípticas cuyo anillo de endomorfismos es isomorfo a $\mathcal{O}$ y contiene el endomorfismo de Frobenius.

Aunque CSIDH no evita el posible ataque de Childs, Jao y Soukharev sí que supone una ventaja respecto al método de Couveignes, y es que es significativamente mucho más eficiente.

1.5. Estructura del trabajo

La finalidad de este proyecto es entender el funcionamiento del protocolo CSIDH (Commutative Supersingular Isogeny Diffie-Hellman): en qué se basa y cómo funciona.

El primer capítulo es la Introducción, que sirve para presentar y motivar el trabajo realizado. Los capítulos 2 y 3 son la base teórica: el Capítulo 2 se centra en las curvas elípticas y se enuncian las propiedades fundamentales necesarias para entender el algoritmo. Los resultados están formulados para curvas elípticas en forma de Weierstrass, que es la más habitual de representar dichas curvas, y la mayoría de ellos no incluyen demostración (pues no es el propósito de este trabajo) pero sí que se indica la referencia para lectores curiosos. El Capítulo 3 contiene una pequeña introducción a la Teoría Algebraica de Números, dando una especial importancia a los cuerpos cuadráticos imaginarios, pues son los que se consideran en el caso de este protocolo criptográfico, y al grupo de clases de ideales.

El Capítulo 4 recoge el objeto de este trabajo: el intercambio de claves CSIDH. En primer lugar se introducen las curvas de Montgomery, que no son más que curvas elípticas definidas de una forma distinta a la de Weierstrass, y son las que se emplean en este protocolo. A continuación se describe el algoritmo. La última sección del capítulo está destinada a explicar cómo he programado los algoritmos usando el software informático SageMath, que contiene funciones específicas para tratar con curvas elípticas, y a comentar los resultados obtenidos; también se presenta un ejemplo de la implementación del algoritmo con el pretexto de evaluar y mostrar la calidad del método.

El último capítulo recoge las conclusiones de este proyecto y, para finalizar, se añade un apéndice que contiene el código del programa escrito para simular el funcionamiento del algoritmo.

2. Curvas Elípticas

Sea K un cuerpo. Una **curva elíptica** E definida sobre K es el conjunto de soluciones (en K) de una ecuación no singular del tipo

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

juntamente con un punto distinguido, el llamado "punto en el infinito" (que explicaremos luego). La ecuación (2.1), donde $a_1, \ldots, a_6 \in K$ son constantes, es conocida como la **ecuación de Weierstrass generalizada** y es especialmente útil si K tiene característica 2 o 3. En caso contrario (es decir, si $\text{char}(K) \notin \{2, 3\}$) podemos simplificar la expresión de la curva mediante un cambio de variables, obteniendo así la llamada **ecuación (corta) de Weierstrass**:

$$y^2 = x^3 + Ax + B. \tag{2.2}$$

Esta expresión más sencilla se obtiene de (2.1) dividiendo entre 2 y completando cuadrados:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

de modo que, tomando $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ y constantes a_2', a_4', a_6', podemos reescribirlo como

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Considerando el cambio de variable $x_1 = x + \frac{a_2'}{3}$ obtenemos

$$y_1^2 = x_1^3 + Ax_1 + B$$

para ciertas constantes $A, B \in K$ que deben cumplir $4A^3 + 27B^2 \neq 0$. Esta condición es indispensable para garantizar que la curva sea no singular, esto es, el polinomio x^3+Ax+B no debe tener raíces múltiples. Efectivamente, si consideramos $r_1, r_2, r_3 \in \overline{K}$ [6] ceros de dicho polinomio entonces

$$x^3 + Ax + B = (x - r_1)(x - r_2)(x - r_3)$$

y dado que el discriminante de la cúbica es

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2),$$

imponiendo $-(4A^3 + 27B^2) \neq 0$ obtenemos $r_i \neq r_j$ si $i \neq j$, es decir, las raíces son distintas.

2.1. La Ley de Grupo

Una de las características más importantes de las curvas elípticas es que su conjunto de puntos forma un grupo abeliano aditivo. Para poder definirlo con precisión debemos introducir unas ideas previas. Sea $\mathbb{P}^2_K$ el plano proyectivo 2-dimensional, que viene dado por las clases de equivalencia de puntos $(x, y, z) \in K \times K \times K$ con al menos una de las coordenadas no nula. Diremos que dos puntos (x_1, y_1, z_1) y (x_2, y_2, z_2) son equivalentes si existe un elemento $\lambda \in K \setminus \{0\}$ tal que $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$ y escribiremos $(x : y : z)$ para denotar la clase de equivalencia de (x, y, z). Observemos, además, que

[6] $\overline{K}$ = clausura algebraica de K. Para más detalles, ver [22].

si $z \neq 0$ entonces $(x : y : z) = (x/z : y/z : 1)$ y estos son los que llamaremos "puntos finitos" de $\mathbb{P}^2_K$. Por lo contrario, los puntos $(x : y : 0)$ seran los "puntos en el infinito". Consideremos también el plano afín sobre K, definido como

$$\mathbb{A}^2_K = \{(x, y) \in K \times K\},$$

de manera que tenemos la inclusión

$$\mathbb{A}^2_K \hookrightarrow \mathbb{P}^2_K$$

dada por $(x, y) \mapsto (x : y : 1)$, con lo cual el plano afín queda identificado con los puntos finitos del plano proyectivo.

Dado un polinomio $f(x, y)$, podemos homogeneizarlo añadiendo las correspondientes potencias de z para obtener un polinomio $F(x, y, z)$ cuyos términos sean todos del mismo grado. En el caso que nos ocupa, tomando la ecuación de Weierstrass de la curva elíptica $E : y^2 = x^3 + Ax + B$, tenemos la correspondiente expresión $y^2z = x^3 + Axz^2 + Bz^3$ escrita de forma homogénea. Los puntos (x, y) de la curva original corresponden a los puntos $(x : y : 1)$ de la curva proyectiva, mientras que los puntos del infinito, los que tienen coordenada $z = 0$, son aquellos tales que $0 = x^3$, es decir, $x = 0$. Como el punto $(0 : 0 : 0)$ no existe, y puede ser cualquier número no nulo y en consecuencia, reescalando, el punto del infinito de la curva elíptica es el que tiene coordenadas $(0 : y : 0) = (0 : 1 : 0)$ y lo denotaremos por ∞. Aunque pueda parecer un poco antinatural, la adición de este punto en la curva elíptica tiene consecuencias muy útiles; podemos imaginárnoslo, pues, como un punto que yace en el extremo superior del eje y, y además impodremos que pertenezca a cualquier recta vertical, de modo que dos rectas verticales cualesquiera, $x = c_1$ y $x = c_2$, se corten en $(0 : 1 : 0)$. El punto ∞, de hecho, representará el elemento neutro del grupo abeliano que forman los puntos de E y con esto podemos definir una curva elíptica sobre un cuerpo K (de característica distinta de 2 y 3) como

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + Ax + B\} \cup \{\infty\}. \tag{2.3}$$

Hablemos ahora de la operación de este grupo: la adición de puntos, que dados dos puntos de E nos permite producir otro punto que sea también de E. La idea básica es la siguiente: empezamos con dos puntos

$$P_1 = (x_1, y_2), \quad P_2 = (x_2, y_2)$$

de una curva elíptica E dada por la ecuación (2.3) y trazamos la línea L que pase por ambos puntos; observaremos que L corta E en un tercer punto, llamémosle $P'_3 = (x_3, y'_3)$. A continuación reflejamos respecto al eje x (eso es, cambiamos el signo de la coordenada y) y esto nos da $P_3 = (x_3, y_3)$. La descripción gráfica puede verse en la Figura 1. Ahora definimos $P_1 + P_2 = P_3$. Para formalizar esta definición hace falta distinguir casos dependiendo de la forma que tengan P_1 y P_2:

- Supongamos que $P_1 \neq P_2$, $x_1 \neq x_2$ y ninguno de los dos es ∞. La línea que pasa por ambos puntos es

  $$y = m(x - x_1) + y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}.$$

  Sustituyendo en $y^2 = x^3 + Ax + B$ obtenemos

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

Observemos que esta ecuación tiene 3 soluciones, que corresponden a las coordenadas x de los tres puntos de intersección de L y E, así que ya conocemos dos de ellos: x_1 y x_2; el tercero, x_3, será la coordenada x de P_3' y, por tanto, también de P_3. En consecuencia,

$$x^3 + Ax + B - (m(x - x_1) + y_1)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Puesto que el coeficiente de x^2 en el término izquierdo de la ecuación es $-m^2$ y en el término derecho es el opuesto de la traza de la cúbica (eso es, $-(x_1 + x_2 + x_3)$), tenemos que

$$-m^2 = -(x_1 + x_2 + x_3)$$

y por tanto

$$x_3 = -x_1 - x_2 + m^2$$

$$y_3' = m(x_3 - x_1) + y_1.$$

Tomando el opuesto de y_3' nos queda $P_3 = (x_3, -m(x_3 - x_1) - y_1)$.

- Si $P_1 \neq P_2$ pero $x_1 = x_2$ entonces la línea que pasa por P_1, P_2 es vertical y en consecuencia no corta E en ningún otro punto finito, sino que la intersección se produce en ∞. En este caso, pues, $P_1 + P_2 = \infty$.

- Si $P_1 = P_2$ y $y_1 = y_2 \neq 0$ entonces tomamos L que sea la recta tangente a E en este punto (que existe pues sabemos que E es no singular). La pendiente de L se calcula fácilmente derivando implícitamente la ecuación de la curva $y^2 = x^3 + Ax + B$:

$$2ydy = (3x^2 + A)dx$$

de modo que, sustituyendo en P_1,

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

La ecuación de L es, pues, $y = m(x - x_1) + y_1$ (como antes) y sustituyendo en la expresión de E volvemos a tener $(m(x - x_1) + y_1)^2 = x^3 + Ax + B$. Aplicando los mismos argumentos que en el primer caso pero teniendo en cuenta que ahora la coordenada x_1 es una raíz doble obtenemos

$$x_3 = m^2 - 2x_1$$

$$y_3' = m(x_3 - x_1) + y_1$$

y por tanto, tomando el opuesto de y_3', nos queda $P_3 = (x_3, m(x_1 - x_3) - y_1)$.

- Finalmente, si $P_2 = \infty$ entonces la línea que pasa por P_1 y ∞ es vertical y corta E en el punto P_1', que es el simétrico de P_1 respecto al eje x. Si tomamos la reflexión de P_1' respecto al eje de coordenadas, volvemos a encontrarnos con P_1 y en consecuencia $P_1 + \infty = P_1$. Por supuesto, este caso comprende la posibilidad de que $P_1 = \infty$, así que $\infty + \infty = \infty$.

En resumen, si E es una curva elíptica definida sobre un cuerpo K entonces $(E(K), +, \infty)$ es un grupo con la operación "+" que acabamos de describir y además es abeliano (pues la recta que pasa por P_1 y P_2 es la misma que la que pasa por P_2 y P_1 y en consecuencia $P_1 + P_2 = P_2 + P_1$). Cabe remarcar que la existencia de elementos neutro e inverso es evidente, pero la asociatividad no; para la demostración ver [21], Sección 2.4.

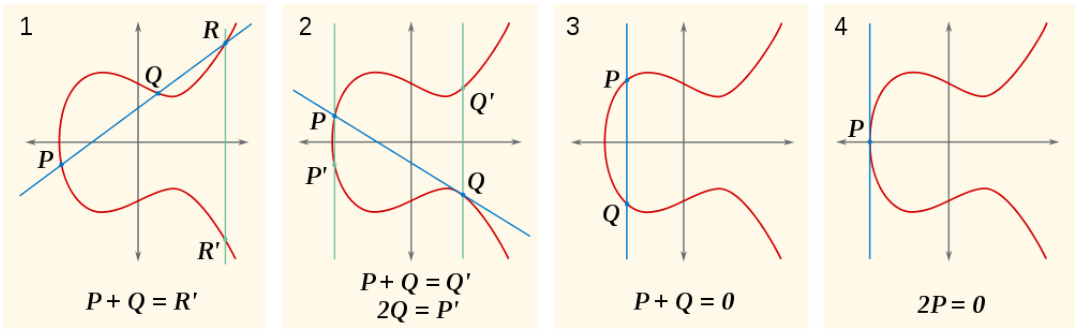

Figura 1: Representación gráfica de la suma de puntos en una curva elíptica.
Fuente: Wikipedia.

2.2. Endomorfismos

Sea E una curva elíptica definida sobre un cuerpo K. Un endomorfismo de E es un homomorfismo $\alpha : E(\overline{K}) \to E(\overline{K})$ dado por funciones racionales, esto es,

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

para todo punto $(x, y) \in E(\overline{K})$ y siendo $R_1(x, y)$, $R_2(x, y)$ cocientes de polinomios con coeficientes en $\overline{K}$. Puesto que α es un homomorfismo se satisface $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ para cualquier par de puntos de la curva y $\alpha(\infty) = \infty$. Si consideramos la curva E en forma de Weierstrass, $y^2 = x^3 + Ax + B$, podemos ir más allá y obtener más información de cómo son las funciones racionales (llamémosles $R(x, y)$) definidas sobre $E(\overline{K})$.

Observemos, para empezar, que $R(x, y)$ es un cociente de polinomios en las variables x, y y que los puntos $(x, y) \in E(\overline{K})$ satisfacen $y^2 = x^3 + Ax + B$, de modo que podemos reemplazar cualquier potencia par de y por una expresión que solamente contenga x y las potencias impares de y las podemos sustituir por y multiplicada por un polinomio en x. En resumen, podemos considerar que

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

Racionalizando el denominador y reemplazando potencias de y cuando sea necesario obtenemos

$$R(x, y) = \frac{(p_1(x) + p_2(x)y)(p_3(x) - p_4(x)y)}{(p_3(x) + p_4(x)y)(p_3(x) - p_4(x)y)} = \frac{q_1(x) + q_2(x)y}{q_3(x)}.$$

Para el caso que nos ocupa escribiremos

$$R_1(x, y) = \frac{q_{1,1}(x) + q_{1,2}(x)y}{q_{1,3}(x)}, \quad R_2(x, y) = \frac{q_{2,1}(x) + q_{2,2}(x)y}{q_{2,3}(x)}.$$

Recordemos ahora que α es un homomorfismo y por tanto $\alpha(-(x, y)) = -\alpha(x, y)$; además, tenemos que $-(x, y) = (x, -y)$ y en consecuencia

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

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

Igualando coordenada a coordenada,

$$R_1(x, -y) = R_1(x, y) \Rightarrow \frac{q_{1,1}(x) + q_{1,2}(x)(-y)}{q_{1,3}(x)} = \frac{q_{1,1}(x) + q_{1,2}(x)y}{q_{1,3}(x)}$$

cosa que implica que $q_{1,2}(x) = 0$ y, análogamente,

$$R_2(x,-y) = -R_2(x,y) \Rightarrow \frac{q_{2,1}(x) + q_{2,2}(x)(-y)}{q_{2,3}(x)} = -\frac{q_{2,1}(x) + q_{2,2}(x)y}{q_{2,3}(x)}$$

de manera que $q_{2,1}(x) = 0$.

En conclusión, podemos escribir el endomorfismo α como

$$\alpha(x,y) = (r_1(x), r_2(x)y), \quad \text{con } r_1(x) = \frac{q_{1,1}(x)}{q_{1,3}(x)},\ r_2(x) = \frac{q_{2,2}(x)}{q_{2,3}(x)}.$$

Introduzcamos, ahora, algunas nociones relacionadas con el concepto de endomorfismo de curvas elípticas. Dado $\alpha(x,y) = (r_1(x), r_2(x)y)$ con $r_1(x) = p(x)/q(x)$, definimos el **grado** de α como

$$\deg(\alpha) = \text{máx}\{\deg p(x), \deg q(x)\}$$

y diremos que α es **separable** si $r_1'(x)$ no es idénticamente 0 (esto es, r_1 no tiene raíces dobles). Esto nos permite enunciar las siguientes propiedades:

Proposición 2.1. *Sea $\alpha \neq 0$ un endomorfismo separable definido sobre una curva elíptica E. Entonces*

$$\deg(\alpha) = \#\ker(\alpha)$$

donde $\ker(\alpha)$ es el núcleo del homomorfismo $\alpha : E(\overline{K}) \to E(\overline{K})$.

Si $\alpha \neq 0$ no es separable, entonces

$$\deg(\alpha) > \#\ker(\alpha).$$

Demostración. Ver [21], Proposición 2.21. □

Teorema 2.2. *Sea E una curva elíptica definida sobre un cuerpo K. Sea $\alpha \neq 0$ un endomorfismo definido en E. Entonces $\alpha : E(\overline{K}) \to E(\overline{K})$ es sobreyectivo.*

Demostración. Ver [21], Teorema 2.22. □

Consideremos ahora el conjunto de endomorfismos de $E(\overline{K})$ y tomemos la suma y la composición de endomorfismos, juntamente con dos elementos distinguidos: el morfismo trivial, $\alpha_0(P) = \infty$ para todo $P \in E(\overline{K})$, y la identidad, $\alpha_1(P) = P$ para todo $P \in E(\overline{K})$. Entonces podemos hablar del **anillo de endomorfismos de** E, cuyas operaciones son precisamente las mencionadas anteriormente, el elemento neutro para la suma es α_0 y el neutro para el producto (o composición, en este caso) es α_1. Comprobemos que efectivamente se satisfacen las propiedades de anillo:

- Para empezar, debemos ver que, si α y β son endomorfismos de $E(\overline{K})$ dados por funciones racionales, $\alpha(x,y) = (r_1(x), r_2(x)y)$, $\beta(x,y) = (r_3(x), r_4(x)y)$ entonces $(\alpha+\beta)(x,y) = \alpha(x,y) + \beta(x,y)$. Notemos que

  $$(\alpha+\beta)(x,y) = ((r_1+r_3)(x), (r_2+r_4)(x)y).$$

  Por otro lado,

  $$\alpha(x,y) + \beta(x,y) = (r_1(x), r_2(x)y) + (r_3(x), r_4(x)y)$$
  $$= (r_1(x) + r_3(x), r_2(x)y + r_4(x)y) = ((r_1+r_3)(x), (r_2+r_4)(x)y),$$

  pues r_1, r_2, r_3, r_4 son funciones racionales. Por tanto, $(\alpha+\beta)(x,y) = \alpha(x,y)+\beta(x,y)$.

- Ver $(\alpha\circ\beta)(x,y) = \alpha(\beta(x,y))$ es inmediato. En efecto, $(\alpha\circ\beta)(x,y) = ((r_1\circ r_3)(x), (r_2\circ r_4)(x)y) = (r_1(r_3(x)), r_2(r_4(x))y) = \alpha(\beta(x,y))$ como queríamos demostrar.

Si nos fijamos únicamente en aquellos endomorfismos con coeficientes en K entonces el conjunto de endomorfismos forma un subanillo de $\mathrm{End}(E)$ que denotaremos por $\mathrm{End}_K(E)$.

El resultado siguiente da una caracterización del anillo de endomorfismos de una curva elíptica E:

Teorema 2.3. *Sea E una curva elíptica sobre $\mathbb{C}$. Entonces $\mathrm{End}(E)$ es isomorfo a $\mathbb{Z}$ o bien a un orden en un cuerpo cuadrático imaginario.*[7]

Demostración. Ver [21], Teorema 10.2. □

2.3. El invariante j

Sea E una curva elíptica dada por la ecuación $y^2 = x^3 + Ax + B$ definida sobre un cuerpo K de característica distinta de 2 y 3. Definimos el **invariante j** como

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2} \in K. \tag{2.4}$$

Teorema 2.4. *Sean $y_1^2 = x_1^3 + A_1x_1 + B_1$ y $y_2^2 = x_2^3 + A_2x_2 + B_2$ dos curvas elípticas con invariantes j j_1 y j_2, respectivamente. Si $j_1 = j_2$, entonces existe $\mu \neq 0$ en $\overline{K}$ tal que*

$$A_2 = \mu^4 A_1, \quad B_2 = \mu^6 B_1.$$

La transformación

$$x_2 = \mu^2 x_1, \quad y_2 = \mu^3 y_1$$

nos permite pasar de una ecuación a la otra.

Demostración. Ver [21], Teorema 2.19. □

El invariante j, pues, nos dice cuándo dos curvas son isomorfas sobre un cuerpo algebraicamente cerrado. Observemos también que si $j \neq 0, 1728$, j es el invariante j de la curva

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}.$$

Para $j = 0$ la curva elíptica tiene la forma $y^2 = x^3 + B$, mientras que si $j = 1728$ tenemos $y^2 = x^3 + Ax$. Cabe remarcar que sobre estas dos curvas se pueden definir automorfismos más allá del que poseen todas las curvas en forma de Weierstrass, definido por $(x, y) \mapsto (x, -y)$: para $y^2 = x^3 + B$ podemos dar el automorfismo $(x, y) \mapsto (\zeta x, -y)$ donde $\zeta^3 = 1$, $\zeta \neq 1$ mientras que para $y^2 = x^3 + Ax$ tenemos $(x, y) \mapsto (-x, iy)$ con $i^2 = -1$.

En consecuencia, para todo j de K, el invariante j da una biyección entre elementos del cuerpo K y clases de $\overline{K}$-isomorfismos de curvas elípticas definidas sobre K (esto es, cada $j \in K$ se corresponde con una curva elíptica definida sobre K y dos curvas elípticas cualesquiera definidas sobre K pueden transformarse la una en la otra usando el cambio de variables dado en el teorema).

[7] Los conceptos de "orden" y "cuerpo cuadrático imaginario" los discutiremos en la sección 3.2.

2.4. Puntos de n-torsión

Los **puntos de n-torsión** de una curva elíptica E sobre K son aquellos que tienen orden finito, de modo que podemos definir los puntos de orden n como

$$E[n] = \{P \in E(\overline{K}) : nP = \infty\}.$$

Observemos que $E[n]$ contiene también puntos con coordenadas en $\overline{K}$ y no solamente en K. Asimismo, podemos definir el **subgrupo de torsión** de E como

$$E_{tors} = \bigcup_{n=1}^{\infty} E[n],$$

es decir, el conjunto de puntos de $E(K)$ que tienen orden finito.

Teorema 2.5. *Sea E una curva elíptica sobre un cuerpo K y sea n un entero positivo. Si la característica de K no divide n, o es igual a 0, entonces*

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

Si la característica de K es $p > 0$ y $p \mid n$, escribimos $n = p^r n'$ con $p \nmid n'$. Entonces

$$E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad \textit{o bien} \quad E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

Demostración. Ver [21], páginas 85-86 (Teorema 3.2). □

Si E es una curva elíptica sobre un cuerpo K de característica p, diremos que E es **ordinaria** si $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Por lo contrario, si $E[p] \simeq 0$ o, equivalentemente, $E[p] = \{\infty\}$ (esto es, E no contiene puntos de orden p) diremos que E es **supersingular**. Además, se tiene que si E es ordinaria entonces su anillo de endomorfismos definidos en $\overline{K}$, $\mathrm{End}(E)$, es un orden en un cuerpo cuadrático imaginario (en particular, conmutativo), mientras que si E es supersingular $\mathrm{End}(E)$ es un orden maximal en un álgebra de cuaterniones (concretamente, no conmutativo).[8]

Supongamos ahora que $p \nmid n$ y elijamos una base $\{\beta_1, \beta_2\}$ de $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, de modo que podemos escribir cualquier elemento de $E[n]$ como $m_1\beta_1 + m_2\beta_2$ con m_1, m_2 enteros, determinados unívocamente módulo n. Sea $\alpha : E(\overline{K}) \to E(\overline{K})$ un homomorfismo; entonces $\alpha(E[n]) \subseteq E[n]$ y en consecuencia existen $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ tales que

$$\alpha(\beta_1) = a\beta_1 + c\beta_2, \quad \alpha(\beta_2) = b\beta_1 + d\beta_2.$$

Por tanto, podemos representar cada homomorfismo α restringido a los puntos de n-torsión (y lo denotaremos por α_n) matricialmente como

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

[8] Para más detalles, ver [21], Sección 10.2.

2.5. Curvas elípticas sobre cuerpos finitos

Ahora nos centraremos en aquellas curvas elípticas E definidas sobre un cuerpo finito de q elementos, que denotaremos por $\mathbb{F}_q$, y donde $q = p^n$ para algún número primo p y algún entero positivo n. Observemos que, puesto que hay un número finito de pares (x, y) con $x, y \in \mathbb{F}_q$ tenemos que el grupo $E(\mathbb{F}_q)$ es finito y por tanto podemos calcular su orden, cosa que, tal y como veremos a continuación, nos proporcionará información útil sobre la curva.

Teorema 2.6. *Sea E una curva elíptica sobre un cuerpo finito $\mathbb{F}_q$. Entonces*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \quad o\ bien \quad E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

para algún entero $n \geq 1$, o para algunos enteros $n_1, n_2 \geq 1$ con $n_1 \mid n_2$.

Demostración. Ver [21], Teorema 4.1. □

Teorema 2.7 (Hasse)**.** *Sea E una curva elíptica sobre un cuerpo finito $\mathbb{F}_q$. Entonces el orden de $E(\mathbb{F}_q)$, denotado por $\#E(\mathbb{F}_q)$, satisface*

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

Demostración. Ver [21], Teorema 4.2 y Sección 4.2. □

Este teorema nos proporciona una herramienta muy importante para calcular el orden de $E(\mathbb{F}_q)$. En efecto, sea $P \in E(\mathbb{F}_q)$; el **orden** de P es el entero más pequeño k que cumple $kP = \infty$. Por el teorema de Lagrange, el orden de un elemento del grupo (en nuestro caso, un punto) siempre divide el orden total del grupo (aquí $E(\mathbb{F}_q)$) y, por otro lado, dado un entero n tenemos que $nP = \infty$ si, y sólo si, el orden de P divide n. Por el teorema de Hasse,

$$\begin{aligned} |q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q} &\Leftrightarrow -2\sqrt{q} \leq q + 1 - \#E(\mathbb{F}_q) \leq 2\sqrt{q} \\ &\Leftrightarrow q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}, \end{aligned}$$

de modo que $\#E(\mathbb{F}_q)$ yace en un intervalo de longitud $4\sqrt{q}$. Entonces, si encontramos un punto de la curva cuyo orden sea mayor que $4\sqrt{q}$, solamente habrá un múltiplo de este orden en el intervalo de Hasse y por tanto este múltiplo será exactamente $\#E(\mathbb{F}_q)$.

2.5.1. El endomorfismo de Frobenius

Sea $\mathbb{F}_q$ un cuerpo finito y $\overline{\mathbb{F}}_q$ su clausura algebraica. Definimos el **endomorfismo de Frobenius** en $\mathbb{F}_q$ como

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

y que satisface que $\phi_q(x) = x$ para todo $x \in \mathbb{F}_q$[9] (diremos que "ϕ_q fija $\mathbb{F}_q$"). Si E es una curva elíptica definida sobre $\mathbb{F}_q$, haciendo un pequeño abuso de notación, podemos pensar

[9]Observemos que $\mathbb{F}_q$ es un cuerpo finito de q elementos y $X^q - X$ es un polinomio definido sobre este cuerpo con q raíces distintas (en efecto, pues la derivada de este polinomio en $\mathbb{F}_q$ es $qX^{q-1} - 1 = -1$, con lo cual el polinomio y su derivada no tienen raíces comunes). Por tanto, los q elementos de $\mathbb{F}_q$ son exactamente las q raíces de $X^q - X$ y en consecuencia, para todo $x \in \mathbb{F}_q$, $x^q - x = 0$, es decir, $x^q = x$.

que ϕ_q actúa sobre los puntos de $E(\overline{\mathbb{F}}_q)$ como

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

Veamos que en efecto ϕ_q es un endomorfismo de E. Claramente viene dado por funciones racionales y tenemos que la imagen del elemento neutro es el propio elemento neutro; solamente falta ver que $\phi_q((x,y)+(z,t)) = \phi_q(x,y)+\phi_q(z,t)$. Si E es una curva en forma de Weierstrass, entonces la adición de puntos viene dada por las fórmulas que hemos visto en la sección 2.1, y debemos tener en cuenta los distintos casos:

- Si $(x,y) \neq (z,t)$ y $x \neq z$ entonces

  $$(x,y)+(z,t) = \big((-x-z+m^2), (m(2x+z-m^2)-y)\big)$$

  con $m = \dfrac{t-y}{z-x}$ de modo que

  $$\begin{aligned}\phi_q((x,y)+(z,t)) &= \big((-x-z+m^2)^q, (m(2x+z-m^2)-y)^q\big)\\ &= \big((-x^q-z^q+m^{2q}), (m^q((2x)^q+z^q-m^{2q})-y^q)\big)\end{aligned}$$

  donde la última igualdad se debe a que E está definida sobre un cuerpo de característica p y q es una potencia de p.

  Por otro lado, $\phi_q(x,y) = (x^q, y^q)$ y $\phi_q(z,t) = (z^q, t^q)$, así que

  $$(x^q,y^q)+(z^q,t^q) = \big((-x^q-z^q+k^2), (k(2x^q+z^q-k^2)-y^q)\big)$$

  y $k = \dfrac{z^q-x^q}{t^q-y^q}$.

  Observemos que $m^q = k$ y que, tal y como ya hemos comentado en la página anterior, $2^q = 2$ puesto que $2 \in \mathbb{F}_p$. Por tanto, para este caso ϕ_q es efectivamente un endomorfismo.

- Si $x \neq z$ pero $y = t$ entonces, ya que la línea que pasa por los dos puntos es vertical, tenemos $(x,y)+(z,t) = \infty$ y por tanto $\phi_q((x,y)+(z,t)) = \infty$. Análogamente, dado que $\phi_q(x,y) = (x^q, y^q)$, $\phi_q(z,t) = (z^q, t^q) = (x^q, t^q)$ la recta que une estos dos puntos es también vertical y entonces $\phi_q(x,y)+\phi_q(z,t) = \infty$. En consecuencia $\phi_q((x,y)+(z,t)) = \phi_q(x,y)+\phi_q(z,t)$, como queríamos ver.

- Cuando $(x,y) = (z,t)$ con $y \neq 0$ lo que tenemos que ver es $\phi_q(2(x,y)) = 2\phi_q(x,y)$. Para empezar recordemos que

  $$2(x,y) = (m^2-2x, m(3x-m^2)-y)$$

  con $m = \dfrac{3x^2+A}{2y}$ donde A es el coeficiente de x en la ecuación de E. Por tanto,

  $$\begin{aligned}\phi_q(2(x,y)) &= \big((m^2-2x)^q, (m(3x-m^2)-y)^q\big)\\ &= \big(m^{2q}-(2x)^q, m^q((3x)^q-m^{2q}))-y^q\big)\\ &= \big(m^{2q}-2x^q, m^q(3x^q-m^{2q}))-y^q\big)\end{aligned}$$

  pues, igual que en el primer caso, $(x,y) \in \overline{\mathbb{F}}_q$, $2 \in \mathbb{F}_q$, $3 \in \mathbb{F}_q$ y q es una potencia de $\mathrm{char}(\overline{\mathbb{F}}_q) = p$. Por otra parte,

  $$2\phi_q(x,y) = 2(x^q, y^q) = (k^2-2x^q, k(3x^q-k^2)-y^q)$$

y $k = \dfrac{3(x^q)^2 + A}{2y^q} = \dfrac{3x^{2q} + A}{2y^q} = \dfrac{3(x^2)^q + A^q}{2y^q} = \left(\dfrac{3x^2 + A}{2y}\right)^q = m^q$. Entonces $\phi_q(2(x,y)) = 2\phi_q(x,y)$.

- Finalmente, si $(x,y) = \infty$ tenemos

  $$(x,y) + (z,t) = \infty + (z,t) = (z,t)$$

  y por tanto

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

  Luego, $\phi_q(x,y) + \phi_q(z,t) = \phi_q(\infty) + (z^q,t^q) = \infty + (z^q,t^q) = (z^q,t^q)$, cosa que muestra que en este caso ϕ_q también es endomorfismo.

En resumen, tenemos que efectivamente ϕ_q es endomorfismo de curvas elípticas que, además, tiene las siguientes propiedades:

Lema 2.8. *Sea E definida sobre $\mathbb{F}_q$ y sea $(x,y) \in E(\overline{\mathbb{F}}_q)$.*

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

Demostración. Para la demostración necesitaremos el hecho de que $(x+y)^q = x^q + y^q$ cuando q es una potencia de la característica del cuerpo y que $x^q = a$ para todo $a \in \mathbb{F}_q$, como ya hemos visto anteriormente.

Sea $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ la ecuación de Weierstrass generalizada de $E(\mathbb{F}_q)$, es decir, $a_i \in \mathbb{F}_q$ para todo i. Si elevamos esta ecuación a la q-ésima potencia obtenemos

$$(y^2)^q + (a_1xy)^q + (a_3y)^q = (x^3)^q + (a_2x^2)^q + (a_4x)^q + (a_6)^q$$

que es equivalente a

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6,$$

lo que significa que (x^q, y^q) es un punto de E y en consecuencia el primer punto del lema queda demostrado.

Para ver el segundo, recordemos que $x \in \mathbb{F}_q$ si, y sólo si, $\phi_q(x) = x$, y lo mismo ocurre con y. Por tanto,

$$(x,y) \in E(\mathbb{F}_q) \Leftrightarrow x,y \in \mathbb{F}_q \Leftrightarrow \phi_q(x) = x \text{ y } \phi_q(y) = y \Leftrightarrow \phi_q(x,y) = (x,y).$$

□

Una consecuencia muy interesante de este resultado es que, si para todo punto $P \in E(\mathbb{F}_q)$ se tiene $\phi_q(P) = P$ entonces $\phi_q(P) - P = \infty$ o, equivalentemente, $(\phi_q - 1)(P) = \infty$, es decir, $P \in \ker(\phi_q - 1)$. Puesto que esto ocurre para todo punto de $E(\mathbb{F}_q)$, obtenemos la igualdad $E(\mathbb{F}_q) = \ker(\phi_q - 1)$.

Lema 2.9. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Entonces ϕ_q es un endomorfismo de E de grado q y ϕ_q no es separable.*

Demostración. Ver [21], Lema 4.6. □

La siguiente proposición nos permitirá establecer una relación más entre $E(\mathbb{F}_q)$ y el endomorfismo de Frobenius:

Proposición 2.10. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Sean r y s dos enteros, por lo menos uno de ellos no nulo. El endomorfismo $r\phi_q + s$ es separable si, y sólo si, $q \nmid s$.*

Demostración. Ver [21], Proposición 2.29. □

Notemos, entonces, que puesto que $q \nmid -1$ el endomorfismo $(\phi_q - 1)$ es separable. Enlazando esto con la Proposición 2.1 tenemos que $\#\ker(\phi_q - 1) = \deg(\phi_q - 1)$ y por tanto $\#E(\mathbb{F}_q) = \deg(\phi_q - 1)$.

Por otro lado, observemos que podemos considerar el endomorfismo de Frobenius restringido a los puntos de un orden en concreto, por ejemplo, a los puntos de m-torsión y en este caso lo denotaremos por $(\phi_q)_m$. Es decir, podemos tomar

$$(\phi_q)_m : E[m] \to E[m]$$

donde $E[m] \subset E(\mathbb{F}_q)$ es el subgrupo de puntos de orden m. Esto nos servirá para el siguiente teorema.

Teorema 2.11. *Sea E una curva elíptica definida sobre $\mathbb{F}_q$ y sea $a = q + 1 - \#E(\mathbb{F}_q)$. Entonces*

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

como endomorfismos de E, y a es el único entero k tal que

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

Dicho de otro modo, si $(x, y) \in E(\overline{\mathbb{F}}_q)$, entonces

$$\left(x^{q^2}, y^{q^2}\right) - a(x^q, y^q) + q(x, y) = \infty,$$

y a es el único entero para el que se cumple esta relación para todo punto $(x, y) \in E(\overline{\mathbb{F}}_q)$. Además, a es el único entero que satisface

$$a \equiv \mathrm{Tr}((\phi_q)_m) \pmod{m}$$

para todo m tal que $\gcd(m, q) = 1$.[10]

Demostración. Ver [21], Teorema 4.10. □

El polinomio $X^2 - aX + q$ suele conocerse como el **polinomio característico del (endomorfismo de) Frobenius**. Los conceptos introducidos hasta aquí nos permiten enunciar algunos resultados referidos a curvas elípticas supersingulares, que son las que mayoritariamente nos ocuparán en este estudio.

[10] **Notación:** $\mathrm{Tr}((\phi_q)_m)$ es la traza de la matriz asociada al endomorfismo de Frobenius restringido a $E[m]$; $\gcd(m, q)$ simboliza el máximo común divisor de m y q.

Proposición 2.12. *Sea E una curva elíptica definida sobre $\mathbb{F}_p$, con p primo y sea $a = p+1-\#E(\mathbb{F}_p)$. Entonces E es supersigular si, y sólo si, $a \equiv 0 \pmod{p}$; equivalentemente, si, y sólo si, $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$.*

Demostración. Ver [21], Proposición 4.31. □

Corolario 2.13. *Supongamos que $p \geq 5$ es primo y E está definida sobre $\mathbb{F}_p$. Entonces E es supersingular si, y sólo si, $a = 0$; es decir, si, y sólo si, $\#E(\mathbb{F}_p) = p + 1$.*

Demostración. Claramente, si $a = 0$ entonces E es supersingular por la proposición anterior. Para la implicación contraria, supongamos que E es supersingular pero $a \neq 0$. Entonces $a \equiv 0 \pmod{p}$ implica que $|a| \geq p$, pero por el teorema de Hasse tenemos que $|a| \leq 2\sqrt{p}$, de modo que $p \leq 2\sqrt{p}$, esto es, $p^2 \leq 4p$, cosa que solamente ocurre si $p \leq 4$. □

Hay otro resultado interesante relativo a curvas supersingulares: puede demostrarse que una curva supersingular sobre un cuerpo perfecto[11] de característica p tiene su invariante j en $\mathbb{F}_{p^2}$ y, en consecuencia, una curva elíptica supersingular sobre $\overline{\mathbb{F}}_p$ siempre puede transformarse en una curva definida sobre $\mathbb{F}_{p^2}$ mediante un cambio de variables en $\overline{\mathbb{F}}_p$. La demostración de que $j(E) \in \mathbb{F}_{p^2}$ puede verse en [18], Teorema V.3.1.

2.6. Isogenias

Dadas dos curvas elípticas E_1 y E_2 sobre un cuerpo K, una **isogenia** es un homomorfismo $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ dado por funciones racionales. Es decir, $\alpha(\infty) = \infty$ y $\alpha(P + Q) = \alpha(P) + \alpha(Q)$ para todo $P, Q \in E_1(\overline{K})$; en particular, si $\alpha(x_1, y_1) = (x_2, y_2)$ entonces existen funciones racionales R_1 y R_2 tales que $x_2 = R_1(x_1, y_1)$ y $y_2 = R_2(x_1, y_1)$. Observemos, además, que si $E_1 = E_2$ una isogenia es simplemente un endomorfismo como los que hemos definido en la sección 2.2. Por tanto, del mismo modo que hemos procedido en ese punto, podemos escribir α como

$$(x_2, y_2) = \alpha(x_1, y_1) = (r_1(x_1), y_1 r_2(x_1)),$$

con r_1, r_2 funciones racionales. Si $r_1(x) = \dfrac{p(x)}{q(x)}$, donde $p(x)$ y $q(x)$ son polinomios tales que $\gcd\{p(x), q(x)\} = 1$, podemos definir el **grado** de α como

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$$

y diremos que α es **separable** si $r_1'(x)$ no es idénticamente 0.

Proposición 2.14. *Sea $\alpha : E_1 \to E_2$ una isogenia. Si α es separable, entonces*

$$\deg(\alpha) = \#\ker(\alpha).$$

Si α no es separable, entonces

$$\deg(\alpha) > \#\ker(\alpha).$$

En particular, el núcleo de una isogenia es un subgrupo finito de $E_1(\overline{K})$.

[11] Un cuerpo perfecto es aquel en el que todo polinomio es separable (esto es, para cualquier polinomio, todas sus raíces son distintas en alguna clausura algebraica del cuerpo). En particular, todos los cuerpos de característica 0 y los cuerpos finitos son perfectos.

Demostración. Es idéntica a la de la Proposición 2.1. □

Proposición 2.15. *Sea $\alpha : E_1 \to E_2$ una isogenia. Entonces $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ es sobreyectiva.*

Demostración. Idéntica a la demostración del Teorema 2.2. □

Proposición 2.16. *Sean E_1, E_2, E_3 curvas elípticas sobre un cuerpo K y supongamos que existen $\alpha_2 : E_1 \to E_2$ y $\alpha_3 : E_1 \to E_3$ isogenias separables definidas sobre $\overline{K}$. Si $\ker(\alpha_2) = \ker(\alpha_3)$ entonces E_2 es isomorfa a E_3 sobre $\overline{K}$. De hecho, hay un isomorfismo $\beta : E_2 \to E_3$ tal que $\beta \circ \alpha_2 = \alpha_3$.*

Demostración. Ver [21], Proposición 12.12. □

3. Teoría algebraica de números

La motivación de este capítulo es introducir los conceptos que nos permitirán entender cómo son los anillos de endomorfismos de las curvas elípticas. Ya hemos visto anteriormente que la multiplicación por enteros es un endomorfismo de curvas elípticas, y haciendo un pequeño abuso de notación podemos identificar el conjunto de estos endomorfismos con el anillo de los enteros, de modo que podemos considerar que $\mathbb{Z}$ es un subanillo de $\mathrm{End}_p(E)$,[12] para cualquier curva E. Además, puesto que el endomorfismo de Frobenius, que a partir de ahora denotaremos por π, está definido en $\mathbb{F}_p$, tenemos que $\mathbb{Z}[\pi]$ también es un subanillo de $\mathrm{End}_p(E)$.

En general se dice que $\mathrm{End}_p(E)$ es un $\mathbb{Z}$-módulo. Esto significa que para todo $\alpha, \beta \in \mathrm{End}_p(E)$ y $r, s \in \mathbb{Z}$, se tiene

$$(r+s)\alpha = r\alpha + s\alpha, \quad r\alpha + r\beta = r(\alpha+\beta), \quad r(s\alpha) = (rs)\alpha, \quad 1\alpha = \alpha,$$

o, dicho de otro modo, $\mathrm{End}_p(E)$ es un grupo abeliano aditivo que admite multiplicación por escalares de $\mathbb{Z}$ compatible con su estructura de grupo abeliano. Aunque muchas veces no tiene sentido hablar del endomorfismo inverso por el producto (pues mayoritariamente no está definido en $\mathrm{End}_p(E)$), por razones prácticas y de una forma puramente abstracta se suele considerar el **álgebra de endomorfismos de** E, que acostumbra a denotarse por $\mathrm{End}_p^0(E)$, y que satisface

$$\mathrm{End}_p^0(E) = \mathrm{End}_p(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Entonces $\mathrm{End}_p^0(E)$ puede ser o bien $\mathbb{Q}$ (esto nunca ocurre si el cuerpo sobre el que trabajamos tiene característica positiva), o bien un cuerpo cuadrático imaginario o bien un álgebra de cuaterniones.

En particular, tal y como ya hemos comentado en la sección 2.4, si E es una curva elíptica ordinaria, entonces $\mathrm{End}(E)$ es un orden en un cuerpo cuadrático imaginario, mientras que si E es supersingular $\mathrm{End}(E)$ es un orden en un álgebra de cuaterniones (no conmutativa); pero si nos restringimos a $\mathrm{End}_p(E)$, para el caso supersingular se tiene que el anillo de endomorfismos definidos sobre $\mathbb{F}_p$ es también un orden en un cuerpo cuadrático imaginario, que sí que es conmutativo y es el que consideraremos en nuestro estudio.

3.1. Cuerpos de números

Un cuerpo K es un **cuerpo de números** (también llamado **cuerpo de números algebraicos** o **cuerpo numérico**) si K es una extensión finita $\mathbb{Q}(\alpha)$ de los números racionales $\mathbb{Q}$. Diremos que el **grado** de K es la dimensión de K sobre $\mathbb{Q}$ como espacio vectorial y lo denotaremos por $\dim_{\mathbb{Q}}(K)$. Además, cada número algebraico[13] $\alpha \in \mathbb{C}$ tiene un polinomio irreducible $p(X) \in \mathbb{Q}[X]$; normalizando los coeficientes podemos asumir que $p(X)$ es mónico y entonces está unívocamente determinado, de modo que podemos hablar de *el* polinomio mínimo. Definimos el **grado** de α como el grado de $p(X)$.

Teorema 3.1. *Sea K un cuerpo de números de grado n. Entonces, existe $\alpha \in K$ tal que $\deg(\alpha) = n$ y, en particular, se tiene*

$$K = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

[12] **Notación:** escribiremos $\mathrm{End}(E)$ para referirnos al anillo de endomorfismos definidos sobre $\overline{\mathbb{F}}_p$ y $\mathrm{End}_p(E)$ para el anillo de endomorfismos definidos en $\mathbb{F}_p$.

[13] Un número algebraico es un número complejo que es raíz de un polinomio de una variable con coeficientes en $\mathbb{Q}$. Por ejemplo, i es un número algebraico porque es una raíz de X^2+1.

En tal caso escribiremos $K = \mathbb{Q}(\alpha)$.

Demostración. Ver [14], Capítulo 2. □

3.2. Enteros algebraicos

Sea $\alpha \in \mathbb{C}$ un número algebraico. El **denominador** de α, denotado por $\text{den}(\alpha)$, es el mínimo común múltiplo de los denominadores de los coeficientes del polinomio mínimo de α. Si $\text{den}(\alpha) = 1$ entonces diremos que α es un **entero algebraico** (dicho de otro modo, todos los coeficientes del polinomio mínimo de α son enteros).

Teorema 3.2. *El conjunto de los enteros algebraicos en* $\mathbb{C}$ *es un anillo.*

Demostración. Ver [14], Capítulo 2. □

Entonces, si K es un cuerpo de números algebraicos de grado n, podemos hablar del **anillo de enteros** de K, que es el anillo de todos los enteros algebraicos en K y se denota por $\mathcal{O}_K$. De momento acotaremos nuestro estudio a un tipo concreto de cuerpos.

Sea $d > 0$ un entero libre de cuadrados. Diremos que K es un **cuerpo cuadrático imaginario** si se tiene

$$K = \mathbb{Q}(\sqrt{-d}) = \{a + b\sqrt{-d} \mid a, b \in \mathbb{Q}\}.$$

El anillo de enteros de K, que es un grupo abeliano finitamente generado, es

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] & \text{si } d \equiv 3 \pmod 4 \\ \mathbb{Z}[\sqrt{-d}] & \text{si } d \equiv 1, 2 \pmod 4 \end{cases}$$

donde $\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] = \{a+b(\frac{1+\sqrt{-d}}{2}) \mid a, b \in \mathbb{Z}\}$ y, análogamente, $\mathbb{Z}[\sqrt{-d}] = \{a+b\sqrt{-d} \mid a, b \in \mathbb{Z}\}$. Diremos que un **orden** en un cuerpo cuadrático imaginario es un anillo A tal que $\mathbb{Z} \subset A \subseteq \mathcal{O}_K$ (observemos que $\mathbb{Z} \neq A$). Este anillo A también es un grupo abeliano finitamente generado y es de la forma $A = \mathbb{Z} + \mathbb{Z}f\delta$ donde $\delta = \frac{1+\sqrt{-d}}{2}$ o bien $\delta = \sqrt{-d}$ y $f = [\mathcal{O}_K : A]$ es el **conductor de** A. Entonces, si β es un entero algebraico en un cuerpo cuadrático imaginario, existen enteros b, c tales que $\beta^2 + b\beta + c = 0$.

3.3. Ideales

Sea K un cuerpo de números algebraicos y $\mathcal{O}$ un orden en K. Un **ideal** I en $\mathcal{O}$ es un conjunto no vacío de $\mathcal{O}$ que satisface las siguientes propiedades:

- $a, b \in I \Rightarrow a + b \in I$.
- $a \in I$, $r \in \mathcal{O} \Rightarrow ra \in I$.

Observemos que la primera propiedad nos dice que cualquier ideal es un subgrupo aditivo de $\mathcal{O}$, y en general, podemos decir que los ideales de $\mathcal{O}$ son los $\mathcal{O}$-módulos finitamente generados contenidos en $\mathcal{O}$. Además, diremos que J es un **ideal fraccionario** si es un $\mathcal{O}$-submódulo no nulo contenido en K para el que existe un elemento no nulo $a \in \mathcal{O}$ tal que $aJ \subset \mathcal{O}$; es decir, $I = aJ$ es un ideal de $\mathcal{O}$. Un ideal fraccionario J es **invertible** si

existe otro ideal fraccionario $\tilde{J}$ tal que $J\tilde{J} = \mathcal{O}$. En general no es cierto que todo ideal fraccionario sea invertible, pero sí que lo es cuando J es un ideal propio (es decir, $J \neq \mathcal{O}$) y $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario.[14]

Dados dos ideales fraccionarios I, J podemos definir su producto y su suma, respectivamente, como

$$IJ = \Big\{ \sum_i a_i b_i \mid a_i \in I, b_i \in J \Big\}, \quad I + J = \{a + b \mid a \in I, b \in J\}.$$

El conjunto de ideales fraccionarios invertibles forman un grupo abeliano con la multiplicación, que denotaremos por $I(\mathcal{O})$, del cual el conjunto de ideales fraccionarios principales[15], $P(\mathcal{O})$, es un subgrupo. Con esto podemos definir el **grupo de clases de ideales de** $\mathcal{O}$ como

$$\mathrm{cl}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$$

que en particular es un grupo abeliano (pues es el cociente de dos grupos abelianos) y cada clase de ideales $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ tiene un representante entero.

Teorema 3.3. *El grupo de clases de ideales* $\mathrm{cl}(\mathcal{O})$ *es finito.*

Demostración. Ver [8], Teorema 7.7. □

Definamos $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ como el conjunto de curvas elípticas E definidas sobre un cuerpo finito de p elementos $\mathbb{F}_p$ con $\mathrm{End}_p(E) \cong \mathcal{O}$ y tales que el endomorfismo de Frobenius π es un elemento de $\mathcal{O}$. Nuestro objetivo ahora es establecer una relación entre el grupo de clases de ideales $\mathrm{cl}(\mathcal{O})$ y $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$. Para ello primero debemos introducir el concepto de "curva cociente", motivo por el cual nos referiremos al siguiente resultado:

Lema 3.4. *Sea* $E(\mathbb{F}_p)$ *una curva elíptica y* G *un subgrupo de* E *estable por el endomorfismo de Frobenius (esto es, si* $x \in G$ *entonces* $\pi(x) = y \in G$*). Entonces, existe una curva elíptica* $E'(\mathbb{F}_p)$ *y una isogenia separable* $\varphi : E \to E'$ *sobre* $\mathbb{F}_p$ *con* $G = \ker \varphi$*.*

Demostración. Ver [4], Lema 6. □

Habitualmente la curva codominio E' se denota por E/G, de allí el nombre de curva cociente.

Ahora bien, resulta que para todo ideal $\mathfrak{a} \subseteq \mathcal{O} \cong \mathrm{End}_p(E)$ podemos definir, de una forma parecida a la del Lema anterior, la curva $E/\mathfrak{a}$. En efecto, tenemos que cualquier ideal invertible $\mathfrak{a}$ de $\mathcal{O}$ descompone como producto de $\mathcal{O}$-ideales de la forma $(\pi\mathcal{O})^r \mathfrak{a}_s$, donde $\mathfrak{a}_s \not\subseteq \pi\mathcal{O}$ y $\pi\mathcal{O}$ es el ideal de $\mathcal{O}$ generado por el endomorfismo de Frobenius. Fijémonos que todo $\alpha \in \mathfrak{a}_s$ es un endomorfismo de E (separable) cuyo núcleo es un subgrupo de E, de modo que la intersección de los núcleos de todos estos endomorfismos, $\bigcap_{\alpha \in \mathfrak{a}_s} \ker \alpha$, forma un subgrupo G de E. Usando el Lema previo, esto nos da una isogenia $\varphi_G : E \to E/G = E/\mathfrak{a}$. Componiendo esta isogenia φ_G con la potencia r-ésima del endomorfismo de Frobenius, obtenemos una isogenia de grado $|\mathcal{O}/\mathfrak{a}|$ que denotaremos por

$$\varphi_{\mathfrak{a}} : E \to E/\mathfrak{a},$$

[14] Ver [12], Proposición 2, para la demostración.

[15] Es decir, aquellos ideales fraccionarios generados por un solo elemento.

cosa que justifica la notación $E/\mathfrak{a}$. Observemos, además, que $\ker \varphi_{\mathfrak{a}} = G$, pues el núcleo del endomorfismo de Frobenius es trivial, así que otra manera de expresar la curva codominio es $E/\ker \varphi_{\mathfrak{a}}$. Resumiendo, todo esto nos dice que la multiplicación de ideales corresponde a la composición de isogenias.

Esta construcción de $E/\mathfrak{a}$ nos permite definir una aplicación que establece una correspondencia entre el par $(\mathfrak{a}, E)$ y la curva $E/\mathfrak{a}$ y que resulta ser una acción de $\mathrm{cl}(\mathcal{O})$ en $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$, tal y como se muestra en el siguiente resultado:

Teorema 3.5. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario y $\pi \in \mathcal{O}$ tal que $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ es no vacío. Entonces el grupo de clases de ideales $\mathrm{cl}(\mathcal{O})$ actúa libre y transitivamente sobre el conjunto $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ via la función*

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) &\longrightarrow \mathcal{E}\ell\ell_p(\mathcal{O}, \pi) \\ ([\mathfrak{a}], E) &\longmapsto E/\mathfrak{a}, \end{aligned}$$

donde $\mathfrak{a}$ es elegido como un representante entero.

Demostración. Ver [4], Teorema 7. □

Para enfatizar que estamos trabajando con una acción de grupo, en general escribiremos $[\mathfrak{a}] * E$ o simplemente $[\mathfrak{a}]E$ para representar la curva $E/\mathfrak{a}$.

3.4. Factorización de primos

Notemos que todo ideal primo en $\mathbb{Z}$ está generado por un número primo, de modo que una cuestión interesante y de relativa importancia es ver cómo factorizan estos mismos ideales en $\mathcal{O}$. Por ejemplo, si consideramos un entero d libre de cuadrados (en particular, $d \neq 1$) y tomamos $K = \mathbb{Q}(\sqrt{d})$ y p un primo cualquiera, entonces el ideal (p) puede factorizar de tres formas distintas en $\mathcal{O}$:

- (p) es un ideal primo. En este caso, diremos que p es **inerte** en $\mathcal{O}$.
- $(p) = P_1P_2$ donde P_1 y P_2 son ideales primos distintos. Entonces decimos que p **descompone** en $\mathcal{O}$.
- $(p) = P^2$ para algún ideal primo P. Cuando esto ocurre, se dice que p **ramifica** en $\mathcal{O}$.

Si además definimos el **discriminante** de $K = \mathbb{Q}(\sqrt{d})$, con d definido igual antes, como

$$\mathrm{disc}(K) = \begin{cases} d & \text{si } d \equiv 1 \pmod 4 \\ 4d & \text{si } d \equiv 2, 3 \pmod 4 \end{cases}$$

entonces tenemos que (p) descompone en $\mathcal{O}$ si, y solo si, $p \nmid \mathrm{disc}(K)$ y $\mathrm{disc}(K)$ es un cuadrado módulo p; (p) es inerte en $\mathcal{O}$ si, y solo si, $\mathrm{disc}(K)$ no es un cuadrado módulo p, y (p) ramifica en $\mathcal{O}$ si, y solo si, $p \mid \mathrm{disc}(K)$.[16]

[16] Ver [14], Teorema 25.

4. CSIDH

En este capítulo presentaré el funcionamiento de CSIDH. Primero describiré el algoritmo sin entrar en muchos detalles y a continuación explicaré en profundidad los conceptos que intervienen en este intercambio de claves y el papel que desempeñan en él.

4.1. Curvas de Montgomery

Anteriormente hemos descrito el concepto de curva elíptica E sobre un cuerpo K cualquiera como

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

y si $\text{char}(K) \neq 2, 3$ podemos simplificar esta expresión y escribirla como

$$E(K) = \{(x, y) \in K : y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

Pero de hecho las ecuaciones de Weierstrass, aunque quizá sean las más conocidas y habituales, no son las únicas que usan en teoría de curvas elípticas. Para nuestro estudio nos resultará más conveniente trabajar con curvas de otra forma, las llamadas **curvas de Montgomery**, que vienen dadas por la ecuación

$$E_M(K) : By^2 = x^3 + Ax^2 + x \tag{4.1}$$

donde A y B son parámetros en K (con $\text{char}(K) \neq 2$) que satisfacen $B \neq 0$ y $A^2 \neq 4$. El punto del infinito sigue siendo $\infty = (0 : 1 : 0) \in \mathbb{P}^2$ y el invariante j se define como

$$j(E_M) = \frac{256(A^2 - 3)^3}{A^2 - 4}. \tag{4.2}$$

Cabe remarcar que no todas las curvas en forma corta de Weierstrass pueden transformarse en una curva de Montgomery (pero el recíproco sí que es cierto) pues no todo elemento de K (y, en consecuencia, no todo invariante j posible) puede escribirse como en (4.2) para algún $A \in K$.

Puesto que E_M es una curva elíptica, sus puntos también forman un grupo abeliano donde el elemento neutro es el punto en el infinito ∞ y para cada punto $P = (x, y) \in E_M(K)$ su elemento opuesto es $-P = (x, -y)$. La adición de puntos, dados $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$, que expresaremos como $P + Q = (x_+, y_+)$ viene dada por las siguientes fórmulas:

$$x_+ = B\lambda^2 - (x_P + x_Q) - A$$

$$y_+ = (2x_P + x_Q + A)\lambda - B\lambda^3 - y_P = \lambda(x_P - x_+) - y_P$$

donde

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{si } P \neq Q, P \neq -Q; \\ \dfrac{3x_P^2 + 2Ax_P + 1}{2By_P} & \text{si } P = Q \end{cases}$$

y si $P = -Q$ entonces $P + Q = \infty$. Observemos, pues, que λ es la pendiente de la recta que pasa por P y Q, si son distintos, o de la recta tangente al punto P, si $P = Q$.

4.2. El algoritmo de intercambio de claves

Para empezar veamos, paso a paso, qué se necesita y cómo podemos implementar el algoritmo.

1. Tomamos un número primo de la forma $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ donde los ℓ_i son primos pequeños distintos e impares.

2. Consideramos una curva elíptica $E_0 : y^2 = x^3 + x$ definida sobre $\mathbb{F}_p$, que es supersingular y cuyo anillo de endomorfismos definidos sobre $\mathbb{F}_p$ es $\mathcal{O} = \mathbb{Z}[\pi]$ (comprobaremos ambas propiedades al finalizar la descripción del algoritmo) donde π es el endomorfismo de Frobenius en $E(\mathbb{F}_p)$ y por tanto satisface la ecuación

$$x^2 - \mathrm{Tr}(\pi)x + p = 0.$$

   Puesto que E_0 es supersingular, $\mathrm{Tr}(\pi) = 0$ y en consecuencia tenemos que π satisface $x^2 + p = 0$; es decir, $\pi = \sqrt{-p}$.
   Observación: tanto p, como su factorización (es decir, los ℓ_i's), como la curva E_0 son públicos.

3. La generación de claves.

   Para la clave privada elegimos un vector $(e_1, \ldots, e_n)$ con $e_i \in \mathbb{Z}$ aleatorios, $e_i \in \{-m, \ldots, m\}$ para algún entero m. Estos elementos representan la clase de ideales

$$[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \in \mathrm{cl}(\mathcal{O})$$

   donde $\mathfrak{l}_i = (\ell_i, \pi - 1)$ y $\mathfrak{l}_i^{-1} = (\ell_i, \pi + 1)$ (es decir, los ideales primos generados por estos dos elementos).

   A continuación calculamos

$$[\mathfrak{a}]E_0 = E_A : y^2 = x^3 + Ax^2 + x.$$

   La curva E_A es el resultado de aplicar la acción de $\mathfrak{a}$ a E_0. Esta acción es una isogenia

$$\varphi_A : E_0 \to E_A = {}^{E_0}\!/_{\ker \varphi_A}.$$

   El coeficiente $A \in \mathbb{F}_p$ es la clave púbilca.

4. Intercambio de claves.

   Para empezar, recordemos que $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ es el conjunto de curvas elípticas definidas sobre $\mathbb{F}_p$ cuyo anillo de endomorfismos definido sobre $\mathbb{F}_p$, $\mathrm{End}_p(E)$, es isomorfo a un orden $\mathcal{O}$ y el endomorfismo de Frobenius $\pi \in \mathcal{O}$.

   Supongamos que tenemos dos personajes: Alice y Bob, y cada uno de ellos posee una clave privada y una pública. En efecto, podemos considerar que $([\mathfrak{a}], A)$ son la clave privada y pública de Alice, respectivamente, y $([\mathfrak{b}], B)$ son las de Bob. De hecho, puesto que

$$[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}], \quad [\mathfrak{b}] = [\mathfrak{l}_1^{f_1} \cdots \mathfrak{l}_n^{f_n}]$$

   podríamos pensar en las claves secretas como $(e_1, \ldots, e_n)$ y $(f_1, \ldots, f_n)$, respectivamente, pues los ideales $\mathfrak{l}_i$ son conocidos públicamente.

Alice recibe $B \in \mathbb{F}_p \setminus \{\pm 2\}$ y verifica que efectivamente $y^2 = x^3 + Bx^2 + x$ define una curva elíptica (supersingular) en $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ usando el Algoritmo 1, que detallaré más adelante, y a continuación calcula

$$[\mathfrak{a}]E_B = [\mathfrak{a}][\mathfrak{b}]E_0.$$

Bob hace lo mismo: recibe $A \in \mathbb{F}_p \setminus \{\pm 2\}$ y verifica que $y^2 = x^3 + Ax^2 + x \in \mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ con el Algoritmo 1 y después calcula

$$[\mathfrak{b}]E_A = [\mathfrak{b}][\mathfrak{a}]E_0.$$

Como $\mathrm{cl}(\mathcal{O})$ es conmutativo, con estas operaciones obtenemos $E_S = [\mathfrak{a}][\mathfrak{b}]E_0 = [\mathfrak{b}][\mathfrak{a}]E_0 : y^2 = x^3 + Sx^2 + x$ y entonces S es el secreto compartido.

Veamos ahora por qué E_0 es supersingular en $\mathbb{F}_p$ cuando $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, pero para ello primero necesitamos introducir algunos conceptos más.

Cuando $p \equiv 3 \pmod 4$ podemos escribir la ecuación de la curva elíptica en **forma de Legendre**, esto es, como $y^2 = x(x-1)(x-\lambda)$ con $\lambda \notin \{0, 1\}$.[17] Por otro lado, definimos el **símbolo de Legendre** como

$$\left(\frac{x}{p}\right) := \begin{cases} -1 & \text{si } x \text{ no es un cuadrado módulo } p; \\ 0 & \text{si } x \text{ es divisible por } p; \\ 1 & \text{si } x \text{ es un cuadrado módulo } p \text{ y } x \neq 0; \end{cases}$$

y podemos extender esta definición a $\mathbb{F}_p$, de modo que

$$\left(\frac{x}{\mathbb{F}_p}\right) := \begin{cases} -1 & \text{si } x \text{ no es un cuadrado en } \mathbb{F}_p^\times; \\ 0 & \text{si } x = 0; \\ 1 & \text{si } x \text{ es un cuadrado en } \mathbb{F}_p^\times; \end{cases}$$

donde $\mathbb{F}_p^\times$ denota el subgrupo multiplicativo de $\mathbb{F}_p$ (esto es, el subgrupo de los elementos invertibles). Entonces tenemos:

Teorema 4.1. *Sea $E(\mathbb{F}_p) : y^2 = x(x-1)(x-\lambda)$ una curva elíptica. Entonces,*

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right).$$

Demostración. Fijemos $x_0 \in \mathbb{F}_p$, de modo que $y^2 = x_0(x_0-1)(x_0-\lambda)$. Observemos que el número de y's es precisamente $1 + \left(\frac{x_0(x_0-1)(x_0-\lambda)}{\mathbb{F}_p}\right)$: si $x_0(x_0-1)(x_0-\lambda)$ es un cuadrado en $\mathbb{F}_p$ entonces existen dos puntos distintos con la misma coordenada x y el correspondiente símbolo de Legendre será 1, de modo que tendremos 2 y's; si contrariamente $x_0(x_0-1)(x_0-\lambda)$ no es un cuadrado en $\mathbb{F}_p$, entonces no hay ningún punto en E con esta coordenada x y el símbolo de Legendre es -1, con lo que obtenemos 0 y's; finalmente, si $x_0(x_0-1)(x_0-\lambda) = 0$ entonces hay un único punto con esta x y, al ser el símbolo de Legendre 0, obtenemos una única y. Aplicando este mismo argumento a

[17] Ver [1] para más detalles.

todos los $x \in \mathbb{F}_p$ y teniendo en cuenta que ∞ también es un punto de E obtenemos lo que queríamos, es decir,

$$\#E(\mathbb{F}_p) = 1 + \sum_{x\in\mathbb{F}_p} \left(1 + \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right)\right) = 1 + p + \sum_{x\in\mathbb{F}_p} \left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right).$$

□

También debemos tener en cuenta lo siguiente:

Lema 4.2. *Sea $i > 0$ un entero. Entonces*

$$\sum_{x\in\mathbb{F}_p} x^i = \begin{cases} 0 & si\ p-1 \nmid i; \\ -1 & si\ p-1 \mid i. \end{cases}$$

Demostración. Notemos que $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\} = \langle g\rangle = \{g^0, g^1, \ldots, g^{p-2}\}$, donde g es un elemento primitivo. En consecuencia, cualquier elemento de $\mathbb{F}_p$ puede escribirse como una potencia de g.
Cuando $p-1 \nmid i$ tenemos

$$\sum_{x\in\mathbb{F}_p} x^i = 0 + \sum_{x\in\mathbb{F}_p^\times} x^i = \sum_{j=0}^{p-2} (g^j)^i = \sum_{j=0}^{p-2} (g^i)^j = \frac{(g^i)^{p-1} - 1}{g^i - 1} = 0$$

pues $(g^i)^{p-1} = (g^{p-1})^i = 1^i = 1$ ya que g tiene orden $p-1$. En caso contrario, si $p-1 \mid i$, entonces podemos escribir $i = (p-1)j$ y por tanto

$$\sum_{x\in\mathbb{F}_p} x^i = 0 + \sum_{x\in\mathbb{F}_p^\times} x^{(p-1)j} = \sum_{x\in\mathbb{F}_p^\times} 1^j = p - 1 = -1 \pmod p.$$

□

Observemos que usando el Criterio de Euler[18] podemos escribir

$$\left(\frac{x(x-1)(x-\lambda)}{\mathbb{F}_p}\right) = (x(x-1)(x-\lambda))^{\frac{p-1}{2}} \text{ en } \mathbb{F}_p$$

y expandiendo el lado derecho de la igualdad obtenemos un polinomio de grado $\frac{3(p-1)}{2}$, $\sum_{i=0}^{3\frac{p-1}{2}} c_i x^i$, cuyo único exponente divisible por $p-1$ es él mismo. Por tanto, si llamamos A_p al coeficiente del término de grado $p-1$, aplicando el lema anterior, tenemos que

$$\sum_{x\in\mathbb{F}_p} (x(x-1)(x-\lambda))^{\frac{p-1}{2}} = \sum_{x\in\mathbb{F}_p} \left(x^{3\frac{p-1}{2}} + \cdots + A_p x^{p-1} + \ldots\right) = -A_p.$$

En consecuencia $\#E(\mathbb{F}_p) = 1 + p - A_p$ y usando el criterio de supersingularidad del Corolario 2.13 obtenemos que $E(\mathbb{F}_p)$ es supersingular si, y sólo si, $A_p = 0$.

Llegados a este punto ya podemos demostrar que, en efecto, la curva $E_0 : y^2 = x^3 + x$ definida sobre $\mathbb{F}_p$, con $p \equiv 3 \pmod 4$, es supersingular. Notemos que $x^3 + x = x(x^2+1)$ y por tanto

$$\#E(\mathbb{F}_p) = 1 + p + \sum_{x\in\mathbb{F}_p} x^{\frac{p-1}{2}} (x^2+1)^{\frac{p-1}{2}}.$$

[18] Ver [24] para la definición.

Si A_p es el coeficiente del término de grado $p-1$, entonces es también el coeficiente de $x^{\frac{p-1}{2}}$ en $(x^2+1)^{\frac{p-1}{2}}$, donde todos los exponentes son pares (pues $p-1$ es par). Pero puesto que $p \equiv 3 \pmod 4$, entonces $p-1 \equiv 2 \pmod 4$ y por tanto $\frac{p-1}{2} \equiv 1 \pmod 2$ o, equivalentemente, $\frac{p-1}{2}$ es impar. En consecuencia, el exponente $\frac{p-1}{2}$ no aparece en el desarrollo de $(x^2+1)^{\frac{p-1}{2}}$ y por tanto $A_p = 0$, lo que prueba que E_0 es supersingular.

Para mostrar que el anillo de endomorfismos de E_0 es isomorfo a $\mathbb{Z}[\pi]$ nos valdremos del siguiente resultado:

Proposición 4.3. *Sea $p \geq 5$ un número primo tal que $p \equiv 3 \pmod 8$, y sea $E(\mathbb{F}_p)$ una curva elíptica supersingular. Entonces $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$ si, y sólo si, existe $A \in \mathbb{F}_p$ tal que E es $\mathbb{F}_p$-isomorfa a la curva $E_A : y^2 = x^3 + Ax^2 + x$. Además, si dicho A existe, es único.*

Demostración. Ver [4], Proposición 8. □

En el caso que nos ocupa, $E_0 : y^2 = x^3 + x$, con lo cual existe este tal A y es exactamente 0. Para poder aplicar la Proposición solamente nos falta comprobar que $p \equiv 3 \pmod 8$. Puesto que $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ donde los ℓ_i's son primos distintos impares para todo i, entonces $p \equiv 3 \pmod 4$, lo que significa que $p+1 \equiv 0 \pmod 4$. Si lo miramos módulo 8, podemos tener $p+1 \equiv 0 \pmod 8$ o bien $p+1 \equiv 4 \pmod 8$; dado que $p+1 = 4 \cdot \ell_1 \cdots \ell_n$ y los ℓ_i's son primos impares, entonces $4 \mid p+1$ pero $8 \nmid p+1$ y en consecuencia solamente puede ser $p+1 \equiv 4 \pmod 8$ o, dicho de otro modo, $p \equiv 3 \pmod 8$.

En resumen, E_0 está bajo las hipótesis de la Proposición y por tanto podemos concluir que su anillo de endomorfismos es (isomorfo a) $\mathbb{Z}[\pi]$.

4.3. Verificar que una curva es supersingular

Tal y como hemos visto en la sección anterior, cuando Alice recibe la clave pública de Bob lo primero que debe hacer es comprobar que E_B es una curva elíptica supersingular; esto da una garantía a Alice de que Bob es quien dice ser y no un atacante (además de asegurar que los cálculos funcionarán y el resultado será el deseado).

Recordemos que una curva E definida sobre $\mathbb{F}_p$, con $p \geq 5$, es supersingular si, y sólo si, $\#E(\mathbb{F}_p) = p+1$. Ver que una curva tiene orden $N = p+1$ es relativamente fácil: tenemos que encontrar un subgrupo (en particular, un punto) que tenga orden d siendo d un divisor de N y tal que $d > 4\sqrt{p}$. Esto es consecuencia directa del Teorema de Hasse (ver Teorema 2.7), pues si $|\#E(\mathbb{F}_p) - (1+p)| \leq 2\sqrt{p}$ entonces $-2\sqrt{p} \leq \#E(\mathbb{F}_p) - (1+p) \leq 2\sqrt{p}$, cosa que implica $1+p-2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq 1+p+2\sqrt{p}$; es decir, $\#E(\mathbb{F}_p)$ yace en un intervalo de longitud $4\sqrt{d}$. Por tanto, si encontramos un d que cumpla $d \mid \#E(\mathbb{F}_p)$ y $d > 4\sqrt{p}$ tendremos que solamente habrá un múltiplo de d en el intervalo $(1+p-2\sqrt{p}, 1+p+2\sqrt{p})$ que será exactamente N.

A continuación se muestra un algoritmo para determinar si una curva elíptica dada es supersingular u ordinaria.

Algorithm 1: Verificar supersingularidad

Input: Curva elíptica $E(\mathbb{F}_p)$ con $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, donde $\ell_1 \cdots \ell_n$ son primos distintos e impares.

Output: *supersingular* u *ordinaria.*

Elegimos un punto $P \in E(\mathbb{F}_p)$ aleatoriamente.

Ponemos $d = 1$.

for $i = 1, \ldots, n$ **do**

$Q_i = \dfrac{p+1}{\ell_i} \cdot P$ (es decir, $Q_i = 4 \cdot \ell_1 \cdots \hat{\ell_i} \cdots \ell_n \cdot P$)

if $[\ell_i]Q_i = 4 \cdot \ell_1 \cdots \ell_n \cdot P \neq \infty$ **then return** *ordinaria.*

if $[\ell_i]Q_i = 4 \cdot \ell_1 \cdots \ell_n \cdot P = \infty$ *y* $Q_i \neq \infty$ **then** ponemos $d \leftarrow \ell_i \cdot d$.

if $d > 4\sqrt{p}$ **then return** *supersingular.*

end

Veamos por qué si $[\ell_i]Q_i \neq \infty$ la curva es ordinaria. Observemos que el hecho que $4 \cdot \ell_1 \cdots \ell_n \cdot P \neq \infty$ implica que $\mathrm{ord}P \neq 4 \cdot \ell_1 \cdots \ell_n = p + 1$ y además $\mathrm{ord}P \nmid p + 1$. Sin embargo, como $P \in E(\mathbb{F}_p)$, $\mathrm{ord}P \mid \#E(\mathbb{F}_p)$ y entonces podemos poner $\#E(\mathbb{F}_p) = \mathrm{ord}P \cdot k$ para algun k entero positivo.
Si fuese $\#E(\mathbb{F}_p) = \mathrm{ord}P \cdot (p+1)k' = (p+1)m$ (es decir, k es múltiplo de $p+1$), por el Teorema de Hasse tendríamos

$$\#E(\mathbb{F}_p) = (p+1)m \leq p + 1 + 2\sqrt{p} \Rightarrow m \leq 1 + \frac{2\sqrt{p}}{p+1}.$$

Por otro lado, $\frac{2\sqrt{p}}{p+1} \leq 1$ pues

$$\frac{2\sqrt{p}}{p+1} \leq 1 \Rightarrow 2\sqrt{p} \leq p + 1 \Rightarrow 4p \leq p^2 + 2p + 1 \Rightarrow 0 \leq p^2 - 2p + 1 = (p-1)^2$$

y la última desigualdad es siempre cierta; de hecho es una desigualdad estricta pues por hipótesis $p \geq 5$ y entonces $0 < (p-1)^2$, cosa que implica que $\frac{2\sqrt{p}}{p+1} < 1$ y por tanto forzosamente tiene que ser $m = 1$ (pues $m \in \mathbb{Z}$). En este caso el hecho de tener $\#E(\mathbb{F}_p) = p+1$, $\mathrm{ord}P \mid \#E(\mathbb{F}_p)$ y $\mathrm{ord}P \nmid p+1$ nos lleva a contradicción y en consecuencia $\#E(\mathbb{F}_p) \nmid p + 1$, cosa que implica que $E(\mathbb{F}_p)$ no es supersingular.

Observemos que si la curva es supersingular y P tiene orden menor que $4\sqrt{p}$ entonces el algoritmo no devuelve nada. En este caso, tendríamos que volver a correr el programa hasta que el punto P elegido aleatoriamente tenga orden mayor que $4\sqrt{p}$. Además, teniendo en cuenta que $E(\mathbb{F}_p)$ tiene un número finito de puntos y la probabilidad de elegir cada uno de ellos es la misma, podemos pensar que en algún momento daremos con un punto cuyo orden sea mayor que $4\sqrt{p}$, con lo cual el algoritmo nos proporcionará el resultado en un tiempo razonable.

4.4. Cómo calcular la acción de un ideal en una curva elíptica

En nuestro caso lo que nos interesa es calcular la acción del ideal $\mathfrak{l}_1^{e_1}\mathfrak{l}_2^{e_2}\cdots\mathfrak{l}_n^{e_n}$ en $E \in \mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$, donde $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ es el conjunto de curvas elípticas definidas en $\mathbb{F}_p$ que tienen anillo de endomorfismos $\mathrm{End}_p(E)$ isomorfo a $\mathcal{O} = \mathbb{Z}[\pi]$ y π es el endomorfismo de Frobenius (por tanto π satisface $\pi^2 - \mathrm{Tr}(\pi) + p = 0$ y si E es supersingular entonces $\pi^2 = -p$, es decir, $\pi = \pm\sqrt{-p}$). Recordemos, además, que $p \equiv 3 \pmod 8$ y en consecuencia nos encontramos bajo las hipótesis de la Proposición 4.3; es decir, existe $A \in \mathbb{F}_p$ tal

que E es $\mathbb{F}_p$-isomorfa a $E_A : y^2 = x^3 + Ax^2 + x$ y A es único. En resumen, podemos escribir la curva E en la forma de Montgomery, cosa que nos resulta útil ya que esta ecuación permite hacer cálculos de forma más rápida, tanto en la curva propiamente como con las isogenias.

Hablemos ahora de los $\mathfrak{l}_i$'s. Recordemos que hemos elegido números primos impares $\ell_1, \ldots, \ell_n$, de modo que cada uno de ellos genera un ideal en $\mathbb{Z}$, pero ahora nos interesa ver cómo factorizan en $\mathcal{O} = \mathbb{Z}[\pi]$. Tal y como ya hemos visto en el Capítulo 3, $\mathcal{O}$ es un orden en un cuerpo cuadrático imaginario, concretamente en el cuerpo $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-p})$. Apelando a la definición de discriminante dada en la sección 3.4 tenemos que

$$\operatorname{disc}\left(\mathbb{Q}(\sqrt{-p})\right) = \begin{cases} -p & \text{si } -p \equiv 1 \pmod 4 \\ -4p & \text{si } -p \equiv 2, 3 \pmod 4. \end{cases}$$

Puesto que $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, entonces $-p = -(4 \cdot \ell_1 \cdots \ell_n - 1)$ y por tanto $-p \equiv 1 \pmod 4$, con lo cual tenemos que $\operatorname{disc}(\mathbb{Q}(\sqrt{-p})) = -p$. Ahora bien, $-p = -4 \cdot \ell_1 \cdots \ell_n + 1 \equiv 1 \pmod{\ell_i}$ para todo $i = 1, \ldots, n$, así que $\operatorname{disc}(\mathbb{Q}(\sqrt{-p}))$ es un cuadrado módulo ℓ_i para todo i y en consecuencia los números $\ell_1, \ldots, \ell_n$ descomponen (en inglés, "split") en $\mathcal{O} = \mathbb{Z}[\pi]$; esto significa que existen ideales primos $\mathfrak{l}_i, \bar{\mathfrak{l}}_i$ de $\mathcal{O}$ con $\ell_i\mathcal{O} = \mathfrak{l}_i\bar{\mathfrak{l}}_i$[19]. Estos primos ℓ_i son conocidos como los "primos de Elkies"[20], cosa que se traduce, en nuestra situación, a que, para todo i, $\ell_i \nmid p$ tiene que ser primo impar y $-4p$ tiene que ser un cuadrado módulo ℓ_i (es decir, $-4p \equiv x^2 \pmod{\ell_i}$). Observemos que en este caso $-p \equiv 1 \pmod{\ell_i}$, con lo cual $-4p \equiv 4 \pmod{\ell_i}$ y puesto que $\ell_i \geq 3$ y es primo, 4 es en efecto un cuadrado módulo ℓ_i. Además el ideal $\mathfrak{l}_i$ está generado por ℓ_i y $\pi - \lambda$, esto es, $\mathfrak{l}_i = (\ell_i, \pi - \lambda)$, donde $\lambda \in \mathbb{Z}/\ell_i$ es el valor propio del endomorfismo de Frobenius módulo ℓ_i y $\bar{\mathfrak{l}}_i = (\ell_i, \pi - \frac{p}{\lambda})$[21].

Veamos ahora quién es λ. Recordemos que en nuestro caso, al ser E supersingular, la traza del endomorfismo de Frobenius es 0 y por tanto tenemos $\pi^2 + p = 0$, es decir, $\pi^2 = -p$. No obstante, $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ (equivalentemente $-p = -4 \cdot \ell_1 \cdots \ell_n + 1$), cosa que implica que $\pi^2 = -4 \cdot \ell_1 \cdots \ell_n + 1 \equiv 1 \pmod{\ell_i}$ y por tanto $\pi \equiv 1 \pmod{\ell_i}$ o bien $\pi \equiv -1 \pmod{\ell_i}$. Dicho de otro modo, los valores propios del endomorfismo de Frobenius en todos los subgrupos de cardinal ℓ_i son 1 y -1 para todo i y en consecuencia obtenemos que

$$\mathfrak{l}_i = (\ell_i, \pi - 1), \quad \bar{\mathfrak{l}}_i = (\ell_i, \pi + 1).$$

El siguiente paso es calcular la acción de $\mathfrak{l}_i$ (resp. $\bar{\mathfrak{l}}_i$) sobre la curva E, que denotaremos por $[\mathfrak{l}_i]E$ (resp. $[\bar{\mathfrak{l}}_i]E$). En otras palabras, tal y como ya hemos visto en la sección 3.3, estamos buscando una isogenia

$$\varphi_{\mathfrak{l}_i} : E \to {}^{E}\!/_{\ker \varphi_{\mathfrak{l}_i}}$$

(respectivamente, $\varphi_{\bar{\mathfrak{l}}_i} : E \to {}^{E}\!/_{\ker \varphi_{\bar{\mathfrak{l}}_i}}$). Por tanto, lo que en realidad nos interesa es calcular el núcleo de dicha isogenia.

En cuanto tengamos el núcleo calculado podremos encontrar la isogenia explícitamente aplicando las fórmulas de Vélu, que introduciremos más adelante. Procedamos, pues, a ver cómo se calculan $\ker \varphi_{\mathfrak{l}_i}$ y $\ker \varphi_{\bar{\mathfrak{l}}_i}$.

[19] **Notación:** $\ell_i\mathcal{O}$ significa el ideal (ℓ_i) en $\mathcal{O}$.

[20] Decimos que ℓ_i es un primo de Elkies para $E(\mathbb{F}_p)$ si $\operatorname{Tr}(\pi)^2 - 4p$ es un cuadrado módulo ℓ_i, con $\operatorname{Tr}(\pi) = p + 1 - \#E(\mathbb{F}_p)$.

[21] De hecho, $\frac{p}{\lambda}$ es un abuso de notación, lo que realmente significa es cualquier representante entero de este cociente módulo ℓ_i.

Recordemos que $\mathfrak{l}_i = (\ell_i, \pi - 1)$ y entonces, como hemos expuesto en la sección 3.3, $\ker \varphi_{\mathfrak{l}_i} = \ker[\ell_i] \cap \ker[\pi - 1]$, de modo que es suficiente con encontrar un punto $P \in E(\mathbb{F}_p)$ tal que $\mathrm{ord} P = \ell_i$ y que quede fijo por el endomorfismo de Frobenius, pues si $P \in \ker[\pi - 1]$ entonces $(\pi - 1)(P) = \infty$, cosa que implica $\pi(P) - P = \infty$ y por tanto $\pi(P) = P$; equivalentemente, $P \in \mathbb{F}_p$. Para el caso de $\bar{\mathfrak{l}}_i$ tenemos que $\ker \varphi_{\bar{\mathfrak{l}}_i} = \ker[\ell_i] \cap \ker[\pi + 1]$, así que necesitamos que $P \in E$ tenga orden ℓ_i y $P \in \ker[\pi + 1]$, es decir, $(\pi + 1)(P) = \infty$, que es equivalente a $\pi(P) = -P$ y esto implica $\pi^2(P) = -\pi(P) = -(-P) = P$; por tanto, $P \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Todo esto nos dice, pues, que para empezar necesitamos este tal P y de hecho puede hallarse fácilmente siguiendo el siguiente procedimiento:

1. Elegimos una coordenada x aleatoriamente, $x \in \mathbb{F}_p$.
2. Comprobamos si $x^3 + Ax^2 + x$ es un cuadrado módulo p o no lo es. En el caso que sea un cuadrado, entonces el punto $Q = (x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ (donde hemos elegido y una de las raíces cuadradas de $x^3 + Ax^2 + x$) mientras que si no es un cuadrado entonces $Q = (x, y) \in \left(\mathbb{F}_{p^2} \setminus \mathbb{F}_p\right) \times \left(\mathbb{F}_{p^2} \setminus \mathbb{F}_p\right)$.
3. Calculamos $P = \frac{p+1}{\ell_i} Q$. Si $P = \infty$ volvemos a empezar, eligiendo una nueva coordenada x; en caso contrario, hemos encontrado un punto de orden exactamente ℓ_i (esto se debe a que $\ell_i P = (p + 1)Q = \infty$, de modo que $\mathrm{ord} P | \ell_i$, pero al ser ℓ_i primo entonces forzosamente tiene que ser $\mathrm{ord} P = \ell_i$).

En resumen, lo que tendríamos es:

Si $Q \in \mathbb{F}_p \times \mathbb{F}_p$ entonces $\ker \varphi_{\mathfrak{l}_i} = \langle P \rangle$.

Si $Q \in \left(\mathbb{F}_{p^2} \setminus \mathbb{F}_p\right) \times \left(\mathbb{F}_{p^2} \setminus \mathbb{F}_p\right)$ entonces $\ker \varphi_{\bar{\mathfrak{l}}_i} = \langle P \rangle$.

Una vez calculado el núcleo de la isogenia ya tenemos información suficiente para calcular la expresión exacta de la curva de llegada (esto es, el codominio de la isogenia). Para hacerlo, usaremos las fórmulas de Vélu, que aunque fueron definidas para curvas en forma de Weierstrass, hay una variante que las adapta a forma de Montgomery y cuyo resultado se muestra a continuación:

Teorema 4.4. *Para un cuerpo K con $\mathrm{char}(K) \neq 2$, sea $P \in E(\overline{K})$ un punto de orden $\ell = 2d + 1$ de la curva de Montgomery $E(K) : by^2 = x^3 + ax^2 + x$. Escribimos*

$$\sigma = \sum_{i=1}^{d} x_{[i]P}, \quad \tilde{\sigma} = \sum_{i=1}^{d} \frac{1}{x_{[i]P}}, \quad \pi = \prod_{i=1}^{d} x_{[i]P},$$

donde $x_{[i]P}$ denota la coordenada x del punto $[i]P$. La curva de Montgomery

$$E'(K) : b'y^2 = x^3 + a'x^2 + x$$

con

$$a' = (6\tilde{\sigma} - 6\sigma + a) \cdot \pi^2, \quad b' = b \cdot \pi^2$$

es el codominio de la ℓ-isogenia $\phi : E \to E'$ con $\ker(\phi) = \langle P \rangle$, que está definida por

$$\phi : (x, y) \mapsto (f(x), y \cdot f'(x)),$$

donde

$$f(x) = x \cdot \prod_{i=1}^{d} \left(\frac{x \cdot x_{[i]P} - 1}{x - x_{[i]P}} \right)^2,$$

y $f'(x)$ es su derivada.

Demostración. Ver [7], Teorema 1. □

De este teorema podemos deducir el siguiente resultado, que usaremos en el algoritmo para calcular la acción del grupo de clases:

Proposición 4.5. *Sea K un cuerpo finito con* $\mathrm{char}(K) \neq 2$ *y $E : y^2 = x^3 + Ax^2 + x$ una curva elíptica definida sobre K. Sea $\ell \geq 3$ un primo fijado y $P \in E(\overline{K})$ un punto de orden ℓ. Consideremos un entero $k \in \{1, \ldots, \ell - 1\}$ y sea $(X_k : Z_k)$ la coordenada x proyectivizada de $[k]P$. Entonces podemos calcular*

$$\tau = \prod_{i=1}^{\ell-1} \frac{X_i}{Z_i}, \quad \sigma = \sum_{i=1}^{\ell-1} \left(\frac{X_i}{Z_i} - \frac{Z_i}{X_i} \right)$$

de modo que $\tau(A - 3\sigma)$ es el coeficiente de Montgomery de la curva codominio de una isogenia de núcleo $\langle P \rangle$.

Demostración. Para empezar, consideremos la curva del teorema anterior con $b = 1$ y $a = A$ y notemos que $x = \frac{X}{Z}$ y, por tanto, $\frac{1}{x} = \frac{Z}{X}$. Observemos también que puesto que $\ell = 2d + 1$ entonces $d = \frac{\ell-1}{2}$ y además, $x_{[k]P} = x_{[\ell-k]P}$ para todo $k \in \{1, \ldots, (\ell - 1)/2\}$. Por tanto,

$$\pi = \prod_{k=1}^{d} x_{[k]P} = \prod_{k=1}^{\frac{\ell-1}{2}} x_{[k]P}$$

de modo que $\pi^2 = \tau$.
Para evitar confusiones de notación, pondremos $\sigma_* = \sum_{i=1}^{\ell-1} \left(\frac{X_i}{Z_i} - \frac{Z_i}{X_i} \right)$ y como

$$\sigma = \sum_{k=1}^{d} x_{[k]P} = \sum_{k=1}^{\frac{\ell-1}{2}} x_{[k]P}, \quad \tilde{\sigma} = \sum_{k=1}^{d} \frac{1}{x_{[k]P}} = \sum_{k=1}^{\frac{\ell-1}{2}} \frac{1}{x_{[k]P}}$$

entonces $\sigma_* = 2(\sigma - \tilde{\sigma})$. El teorema dice que $a' = (6\tilde{\sigma} - 6\sigma + a) \cdot \pi^2$ y $b' = b \cdot \pi^2$ de modo que, sustituyendo, obtenemos

$$a' = (A - 3\sigma_*)\tau, \quad b' = \tau$$

y por tanto $E' : \tau y^2 = x^3 + \tau(A - 3\sigma_*)x^2 + x$. Si consideramos el cambio de variables $\tilde{y} = \sqrt{\tau} y$ (este cambio es totalmente válido pues $\tau = \pi^2$, lo que significa que τ es un cuadrado módulo p y entonces podemos tomar su raíz cuadrada) entonces la curva que obtenemos es

$$\tilde{E}' : \tilde{y}^2 = x^3 + \tau(A - 3\sigma_*)x^2 + x,$$

que es exactamente la que nos proporciona la proposición. □

En resumen, el procedimiento de cálculo puede implementarse paso a paso mediante el siguiente algoritmo:

Algorithm 2: Calcular la acción del grupo de clases

Input: p primo, lista de primos distintos e impares $l = (\ell_1, \ldots, \ell_n)$ tales que $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, $A \in \mathbb{F}_p$, lista de enteros $e = (e_1, \ldots, e_n)$.

Output: B tal que $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E_A = E_B$, con $E_A : y^2 = x^3 + Ax^2 + x$ y $E_B : y^2 = x^3 + Bx^2 + x$.

while algún $e_i \neq 0$ **do**
  Elegimos $x \in \mathbb{F}_p$ aleatoriamente.
  if $x^3 + Ax^2 + x$ es un cuadrado en $\mathbb{F}_p$ **then** tomamos $s = +1$
  else $s = -1$.
  Definimos $S = \{i \mid e_i \neq 0,\ \text{sign}(e_i) = s\}$.
  if $S = \emptyset$ **then** volvemos a empezar eligiendo un nuevo x.
  Ponemos $k = \prod_{i \in S} \ell_i$.
  Calculamos $Q = [(p+1)/k]P$.
  for cada $i \in S$ **do**
    Calculamos $R = [k/\ell_i]Q$.
    if $R = \infty$ **then** pasamos al siguiente i.
    Calculamos la isogenia $\varphi : E_A \to E_B$ con $\ker \varphi = R$.
    Ponemos $A = B$, $Q = \varphi(Q)$, $k = k/\ell_i$, $e_i = e_i - s$.
  end
end
return A.

Puesto que $\text{cl}(\mathcal{O})$ es conmutativo y únicamente modificamos el valor de e_i cuando ya hemos aplicado la acción del ideal $\mathfrak{l}_i^{\pm}$ a la curva correspondiente, este algoritmo calcula la acción de $[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]$.

4.5. Implementación de los algoritmos

Después de haber estudiado detalladamente el funcionamiento del protocolo de intercambio de claves CSIDH, he decidido implementarlo yo misma y comprobar que realmente funciona. Para llevar a cabo esta tarea he usado SageMath, un sistema algebraico computacional que, aunque abarca muchas ramas de las matemáticas, fue inicialmente desarrollado para trabajar con curvas elípticas y formas modulares.[22] El código puede encontrarse en el apéndice.

Para reproducir el Algoritmo 1 he escrito una función `supersing` que dada una curva elíptica E sobre un cuerpo finito de p elementos y una lista de primos `l`=$[\ell_1, \ldots, \ell_n]$ (de manera que $p = 4 \cdot \ell_1 \cdots \ell_n - 1$) nos dice si la curva es supersingular u ordinaria. En el caso de que únicamente considerásemos curvas de Montgomery, me he permitido la licencia de modificar ligeramente el algoritmo y, en vez de pasar la curva elíptica `E` como argumento, lo he simplificado de modo que solamente sea necesario pasar el coeficiente `A` de la ecuación (y la lista `l` también, por supuesto); luego defino la curva dentro de la función, cosa que supone un ahorro de cálculos previos a la invocación del algoritmo. A esta segunda función la he llamado `supersing_A`.

Para comprobar el funcionamiento del código he calculado (mediante prueba y error) varios valores para p, considerando diversos números primos pequeños $\ell_1, \ldots, \ell_n$ y probando si $4 \cdot \ell_1 \cdots \ell_n - 1$ era primo. A continuación he definido una curva elíptica en forma

[22] Ver [19] para más detalles.

de Montgomery sobre $\mathbb{F}_p$, tomando un valor aleatorio para A, y he probado el algoritmo; para confirmar que el resultado obtenido era el correcto he usado el método ya implementado en SageMath llamado `is_supersingular`. Después de múltiples experimentos puedo concluir que, aunque en general el algoritmo funciona, si p es demasiado pequeño falla. Por ejemplo, si tomamos $p = 4 \cdot 3 \cdot 7 - 1 = 83$ y $A = 11$ el método nunca llega a decir que, en efecto, la curva $y^2 = x^3 + 11x^2 + x$ es supersingular; esto se debe a que $d \leq \ell_1 \cdot \ell_2 = 21$ y $4\sqrt{p} \approx 36{,}44$ de modo que nunca se llega a tener $d > 4\sqrt{p}$. En resumen, para garantizar un correcto funcionamiento del algoritmo debemos tener en cuenta que el producto de todos los elementos de `l` sea mayor que $4\sqrt{p}$.

El Algoritmo 2 es más complicado que el anterior, así que para facilitar la escritura del programa he definido cuatro rutinas que, combinadas, permiten calcular la acción de un ideal en una curva elíptica. Las tres primeras funciones– `mult_P`, `tau`, `sigma`– son sencillas y calculan, respectivamente, todos los múltiplos de un punto P y las funciones τ y σ presentadas en la Proposición 4.5. La última función y la que propiamente calcula la acción del grupo de clases la he llamado `class_group_action`; esta rutina recibe un número primo `p` (del tipo `p` $= 4 \cdot \ell_1 \cdots \ell_n - 1$), el coeficiente `A` de una curva elíptica escrita en forma de Montgomery (es decir, con ecuación $y^2 = x^3 + Ax^2 + x$), una lista `l` $= [\ell_1, \ldots, \ell_n]$ y otra lista `es` de longitud n que contiene los exponentes de cada ideal $\mathfrak{l}_i$ (que está generado por ℓ_i y $\pi - 1$ o bien por ℓ_i y $\pi + 1$).

La descripción del código es la siguiente. Para empezar, copio en `e` la lista `es`, porque en la función vamos a modificar las componentes pero después nos interesará recuperar las originales. A continuación, para cada índice de `e`, mientras la componente de esa posición no sea cero, elegimos aleatoriamente un elemento de $\mathbb{F}_p$ que llamaremos `x`; calculamos `x`$^3 +$ `A`$x^2 +$ `x` módulo `p` con la función `Mod` y, utilizando el método `is_square`, comprobamos si es un cuadrado. En caso de serlo, ponemos `s=1` y definimos el cuerpo base `K` como un cuerpo finito de `p` elementos (`GF(p)`) y la curva `E` sobre `K`; para obtener un punto `P` en `E` con coordenada `x` utilizo el método `lift_x`. Si `x`$^3 +$ `A`$x^2 +$ `x` no es un cuadrado módulo `p` entonces defino `s=-1` y el cuerpo base `K` como el cuerpo finito de `p`^{2} elementos (`GF(p`^{2}`)`) y procedo de manera análoga.

Después defino `S` como una lista de los índices de `e` tales que el signo del elemento correspondiente coincide con `s`; si no hubiese ningún elemento con estas características, entonces volvemos a empezar eligiendo un nuevo `x`. A continuación defino `k` como el producto de los ℓ_i's cuyo índice se corresponde con los índices de la lista `S` y calculo el punto `Q` $=$ `(p + 1)/k * P` (en el código indico explícitamente que $(p+1)/k$ es un entero para que se pueda realizar el producto correctamente, pues si no se especifica da error). Luego, para cada índice de `S`, defino el punto `R` a partir de `Q` tal y como se indica en la descripción del Algoritmo 2; si resulta que `R` es el elemento neutro pasamos al siguiente índice y en caso contrario procedemos con el algoritmo, calculando el valor de `tau`. Si `tau` es cero, entonces ya sé que `B` será también cero (pues se obtiene a partir de un producto que involucra `tau`) y por tanto puedo poner directamente `B=0` y ahorrarme el paso de calcular `sigma`; si en cambio `tau` es no nulo, calculo `sigma` y a continuación `B` a partir de ambos valores. Ya para acabar, defino la curva codominio `EB` con coeficiente de Montgomery `B` y usando el método `EllipticCurveIsogeny` calculo la isogenia `phi` entre `E` y `EB`. Redefino `A, E, Q` a partir de los nuevos valores calculados, actualizo `k` y resto (si `s=1`) o sumo (si `s=-1`) una unidad a la componente de `e` del índice sobre el que estemos trabajando. Cuando todas las componentes del vector `e` son cero, el algoritmo acaba y devuelve el último coeficiente de Montgomery que haya encontrado.

Para verificar el funcionamiento del algoritmo, igual que en el caso del Algoritmo 1, he

probado con distintos valores de p que he calculado mediante prueba y error. Las claves secretas de Alice y Bob (que he llamado `eA` y `eB`, respectivamente) las he definido creando una lista de enteros aleatorios en el rango $\{-m, m\}$ de longitud igual a la de `l`. Primero he calculado la clave pública de Alice aplicando `class_group_action` con su clave secreta `eA` y luego he calculado la de Bob, esta vez usando `eB`. Para calcular el secreto compartido he invocado el algoritmo usando primero el coeficiente de Bob (que he denotado simplemente por `Bob`) y el secreto de Alice `eA` y a continuación he usado el coeficiente de Alice (definido como `Ali`) y la clave de Bob `eB`. He verificado que efectivamente el resultado de ambas operaciones sea el mismo y, en el caso de coincidir (cosa que debe pasar si el método funciona), imprimo este valor. He podido observar que, como era de esperar, como mayor sea p más tarda el programa en realizar los cálculos y dar el resultado.

El siguiente ejemplo es una muestra de lo que permite calcular el código. Si tomamos `l =[3,5,7,11,13,17,19,23,29,31,37,41,47,73,79,83,89,97,103,113,131,157,167, 181,193,257]` obtenemos el siguiente resultado:

```
La clave secreta de Alice es [9, -8, -8, 2, -6, 3, 6, -5, 7, -2, 0, 7, -3,
8, -9, 9, 3, -1, 0, 3, -2, 9, -10, -5, -2, 10]
La clave secreta de Bob es [-1, -9, -9, -5, 4, 1, -3, -9, -2, -2, 10, -2, -8,
6, -7, 10, -8, 2, -10, -10, 9, 0, 3, -6, 1, -8]
El primo p es 424151196033164929603179190681304373361096l9
La clave pública de Alice es 191274861661783577218873727258l7633640410807
La clave pública de Bob es 9863574789389674139576666409589259236539107
El secreto compartido es 335037136619083992338037233794673641763l6993
```

Es decir, la curva elíptica que obtiene Alice después de aplicar la acción de su correspondiente ideal es

$$E_A : y^2 = x^3 + 191274861661783577218873727258l7633640410807x^2 + x$$

mientras que Bob obtiene

$$E_B : y^2 = x^3 + 9863574789389674139576666409589259236539107x^2 + x.$$

Finalmente, la curva compartida es

$$E_S : y^2 = x^3 + 335037136619083992338037233794673641763l6993x^2 + x.$$

Haciendo un análisis del tiempo de cálculo, he podido observar que el tiempo que tarda el programa en calcular solamente una acción del grupo de clases (es decir, calcular A o B o S una vez ya tenemos A y B) es del orden de 3 minutos. Por tanto, para calcular el intercambio de claves completo (que supone calcular cuatro acciones del grupo de clases) usando este primo p de 44 cifras, se tarda un total de 12 minutos, aproximadamente.

5. Conclusiones

A través de este trabajo hemos podido entender el funcionamiento del protocolo de intercambio de claves CSIDH, presentado como un método de encriptación posiblemente resistente a los ataques realizados por ordenadores cuánticos.

Este algoritmo se basa en la idea propuesta por Couveignes en 2006 (recordemos que aunque su hallazgo data de 1997 no fue publicado hasta 9 años más tarde) que, aunque parecía prometedora, tiene un gran inconveniente que es la ineficiencia computacional. Por este motivo Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny y Joost Renes decidieron aprovechar la base matemática ya existente y desarrollar un nuevo criptosistema. Podríamos pensar, pues, en el algoritmo CSIDH como una mejora del método que propuso Couveignes. Las ideas claves están en el uso de curvas elípticas supersingulares definidas sobre un cuerpo finito de p elementos $\mathbb{F}_p$, donde p es un primo de la forma $4 \cdot \ell_1 \cdots \ell_n - 1$ con $\ell_1, \ldots, \ell_n$ primos distintos impares, y en considerar únicamente aquellos endomorfismos definidos en $\mathbb{F}_p$ en vez de tomar el anillo de endomorfismos completo. La principal ventaja de esta segunda elección, tal y como hemos visto en el trabajo, es que $\mathrm{End}_p(E)$ es isomorfo a un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario y, en particular, es conmutativo. Con esto podemos definir el grupo de clases de ideales de $\mathcal{O}$, $\mathrm{cl}(\mathcal{O})$, que también es conmutativo, y una acción de $\mathrm{cl}(\mathcal{O})$ en $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$.

Una vez tenemos $\mathrm{cl}(\mathcal{O})$ y $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ ya podemos proceder con el intercambio de claves. Dos individuos, Alice y Bob, eligen un número primo p de la forma descrita anteriormente; esta información es pública. Las claves privadas corresponden a ideales de $\mathcal{O}$. Tomando como curva de partida $E_0 : y^2 = x^3 + x$ (que ya hemos demostrado que es supersingular), Alice y Bob calculan la acción de su correspondiente ideal sobre E_0 y obtienen, respectivamente, las curvas supersingulares $E_A : y^2 = x^3 + Ax^2 + x$ y $E_B : y^2 = x^3 + Bx^2 + x$. Los coeficientes A y B son las claves públicas de su correspondiente propietario y son las que se usan para calcular el secreto compartido. En efecto, si Alice calcula la acción de su ideal sobre E_B obtiene una curva E_S, que gracias a la conmutatividad de $\mathrm{cl}(\mathcal{O})$ resulta ser la misma que la que Bob obtiene al calcular la acción de su ideal sobre la curva de Alice E_A.

En resumen, aunque este protocolo criptográfico tenga una base matemática potente y no especialmente fácil de comprender, resulta eficiente y ofrece un futuro alentador para la criptografía postcuántica. Por supuesto, todavía hay mucho trabajo que hacer para convenir si este algoritmo es realmente resistente a los ataques cuánticos, pero quién sabe, quizá dentro de unos años CSIDH esté presente en nuestro día a día.

A. El código

En esta sección adjunto el código que he escrito en Sage implementando los algoritmos. El Algoritmo 1 es simplemente el descrito en la sección 4.3 y el Algoritmo 1_bis es una pequeña modificación del anterior para curvas de Montgomery. El Algoritmo 2 corresponde al expuesto en la sección 4.4.

```
# ALGORITMO 1
def supersing(E, l):
    p= 4*prod(l)-1
    d=1
    fin= None
    P= E.random_point()
    for i in range(len(l)):
        Q= Integer((p+1)/l[i])*P
        if(l[i]*Q!= E(0)):
            print("Ordinaria")
            fin= 1
            break
        else:
            d= d*l[i]
            4*sqrt(p).numerical_approx()
            if(bool(d>4*sqrt(p))==True):
                print("Supersingular")
                fin= 1
                break
    if(fin!=1):
        print("El orden del punto aleatorio es demasiado pequeño.
              Vuélvelo a intentar")


# ALGORITMO 1_bis para curvas de Montgomery
def supersing_A(A, l):
    p= 4*prod(l)-1
    E= EllipticCurve(GF(p), [0,A,0,1,0])
    d=1
    fin= None
    P= E.random_point()
    for i in range(len(l)):
        Q= Integer((p+1)/l[i])*P
        if(l[i]*Q!= E(0)):
            print("Ordinaria")
            fin= 1
            break
        else:
            d= d*l[i]
            4*sqrt(p).numerical_approx()
            if(bool(d>4*sqrt(p))==True):
                print("Supersingular")
```

```
                fin= 1
                break
    if(fin!=1):
        print("El orden del punto aleatorio es demasiado pequeño.
              Vuélvelo a intentar")


# ALGORITMO 2
import numpy
def mult_P(P): # función que devuelve una lista con las coordenadas x de los
 múltiplos de P (excepto el neutro). La lista tiene tamaño l-1.
    l= P.order()
    P_list= [P[0]]
    for i in range(2, l):
        P_list.append((i*P)[0])
    return P_list

def tau(P):
    P_list= mult_P(P)
    return numpy.prod(P_list)


def sigma(P):
    P_list= mult_P(P)
    sigma= P_list[0]-1/P_list[0]
    for i in range(1, len(P_list)):
        sigma+= (P_list[i]-1/P_list[i])
    return sigma

def class_group_action(p, A, l, es):
    F= GF(p)
    e= copy(es)
    for i in range(len(e)):
        while(e[i]!=0):
            k=1
            x= F.random_element(); 'x=' + str(x)
            if(Mod(x^3+A*x^2+x, p).is_square()): # si es un cuadrado entra
                en el bucle
                s= 1
                K= GF(p)
                E= EllipticCurve(K, [0,A,0,1,0]); E
                P= E.lift_x(x); P # da un punto de E con coordenada x
            else:
                s= -1
                K= GF(p^2, 'a')
                E= EllipticCurve(K, [0,A,0,1,0]); E
                P= E.lift_x(x); P # da un punto de E con coordenada x
            S= [idx for idx, val in enumerate(e) if val != 0 and sgn(val)==s];
```

```
            if not S:
                continue # si S es vacío, elegimos otro x
            for idx in S:
                k*=l[idx]
            Q= Integer((p+1)/k)*P
            for idx in S:
                R= Integer(k/l[idx])*Q
                if(R==E(0)):
                    continue # pasamos al siguiente índice
                tau_0= tau(R)
                if(tau_0 != 0): # si ningún x_i es 0 entonces tau!=0
                    y por tanto necesitamos sigma
                    sigma_0= sigma(R)
                    B= tau_0*(A-3*sigma_0)
                else:
                    B=0 # si tau=0 entonces B=0
                EB= EllipticCurve(K, [0,B,0,1,0])
                phi= EllipticCurveIsogeny(E, R, codomain=EB) # fórmula
                    explícita de la isogenia de E a EB
                A= B
                E= EB
                Q= phi(Q); Q
                k= k/l[idx]
                e[idx]-= s
    return A
```

Finalmente, para probar el código y obtener el resultado como el que se muestra en la sección 4.5 he escrito el siguiente programa:

```
# Simulación del intercambio de claves
# eA:= clave secreta Alice, eB:= clave secreta Bob
l=l_5  # Definimos la lista l
eA= [randint(-10,10) for i in range(len(l))]
print 'La clave secreta de Alice es', eA
eB= [randint(-10,10) for i in range(len(l))]
print 'La clave secreta de Bob es', eB
p= 4*prod(l)-1
print 'El primo p es', p

Ali= class_group_action(p,0,l,eA)
print 'La clave pública de Alice es', Ali
Bob= class_group_action(p,0,l,eB)
print 'La clave pública de Bob es', Bob

Ali_S= class_group_action(p,Bob,l,eA)
Bob_S= class_group_action(p,Ali,l,eB)

if(Ali_S==Bob_S):
    print 'El secreto compartido es', Ali_S
```

Referencias

[1] Roland Auer and Jaap Top. Legendre elliptic curves over finite fields, 2001.

[2] Frits Beukers. Algebraic number theory. Notas proporcionadas por mi director, February 2011.

[3] Brian Koziel, A.-Bon Ackie, Rami El Khatib, Reza Azarderakhsh and Mehran Mozaffari Kermani. SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. *IEEE Transactions on Circuits and Systems I-regular Papers*, pages 1–13, 2020.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An Efficient Post-Quantum Commutative Group Action. In *Advances in Cryptology –ASIACRYPT 2018*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[5] Cathal O'Connell. Quantum computing for the qubit curious. [Online; consultado 10-Junio-2020].

[6] Chris Peikert. He Gives C-Sieves on the CSIDH. Cryptology ePrint Archive, Report 2019/725, 2019.

[7] Craig Costello and Hüseyin Hisil. A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. *IACR Cryptol. ePrint Arch.*, 2017:504, 2017.

[8] Cox, D.A. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.

[9] Jean Marc Couveignes. Hard Homogeneous Spaces. *IACR Cryptol. ePrint Arch.*, 2006:291, 2006.

[10] Josh Lake. What is the Diffie–Hellman key exchange and how does it work? [Online; consultado 11-Junio-2020].

[11] José Manuel Udías Monielo. ¿Qué es el momento angular de una partícula? ¿Y el espín? [Online; consultado 10-Junio-2020].

[12] Janis Klaise. Orders in quadratic imaginary fields of small class number. *Preprint*, 2012.

[13] Luca De Feo and David Jao and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506, 2011.

[14] Marcus, D.A. *Number Fields*. Universitext. Springer International Publishing, 2018.

[15] Martin Giles. Explainer: What is a quantum computer? [Online; consultado 10-Junio-2020].

[16] NIST. NIST, Post-Quantum Cryptography, 2017-2020. [Online; consultado 17-Junio-2020].

[17] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[18] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[19] William Stein and David Joyner. Sage: System for algebra and geometry experimentation. *Communications in Computer Algebra (SIGSAM Bulletin)*, 39, 07 2005.

[20] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[21] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and Its Applications. CRC Press, 2008.

[22] Eric W. Weisstein. Algebraic closure. From MathWorld–A Wolfram Web Resource. Online; última consulta 19-Junio-2020.

[23] Wikipedia contributors. Elliptic-curve Diffie–Hellman — Wikipedia, The Free Encyclopedia, 2020. [Online; consultado 19-Junio-2020].

[24] Wikipedia contributors. Euler's criterion — Wikipedia, the free encyclopedia, 2020. [Online; consultado 1-Junio-2020].