Criptografía basada en Isogenias

Dr. Carlos Vela Cabello

Criptografía basada en Isogenias

Dr. Carlos Vela Cabello

Memoria presentada como parte de los requisitos para la obtención del título de Máster Universitario en Matemáticas por la Universidad de Sevilla.

Tutorizada por

Prof. Dra. Sara Arias de Reyna

Índice general

English Abstract

In this project we will make an introduction to the Diffie-Hellman key exchange protocol based on iogenies of supersingular elliptic curves. Firstly, we will study some bibliography about elliptic curves and define the supersingular elliptic curves. Secondly, we will review the concept of isogeny and construct the base for our key exchange protocol, the ℓ-isogeny graphs. Later, a detailed explanation of this protocol will be given together with an exhaustive example of it. Finally, a SAGEMath programm will be developed to make instances of the protocol according to this project.

1 Curvas Elípticas

En este capítulo haremos una introducción de todos los conceptos previos necesarios para cumplir con el objetivo de este trabajo de fin de máster, comprender la criptografía basada en isogenias. Para ello, comenzaremos definiendo qué son las curvas elíticas y veremos algunos aspectos y resultados sobre ellas. Acabaremos estudiando las aplicaciones entre curvas elípticas, como son los isomorfismos.

Para este capítulo supondremos que K es un cuerpo y $\bar{K}$ es su clausura algebraica.

Empezaremos con la definición de curvas elípticas para continuar describiendo muchas de sus propiedades las cuales nos servirán para poder construir un protocolo criptográfico basado en aplicaciones entre curvas elípticas, las isogenias.

Definición 1.1. *El* **espacio proyectivo de dimensión** *n, es el conjunto de clases*

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{\mathbf{0}\})/\sim$$

donde dos vectores u y v están relacionados:

$$u \sim v \iff \text{existe un } \lambda \neq 0 \text{ tal que } u = \lambda v.$$

Nótese que los puntos en el **plano proyectivo** tienen tres coordenadas $[x_0 : x_1 : x_2]$, no simultaneamente nulas que verifican que:

$$[x_0 : x_1 : x_2] = [x_0' : x_1' : x_2'] \iff rango\left(\begin{bmatrix} x_0 & x_1 & x_2 \\ x_0' & x_1' & x_2' \end{bmatrix}\right) = 1$$

Con respecto al plano proyectivo, nos queda recordar que contiene al plano afín habitual (recordemos que el espacio afín es el conjunto $\mathbb{A}^n(K) = K^n$), con la aplica-

ción:

$$\begin{array}{rcl} \phi_0 : K^2 & \to & \mathbb{P}^2(K) \\ (a,b) & \mapsto & [1:a:b] \end{array}$$

De igual forma que esta aplicación, también están definidas ϕ_i con $i \in 1,2$ donde se fija el 1 en cualquiera de las otras dos coordenadas. Esta contención puede considerarse con cualquiera de las tres aplicaciones.

Definición 1.2. *Sea $d \geq 1$ un entero. A un polinomio de $K[X,Y,Z]$ se le llama* **homogeneo de grado** *d si*

$$F(X,Y,Z) = \sum_{\substack{i+j+k=d \\ i,j,k\geq 0}} c_{ijk} X^i Y^j Z^k$$

donde los coeficientes $c_{ijk} \in K$.

Definición 1.3. *Sea $F \in K[X,Y,Z]$ un polinomio homogéneo de grado d. Se define el lugar de F en el plano proyectivo $\mathbb{P}^n(K)$ como*

$$C_F(K) = \{P \in \mathbb{P}^n(K) | F(P) = 0\}.$$

De forma análoga se puede definir el lugar en el plano afín de un polinomio $f \in K[x,y]$, como

$$C_f(K) = \{P \in K^n | f(P) = 0\}.$$

Es decir, estamos considerando los puntos del espacio en los que un polinomio sobre un cuerpo K sea nulo.

Ejemplo 1.1. Sea $K = \mathbb{F}_3$, consideramos el polinomio $F[X,Y,Z] \in = X^2 + Y^2 - Z^2$, y nótese que es homogéneo de grado 2. Entonces

$$C_F(K) = \{[1:0:1],[0:1:1],[0:2:1],[2:0:1]\}$$

Vamos a considerar ahora el siguiente conjunto de pares, polinomios homogéneos y sus lugares en el espacio:

$$M = \{(C,F) \mid F \in K[X,Y,Z] \text{ homogéneo}, C = C_F(K)\},$$

y dentro de este conjunto la siguiente relación de equivalencia:

$$(C_1,F_1) \sim (C_2,F_2) \Leftrightarrow C_1 = C_2 \text{ y existe } \lambda \in K^\times \text{ tal que } F_1 = \lambda F_2$$

Una **curva proyectiva** es una clase de equivalencia de $M/\sim$. Cuando hablemos de una de estas clases de equivalencia, (C_F, K), la denotaremos como C_F/K o bien C/K.

Definición 1.4. *Dada una curva afín C_f/K con f homogéneo, existe una curva proyectiva, denotada C_F/K, del mismo grado que C_f/K, tal que*

$$C_F(K) \cap U_2 = \phi_2(C_f(K))$$

Una tal curva se llama **clausura proyectiva** *o* **proyectivización de** C_f.

Para ver de forma general este proceso vamos a considerar el siguiente polinomio afín de grado d:

$$f(x,y) = \sum_{0\le k\le d} \left(\sum_{i+j=k} c_{ijk} x^i y^j \right)$$

Entonces, su clausura proyectiva F correspondiente a la definición será:

$$F(X,Y,Z) = \sum_{0\le k\le d} \left(\sum_{i+j=k} c_{ijk} X^i Y^j Z^{d-k} \right)$$

De esta manera a cada polinomio afín f de grado d se le asigna un polinomio proyectivo F homogéneo de grado d. También se puede considerar a la inversa y asignar un polinomio afín f a un polinomio proyectivo homogéneo F, en ese caso f es la **deshomogeneización** de F respecto de la variable Z.

Ejemplo 1.2. Si retomamos el ejemplo 1.1, tenemos un polinomio $F \in \mathbb{F}_3[X,Y,Z]$ definido como $F(X,Y,Z) = X^2 + Y^2 - Z^2$. La desproyectivización de F entonces será $f \in K[x,y]$ definido como $f(x,y) = x^2 + y^2 - 1 = x^2 + y^2 + 2$. De esta manera podemos ver que:

$$C_f(K) = \{(0,1),(0,2),(1,0),(2,0)\}.$$

Además, es fácil ver que se cumple que la definición ya que

$$\phi_2(C_f(K)) = \{[0:1:1],[0:2:1],[1:0:1],[2:0:1]\}.$$

.

Definición 1.5. *Sea K un cuerpo. Una* **ecuación de Weierstraβ** *es una ecuación $f = 0$ donde $f \in K[X,Y,Z]$ es un polinomio homogéneo de grado 3 de la forma:*

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

o, equivalentemente,

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$.

La deshomogeneización de una ecuación de Weiestraβ con respecto a la variable Z es el polinomio afín

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6. \tag{1.1}$$

En lo que resta de trabajo, cada vez que nos refiramos a una ecuación de Weiestraβ nos estaremos refiriendo a esta o su forma deshomogeneizada dependiendo del contexto. Si hubiera cabida a diferentes interpretaciones se aclarará a cual se hace referencia.

Antes de continuar es importante hablar sobre las extensiones del cuerpo sobre el que se define una curva y como afecta esto a la curva. Empecemos con un ejemplo, tomemos la ecuación $f(x, y) = \frac{x^2}{4} + \frac{y^2}{9} + 1$. Es fácil ver que $C_f(\mathbb{R}) = \emptyset$ y sin embargo $C_f(\mathbb{C}) \neq \emptyset$ ya que, por ejemplo $(0, 3i) \in C_f(\mathbb{C})$. Este es un ejemplo trivial de algo que se da en general en una extensión de cuerpos (incluidos cuerpos finitos) y es que dada dicha extensión $K \subseteq E$ tenemos que $C_f(K) = C_f(E) \cap \mathbb{A}^2(K)$. Concretamente, y es el caso que más nos interesa, se da que $C_f(K) \subseteq C_f(\bar{K})$. Para más *inri*, esta igualdad también se da en el plano proyectivo, i.e., dado un polinomio homogéneo F, bajo la misma extensión de cuerpos tenemos que $C_F(K) = \mathbb{P}^2(K) \cap C_F(E)$.

Definición 1.6. *Sea* $F \in K[X, Y, Z]$ *un polinomio homogéneo de grado* d*, sea* $C_F(K)$ *la curva proyectiva definida por* F*, y sea* $[a : b : c] \in \mathbb{P}^2(K)$ *un punto de la curva* ($F(a, b, c) = 0$)*. Diremos que la curva* C_F/K *es* **singular en el punto** $[a : b : c]$ *si*

$$\frac{\partial F}{\partial X}(a, b, c) = \frac{\partial F}{\partial Y}(a, b, c) = \frac{\partial F}{\partial Z}(a, b, c) = 0$$

Diremos que la curva C_F/K *es* **regular, no singular o lisa** *si la curva* $C_F(\bar{K})$ *es no singular en todos sus puntos.*

Es importante observar que para que una curva C_F/K sea regular o lisa no debe haber ningún punto singular sobre la extensión del cuerpo. Nótese que se puede definir de igual forma una curva afín C_f/K **regular o lisa** de forma análoga, i.e., que será lisa si la derivada en todos sus puntos es distinta de 0.

Un detalle a destacar es que, a pesar de que la definición de curva lisa es análoga en ambos contextos, afín y proyectivo, la proyectivización de una curva lisa C_f (desproyectivización de una curva C_F) no tiene porqué ser lisa.

Ejemplo 1.3. Esta vez vamos a considerar el polinomio $f \in \mathbb{F}_5[x, y]$ definido como $f(x, y) = x^3 - y + 3x + 2$. Ahora calculamos,

$$\frac{\partial f}{\partial x}(x, y) = 3x^2 + 3 \; ; \quad \frac{\partial f}{\partial y}(x, y) = -1 = 4$$

Por lo que podemos deducir que la curva es lisa ya que sus derivadas nunca podrán ser nulas. Veamos ahora si la proyectivización de esta ecuación $F \in \mathbb{F}_5[X, Y, Z]$ es, o no, lisa:

$$F(X, Y, Z) = X^3 - YZ^2 + 3XZ^2 + 2Z^3$$

$$\frac{\partial F}{\partial X}(X, Y, Z) = 3X^2 + 3Z^2$$
$$\frac{\partial F}{\partial Y}(X, Y, Z) = -Z^2$$
$$\frac{\partial F}{\partial X}(X, Y, Z) = -2YZ + XZ + Z^2$$

En este caso, la curva NO es lisa ya que tiene un punto (del infinito) $[0 : 1 : 0]$ que es singular.

Definición 1.7. *[7, I.3] Sean C_{F_1} y C_{F_2} dos curvas definidas por ecuaciones de Weiestraß en $\mathbb{P}^2(K)$. Una aplicación racional de C_{F_1} a C_{F_2} es una aplicación de la forma:*

$$\phi : C_{F_1} \longrightarrow C_{F_2}, \quad \phi = [g_0, g_1, g_2]$$

donde las funciones $g_1, g_2, g_3 \in \bar{K}(V_1)$ tienen la propiedad de que en cada punto $P \in C_{F_1}$ en el que g_1, g_2 y g_3 están definidas se cumple que:

$$\phi(P) = [g_1(P), g_2(P), g_3(P)] \in C_{F_2}$$

donde las aplicaciones g_i son funciones racionales.

Proposición 1.1. [7, II.2] Sea C_{F_1} una curva lisa y C_{F_2} otra curva, ambas proyectivas y $\phi : C_{F_1} \to C_{F_2}$ una aplicación racional. Entonces ϕ es un morfismo.

Definición 1.8. *Dos curvas C_{F_1} y C_{F_2} son* **isomorfas** *si existen dos morfismos $\phi_1 : C_{F_1} \longrightarrow C_{F_2}$ y $\phi_2 : C_{F_2} \longrightarrow C_{F_1}$ tales que $\phi_1 \circ \phi_2 = Id$ donde Id es el el morfismo identidad, que manda cada punto a sí mismo.*

Teorema 1.1. *Sea C_f una curva dada por una fórmula de Weiestraβ definida sobre un cuerpo K que cumple que $char(K) \neq 2, 3$. Entonces, es isomorfa a otra curva $C_{f'}$, donde:*

$$f' = y^2 - x^3 - Ax - B \tag{1.2}$$

donde $A, B \in K$.

De esta manera, si la característica del cuerpo es distinta de 2 ó 3 nos bastará con dos elementos del cuerpo para identificar la curva.

Definición 1.9. *Una* **curva elíptica** *sobre un cuerpo K es una curva proyectiva C_f/K no singular tal que f es de Weiertraβ. Denotaremos las curvas elípticas por E_f/K o bien E/K si el polinomio es claro en el contexto.*

Para cada ecuación de Weiestraβ (1.1), se define el **discriminante** de la fórmula, Δ, como:

$$\begin{aligned}\Delta = -(a_1^2 + 4a_3)^2(a_1^2a_6 + 4a_3a_6 - a_1a_2a_4 + a_3a_2^2 - a_4^2) - 8(2a_4 + a_1a_2)^3 \\ - 27(a_2^2 + 4a_6)^2 + 9(a_1^2 + 4a_3)(2a_4 + a_1a_2)(a_2^2 + 4a_6).\end{aligned} \tag{1.3}$$

Si la característica del cuerpo sobre el que está definida la ecuación es distinta de 2 o 3, el caso de 1.2, el discriminante se puede simplificar de la siguiente manera:

$$\Delta = -16(4A^3 + 27B^2).$$

Ya tenemos una ligera idea de lo que es una curva elíptica sobre un cuerpo e incluso podemos definirla con dos elementos del cuerpo (A y B). Veamos ahora algunas propiedades de estas que nos interesan para nuestro fin. A partir de este momento, y con la intención de simplificar los resultado, supondremos que la característica de K es distinta de 2 y 3, i.e., $char(K) \neq 2, 3$.

Lema 1.1. Dada Una curva C_F/K donde F es una fórmula de Weiestraβ definida sobre un cuerpo K, C_F/K es una curva elíptica, si y solo si, $\Delta \neq 0$.

Como puede apreciarse, el discriminante nos permite identificar rápidamente si una fórmula de Weiestraβ es, o no, una curva elíptica. A continuación vamos a definir otro entero asociado a estas ecuaciones, el j-invariante:

$$j = \frac{((a_1^2 + a_3)^2 - 24(2a_4 + a_1a_2))^3}{\Delta}. \tag{1.4}$$

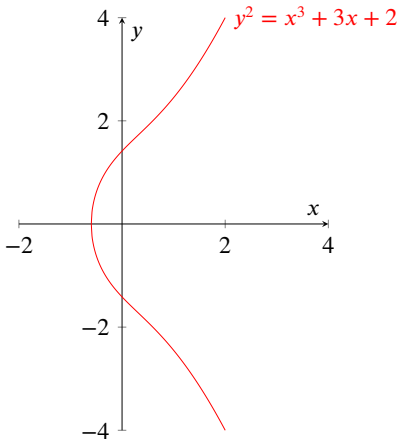


Figura 1.1: La curva elíptica sobre el cuerpo $\mathbb{R}$.

En el caso de que la característica del cuerpo sobre el que está definido la curva sea distinto de 2 ó 3 tendremos que:

$$j = -1728\frac{(4A)^3}{\Delta}$$

Al estar el discriminante, Δ, es de suponer que es un invariante de las curvas elípticas.

Ejemplo 1.4. Sea $K = \mathbb{F}_5$, este cuerpo tiene característica distinta de 2 o 3. Vamos a considerar la ecuación de Weiestraβ, $f \in K[x, y]$ donde $A = 3$ y $B = 2$, i.e.,

$$f(x, y) = y^2 - x^3 - 3x - 2 = y^2 + 4x^3 + 2x + 3.$$

Si calculamos su discriminante $\Delta = -16(4 \cdot 1^3 + 27 \cdot 2^2) = 3$ por lo que es una curva elíptica. También podemos ver que el j-invariante de nuestra curva elíptica es

$$j = -1728\frac{(4 \cdot 3)^3}{3} = -995328 = 3$$

Teorema 1.2. *Dos curvas elípticas son isomorfas sobre $\bar{K}$, si y solo si, tienen el mismo j-invariante.*

Ejemplo 1.5. Sea $p = 107$ y $\overline{\mathbb{F}_{107}}$ vamos a considerar las siguientes curvas elípticas

sobre este cuerpo finito:

$$\begin{aligned} E_1 &: \quad y^2 - x^3 - 39x - 1 \\ E_2 &: \quad y^2 - x^3 - 102x - 63 \end{aligned}$$

Es sencillo comprobar que son curvas elípticas verificando que $\Delta_1 = 4220$ y que $\Delta_2 = 898$. Ahora podemos calcular sus respectivos j-invariantes $j(E_1) = j(E_2) = 72$. Esto nos indica que estas curvas son isomorfas sobre $\overline{\mathbb{F}_{107}}$, la clausura algebraica de $\mathbb{F}_{107}$.

Ahora no sólo podemos identificar si una fórmula de Weiestraβ es elíptica, o no, si no que las podemos clasificar por su j-invariante.

Teorema 1.3. *Sea $j_0 \in \bar{K}$. Existe una curva elíptica definida sobre $\bar{K}$ cuyo j-invariante es j_0.*

Este último teorema nos dice que todas las clases de equivalencia de las curvas elípticas sobre un cuerpo son no vacías.

Debemos introducir el punto $\mathcal{O} = [0 : 1 : 0]$ como el punto del infinito. Éste es el único punto en las curvas elípticas que se encuentra en en la recta $Z = 0$.

Definición 1.10. *Sea $E = C_f/K$ una curva elíptica donde $f : y^2 = x^3 + ax + b$. Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ dos puntos de E diferentes del punto del infinito. Definimos la operación $\oplus$ en E como sigue:*

- $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$ *para todo* $P \in E$
- *Si* $x_1 = x_2$ *y* $y_1 = -y_2$ *entonces* $P_1 \oplus P_2 = \mathcal{O}$.
- *En otro caso tenemos que* $P_1 \oplus P_2 = (x_3, y_3)$ *tales que:*
  - $x_3 = \lambda^2 - x_1 - x_2$
  - $y_3 = -\lambda x_3 - y_1 + \lambda x_1$
  - $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_2} & \text{if } P = Q \end{cases}$

Proposición 1.2. El par $(E(K), \oplus)$ es un grupo abeliano conmutativo, cuyo elemento neutro es $\mathcal{O}$, el punto del infinito.

Esta operación, lejos de ser aleatoria, tiene una explicación geométrica gracias al teorema de Bezout el cual nos explica que dada una curva elíptica y una recta, su intersección son 3 puntos (contando multiplicidades).

Si consideramos las curvas elípticas sobre un cuerpo finito $\mathbb{F}_q$ tenemos una cota en el cardinal del grupo:

Teorema 1.4. *[7, V, Th.1.1] Sea $q \in \mathbb{Z}$ una potencia de primo, $E(\mathbb{F}_q)$ una curva elíptica definida sobre un cuerpo finito, entonces $\#E(\mathbb{F}_q) = q + 1 - t$ donde t cumple que $|t| \leq 2\sqrt{q}$*

En este aspecto de las curvas elípticas vistas como un grupo podemos ir un poquito mas allá. El siguiente resultado nos da una herramienta para saber cuando una curva elíptica existe y además qué estructura tiene:

Teorema 1.5 ([12]). *Sea $\mathbb{F}_q$ el cuerpo de q elemento. Dado un $|t| \leq 2\sqrt{q}$ entero entonces existe una curva elíptica sobre $\mathbb{F}_q$ con $q + 1 - t$ puntos racionales si y solo si, tomando $q = p^r$, se satisfacen alguna de las siguientes condiciones:*

I) $mcd(t, q) = 1$,
II) $t = 0$, *r impar, o* $p \not\equiv 1 \mod 4$,
III) $t = \pm\sqrt{q}$, *r par, o* $p \not\equiv 1 \mod 3$,
IV) $t = \pm 2\sqrt{q}$, *r par,*
V) $t = \pm\sqrt{2q}$, *r impar y* $p = 2$,
VI) $t = \pm\sqrt{3q}$, *r impar y* $p = 3$.

Además, la estructura de grupo en los casos $II) - VI)$ son los siguientes:

II) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/\left(\frac{q+1}{2}\right)\mathbb{Z}$ *o cíclico si* $q \equiv 3 \mod 4$,
III) grupo cíclico,
IV) $\left(\mathbb{Z}/\left(\sqrt{q} \pm 1\right)\mathbb{Z}\right)^2$,
V) grupo cíclico,
VI) grupo cíclico.

Definición 1.11. *Sea $E/\mathbb{F}_q$ una curva elíptica con $q + 1 - t$ puntos. Entonces:*

- *Si $p \nmid t$ entonces E es una curva ordinaria.*
- *Si $p \mid t$ entonces E es una curva supersingular.*

En cuanto al término "supersingular" no tiene nada que ver con que tenga puntos singulares. De hecho en [7, V.3,Remark3.2.2] se cuenta el origen de esta terminología. Desde el punto de vista histórico, a las curvas elípticas definidas sobre $\mathbb{C}$ cuyo anillo

de endomorfismos era más grande que $\mathbb{Z}$ se les llamaba *singulares* en el sentido de "raro o "no usual". De todas formas, en este sentido (como ya veremos), las curvas elípticas definidas sobre cuerpos finitos $\mathbb{F}_p$ son todas singulares. De hecho, el anillo de endomorfismos de la mayoría de curvas elípticas sobre $\mathbb{F}_p$ son órdenes en un cuerpo cuadrático imaginario. Es en el excepcional caso en el que el anillo de endomorfismos de la curva es un orden de un álgebra de cuaternión en el que usaremos el término "supersingular".

2 | Isogenias y sus grafos

En este capítulo veremos cómo se define una isogenia y algunas características que tienen. Además también veremos cómo se definen los grafos de isogenias y cómo construirlos. Estos grafos serán el andamio sobre el que, en el siguiente capítulo, construyamos nuestro protocolos criptográficos.

2.1 Isogenias

Comenzaremos esta sección dando la definición de isogenia y dos propiedades básicas que nos serán de gran utilidad a la hora de construir los mencionados grafos.

Definición 2.1. *Sean E_1 y E_2 dos curvas elípticas. Una* **isogenia** *de E_1 a E_2 es un morfismo $\phi : E_1 \to E_2$ de tal forma que $\phi(\mathcal{O}) = \mathcal{O}$.*

Diremos que dos curvas, E_1 y E_2 son **isógenas** si existe una isogenia ϕ entre ellas de tal forma que $\phi(E_1) \neq \{\mathcal{O}\}$. También diremos que la isogenia ϕ está definida sobre K si sus coeficientes pertenecen a K. Más adelante podremos ver que la relación "ser isógenas" es una relación de equivalencia.

Teorema 2.1. *[7, III.4] Sea $\phi : E_1 \to E_2$ una isogenia. Entonces ϕ o es constante o sobreyectiva.*

Teorema 2.2. *[7, III.4, Corollary 4.9] Sea $\phi : E_1 \to E_2$ una isogenia. Entonces, $ker(\phi)$ es un grupo finito.*

Teorema 2.3. *[4, 9.7, Theorem 9.7.4](Tate) Dos curvas elípticas, E y E' definidas sobre un cuerpo K son isógenas sobre K si y solo si $\#E(K) = \#E'(K)$.*

Un dato sobre las isogenias muy importante para nuestro fin, la criptografía, es el grado de estas. Para poder determinarlo debemos recordar brevemente qué es el

cuerpo de funciones de una curva E. Sea $E = C_f(K)$ una curva elíptica, definimos el conjunto:

$$K(E) = \left\{ \frac{h(x,y)}{g(x,y)} \ : \ \text{con } h, g \in K[E],\ g \neq 0 \right\} \quad ; \quad K[E] = K[X,Y]/\langle f \rangle \tag{2.1}$$

Por las propiedades que hemos visto hasta ahora, una isogenia, $\phi : E_1 \to E_2$ puede verse como una aplicación racional no constante, a excepción de [0]. Entonces, la composición con ϕ induce una inyección de los cuerpos de funciones que fijan K [7, II.2]:

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

De hecho, en [7, II.2,Theorem 2.4] se demuestra que esta inyección es una extensión finita, i.e., que $K(E_1)$ es una extensión finita de $\phi^*(K(C_2)$.

El **grado de una isogenia** no nula se define como el grado del morfismo, pero tambiñen puede definirse como a continuación:

Definición 2.2. *Sean E_1/K y E_2/K dos curvas elípticas y $\phi : E_1 \to E_2$ una isogenia no constante definida sobre K. Entonces, el* **grado de** *ϕ se define como $deg\phi = [k(E) : \phi^*(K(E_2))]$, donde ϕ^* es el pullback[1] de ϕ. Si ϕ es constante, entonces $deg(\phi) = 0$.*

De una manera menos formal, según [4], una isogenia de grado d es una correspondencia "d-to-1 on most points". Esto lo podremos comprobar en el ejemplo 2.1.

Definición 2.4. *A una isogenia se le dice* **separable** *cuando la extensión de cuerpos $k(E)/\phi^*(K(E_2))$ lo es.*

Teorema 2.4. *Sea $\phi : E_1 \to E_2$ una isogenia. Si ϕ es separable, entonces*

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

Las isogenias también pueden ser inseparables y puramente inseparables si la ex-

[1] En caso de que alguien necesite recordarlo:

Definición 2.3. *[4, 5.5, Definition 5.5.21] Sean X e Y variedades sobre K y sea $\phi : X \to Y$ una aplicación racional dominante sobre K. Definimos el* **pullback** *$\phi^* : K(Y) \to K(X)$ como $\phi^*(f) = \phi \circ f$.*

tensión de cuerpos correspondiente lo es. No indagaremos más en la diferencia entre estos tipos de isogenias. Aquellos que deseen saber más sobre las diferencias entre los tipos de isogenias pueden dirigirse a [4], [7].

A continuación, veremos dos isogenias entre una curva y ella misma, es decir, isogenias que son endomorfismos. Son una simple muestra de cómo funcionan, además de introducirnos en los elementos del anillo de endomorfismos de una curva. Profundizaremos en este último concepto y su relación con las isogenias más adelante.

Definición 2.5. *Sea $m \in \mathbb{Z}$ definimos la multiplicación por escalar $[m] : E \to E$ como:*

$$[m](P) = \overbrace{P + P + \cdots + P}^{m}$$

El punto P se suma m veces. En caso de que $m < 0$ fijamos la operación como:

$$[m](P) = [-m](-P)$$

Por último, si $m = 0$ fijamos $[0](P) = \mathcal{O}$.

Teorema 2.5. *[4, 9.6, Corollary 9.6.28] Sea $m \in \mathbb{Z}$, la multiplicación por escalar $[m]$ es una isogenia y tiene grado m^2.*

Definición 2.6. *Sea $m \in \mathbb{Z}$ tal que $m \geq 1$. El subgrupo m-torsión de E, denotado como $E[m]$, es el conjunto de puntos de E cuyo orden divide a m:*

$$E[m] = \left\{ P \in E()\bar{K} \ : \ [m]P = \mathcal{O} \right\}$$

Teorema 2.6. *[12] Sea $m \in \mathbb{Z}$ y E una curva elíptica definida sobre el cuerpo K de tal forma que $char(K) \nmid m$, entonces*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Observación 2.1. Puede apreciarse, por definición, que el subgrupo de m-torsión es el núcleo de la multiplicación por escalar $[m]$. Es decir,

$$ker([m]) \cong E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Ejemplo 2.1. Consideremos la curva elíptica $E = C_f(\mathbb{F}_{11})$ dada por la fórmula $f : y^2 = x^3 + 3x + 3$ definida sobre el cuerpo finito $\mathbb{F}_{11}$ de 11 elementos. Esta curva tiene

8 puntos, vamos a ver como se comporta la isogenia [2]:

$$\begin{array}{rcl} [2] : E_f & \longrightarrow & E_f \\ \phi(0:1:0) & = & (0:1:0) \\ \phi(0:5:1) & = & (9:0:1) \\ \phi(0:6:1) & = & (9:0:1) \\ \phi(5:0:1) & = & (0:1:0) \\ \phi(7:2:1) & = & (9:0:1) \\ \phi(7:9:1) & = & (9:0:1) \\ \phi(8:0:1) & = & (0:1:0) \\ \phi(9:0:1) & = & (0:1:0) \end{array}$$

Por ende el subgrupo de 2-torsión es $E[2] = \{(0:1:0), (5:0:1), (8:0:1), (9:0:1)\} \subset E(\mathbb{F}_{11})$. Nótese que, por lo general, no sabíamos a priori si $E[2] \subseteq E(\mathbb{F}_{11})$. Además, el núcleo de esta isogenia está formado por el mismo subgrupo $ker([2]) = \{(0:1:0), (5:0:1), (8:0:1), (9:0:1)\}$ cuyos elementos tienen todos orden 2. Por ello, se ve que:

$$ker([2]) \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

La aplicación de Frobenius es el segundo ejemplo de isogenia que es un endomorfismo que vamos a presentar:

Definición 2.7. *Sea $K = \mathbb{F}_q$ un cuerpo finito con q elementos. La* **aplicación de Frobenius** *se define como:*

$$\begin{array}{rcl} \pi : E & \to & E \\ (X, Y) & \mapsto & (X^q, Y^q) \end{array}$$

Teorema 2.7. *[4, 9.6] La aplicación de Frobenius es una isogenia y además fija los puntos K-racionales de la curva elíptica:*

$$x^q = x \text{ para todo } x \in \mathbb{F}_q$$
$$y^q = y \text{ para todo } y \in \mathbb{F}_q$$

Observación 2.2. Dada una curva elíptica $E/\mathbb{F}_q$ con $\#E/\mathbb{F}_q = q + 1 - t$, sabemos que el endomorfismo de Frobenius satisface que:

$$\pi^2 - t\pi + q = 0.$$

A este $t = tr\pi$ le llamamos la **traza de Frobenius**. Del teorema 1.4 sabemos que

$|t| \leq 2\sqrt{q}$ o equivalentemente $t^2 - 4q \leq 0$.

Teorema 2.8. *[4, 9.6, Teorema 9.6.21](Isogenia dual) Sea $\phi : E \longrightarrow E'$ una isogenia de grado m. Existe una única isogenia $\hat{\phi} : E' \longrightarrow E$ tal que:*

$$\hat{\phi} \circ \phi = [m]_E, \quad \text{and} \quad \phi \circ \hat{\phi} = [m]_E.$$

Esta $\hat{\phi}$ se llama **isogenia dual de** *ϕ. Además cumple las siguientes propiedades:*

- *$\hat{\phi}$ está definido sobre un cuerpo K si y solo si ϕ está definido sobre K,*
- *$\hat{(\varphi \circ \phi)} = \hat{\phi} \circ \hat{\varphi}$ para cualquier isogenia $\varphi : E' \to E''$*
- *$\hat{(\varphi + \phi)} = \hat{\phi} + \hat{\varphi}$ para cualquier isogenia $\varphi : E' \to E''$,*
- *$deg\ \phi = deg\ \hat{\phi}$*
- *$\hat{\hat{\phi}} = \phi$*

La isogenia dual funciona "casi" como una inversa, lo que hace que éstas se comporten "bien". Lo más destacable, y más adelante veremos porqué, es que **todas** las isogenias tienen su correspondiente dual. En este contexto vale la pena mencionar que los isomorfismos de curvas elípticas son un caso concreto de isogenias, concretamente aquellas que tienen grado 1 (por eso al comoponerlas tenemos $id = [1]$). Gracias a la existencia de esta "dualidad", la relación "ser isogénicas" es relación de equivalencia.

Del anterior teorema 2.2 hemos aprendido que dada una isogenia, su núcleo es un subgrupo finito de la curva dominio. Otro resultado relacionado con este nos dice lo siguiente:

Proposición 2.1. [7, III.4] Sea E una curva elíptica y $G \subseteq E$ un subgrupo de esta. Existe una única curva elíptica E' y una única isogenia separable $\phi_G : E \to E'$ de tal manera que $ker(\phi_G) = G$.

Observación 2.3. Es decir que por cada subgrupo G de una curva elíptica E tendremos una única isogenia ϕ_G y una única curva elíptica E' como codominio de ϕ_G. Además, por el teorema 2.4 si conocemos el orden del grupo G también sabremos el grado de la isogenia. De esta forma podemos saber las isogenias que hay entre los diferentes j-invariantes. Nótese que hemos hablado de existencia de isogenias, no de construcción. Para resolverlo, en [8] se nos facilita un algoritmo para poder construir las isogenias que en el resultado anterior sabemos que existen. El desarrollo de esta fórmula se escapa del propósito de este trabajo por lo que aquellos interesados en profundizar sobre ello pueden consultar [8].

Ejemplo 2.2. Sea $E = C_f(\mathbb{F}_{17})$, la curva elíptica sobre el cuerpo finito $\mathbb{F}_{17}$ definida por la ecuación $f : y^2 = x^3 + 3x + 3$ (usamos la misma ecuación que en el anterior ejemplo pero sobre un cuerpo diferente). En este caso la curva contiene 12 puntos entre los cuales $(2 : 0 : 1)$ tiene orden 2. Si tomamos este punto como generador del subgrupo G, usando la fórmula de Velù encontramos la isogenia φ de tal forma que $ker(\varphi) = G$ como sigue:

$$\begin{array}{rcl} \varphi : E & \to & E_G \\ (x, y) & \mapsto & \left(\dfrac{x^2 - 2x - 2}{x - 2}, \dfrac{x^2 y - 4xy + 6y}{(x^2 - 4x + 4)} \right) \end{array}$$

Como es de esperar, al ser el núcleo un subgrupo de orden 2, φ es una isogenia de orden 2. Su dual $\hat{\varphi}$ viene definida por:

$$\begin{array}{rcl} \hat{\varphi} : E_G & \to & E \\ (x, y) & \mapsto & \left(\dfrac{-4x^2 + x - 6}{x + 4}, \dfrac{-2x^2 y + xy + 5y}{(x^2 + 8x - 1)} \right) \end{array}$$

Vamos a comprobar la propiedad que nos dice que $\varphi \circ \hat{\varphi} = [2]$ usando el punto $P = (6 : 4 : 1) \in E$. Es sencillo ver que $\varphi(P) = (14 : 13 : 1)$, y además que $\hat{\varphi}(\varphi(P)) = (6 : 13 : 1)$. Ahora nos falta conocer $[2](P)$, que tomando la operación de grupo presentada en el anterior capítulo tenemos que es $[2]P = (6 : 13 : 1)$.

Ejemplo 2.3. Vamos a considerar ecuación $f : y^2 = x^3 + 3x + 3$ sobre el cuerpo finito $\mathbb{F}_7$. Los puntos de la curva son :

$$C_f(\mathbb{F}_7) = \{(0 : 1 : 0), (1 : 0 : 1), (3 : 2 : 1), (3 : 5 : 1), (4 : 3 : 1), (4 : 4 : 1)\}$$

Es fácil ver que es una curva elíptica ya que $\Delta = 5 \neq 0$. Si calculamos el orden de los puntos de la curva vemos que son $\{1, 2, 3, 3, 6, 6\}$, respectivamente. Vamos a tomar el subgrupo generado por el punto de orden 2, $G = \{(1 : 0 : 1), (0 : 1 : 0)\}$ como núcleo para definir la siguiente isogenia de orden 2:

$$\begin{array}{rcl} \phi : E & \to & E_1 \\ (x, y) & \mapsto & \left(\dfrac{x^2 - x - 1}{x - 1}, \dfrac{x^2 y - 2xy + 2y}{x^2 - 2x + 1} \right), \end{array}$$

donde la curva $E_1 = C_g(\mathbb{F}_7)$ con $g : y^2 = x^3 + x + 3$. Como estas curvas son isogenias entonces tienen la misma cantidad de puntos:

$$E_1 = \{(0 : 1 : 0), (4 : 1 : 1), (4 : 6 : 1), (5 : 0 : 1), (6 : 1 : 1), (6 : 6 : 1)\},$$

cuyos órdenes son $\{1, 6, 6, 2, 3, 3\}$ respectivamente. Recordando del comentario anterior que habíamos citado de [4, 8.1] que nos describía que el grado d de una isogenia nos indicaba que era una correspondencia "d-to-1 on most points", vemos cómo funciona ϕ:

$$\begin{aligned}
\phi(0:1:0) &= (0:1:0)\\
\phi(1:0:1) &= (0:1:0)\\
\phi(3:2:1) &= (6:6:1)\\
\phi(4:4:1) &= (6:6:1)\\
\phi(3:5:1) &= (6:1:1)\\
\phi(4:3:1) &= (6:1:1)
\end{aligned}$$

En este caso, esa correspondencia se cumple en todos los puntos donde además confirmamos que los dos primeros elementos están en el núcleo de la isogenia.

En un primer momento podríamos pensar que, al tener la misma cantidad de puntos y además los mismos órdenes, estas curvas podrían ser isomorfas. Pero un rápido vistazo a sus j-invariantes nos despeja cualquier atisbo de duda, ya que $j(E) = 4$ y $j(E_1) = 5$.

Algunos de los ejemplos de isogenias que hemos considerado hasta ahora coinciden en dominio y codomino, i.e., son endomorfismos. El conjunto de endomorfismos juega un importante papel a la hora de definir las isogenias. Un endomorfismo de una curva elíptica E o bien es la aplicación nula (aquella que lleva todos los elementos al punto del infinito, i.e., $[0]$) o bien es una isogenia. El conjunto de todos los endomorfismos de una curva E se denota $End(E)$. Este conjunto, $End(E)$, junto con las operaciones suma y composición forma un anillo, i.e., que para todos $\phi, \varphi \in End(E)$ y $P \in E(K)$ las operaciones son:

- $(\phi + \varphi)(P) = \phi(P) + \varphi(P)$,
- $(\phi\varphi)(P) = \phi(\varphi(P))$.

De las isogenias que hemos visto a la largo del capítulo podemos deducir qué elementos se encuentran dentro del anillo de endomorfismos. Para empezar, para todo $n \in \mathbb{Z}$, $[n] \in End(E)$ así que podemos decir que $\mathbb{Z} \subseteq End(E)$. Si seguimos en esta línea, la aplicación de frobenius, π, al ser un endomorfismo también está en $End(E)$ siempre y cuando la característica del cuerpo $p > 0$. Por lo tanto, sabemos que

$$\mathbb{Z}[\pi] \subseteq End(E).$$

Antes de obtener una caracterización del anillo de endomorfismos de una curva vamos a ver unas definiciones previas. Estas definiciones nos van a ir adelantando algo sobre la posible estructura que tendrá este anillo.

Definición 2.8. *Sea K una $\mathbb{Q}$-álgebra finitamente generada. Un* **orden** $\mathcal{O} \subseteq K$ *es un subanillo de K que es un $\mathbb{Z}$- módulo finitamente generado de rango maximal.*

Ejemplo 2.4. En los cuerpos cuadráticos como $K = \mathbb{Q}[\sqrt{m}]$ el anillo de enteros $\mathcal{O}_K$ es un orden. En este caso está demostrado que:

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

Definición 2.9. *Un álgebra de cuaterniones es un álgebra de la forma:*

$$K = \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$$

donde los generadores α, β satisfacen las siguientes relaciones:

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \beta\alpha = -\alpha\beta$$

Teorema 2.9. *[3] Sea K un cuerpo y E una curva elíptica definida sobre este cuerpo. El anillo de endomorfismos de E, $End(E)$ es* **isomorfo** *a uno de los siguientes:*

- $\mathbb{Z}$,
- *un orden en un cuerpo cuadrático imaginario ($\mathbb{Q}[\sqrt{d}]$ tal que $d < 0$),*
- *un orden en un álgebra de cuaternión.*

Este mismo resultado tiene otra versión un tanto más intuitiva:

Teorema 2.10. *[10, Chapter 2],[11] Sea $End_{\mathbb{F}_q}(E)$ el anillo de endomorfismos y t la traza del endomorfismo de frobenius, solo una de las siguientes opciones es posible:*

- *Si $t^2 - 4q < 0$ entonces $\mathbb{Q}(\pi)$ es un cuerpo cuadrático imaginario y*

  $$End_{\mathbb{F}_q}(E) \hookrightarrow \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q})$$

  es un orden $\mathcal{O}$ que contiene a $\mathbb{Z}[\pi]$.

- *Si* $t^2 - 4q = 0$ *entonces* $\pi = \pm\sqrt{q} = \pm p^{n/2}$ *y*

$$End_{\mathbb{F}_q}(E) \hookrightarrow B_{p,\infty}$$

es un orden maximal $\mathcal{O}$ *en un álgebra de cuaternión ramificada en* p *y en el infinito.*

Vamos a ver un ejemplo de cada uno de los casos del resultado anterior.

Ejemplo 2.5. Consideramos la cuerva elíptica $E/\mathbb{F}_{31}$ dada por $E : y^2 = x^3 + x + 4$. Tenemos que:

$$\#E(\mathbb{F}_{31}) = 26 = 31 + 1 - 6 \rightarrow t = 6 \text{ y que } t^2 - 4q = -88 \neq 0.$$

La aplicación de Frobenius en esta caso satisface que:

$$\pi^2 - 6\pi + 31 = 0 \Rightarrow \pi = 3 \pm \sqrt{-22}.$$

Por lo tanto $End_{\mathbb{F}_{31}}(E)$ es un orden en $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{-22})$ que contiene a $\mathbb{Z}[\sqrt{-22}]$. Pero además se puede ver que $\mathbb{Z}[\sqrt{-22}]$ es un orden maximal, por lo tanto $End_{\mathbb{F}_{31}}(E) = \mathbb{Z}[\sqrt{-22}]$.

Ejemplo 2.6. Sea ahora, $E/\mathbb{F}_{31^2}$ dada por $E : y^2 = x^3 - x$. Sabemos que:

$$\#E(\mathbb{F}_{31}) = 1024 \rightarrow t = -62 = 2 \cdot -31 = -2\sqrt{q} \text{ y } t^2 - 4q = 0.$$

Por lo que $End_{\mathbb{F}_{31^2}}(E)$ es un orden maximal en el álgebra de cuaterniones $B_{31,\infty}$. Más concretamente:

$$End_{\mathbb{F}_{31^2}}(E) \equiv \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{i+j}{2} + \mathbb{Z}\frac{1+ij}{2},$$

donde $i^2 = -1$, $j^2 = -3$ y $ij = -ji$.

Una pregunta que puede surgir en este momento es ¿Porqué hablar ahora del anillo de endomorfismos? Debido a la conexión que existe entre las curvas que son isogénicas y las clases de ideales del anillo de endomorfismos. Para ello veamos los siguientes resultados:

Proposición 2.2. [6, Chapter 2, sect. 4] Sea E una curva elíptica definida sobre un cuerpo k y sea $\mathcal{O} := End_k(E)$. Todo ideal $\mathcal{I} \subseteq \mathcal{O}$ define un subgrupo finito de E como sigue:

$$E[\mathcal{I}] := \bigcap_{\alpha \in \mathcal{I}} ker(\alpha).$$

Basta con iterar en los generadores de $\mathcal{I}$ para obtener el subgrupo $E[\mathcal{I}]$. Además si el ideal es de la forma $\mathcal{I} = \mathcal{O} \cdot \nu$ entonces $E[\mathcal{I}] = E[\nu] := ker(\nu)$ donde $\nu \in \mathcal{O}$.

Como cada ideal $\mathcal{I}$ del anillo de endomorfismos $End(E)$ define un subgrupo finito G dentro de una curva elíptica E, entonces cada uno de ellos define una isogenia:

Definición 2.10. *Sea $\mathcal{I} \subseteq End(E)$, y sea $\varphi_{\mathcal{I}}$ la isogenia cuyo núcleo es $E[\mathcal{I}]$, $\varphi_{\mathcal{I}} = \varphi_{E[\mathcal{I}]}$ que se corresponde lo la isogenia mencionada en la Proposición 2.1.*

Teorema 2.11. *[7, 9.10] Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$, tal que $q = p^m$. Las siguientes afirmaciones son equivalentes:*

- *E es supersingular,*
- *$E[p^r] = \{\mathcal{O}_E\}$ para $r \in \{1, \dots, m\}$.*
- *la aplicación $[p] : E \to E$ es puramente inseparable y $j(E) \in \mathbb{F}_{p^2}$.*
- *$End(E)$ es orden de un álgebra de cuaternión.*

Nótese que, tenemos una caracterización de las curvas **supersingulares** definidas sobre un cuerpo finito $\mathbb{F}_q$ con $q = p^m$. Si una curva no cumple esta definición será una curva **ordinaria**. Usando las curvas supersingulares y las isogenias entre ellas montaremos el grafo de isogenias, andamiaje sobre el cual construiremos la criptografia basada en isogenias.

Observación 2.4. Es importante destacar una consecuencia de la diferenciación entre curvas elípticas supersingulares y curvas elípticas ordinarias. Por construcción las curvas isogénicas a una curva supersingular han de ser supersingulares. Esto refuerza la idea de que la relación "ser isogénicas" es una relación de equivalencia, pues en una misma clase de equivalencia no podrá haber se los dos tipos de curvas.

2.2 grafo de isogenias

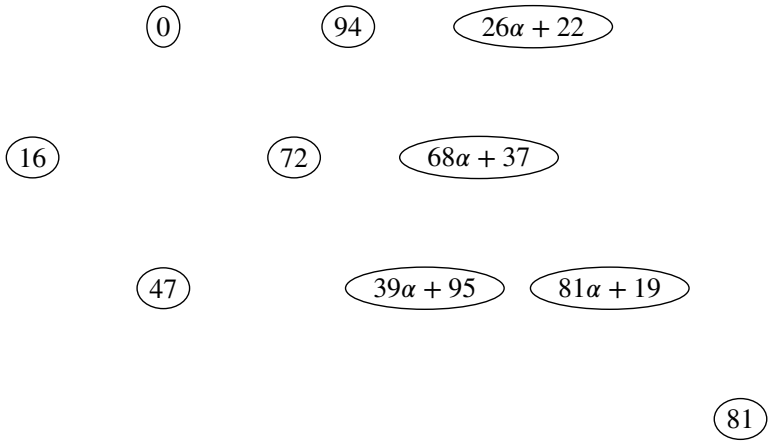
En esta sección definiremos y construiremos los grafos de Isogenias. También veremos algunas propiedades importantes que cumplen y porqué son ideales para hacer criptografía.

Definición 2.11. *Un grafo de isogenias es un (multi-)grafo $G = (V, E)$, cuyos nodos son los j-invariantes de curvas elípticas y sus aristas representan isogenias entre las curvas con ese j-invariante.*

Definición 2.12. *El grafo de ℓ-isogenias, $G_\ell(K)$ es un subgrafo del grafo de isogenias, definidas sobre K, en el que solo se consideran las aristas definidas por isogenias de grado ℓ.*

Realmente, nosotros usaremos los grafos de 2-isogenias y 3-isogenias para construir los protocolos. El concepto de grafo de isogenias es algo bastante más amplio que no nos concierne, aquellos que deseen ampliar la información sobre estos véase [6]. Nos limitaremos a hablar de los grafos de ℓ-isogenias.

Ejemplo 2.7. Sea $p = 107$, vamos a considerar todos los j-invariantes de curvas elípticas supersingulares en $\mathbb{F}_{107^2}$. Tanto los cálculos como la representación del grafo se han desarrollado utilizando el software de código abierto SageMath.



Recondando la última observación que hicimos en la sección anterior, la relación "ser isógenas" es una clase de equivalencia, se puede deducir que el grafo de ℓ-isogenias será un grafo no conexo. Es decir, puede haber componentes en que los vértices sean j-invariantes de curvas elípticas ordinarias o de curvas elípticas supersingulares pero nunca habrá de los dos tipos en la misma componente conexa (del grafo). Nosotros nos centraremos en la componente en la que los vértices son j-invariantes de curvas elípticas supersingulares, también llamada, **componente supersingular**. El resto de componentes, llamadas **comoponentes ordinarias** tienen una estructura regular la cual se denomina volcán. Estos volcanes escapan del fin de este estudio por lo que los interesados pueden consultar, por ejemplo [9]. Según la Teorema 2.11, toda curva elíptica supersingular sobre un cuerpo $\mathbb{F}_q$ con $q = p^r$, se puede definir sobre una extensión cuadrática de un cuerpo primo[2]. Por lo tanto todo

[2]Un cuerpo primo es aquel que no tiene subcuerpos propios, como son $\mathbb{Q}$ y $\mathbb{Z}/(p)$ con p un número primo.

j-invariante supersingular en $\mathbb{F}_q$ está contenido en $\mathbb{F}_{p^2}$.

Teorema 2.12. *[7, V.4, Theorem 4.1] Sea $\mathbb{F}_q$ con $q = p^r$ y p primo. El número de j-invariantes de curvas supersingulares es:*

$$\left\lfloor \frac{p}{12} \right\rfloor + 1 + \epsilon \quad \textit{donde} \quad \epsilon = \begin{cases} -1 & \textit{si } p \equiv 1 \mod 12, \\ 1 & \textit{si } p \equiv -1 \mod 12, \\ 0 & \textit{en otro caso.} \end{cases}$$

Ejemplo 2.8. En el ejemplo anterior hemos visto los j-invariantes de curvas supersingulares contenidos en $\mathbb{F}_{107^2}$. En este caso, como $p = 107$ tenemos que $107 \equiv -1$ y por tanto $\epsilon_{107} = 1$. Habrá un total de $\left\lfloor \frac{107}{12} \right\rfloor + 2 = 10$ j-invariantes.

Ya sabemos identificar los j-invariantes de curvas elípticas supersingulares y además sabemos cuantos hay. Ahora nos toca ver las ℓ-isogenias que hay entre ellos para poder dibujar las aristas que tiene el grafo $G_\ell(\mathbb{F}_q)$. Con este fin, definiremos el polinomio modular, cuyas raíces son los pares de j-invariantes cuyas correspondientes curvas son isogénicas.

Teorema 2.13. *[9] Sea $N \in \mathbb{Z}$, existe un polinomio $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ que es simétrico en X e Y de grado $N + 1$ en ambas variables tal que, para todo $j_1, j_2 \in K$, $\Phi_N(j_1, j_2) = 0$ si y solo si j_1 y j_2 son los j-invariantes de curvas elípticas definidas sobre el cuerpo K relacionadas entre si por una isogenia de grado N definida sobre K. A este polinomio se le denomina* **polinomio modular**.

Ejemplo 2.9. Existe una base de datos pública de las fórmulas modulares para las ℓ-isogenias disponible aquí. Las mórmulas para $\ell = 2, 3$ son

$$\begin{aligned} \Phi_2(x, y) = {} & x^3 - x^2y^2 + 1488x^2y - 162000x^2 + 1488xy^2 + 40773375xy + 8748000000x \\ & + y^3 - 162000y^2 + 8748000000y - 157464000000000; \end{aligned}$$

$$\begin{aligned} \Phi_3(x, y) = {} & x^4 + 36864000x^3 + 452984832000000x^2 + 1855425871872000000000x \\ & + y^4 + 36864000y^3 + 452984832000000y^2 + 1855425871872000000000y \\ & - x^3y^3 + 2587918086x^2y^2 - 770845966336000000xy + 2232x^3y^2 - 1069956x^3y \\ & + 8900222976000x^2y + 2232y^3x^2 - 1069956y^3x + 8900222976000y^2x \end{aligned}$$

Dado que los polinomios modulares son simétricos, i.e., $\Phi_\ell(j, j') = \Phi_\ell(j', j)$ cuando $j, j' \neq 0, 1728$ podemos considerar el grafo $G_\ell(K)$ como un grafo no dirigido.

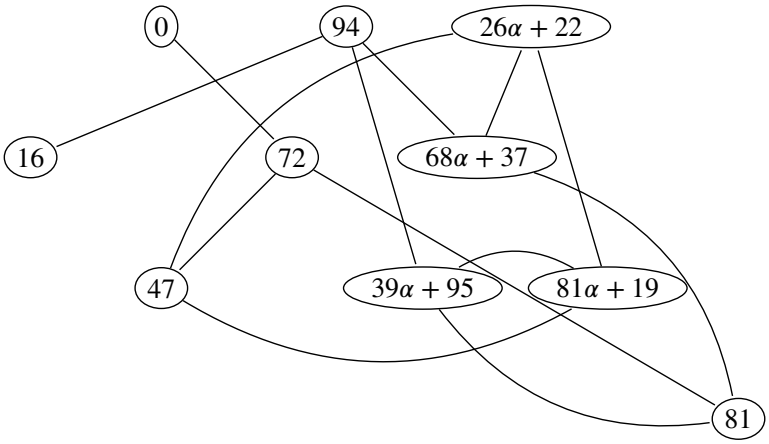


Figura 2.1: El grafo de 2-isogenias de la componente de curvas supersingulares.

Entiéndase esto último, también, como consecuencia de la existencia de una isogenia dual.

Ejemplo 2.10. Las figuras 2.1 y 2.2 representan los grafos de 2-isogenias y 3-isogenias. Cada uno de ellos serán usados en los procolos basado en isogenias.

Antes hemos visto que los j-invariantes de las curvas elípticas supersingulares están en $\mathbb{F}_{p^2}$, por tanto, las raíces de $\Phi_\ell(j, y)$ o $\Phi_\ell(x, j)$ pertenecerán a $\mathbb{F}_{p^2}$ para estos j-invariantes.

Teorema 2.14. *[1] El grafo de ℓ-isogenias de curvas elípticas supersingulares sobre $\mathbb{F}_q$ es conexo, $\ell + 1$-regular y tiene la propiedad de Ramanujan.*

En este último teorema se nos dice que la componente supersingular es siempre conexa, y que es $\ell+1$-regular, lo que quiere decir que todos los vértices (j-invariantes) del grafo tienen $\ell + 1$ aristas saliendo (o entrando) de él. Por último se dice que tiene la propiedad de Ramanujan, propiedad que se relaciona con la topología del grafo y por tanto con la seguridad del protocolo criptográfico.

Un grafo de Ramanujan en concreto es un *grafo de expansión*. Esto quiere decir que, en general, hay un "camino corto" entre dos cualesquiera vértices del grafo. Que un grafo cumpla la propiedad de Ramanujan quiere decir que, con respecto a las propiedades de expansión, está muy cerca del óptimo. De esta manera, la probabilidad de encontrar un camino de cierta longitud a un vértice (o conjunto de ellos) empezando en uno dado es muy baja.

En el siguiente capítulo veremos cómo emplean los grafos de ℓ-isogenias para pro-

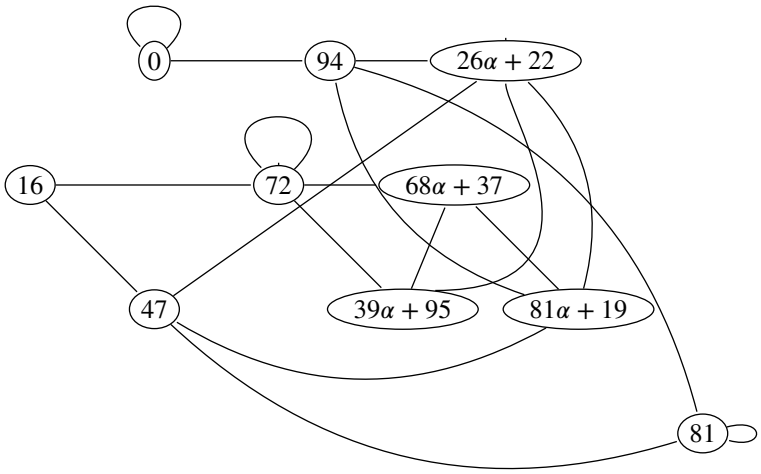


Figura 2.2: El grafo de 3-isogenias de la componente de curvas supersingulares.

poner un protocolo de intercambio de clave tipo *Diffie-Hellman* y porqué es computacionalmente seguro.

3 Criptografía basada en Isogenias

En esta sección vamos a presentar el protocolo de intercambio de clave de Diffie-Hellman basado en isogenias. Para ello comenzaremos eligiendo los parámetros del protocolo, para a continuación, precisar los cambios de información. Acabaremos por ver la razón por la que, hasta este mismo año, ha sido un candidato en el Proceso de estandarización de criptografía post-cuántica del Instituto Nacional de estándares y tecnología (NIST por sus siglas en inglés).

3.1 Protocolo de intercambio de clave

Dentro de la biliografía disponible, tanto a nivel teórico como a nivel computacional, la elección del primo p sobre el que construiremos el protocolo es, por lo general, de la forma siguiente:

$$p = 2^{e_A}3^{e_B} - 1,$$

donde $e_A, e_B \in \mathbb{N}$ de tal forma que $2^{e_a} \approx 3^{e_B}$. Algunas referencias incluso dan un poco más de flexibilidad permitiendo un "factor", f de tal forma que $p = f2^{e_A}3^{e_B} - 1$. Una razón de peso la tenemos en el teorema 1.5, ya que nos permite saber que existe una curva $E(\mathbb{F}_{p^2})$ que,

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z} = \mathbb{Z}/(2^{e_a}3^{e_B})\mathbb{Z} \times \mathbb{Z}/(2^{e_a}3^{e_B})\mathbb{Z}.$$

Por ello, sabemos que podemos encontrar dos puntos P y Q de la curva, ambos de orden $2^{e_a}3^{e_B}$ que pueden generar el grupo, i.e., son una base para este. Recordando la relación de los subgrupos de una curva elíptica con las isogenias y teniendo presente el teorema de Lagrange, la elección de estos primos nos permite restringirnos a los grafos de 2 y 3-isogenias.

Primero, fijamos todos **parámetros públicos**: una curva elíptica supersingular E_0 y dos bases de puntos $\{P_A, Q_A\}$ y $\{P_B, Q_B\}$. La curva E_0 definida sobre $\mathbb{F}_{p^2}$ y las bases de puntos han de generar $E[2^{e_A}]$ y $E[3^{e_B}]$ respectivamente, i.e.,

$$\langle P_A, Q_A\rangle = E[2^{e_A}] \cong \mathbb{Z}/2^{e_A}\mathbb{Z} \times \mathbb{Z}/2^{e_A}\mathbb{Z}\,;\, \langle P_B, Q_B\rangle = E[3^{e_B}] \cong \mathbb{Z}/3^{e_B}\mathbb{Z} \times \mathbb{Z}/3^{e_B}\mathbb{Z}.$$

De esta manera, los pares de puntos públicos $\{P_A, Q_A\}$ y $\{P_B, Q_B\}$ tienen, necesariamente, orden 2^{e_A} y $3e_B$ respectivamente.

Con esta información pública ya podemos empezar a escoger las claves privadas y calcular las claves públicas de los usuarios que, como no podía ser de otra manera, son Alicia y Bernardo. Cuando un elemento tenga el subíndice A querrá decir que es de Alicia, mientras que si tiene el subíndice B querrá decir que es de Bernardo. Comenzaremos por pedirle a nuestros usuarios que escojan una clave privada $k_A \in [0, 2^{e_A})$ y $k_B \in [0, 3^{e_B})$, para, a continuación empezar a calcular su clave pública:

$$S_A = P_A + [k_A]P_A \quad \text{y} \quad S_B = P_B + [k_B]P_B$$

Una vez tenemos los puntos S_A y S_B han de calcular sus isogenias secretas, haciendo uso del algoritmo de Velú [8]:

$$\begin{aligned} \phi_A &: E_0 \to E_A = E/\langle S_A\rangle \\ \phi_B &: E_0 \to E_B = E/\langle S_B\rangle \end{aligned}$$

Esta, ϕ_A será el resultado de componer e_A isogenias de orden 2, i.e., dar e_A pasos en el grafo de 2-isogenias. Esta secuencia de isogenias está determinada por S_A. Análogamente, ϕ_B es el resultado de componer e_B isogenias de grado 3, i.e., de dar e_B pasos por el grafo de 3-isogenias. Las claves públicas de Alicia y Bernardo son,

$$\begin{aligned} PK_A &= (E_A, P'_B, Q'_B) = (\phi_A(E), \phi_A(P_B), \phi_A(Q_B)), \\ PK_B &= (E_B, P'_A, Q'_A) = (\phi_B(E), \phi_B(P_A), \phi_B(Q_A)). \end{aligned}$$

Ahora, Alicia, usando su clave secreta k_A y la clave pública de Bob calcula el subgrupo secreto generado por el punto $S'_A = P'_A + [k_A]Q'_A$ de la curva E_B. Después, calcula la isogenia secreta $\phi'_A : E_B \to E_{A,B}$ donde $E_{A,B} = E_B/\langle S'_A\rangle$. Finalmente la clave intercambiada será $j_{A,B} = j(E_{A,B})$ que es el j-invariante de la curva $E_{A,B}$. Por su parte Bernardo hace los cálculos análogamente, i.e., con su clave privada k_B y la clave pública de Alicia calcula el punto $S'_B = P'_B + [k_B]Q'_B$ de la curva E_A. Posteriormente, obtiene la isogenia secreta $\phi'_B : E_A \to E_{B,A}$ donde $E_{B,A} = E_A/\langle S'_B\rangle$. Finalmente la clave intercambiada será $j_{A,B} = j(E_{A,B}) = j(E_{B,A}) = j_{B,A}$. En el Cuadro 3.1 puede

verse resumido el protocolo de una forma muy esquemática.

Parámetros públicos	Primos ℓ_A, ℓ_B y $p = \ell_A^{e_A}\ell_B^{e_B} \pm 1$ Curva elíptica supersingular $E/\mathbb{F}_{p^2}$ de orden $(p \pm 1)^2$ Una base $\langle P_A, Q_A\rangle$ de $E[\ell_A^{e_A}]$ Una base $\langle P_B, Q_B\rangle$ de $E[\ell_B^{e_B}]$		
	Alicia		**Bernardo**
Elegir la clave secreta	$S_A = P_A + [k_A]Q_A$		$S_B = P_B + [k_B]Q_B$
Calcula la isogenia secreta	$\phi_A : E \to E_A = E/\langle S_A\rangle$		$\phi_B : E \to E_B = E/\langle S_B\rangle$
Cambiar datos	$E_A, \phi_A(P_B), \phi_A(Q_B)$	$\to \quad \leftarrow$	$E_B, \phi_B(P_A), \phi_B(Q_A)$
Calcular el secreto común	$E/\langle S_A, S_B\rangle = E_B/\langle\phi_B(S_A)\rangle$		$E/\langle S_B, S_A\rangle = E_A/\langle\phi_A(S_B)\rangle$

Cuadro 3.1: Esquema del protocolo SIDH

Para ver que ambos j-invariantes son el mismo se puede argumentar que ambos corresponden a la misma clase de isomorfía $E/\langle S_A, S_B\rangle$ usando la identidad $E/\langle S_A, S_B\rangle \cong (E/\langle S_A\rangle)/\langle\phi(S_B)\rangle$ con $\phi : E \to E/\langle S_A\rangle$ [1]. Este protocolo, y otros basados en isogenias que veremos al final del capítulo, se apoyan en el siguiente diagrama conmutativo:

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E/\langle S_A\rangle \\ \downarrow{\scriptstyle \phi_B} & & \downarrow \\ E/\langle S_B\rangle & \longrightarrow & E/\langle S_A, S_B\rangle \end{array}$$

Ahora vamos a construir un ejemplo de protocolo de intercambio de clave entre Alicia y Bernardo:

Parámetros públicos

Vamos a retomar los grafos que construimos en la sección anterior con $p = 107 = 2^2 3^3 - 1$, y tomamos la curva elíptica pública

$$E_0 : y^2 = x^3 + (24j + 33)x + (59j + 42), \quad \text{con} \quad j(E_0) = 81\alpha + 19$$

También vamos a tomar cuatro cualesquiera puntos de E_0 de tal forma que $E[2^2] = \langle P_A, Q_A \rangle$ y $E[3^3] = \langle P_B, Q_B \rangle$. Vamos a fijar los puntos:

$$P_A := (69\alpha + 52 : 20\alpha + 3 : 1) \quad Q_A := (51\alpha + 28 : 77\alpha + 65 : 1)$$
$$P_B := (48\alpha + 8 : 55\alpha + 85 : 1) \quad Q_B := (26\alpha + 89 : 98\alpha + 77 : 1)$$

Alicia: Supongamos que escoge la clave secreta $k_A = 1$, su primer paso será calcular el punto secreto:

$$\begin{aligned} S_A &= P_A + [k_A]Q_A \\ &= (69\alpha + 52 : 20\alpha + 3 : 1) + (51\alpha + 28 : 77\alpha + 65 : 1) \\ &= (84\alpha + 7 : 35\alpha + 106 : 1). \end{aligned}$$

Este último punto es de orden 4 en la curva E_0. Ahora Alicia, ha de calcular su clave pública, para ello necesita calcular (usando la fórmula de Velú [8]) la isogenia:

$$\phi_A : E_0 \longrightarrow E_A = E/\langle S_A \rangle$$

Esta isogenia tiene las siguiente representación racional:

$$\phi_A(x, y) = \left(\frac{x^4 + (-38\alpha - 9)x^3 + (-53\alpha - 51)x^2 + (15\alpha - 18)x + (31\alpha + 24)}{x^3 + (48\alpha - 43)}, \right.$$
$$\left. \frac{x^5 y + (8\alpha - 11)x^4 y + (27\alpha + 41)x^3 y + (15\alpha + 11)x^2 y + (32\alpha - 16)xy + (-\alpha - 21)y}{x^5 + (8\alpha - 11)x^4 + (32\alpha - 25)x^3 + (-28\alpha + 43)x^2 + (-44\alpha + 45)x + (22\alpha + 5)} \right)$$

y la curva E_A que es codominio de ϕ_A es:

$$E_A : y^2 = x^3 + (106\alpha + 42)x + (13\alpha + 51) \quad \text{con} \quad j(E_A) = 72.$$

Nos falta encontrar la imagen, a través de la isogenia, de los puntos P_B y Q_B.

$$P'_B = \phi_A(P_B) = (16\alpha + 38 : 20\alpha + 54 : 1) \quad Q'_B = \phi_A(Q_B) = (8\alpha + 73 : 43\alpha + 54 : 1)$$

Por lo tanto la clave pública de Alicia es:

$$PK_A = ((106\alpha{+}42), (13\alpha{+}51), P'_B = (8\alpha{+}1 : 83\alpha{+}45 : 1), Q'_B = (8\alpha{+}1 : 24\alpha{+}62 : 1)).$$

Para identificar la curva basta dar el coeficiente de x y el coeficiente libre ya que el resto son iguales.

Bernardo: Supongamos que escoge la clave secreta $k_B = 1$, este, hace los cálculos de forma análoga a los de Alicia:

$$\begin{aligned} S_B &= P_B + [k_B]Q_B \\ &= (48\alpha + 8 : 55\alpha + 85 : 1) + (26\alpha + 89 : 98\alpha + 77 : 1) \\ &= (103\alpha + 43 : 22\alpha + 9 : 1). \end{aligned}$$

Este último punto es de orden 27 en la curva E_0. Ahora calcula su clave pública:

$$\phi_B : E_0 \longrightarrow E_B = E/\langle S_B \rangle$$

En este caso las ecuaciones racionales de la isogenia son demasiado voluminosas como para escribirla en una sola página, por ello, nos limitaremos a ver el codominio, E_B, de ϕ_B que es la curva:

$$E_B : y^2 = x^3 + (5\alpha + 57)x \quad \text{con} \quad j(E_B) = 16.$$

Nos falta encontrar la imagen, a través de ϕ_B, de los puntos P_A y Q_A.

$$P'_A = \phi_B(P_A) = (56\alpha + 103 : 32\alpha + 30 : 1) \quad Q'_A = \phi_B(Q_A) = (45\alpha + 10 : 94\alpha + 18 : 1)$$

Por lo tanto la clave pública de Bernardo es:

$$PK_B = ((5\alpha{+}57), 0, P'_A = (56\alpha{+}103 : 32\alpha{+}30 : 1), Q'_A = (45\alpha{+}10 : 94\alpha{+}18 : 1))$$

Ya tenemos la elección de ambas claves secretas y la publicación de ambas claves públicas. Para el cálculo de estas últimas hemos obtenido dos isogenias de grado 4 y 27 para Alicia y Bernardo, respectivamente, partiendo ambas de la curva E_0. Ya podemos comenzar con el cálculo de la clave compartida, pero antes vamos a conocer un poco más de estas isogénias.

Como bien hemos visto tenemos dos isogenias de grado 4 y 27 respectivamente, pero no sabemos cual es el camino aleatorio dentro de los grafos de isogenias. Vamos a descomponer ϕ_A y ϕ_B en isogenias de grado 2 y 3 respectivamente para saber cual ha sido el camino que han tomado dentro del grafo correspondiente. Conociendo las claves privadas podemos describir estos caminos. En el caso de Alicia el camino será a través del grafo de 2-isogenias y en el caso de Bernardo a través del grafo de 3-isogenias.

Alicia: al ser S_A un punto de orden 2^2, la isogenia ϕ_A tiene grado 4 lo que quiere

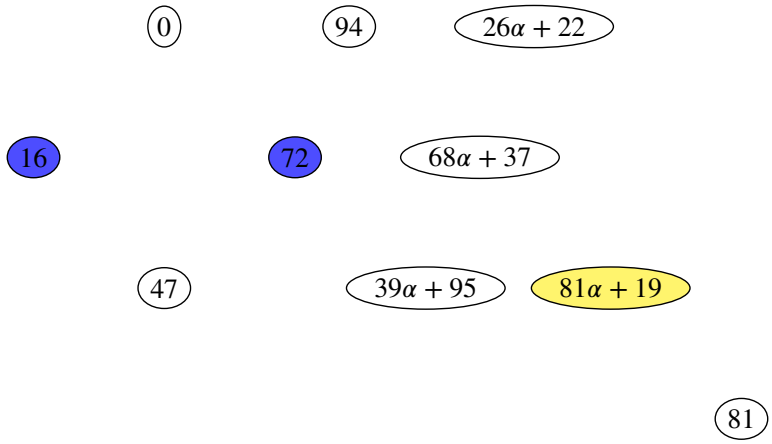


Figura 3.1: El nodo amarillo es el inicial, los nodos azules son los correspondientes a las curvas E_A y E_B.

decir que es una composición de dos isogenias de grado 2. Para obtener, esas dos isogenias debemos tomas el punto S_A, calcular $R_A = [2]S_A$ y usamos el algoritmo de Velú para obtener:

$$\phi_0 : E_0 \longrightarrow E_1, \quad \text{donde} \quad E_1 = E_0/\langle R_A \rangle,$$
$$\phi(x, y) = \left(\frac{x^2 + (23\alpha + 5)x + 37}{x + (23\alpha + 5)}, \frac{x^2 y + (46\alpha + 10)xy + (-8\alpha)y}{x^2 + (46\alpha + 10)x + (-8\alpha + 37)} \right)$$

Esta ϕ_0 es una isogenia de orden 2, cuyo codominio es la curva E_1 que tiene como j-invariante $j(E_1) = 47$. Debemos observar que el punto $S'_A = \phi_0(S_A)$ es un punto de orden 2 en la curva E_1. Una vez ya tenemos ϕ_0, podemos calcular ϕ_1 de forma similar:

$$\phi_1 : E_1 \longrightarrow E_A \quad \text{donde } E_A = E_1/\langle S'_A \rangle$$
$$\phi(x, y) = \left(\frac{x^2 + (23\alpha - 19)x + (5\alpha + 4)}{x + (23\alpha - 19)}, \frac{x^2 y + (46\alpha - 38)xy + (-47\alpha + 48)y}{x^2 + (46\alpha - 38)x + (-42\alpha + 52)} \right)$$

Así ya sabemos que el camino aleatório ϕ_A que ha tomado Alicia consiste en la composición de las isogenias ϕ_0 y ϕ_1, i.e., $\phi_A = \phi_0 \circ \phi_1$. En la figura 3.4 podemos ver cual es el correspondiente camino en el grafo.

Bernardo: los cálculos en este caso son algo más complejos, no porque a nivel teórico conlleve más tarea si no porque las isogenias son algo más aparatosas de manejar, como ya hicimos notar en la generación de la clave pública. Bernardo hará lo

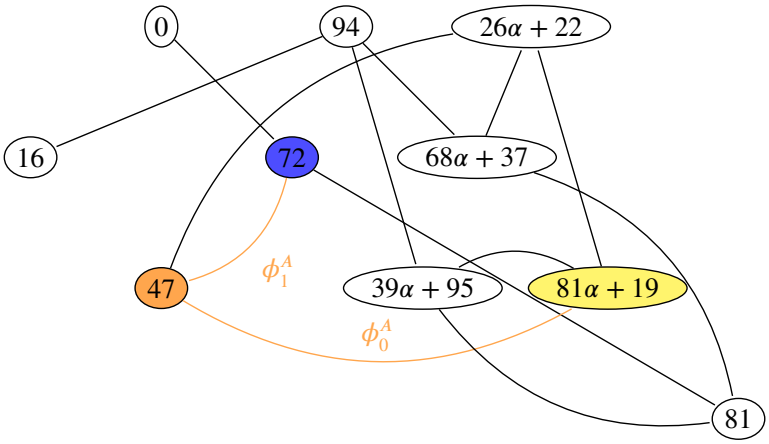


Figura 3.2: El camino aleatorio de Alice a través del grafo de 2-isogenias.

mismo que ha hecho Alicia, tomar su punto secreto S_B e ir tomando múltiplos de este y sus imágenes para crear el camino hasta el nodo anteriormente indicado. El camino de Bernardo será:

$$\begin{aligned}
&\phi_0^B : E_0 \to E_1' \text{ con } E_1' : y^2 = x^3 + (9\alpha + 4)x + (62\alpha + 2) && \text{y } j(E_1') = 68\alpha + 37 \\
&\phi_1^B : E_1' \to E_2' \text{ con } E_2' : y^2 = x^3 + (79\alpha + 66)x + (94\alpha + 4) && \text{y } j(E_2') = 72 \\
&\phi_2^B : E_2' \to E_3' \text{ con } E_B : y^2 = x^3 + (5\alpha + 57)x && \text{y } j(E_3') = 16
\end{aligned}$$

Entonces tenemos que $\phi_B = \phi_0 \circ \phi_1 \circ \phi_2$, lo cual nos define el camino dentro del grafos de 3-isogenias que se muestra en la figura 3.5.

Intercambio de clave

Alicia: Va a hacer el mismo camino que ha hecho en el paso anterior, pero con unas variaciones. Comenzando en la curva de la clave pública de Bernardo y usaremos los puntos de la misma clave para crear, con su clave privada un generador de la isogenia. Es decir, debemos tomar como curva inicial E_B cuyo j-invariante es 16 y proceder como antes. Primero calculamos el punto secreto:

$$\begin{aligned}
S_{AB} &= P_A' + [k_A]Q_A' \\
&= (56\alpha + 103 : 32\alpha + 30 : 1) + (45\alpha + 10 : 94\alpha + 18 : 1) \\
&= (62\alpha + 97 : 17\alpha + 48 : 1).
\end{aligned}$$

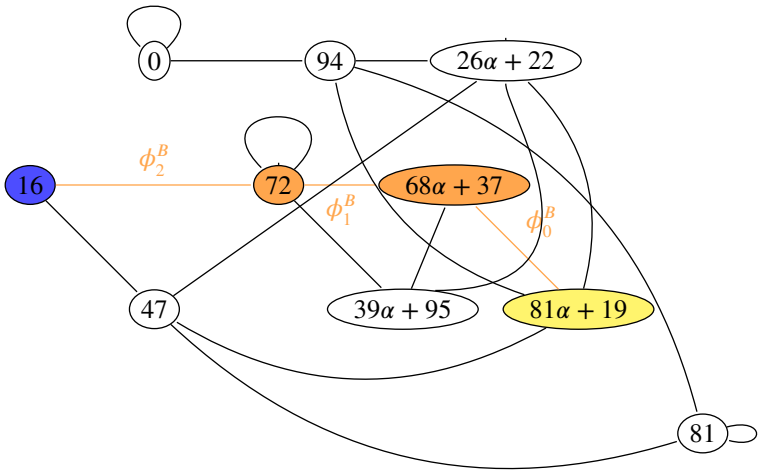


Figura 3.3: El camino aleatorio de Bernardo a través del grafo de 3-isogenias.

Y luego la isogenia correspondiente:

$$\phi_{AB} : E_B \longrightarrow E_{BA} \quad \text{donde} E_{BA} = E_B/\langle S_{AB} \rangle$$

donde:

$$E_{BA} : y^2 + (73\alpha + 1)x + (73\alpha + 99) \qquad j(E_{BA}) = 68\alpha + 37.$$

Por lo tanto la clave compartida es $j(E_{BA}) = 68\alpha + 37$. El camino, a través del grafo, que ha seguido en el grafo de 2-isogenias (dibujado en la Figura 3.2) es el siguiente:

$$\phi_0^{BA} : E_B \to E_{B,1} \quad \text{con } E_{B,1} : y^2 = x^3 + (55\alpha + 92)x + (45\alpha + 52) \text{ y } j(E_{B,1}) = 94$$
$$\phi_1^{BA} : E_{B,1} \to E_{BA} \text{ con } E_{BA} : y^2 = x^3 + (73\alpha + 1)x + (73\alpha + 99) \quad \text{y } j(E_{BA}) = 68\alpha + 37$$

Bernardo: Vamos a repetir lo que ha hecho Alicia pero con sus claves públicas. Es decir, debemos tomar como curva inicial E_A cuyo j-invariante es 72 y proceder como antes. Primero calculamos el punto secreto:

$$\begin{aligned} S_{BA} &= P'_B + [k_B]Q'_B \\ &= (16\alpha + 38 : 20\alpha + 54 : 1) + (8\alpha + 73 : 43\alpha + 54 : 1) \\ &= (51\alpha + 79 : 85\alpha + 51 : 1). \end{aligned}$$

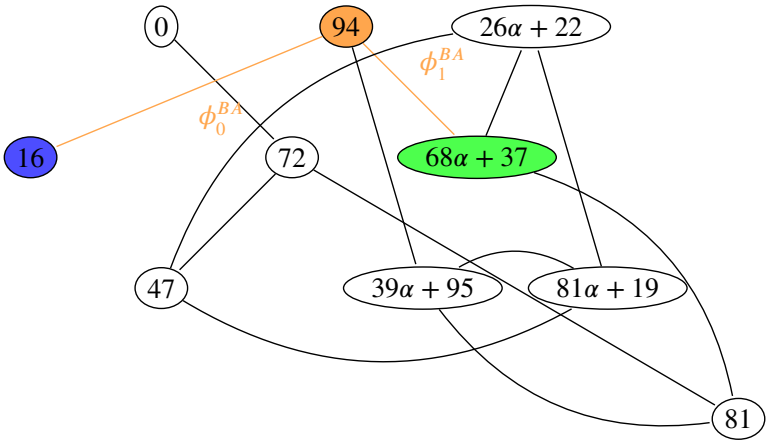


Figura 3.4: El camino aleatorio de Alice a través del grafo de 2-isogenias.

Y luego la isogenia correspondiente:

$$\phi_{AB} : E_B \longrightarrow E_{AB} \quad \text{donde} E_{AB} = E_A/\langle S_{BA} \rangle$$

donde:

$$E_{AB} : y^2 = x^3 + (73\alpha + 1)x + (73\alpha + 99) \qquad j(E_{AB}) = 68\alpha + 37.$$

Por lo tanto la clave compartida es $j(E_{BA}) = 68\alpha + 37$ también. El camino, a través del grafo, que ha seguido en el grafo de 3-isogenias (dibujado en la Figura 3.3) es el siguiente:

$$\phi_0^{BA} : E_A \to E_{A,1} \quad \text{con } E_{A,1} : y^2 = x^3 + (98\alpha + 57)x + (77\alpha + 14) \text{ y } j(E_{A,1}) = 72$$
$$\phi_1^{BA} : E_{A,1} \to E_{A,2} \text{ con } E_{A,2} : y^2 = x^3 + (85\alpha + 19)x + (89\alpha + 34) \text{ y } j(E_{A,2}) = 39\alpha + 95$$
$$\phi_1^{BA} : E_{A,2} \to E_{AB} \text{ con } E_{AB} : y^2 = x^3 + (73\alpha + 1)x + (73\alpha + 99) \quad \text{y } j(E_{BA}) = 68\alpha + 37$$

Con este protocolo, Alicia y Bernardo han podido compartir una clave, $68\alpha + 37$, sin que un tercero pueda obtenerla a pesar de la información pública.

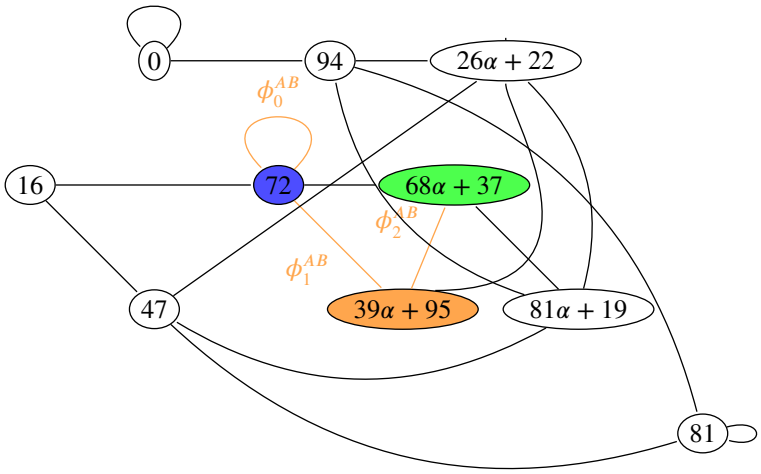


Figura 3.5: El camino aleatorio de Bernardo a través del grafo de 3-isogenias.

3.2 ¿Por qué es tan seguro?

En [1, Section 6] y en [5] los autores nos presentan una serie de "problemas" a la hora de intentar atacar este protocolo criptográfico y otros basados en isogenias. En el mismo artículo conjeturan sobre la complejidad en la resolución de estos y cómo esta dificultad les permite conjeturar igualmente sobre la seguridad del protocolo, incluso en un contexto post-cuántico. A continuación se presentan los problemas relacionados con el protocolo de intercambio de clave:

Problema 3.1 (El problema general de la isogenia). Dados $j, j' \in \mathbb{F}_q$ encontrar una isogenia $\phi : E \to E'$, si existe, donde $j(E) = j$ y $j(E') = j'$.

Un problema añadido al de encontrar dicha isogenia es la memoria que requiere representarla. Ya pudimos intuir en un ejemplo de la sección anterior que una isogenia de grado 27, que representa un paseo de longitud 3 en el grafo, requería mucho "espacio" para ser representada. Cuando el paseo crece también lo hace el tamaño de esta representación. Por otro lado, el problema de decisión que se nos presenta si tiene una solución polinomial. Para decidir si existe una isogenia entre dos curvas basta contar el número de puntos que tienen, por el Teorema 1.4, y para ello si existen algoritmos polinomiales. Dentro de este contexto, encontrar una isogenia de grado minimal sí es un problema que no tiene una solución polinomial.

Problema 3.2 (El problema de la isogenia en SIDH). Sea (E, R_1, S_1, R_2, S_2) la clave

pública del intercambio de clave de Diffie-Hellman basado en isogenias de curvas supersingulares. Sea E_A una curva tal que existe una isogenia $\phi_A : E \to E_A$ de grado $\ell_1^{e_1}$. Sean $R'_2 = \phi_A(R_2)$ y $S'_2 = \phi(S_2)$. El problema es: dado $(E, R_1, S_1, R_2, S_2, E_A, R'_2, S'_2)$ determinar la isogenia ϕ_A de grado $\ell_A^{E_A}$ tal que $R'_2 = \phi_A(R_2)$ y $S'_2 = \phi(S_2)$. Vamos a hacer un par de observaciones

- Este problema contiene mucha más información que el anterior. Sean $0 \leq x, y \leq \ell_1^{e_1}$ y $T = [x]R_2 + [y]S_2$. Entonces $\phi_A(T) = [x]R'_2 + [y]S'_2$ se puede encontrar. Por lo tanto, un atacante puede calcular tantos pares $(T, \phi_A(T))$ en el grafo en el que está ϕ_A como quieran. Un manera natural de solucionar el problema es interpolando ϕ_A. Un problema de ello es que ϕ_A tiene grado $\ell_1^{e_1}$ lo que hace que su representación cono una función racional tenga polinomios de grado exponencial. El reto que se presenta es resolver el problema de interpolación usando la descomposición de ϕ_A como e_1 isogenias de grado ℓ_1.
- El protocolo entero sería inseguro si Alicia hiciera públicos los puntos $R'_1 = \phi_A(R_1)$ y $S'_1 = \phi_A(S_1)$. Un atacante podría encontrar $x \in \mathbb{Z}$ tal que $x \notin \mathbb{Z}/\ell_1\mathbb{Z}$ pero que $R'_1 + [x]S'_1 = \mathcal{O}$. Al encontrar este entero tenemos que $R_1 + [x]S_1 \in ker(\phi_A) = \langle P_A \rangle$ donde P_A es el punto calculado por Alicia usando su clave privada. Esto último deja al atacante a una instancia "sencilla" del problema del logaritmo discreto, de encontrar P_A. Es decir, debe encontrar un y tal que $[y](R_1 + [x]S_1) = P_A$. De esta manera podríamos construir la isogenia ϕ_A usando su núcleo.

En [5] a parte de estos problemas se presentan una variante de los mismos como problemas de decisión. También en [1, Section 6] y [5] se hace un criptoanalisis del protocolo de intercambio de clave de Diffie-Hellman basado en isogenias de curvas supersingulares los cuales conjeturan sobre que este protocolo podría ser seguro en un entorno post-cuántico.

Por último, para presentar una prueba de la eficacia del intercambio de clave de de Diffie-Hellamn basado en isogenias de curvas supersingulares nos falta mencionar el SIKE[1] (*Supersingular Isogeny Key Encapsulation*). Este protocolo fue presentado en el concurso de estandarización de protocolos del NIST. Desde que comenzó el concurso en 2017 esta propuesta ha ido superando las diferentes fases. Actualmente se encuentra en proceso de mejora[2].

[1] Toda la información relacionada con este se encuentra en su página web

[2] Aquí Microsoft presenta un concurso público para aquellos que quieran que invita a sus participantes a encontrar y resolver posibles ataques al criptosistema

3.2.1 Otros protocolos

Las isogenias entre curvas supersingulares también se han usado para crear otros protocolos criptográficos:

1. **Criptografía de clave pública**: Es una adaptación del protocolo de intercambio de clave presentado en este trabajo muy parecida a la sucede en el criptosistema de ElGamal con el intercambio de clave de Diffie-Hellman.
2. **Pruebas de conocimiento cero**: consiste en que un usuario le demuestre a otro que conoce un parámetro concreto, en este caso el generador de un subgrupo de la curva, sin revelar ese parámetro concreto.

4 | Programación SAGE

En este capítulo se plasma el código SAGEMath desarrollado para poder ver las instancias del protocolo de intercambio de clave presentado en este trabajo. El código está detelladamente comentado y si se deseara cambiar la instancia bastaría hacerlo acorde a lo presentado en este Trabajo. Una vez escogida la instancia, se ejecuta en una ventana de SAGEMath y devuelve toda la información detallada de la misma.

```
###
#
# Algunas funciones auxiliares.
#
###

###
#
# Esta función devuelve un par recibe un número enter n y devuelve un par de números
#     enteros en el intervalo [0,n-1]. Si T=True entonces escoge dos elementos
#     distintos, si T=False, los eltos pueden ser iguales.
#
###

def random_select_dif_pair(n,T):
    Zi=Integers(n)^2
    es= Zi.random_element()
    if T:
        while es[0]==es[1]:
            es= Zi.random_element()
        return(es)
    else:
```

```
        return(es)

####
#
# Esta función recibe dos listas shortlist y longlist y te devuelve
#     True si shortlist es sublista de longlist.
#
####

def is_sublist(shortlist, longlist):
     for e in shortlist:
         if not (e in longlist):
             return False
     return True

####
#
# Esta función recibe una curva E0 y un punto de la curva SA y
#     te devuelve un camino a través del correspondiente grafo
#     de isogenias. Este camino comienza en E0 y acaba en EA que
#     es la curva E0/<SA>. También facilita los j-invariantes de
#     las curvas por las que pasa.
#
####

def camino_isogenias(E0,SA):
    (pA,eA)=factor(SA.order())[0]
    j0= E0.j_invariant()
    Curv=[(E0,j0)]
    for i in range(eA):
        l=len(Curv)
        RA=(pA^(eA-1-i))*SA
        Ef=Curv[l-1][0].isogeny(RA).codomain()
        SA=Curv[l-1][0].isogeny(RA)(SA)
        Curv.append((Ef,Ef.j_invariant()))

    return Curv
```

```
########################
#
# Primero vamos a escoger el primo sobre el que vamos a trabajar. Para ello
#     fijaremos pA=2 y pB=3. Tendremos la libertad de escoger los exponentes,
#     el factor f también lo fijaremos.
#
########################

pA=2
pB=3
eA=2
eB=3

#########################
#
# Esta función recibe dos primos y una cota N y encuentra casi todos
#     primos de la forma pA^eA+pB^eB+-1 que sean menores que la cota
#     dada. Nos devuelve cada primo con la pareja de exponentes y el
#     signo del 1.
#
#########################

def primer_prime2(pA,pB,N):
    i=0
    p=pA^i*pB^i
    while p<N:
        i=i+1
        p=pA^i*pB^i
    L=[]
    for k in [1..i]:
        for j in [1..i]:
            if is_prime(pA^k*pB^j-1):
                L.append((pA^k*pB^j-1,k,j,-1))
            if is_prime(pA^k*pB^j+1):
                L.append((pA^k*pB^j+1,k,j,1))
            elif is_prime(pA^k*pB^j+1):
                L.append((pA^k*pB^j+1,k,j,1))
    L.sort()
```

```
    return L

######
#
# A partir de quí ya podemos escoger el p de la lista que más nos interese.
#
#####

N=200

p=primer_prime2(pA,pB,N)[11][0]

print(' --- La elección del primo ha sido: '"{}".format(p))
print(' ')

#############
#
# El siguiente procedimiento nos sirve para encontrar los j-invariantes
#     de curvas supersingulares en Fp^2.
#
##############

from sage.schemes.elliptic_curves.ell_finite_field import
                          is_j_supersingular, supersingular_j_polynomials

S=[j for j in GF(p^2,'j') if is_j_supersingular(j)]

print(' --- Los j-invariantes de curvas supersingulares --- ')
print(' ')
print(S)
print(' ')

############
#
# A continuación definimos los polinomios l-modulares. Cuyas
#     raíces (j1,j2) nos indican las aristas entre j-invariantes
#     (isomorfas en ext(K)) que son isogenas entre si, es
#     decir, que existe una isogenia entre una curva con
```

```
#     j-invariante j1 y otra con j-invariante j2.
#
#############

R.<x,y>=PolynomialRing(GF(p^2,'j'));
x, y = R.gens()

Phi2=x^3-x^2*y^2 + 1488*x^2*y- 162000*x^2 + 1488*x*y^2+
40773375*x*y + 8748000000*x + y^3- 162000*y^2 + 8748000000*y-
157464000000000;

Phi3=x^4+36864000*x^3+452984832000000*x^2+1855425871872000000000*x+
y^4+36864000*y^3+452984832000000*y^2+1855425871872000000000*y
-x^3*y^3+2587918086*x^2*y^2-770845966336000000*x*y+2232*x^3*y^2
-1069956*x^3*y+8900222976000*x^2*y+2232*y^3*x^2-1069956*y^3*x
+8900222976000*y^2*x

###############
#
# Usamos los polinomios modulares para obtener las aristas de los
#     grafos de 2-isogenias y 3-isogenias.
#
###############

Graph_edges2=[]
s=len(S)
for i in range(s):
    for k in range(i,s):
        if Phi2(S[i],S[k])==0:
            Graph_edges2.append((S[i],S[k]))

print(' --- Aristas de 2-isogenias ---')
print(Graph_edges2)
print(' ')

Graph_edges3=[]
s=len(S)
for i in range(s):
```

```
    for k in range(i,s):
        if Phi3(S[i],S[k])==0:
            Graph_edges3.append((S[i],S[k]))

print('--- Aristas de 3-isogenias ---')
print(Graph_edges3)
print(' ')

################
#
# Construímos el grafo que vamos a usar para hacer el protocolo
#     de intercambio de clave.
#
#############

print('--- Dibujamos los grafos:')

g2 = Graph({}, loops=True, sparse=True)
g2.add_edges(Graph_edges2)
g2.name("Grafo de 2-isogenias")
g2.show()

g3 = Graph({}, loops=True, sparse=True)
g3.add_edges(Graph_edges3)
g3.name("Grafo de 2-isogenias")
g3.show()

Graph_edgesL2=[i for i in Graph_edges2 if not i[0]==i[1]]
Graph_edgesL3=[i for i in Graph_edges3 if not i[0]==i[1]]

##############
#
# Escojemos uno de los j-invariantes y encontramos una curva de
#     la clase de isomorfismo. Esta curva será la curva común
#     para Alice y Bob. Vamos a tomar un j-invariante que
#     tenga el máximo grado en ambos grafos. Con el fin de el
#     ejercicio sea más visual.
#
```

```
##############

#####
#
# Calculamos el grado de los j-invariantes en cada grafo.
#
#####

Grade_List2=[]
s=len(S)
t=len(Graph_edgesL2)
for i in range(s):
    count=0
    for j in range(t):
        if (S[i]==Graph_edgesL2[j][0] or S[i]==Graph_edgesL2[j][1]):
            count=count+1
    Grade_List2.append([S[i],count])

Grade_List3=[]
s=len(S)
t=len(Graph_edgesL3)
for i in range(s):
    count=0
    for j in range(t):
        if (S[i]==Graph_edgesL3[j][0] or S[i]==Graph_edgesL3[j][1]):
            count=count+1
    Grade_List3.append([S[i],count])

#####
#
# Calculamos aquellos que tengan grado máximo en ambos grafos.
#
#####

Max_Grade=[S[i] for i in range(len(S)) if (Grade_List2[i][1]==3
                                        and Grade_List3[i][1]==4)]

#####
```

```
#
# Tomamos un j-invariante aleatoriamente y generamos una curva con
#     ese j-invariante.
#
#####

j0=Set(Max_Grade).random_element()

E_0=EllipticCurve(j=j0)

print(' ')
print('--- La curva pública es: '"{}".format(E_0))
print('--- --- su j-invariante es: '"{}".format(j0))
print(' ')

##
# Veamos qué estructura tiene como grupo.
##

A = E_0.abelian_group()

print('La estructura de grupo de la curva es: '"{}".format(A))

##########
#
# Buscamos P_A, Q_A puntos que generan E[pA^eA]. Para ello,
#     encontramos el grupo de torsión y luego escogemos dos
#     puntos distintos que generen el cjto.
#
##########

Ta=E_0.torsion_polynomial(pA^eA).roots(multiplicities=0)

############################################################
#
# La diferencia entre E_torsion_A_red y E_torsion_A es que en el
#     segundo solo hay un elemento con primera coordenada igual.
#     De esta manera nos aseguramos que al escoger dos puntos
```

```
#     sean distintos y que te generen todo el grupo de torsión.
#     La siguiente lista E_torsion_A_red_red se encarga de tomar
#     los puntos de máximo orden para encontrar más fácilmente
#     los generadores.
#
############################################################

E_torsion_A=[E_0.lift_x(a, all=True) for a in Ta ]
E_torsion_A_red=[E_0.lift_x(a) for a in Ta ]
E_torsion_A_red_red=[i for i in E_torsion_A_red if i.order() == pA^eA ]

Comp2=[]
tc_a= len(E_torsion_A_red_red)
while (is_sublist(Comp2,flatten(E_torsion_A)) &
                         is_sublist(flatten(E_torsion_A),Comp2))== False:
    rtc_a=random_select_dif_pair(tc_a,True)
    (P_A, Q_A)= (E_torsion_A_red_red[rtc_a[0]],E_torsion_A_red_red[rtc_a[1]])
    Comp2=[n*P_A+m*Q_A for n in range(pA^eA) for m in range(pA^eA)]
    Comp2.pop(0) # Quitamos el primer elemento que es el (0:1:0)

Tr2=is_sublist(Comp2,flatten(E_torsion_A)) &
                             is_sublist(flatten(E_torsion_A),Comp2)

print(' ')
print(' --- Los puntos que generan E[pA^eA] son:')
print(' --- --- P_A='"{}".format(P_A))
print(' --- --- Q_A='"{}".format(Q_A))
print(' --- --- ¿Generan E[pA^eA]? '"{}".format(Tr2))

######
#
# Repetimos el proceso para obtener los puntos P_B y Q_B que generen E[pB^eB].
#
######

E_0.torsion_polynomial(pB^eB)
Tb=E_0.torsion_polynomial(pB^eB).roots(multiplicities=0)
```

```
E_torsion_B=[E_0.lift_x(b, all=True) for b in Tb ]
E_torsion_B_red=[E_0.lift_x(b) for b in Tb ]
E_torsion_B_red_red=[i for i in E_torsion_B_red if i.order() == pB^eB ]

Comp3=[]
tc_b= len(E_torsion_B_red_red)
while (is_sublist(Comp3,flatten(E_torsion_B)) &
                            is_sublist(flatten(E_torsion_B),Comp3))== False:
    rtc_b=random_select_dif_pair(tc_b,True)
    (P_B, Q_B)= (E_torsion_B_red_red[rtc_b[0]],E_torsion_B_red_red[rtc_b[1]])
    Comp3=[n*P_B+m*Q_B for n in range(pB^eB) for m in range(pB^eB)]
    Comp3.pop(0) # Quitamos el primer elemento que es el (0:1:0)

Tr3=is_sublist(Comp3,flatten(E_torsion_B)) & is_sublist(flatten(E_torsion_B),Co

print(' ')
print(' --- Los puntos que generan E[pB^eB] son:')
print(' --- --- P_B='"{}".format(P_B))
print(' --- --- Q_B='"{}".format(Q_B))
print(' --- --- ¿Generan E[pB^eB]? '"{}".format(Tr3))

######
#
# Ahora llega el momento de que Alicia escoja una clave privada y calcule
#     su clave pública.
#
######

########################################
#                                      #
# Ahora Alice debe escoger kA en       #
#   Z/ZpA^eA SECRETA de tal manera     #
#   que no sea divisible por pA        #
kA= 1                                  #
#                                      #
########################################

Sa=P_A+kA*Q_A
```

```
print(' ')
print(' --- La clave secreta de Alicia es:')
print(' --- --- kA='"{}".format(kA))
print(' --- --- Sa='"{}".format(Sa))
print(' ')

######
#
# Vamos a calcular la Isogenia cuyo kernel lo genere Sa.
#
######

PhiA = E_0.isogeny([Sa]);

E_A=PhiA.codomain()
j_A=E_A.j_invariant()

print(' --- La isogenia secreta de Alicia es:')
print(' --- --- '"{}".format(PhiA))
print(' --- --- El codominio es '"{}".format(E_A))
print(' --- --- j(E_A)='"{}".format(j_A))

P_Bp=PhiA(P_B)
Q_Bp=PhiA(Q_B)

print(' --- El camino que sigue en el grafo es:')
L2=camino_isogenias(E_0,Sa)
print(table(L2,header_row=["Curva","j-invariante"]))

########################################
#                                      #
# Ahora Bernardo debe escoger kB       #
#   en Z/ZpB^eB SECRETO de tal manera  #
#   que no sea divisible por pB        #
kB= 1                                  #
#                                      #
########################################
```

```
Sb=P_B+kB*Q_B

print(' ')
print(' --- La clave secreta de Bernardo es:')
print(' --- --- kB='"{}".format(kB))
print(' --- --- Sb='"{}".format(Sb))
print(' ')

######
#
# Vamos a calcular la Isogenia cuyo kernel lo genere Sa.
#
######

PhiB = E_0.isogeny([Sb]);

E_B=PhiB.codomain()
j_B=E_B.j_invariant()

print(' --- La isogenia secreta de Bernardo es:')
print(' --- --- '"{}".format(PhiB))
print(' --- --- El codominio es '"{}".format(E_B))
print(' --- --- j(E_B)='"{}".format(j_B))
print(' ')

P_Ap=PhiB(P_A)
Q_Ap=PhiB(Q_A)

print(' --- El camino que sigue en el grafo es:')
L3=camino_isogenias(E_0,Sb)
print(table(L3,header_row=["Curva","j-invariante"]))

#########
#
# Las claves de cada uno son:
print(' --- Alicia PKa:')
print(' --- E_A:'"{}".format(E_A))
```

```
print(' --- P_Bp:'"{}".format(P_Bp))
print(' --- Q_Bp:'"{}".format(Q_Bp))
print(' ')
print(' --- Bernardo PKb:')
print(' --- E_B:'"{}".format(E_B))
print(' --- P_Ap:'"{}".format(P_Ap))
print(' --- Q_Ap:'"{}".format(Q_Ap))
#
#########

###############
#
# Ahora vamos a calcular el intercambio de clave.
#
###############

###############
#
# Vamos a empezar por Alicia. Primero calculamos el punto Sap y
#     luego calculamos la isogenia que tiene como núcleo el
#     espacio que genera Sap.
#
###############

Sap=P_Ap+kA*Q_Ap

PhiAB=E_B.isogeny(Sap)
E_AB=PhiAB.codomain()
j_AB=E_AB.j_invariant()

print(' ')
print(' --- El j-invariante al que llega Alicia es '"{}".format(j_AB))

###############
#
# Continuamos con Bernardo. Primero calculamos el punto Sbp y
#     luego calculamos la isogenia que tiene como núcleo el
#     espacio que genera Sbp.
```

```
#
###############

Sbp=P_Bp+kB*Q_Bp

PhiBA=E_A.isogeny(Sbp)
E_BA=PhiBA.codomain()
j_BA=E_BA.j_invariant()

print(' ')
print(' --- El j-invariante al que llega Bernardo es '"{}".format(j_BA))

#########
#
# Finalmente acabamos dibujando sobre el grafo los itinerarios
#     que han seguido Alcia y Bernardo en los grafos de isogenias.
#     En verde aparece el camino que siguen a la hora de generar
#     la clave pública y en azul el que siguen para encontrar
#     la clave compartida.
#
##########

#####
#
# Caminos de Alicia:
#
#####

CaminoGen2=camino_isogenias(E_0,Sa)
cg=len(CaminoGen2)
AristasCaminoGen2=[]
for i in [0..cg-2]:
    AristasCaminoGen2.append((CaminoGen2[i][1],CaminoGen2[i+1][1]))
    AristasCaminoGen2.append((CaminoGen2[i+1][1],CaminoGen2[i][1]))

CaminoClave2=camino_isogenias(E_B,Sap)
AristasCaminoClave2=[]
for i in [0..cg-2]:
```

```
    AristasCaminoClave2.append((CaminoClave2[i][1],CaminoClave2[i+1][1]))
    AristasCaminoClave2.append((CaminoClave2[i+1][1],CaminoClave2[i][1]))

for e in AristasCaminoGen2:
    g2.set_edge_label(e[0],e[1],1)
for e in AristasCaminoClave2:
    g2.set_edge_label(e[0],e[1],2)

GP2 = g2.graphplot(edge_labels=False, color_by_label={1: "green", 2: "blue"})
GP2.show()

#####
#
# Caminos de Bernardo:
#
#####

CaminoGen3=camino_isogenias(E_0,Sb)
cg=len(CaminoGen3)
AristasCaminoGen3=[]
for i in [0..cg-2]:
    AristasCaminoGen3.append((CaminoGen3[i][1],CaminoGen3[i+1][1]))
    AristasCaminoGen3.append((CaminoGen3[i+1][1],CaminoGen3[i][1]))

CaminoClave3=camino_isogenias(E_A,Sbp)
AristasCaminoClave3=[]
for i in [0..cg-2]:
    AristasCaminoClave3.append((CaminoClave3[i][1],CaminoClave3[i+1][1]))
    AristasCaminoClave3.append((CaminoClave3[i+1][1],CaminoClave3[i][1]))

for e in AristasCaminoGen3:
    g3.set_edge_label(e[0],e[1],1)
for e in AristasCaminoClave3:
    g3.set_edge_label(e[0],e[1],2)

GP3 = g3.graphplot(edge_labels=False, color_by_label={1: "green", 2: "blue"})
GP3.show()
```

Bibliografía

[1] L. De Feo, D. Jao, and J. Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* Journal of Mathematical Cryptology, 8(3), pp. 209–247, 2014.

[2] L. De Feo, J. Kieffer and B. Smith, *Towards practical key exchange from.* Journal of Mathematical Cryptology, 8(3), pp. 209–247, 2014.

[3] M. Deuring. *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hamburg, 14:197–272, 1941.

[4] Steven D Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, 2012.

[5] Galbraith, S.D., Vercauteren, F. Computational problems in supersingular elliptic curve isogenies. Quantum Inf Process 17, 265 (2018). https://doi.org/10.1007/s11128-018-2023-6

[6] L. Panny, *Cryptography on Isogeny Graphs.* Eindhoven: Technische Universiteit Eindhoven, 2021.

[7] J. H. Silverman *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1992.

[8] J. Vélu. *Isogénies entre courbes elliptiques.* Comptes Rendus de l'Académie des Sciences de Paris, 273, pp. 238–241, 1971.

[9] A.V. Sutherland *Isogeny volcanoes* Proceedings of the tenth algorithmic number theory symposium, 1, pp. 507-530, 2013.

[10] D. Kohel,*Endomorphism ring of elliptic curves ovr finite fields* University of California, 1996.

[11] W. C. Waterhouse, *Abelian varieties over finite fields.* Ann. scient. Ec. Norm. Sup., 2:521–560, 1969.

[12] J.F. Voloch, *A note on Elliptic curves over finite fields.* Bulletin de la S.M.F., 116, 4, pp. 455-458, 1988.