Centro de Matemática

Facultad de Ciencias

Universidad de la República

Montevideo, Uruguay

Criptografía de Curvas Elípticas y Logaritmo Discreto.

Implementación de Autoreducibilidad aleatoria.

Tesis de Maestría en Matemática

Claudio Qureshi, Orientado por Gonzalo Tornaria.

Índice general

Introducción.

Este trabajo se enmarca en el contexto de Criptografía de Curvas Elípticas[1]. Uno de los tópicos principales en dicha área son los criptosistemas basados en el Problema del Logaritmo Discreto[2] (PLD) en Curvas elípticas. Este es un caso particular de criptosistemas de clave pública que basa su seguridad en la dificultad de resolver el PLD en un grupo abeliano.

Inicialmente se tomó como grupo, el grupo multiplicativo de un cuerpo finito. Al ser descubierto un algoritmo de tiempo subexponencial para resolver el PLD en esos grupos (basado en el Index Calculus) se necesitaban claves cada vez más largas para garantizar un buen nivel de seguridad.

En 1985 independientemente Koblitz y Miller propusieron utilizar el grupo formado por los puntos racionales de una curva elíptica definida sobre un cuerpo finito. La ventaja primordial, es que se lograban alcanzar los mismos niveles de seguridad que utilizando el grupo multiplicativo de un cuerpo finito utilizando claves mucho más cortas. Esta característica lo hacía ideal para ser utilizado en dispositivos con entornos operativos restringidos (limitaciones de memoria, ancho de banda, potencia, etc).

Hasta el momento no se ha encontrado un algoritmo de tiempo subexponencial capaz de resolver el PLD en curvas elípticas en general y se ha convertido en uno de los principales estándares a ser utilizado en la actualidad. No todas las curvas elípticas definidas sobre el mismo cuerpo finito ofrecen el mismo nivel de seguridad respecto del PLD. Se conocen criterios que hacen a una curva débil, todos ellos se reducen de alguna forma a alguna condición sobre la cantidad de puntos racionales que posea la curva. Sin embrago, aún es un problema en abierto determinar si el hecho de que dos curvas (definidas sobre el mismo cuerpo finito) posean la misma cantidad de puntos racionales implica necesariamente que la dificultad de resolver el PLD en ambas curvas sea equivalente.

Una manera de probar la equivalencia del PLD en dos grupos es encontrando un isomorfismo entre ambos grupos que tanto él, como su inversa puedan ser computados eficientemente (digamos, en tiempo polinomial por ejemplo). Esto es fácil de ver, dado que los isomorfismos preservan el orden de los elementos. Generalizando esta idea, se puede llegar a la conclusión que basta con que haya una cadena de homomorfismos de grupo (cada una con kernel de cardinal pequeño[3] y conocido) que partiendo de uno de los grupos llegue al otro; en este caso cada homomorfismo debe ser eficientemente computable.

[1] Abreviado ECC, por sus siglas en inglés.

[2] Se recuerda que el Problema del Logaritmo Discreto (PLD) en un grupo $(G, +)$ consiste en, dados dos elementos P y Q del grupo G con $Q \in \langle P \rangle$, hallar $n \in \mathbb{Z}$ tal que $Q = nP$.

[3] Suficientemente pequeño para poder calcular el PLD en ellos.

Para el caso particular de curvas elípticas, los homomorfismos de grupo más naturales a considerar vienen dado por isogenias (que son mapas racionales entre ambas curvas que preservan el elemento neutro). El tipo de curvas elípticas consideradas para criptografía (en el contexto del logaritmo discreto) son las llamadas ordinarias. De ese modo, para poder probar algún resultado de equivalencia entre el PLD entre diferentes curvas elípticas, resulta natural considerar como objeto natural de estudio al grafo formado por curvas elípticas ordinarias y aristas dada por isogenias.

En 1996 Kohel realizó un estudio sobre el grafo de isogenias de curvas ordinarias en su tesis de doctorado [**25**], a partir de ahí una cantidad considerable artículos y trabajos en ECC fueron desarrollados y actualmente sigue siendo un área de desarrollo activa; en la sección final de esta tesis (página 121), se da un resumen de los trabajos más destacados en esta línea y algunos problemas en abierto en los que se sigue trabajando.

En dirección a determinar la equivalencia del PLD entre curvas elípticas de igual cardinal, uno de los principales resultados es un Teorema de Jao, Miller y Venkatesan (Teorema 1.1 de [**24**]) en donde prueban que, asumiendo la Hipótesis de Riemann Generalizada, la respuesta es en cierto sentido afirmativa para curvas elípticas definidas sobre el mismo cuerpo finito, misma cantidad de puntos y mismo tipo de anillo de endomorfismo.

El Teorema de Jao, Miller y Venkatesan es el primer resultado de autoreducibilidad aleatoria en este contexto, el concepto de autoreducibilidad aleatoria se refiere de alguna forma a que es posible reducir el peor caso a un caso aleatorio, de modo que informalmente podríamos decir que la dificultad entre distintas instancias del problema es equivalente.

Visto desde el punto de vista práctico, computacionalmente podemos aprovechar este resultado de dos formas, según como se interprete. Una de ellas es, si tenemos seguridad de que una curva elíptica es buena (por ejemplo porque ha sido usada por mucho tiempo en la práctica y ha resistido a variados ataques), entonces podemos computar masivamente curvas buenas, implementando un algoritmo capaz de producir en forma sistemática curvas con el mismo cardinal que la curva considerada buena, esta idea aparece en el artículo [**30**].

La otra interpretación es, si se llegase a descubrir un algoritmo eficiente para resolver el PLD en un conjunto S de curvas elípticas con el mismo cardinal que una curva elíptica E, en la cual queremos resolver el PLD, entonces tendríamos que poder construir un algoritmo capaz de computar el logaritmo discreto en E a partir de que conocemos como resolver el logaritmo discreto en las curvas de S. Este es justamente el enfoque de esta tesis, estudiar los aspectos computacionales y desarrollar algoritmos que estén vinculados con esta interpretación del resultado de autoreducibilidad aleatoria de Jao, Miller y Venkatesan.

En esta tesis, observando cuales son los puntos clave que debería tener un algoritmo capaz de llevar a cabo esta autoreducción aleatoria, definimos los axiomas de un tipo de algoritmo que llamaremos (Ran,Red) y observamos que la estrategia que proponen Jao Miller y Venkatesan en [**24**] entran en el marco del algoritmo de autoreducibilidad aleatoria (Ran,Red). Analizamos en detalle cada una de las componentes del algoritmo (Ran,Red) para este caso, describiéndolas paso a paso, e implementando todos los algoritmos usando Sage [**37**].

En la mayoría de los casos, se otorga el código Sage para los algoritmos aquí implementados; para algunos algoritmos que son utilizados como subrutinas, se los describe detalladamente pero se deja a disposición el código de Sage en mi página personal `http://www.fing.edu.uy/~cqureshi/`.

Respecto a la estructura de la tesis, esta está constituida de tres capítulos.

En el primer capítulo se exponen resultados clásicos sobre curvas elípticas, algunas ya vistas en la monografía pero desde otro enfoque, siguiendo escencialmente el libro de Silverman "The Arithmetic of Elliptic Curves" (muchas veces dejándolo como referencia para consultar detalles de algunos resultados).

En el segundo capítulo comenzaremos estudiando resultados muchos más específicos en torno al grafo de isogenias de curvas ordinarias, que sirven para comprender el teorema principal de Jao, Miller y Venkatesan sobre autoreducibilidad aleatoria [**24**], y dan base para comprender los algoritmos desarrollados en Sage en el capítulo posterior. También se dará una implementación del grafo de ℓ-isogenias en Sage para un caso concreto basado en el artículo [**14**] y culminaremos el capítulo analizando en detalle los principales pasos del Teorema de Jao, Miller y Venkatesan. En esta parte las referencias principales serán la tesis de doctorado de Kohel, el excelente libro de David.A.Cox "Primes of the form $x^2 + ny^2$" y el artículo de Jao-Miller-Venkatesan referido anteriormente.

En el tercer y último capítulo presentaremos nuestro algoritmo (Ran,Red) de autoreducibilidad aleatoria, analizaremos en detalle todas sus componentes, analizando los principales algoritmos y problemas computacionales relacionados. En particular abordaremos el problema de la computación de polinomios modulares, repasando la teoría de formas modulares relacionada y discutiendo los distintos enfoques utilizados por diversos autores relacionado a su implementación; se incluirá además una implementación realizada en Sage. Se discutirán algunos problemas (teóricos y de implementación) en abierto que giran en torno al Teorema de Jao, Miller y Venkatesan de autoreducibiliada aleatoria (que tiene consecuencia directa con la eficiencia de nuestra implementación del algoritmo (Ran,Red)) y en general respecto a algoritmos relacionados con la estructura del grafo volcán de isogenias. Se culmina dando una idea del estado actual del arte en lo referente a resultados computacionales vinculados con la tesis de Kohel.

Capítulo 1

Conceptos básicos sobre curvas elípticas

En esta sección haremos un repaso de algunos conceptos básicos, pero importantes en el posterior desarrollo de la tesis. Se darán todas las definiciones necesarias para entender los resultados, pero en las pruebas a veces se utilizarán algunos conceptos básicos de geometría algebraica que pueden encontrarse, por ejemplo, en el libro de Fulton [**15**].

1. Geometría Algebraica Racional, Curvas Elípticas e Isogenias.

Denotaremos por $\mathbb{K}$ un cuerpo finito o de característica 0 y fijemos $\overline{\mathbb{K}}$ una clausura algebrica de $\mathbb{K}$, la ventaja de trabajar en tales cuerpos es que son perfectos (es decir, toda extensión algebraica es separable). Recordemos que una extensión $\mathbb{K} \subset \mathbb{L}$ es algebraica si todo $s \in \mathbb{L}$ es algebraico sobre $\mathbb{K}$ (es decir, verifica un polinomio con coeficientes en $\mathbb{K}$) y que la extensión sea separable significa que el polinomio irreducible de cualquier elemento $s \in \mathbb{L}$ sobre $\mathbb{K}$ no posee raíces múltiples cuando factoriza en una clausura algebraica de $\mathbb{K}$ (que será denotada de aquí en más por $\overline{\mathbb{K}}$). A las raíces del polinomio irreducible de s sobre $\mathbb{K}$ en $\overline{\mathbb{K}}$ les llamamos los conjugados de s que denotaremos por $s_1 = s, s_2, s_3, \ldots, s_n$ (donde $n = \deg(Irr_{\mathbb{K}}(s))$). En el caso que $\mathbb{K} \subset \mathbb{L}$ sea separable y finita entonces $\mathbb{L} = \mathbb{K}(s)$ para algún $s \in \mathbb{L}$ (Teorema del elemento primitivo), así que tenemos exactamente n monomorfismos de cuerpos $\sigma_i : \mathbb{L} \to \overline{\mathbb{K}}$ caracterizados por la propiedad $\sigma_i(s) = s_i$ para $i = 1, 2, \ldots, n$. Si todos esos morfismos verifican que su imagen está contenida en $\mathbb{L}$ entonces decimos que la extensión $\mathbb{K} \subset \mathbb{L}$ es normal y el conjunto de tales morfismos forman un grupo con la composición, denotado por $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ (el grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$).

Para el caso que la extensión $\mathbb{K} \subset \mathbb{L}$ sea finita y de Galois (es decir, separable y normal), entonces el teorema de correspondencia de Galois establece una correspondencia biunívoca entre los cuerpos intermedios entre $\mathbb{K}$ y $\mathbb{L}$ y los subgrupos de $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. La correspondencia viene dada por:

$$\{\text{Cuerpos intermedios entre } \mathbb{K} \text{ y } \mathbb{L}\} \xrightarrow{\varphi} \{\text{Subgrupos de } \mathrm{Gal}(\mathbb{L}/\mathbb{K})\}$$
$$\mathbb{H} \mapsto \mathrm{Gal}(\mathbb{L}/\mathbb{H})$$

Cuya inversa viene dada por:

$$\{\text{Subgrupos de } \mathrm{Gal}(\mathbb{L}/\mathbb{K})\} \xrightarrow{\psi} \{\text{Cuerpos intermedios entre } \mathbb{K} \text{ y } \mathbb{L}\}$$
$$H \mapsto \mathbb{L}^H = \{x \in \mathbb{L} : \sigma(x) = x \text{ para toda } \sigma \in H\}$$

Además tanto φ como ψ revierten las inclusiones y preservan los grados, es decir:

$$[\mathbb{H}_1 : \mathbb{H}_2] = [\varphi(\mathbb{H}_2) : \varphi(\mathbb{H}_1)] \text{ y } [H_1 : H_2] = [\psi(H_2) : \psi(H_1)].$$

En muchas ocasiones, especialmente cuando deseamos verificar racionalidad, nos interesará trabajar con el grupo de Galois absoluto, que cuando el cuerpo base $\mathbb{K}$ es perfecto

no es otra cosa que $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}) = \{\theta : \overline{\mathbb{K}} \to \overline{\mathbb{K}} : \theta|_{\mathbb{K}} = id_{\mathbb{K}}\}$ (observemos que la extensión algebraica $\mathbb{K} \subset \overline{\mathbb{K}}$ es automáticamente normal y es separable porque $\mathbb{K}$ es perfecto así que es una extensión de Galois). El teorema de correspondencia de Galois en este caso establece una biyección entre los cuerpos intermedios entre $\mathbb{K}$ y $\overline{\mathbb{K}}$ y los subgrupos cerrados de $G = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ (donde la topología en G es la inducida por la topología producto $\Pi_{x\in\overline{\mathbb{K}}}\overline{\mathbb{K}}$, cada factor $\overline{\mathbb{K}}$ con la topología discreta), la correspondencia es similar que para el caso finito.

1.1. Curvas Algebraicas.

Definición 1.1. El espacio afín $n-$dimensional sobre $\mathbb{K}$ viene dado por:

$$\mathbb{A}^n = \mathbb{A}^n(\overline{\mathbb{K}}) = \{(x_1, x_2, \ldots, x_n) : x_i \in \overline{\mathbb{K}}, 1 \leq i \leq n\}$$

Definición 1.2. El espacio proyectivo $n-$dimensional sobre $\mathbb{K}$ viene dado por:

$$\mathbb{P}^n = \frac{\mathbb{A}^{n+1} - \{0\}}{\sim} \quad \text{donde } P \sim Q \Leftrightarrow \exists \lambda \in \overline{\mathbb{K}}, \lambda \neq 0 \text{ tal que } P = \lambda Q$$

La clase de equivalencia de $P = (x_1, x_2, \ldots, x_{n+1})$ será denotada por $[x_1 : x_2 : \ldots : x_{n+1}] = \{\lambda P : \lambda \in \overline{\mathbb{K}}^*\}$.

Si $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ y $P = (x_1, x_2, \ldots, x_n) \in \mathbb{A}^n$ definimos $\sigma(P) = (\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_n))$, esto define una acción de grupos $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}) \times \mathbb{A}^n \to \mathbb{A}^n$. Esta acción verifica $\sigma(\lambda P) = \sigma(\lambda)\sigma(P)$ para todo $P \in \mathbb{A}^{n+1}$ y $\lambda \in \overline{\mathbb{K}}^*$ (es decir $P \sim Q \Rightarrow \sigma(P) \sim \sigma(Q)$) así que induce una acción $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K}) \times \mathbb{P}^n \to \mathbb{P}^n$.

Definición 1.3. Decimos que un subconjunto $D \subset \mathbb{P}^n$ (ó $\subset \mathbb{A}^n$) está definido sobre $\mathbb{K}$ si $D = \sigma(D) = \{\sigma(x) : x \in D\}$ para todo $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ (obs: que D esté definido sobre $\mathbb{K}$ no significa que los elementos de D estén definidos sobre $\mathbb{K}$).

Si $F \in \mathbb{K}[X, Y, Z]$ es un polinomio homogéneo de grado k (i.e. suma de monomios de grado k) y $P = (x_0, y_0, z_0) \in \mathbb{A}^3$ es tal que $F(P) = 0$ entonces para todo $\lambda \in \overline{\mathbb{K}}$ tenemos que $F(\lambda P) = F(\lambda x_0, \lambda y_0, \lambda z_0) = \lambda^k F(x_0, y_0, z_0) = 0$, por lo tanto ser un cero de F no depende de la clase de equivalencia así que tiene sentido hablar de los ceros de F en $\mathbb{P}^2$.

Definición 1.4. Una curva plana proyectiva $\mathcal{C}$ es el conjunto de ceros en $\mathbb{P}^2$ de un polinomio homogéneo irreducible $F \in \overline{\mathbb{K}}[X, Y, Z]$:

$$\mathcal{C} = \{P \in \mathbb{P}^2 : F(P) = 0\}$$

Decimos que la curva $\mathcal{C}$ está definida sobre $\mathbb{K}$ si es el conjunto de ceros de un polinomio F definido sobre $\mathbb{K}$ (es decir, tal que sus coeficientes están en $\mathbb{K}$). En este caso definimos el conjunto de sus puntos racionales como:

$$\mathcal{C}(\mathbb{K}) = \{P \in \mathcal{C} : \sigma(P) = P \text{ para todo } \sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})\}$$

Si un punto $P = [x_1 : \ldots : x_{n+1}] \in \mathbb{P}^n$ permanece fijo por todos los elementos de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ entonces tomando cualquier coordenada $x_i \neq 0$ tenemos que $x_j/x_i \in \mathbb{K}$ para $1 \leq j \leq n+1$, cuando esto pasa se dice que el punto P es $\mathbb{K}-$racional o que está definido

sobre $\mathbb{K}$.

Con esta última nomenclatura, los puntos $\mathbb{K}-$racionales de la curva $\mathcal{C}/\mathbb{K}$ no son otra cosa que las raíces de F que están definidas sobre $\mathbb{K}$. Se observa que este conjunto podría ser vacío (por ejemplo si $F(X,Y,Z) = X^2 + Y^2 + Z^2$ y $\mathbb{K} = \mathbb{Q}$).

Definición 1.5. El anillo de polinomios sobre la curva $\mathcal{C} : F(X,Y,Z) = 0$ viene dado por:

$$\Gamma(\mathcal{C}) = \frac{\overline{\mathbb{K}}[X,Y,Z]}{(F(X,Y,Z))}$$

El ideal $I = (F)$ es homogéneo, es decir, si $G = G_0 + G_1 + \ldots + G_m \in I$ con G_i polinomio homogéneo de grado i (convenimos que el polinomio nulo es homogéneo de todos los grados) entonces cada $G_i \in I$. En efecto, si $H = H_0 + H_1 + \ldots + H_k$ con H_i homogéneo de grado i entonces $HF = H_0F + H_1F + \ldots + H_kF$, donde los H_iF son homogéneos de distinto grado (pues F lo es) para $i = 1, 2, \ldots, k$. Concluimos entonces que cada una de las componentes homogeneas de HF van a ser también múltiplo de F.

Definición 1.6. Si $g \in \Gamma(\mathcal{C})$ decimos que g es una d-forma (o simplemente una forma si se sobreentiende el grado) si $g = \overline{G}$ con $G \in \overline{\mathbb{K}}[X,Y,Z]$ homogéneo de grado d (donde $\overline{G}$ denota la clase de G en $\Gamma(\mathcal{C})$). Si existe algún representante $G \in \mathbb{K}[X,Y,Z]$ decimos que la forma g está definida sobre $\mathbb{K}$ o que es $\mathbb{K}-$racional.

Observación 1.7. Todo elemento $g \in \Gamma(\mathcal{C})$ se escribe de forma única como suma de formas no nulas.

Demostración: Todo polinomio es suma de polinomios homogéneos así que g es suma de formas, para la unicidad observemos que si $G - G' \in I = (F)$ con $G = G_0 + G_1 + \ldots + G_k$ y $G' = G'_0 + G'_1 + \ldots + G'_k$ (con G_i y G'_i polinomios homogéneos de grado i para $i = 0, 1, \ldots, k$) entonces $G - G' = \sum_{i=0}^{k}(G_i - G'_i) \in I$ con $G_i - G'_i$ homogéneo de grado i. Puesto que I es homogéneo se tendrá que $G_i - G'_i \in I$ para $i = 1, 2, \ldots, k$ como queriamos probar.

Como F es irreducible, el anillo de polinomios en $\mathcal{C}$ es un dominio de integridad por lo tanto podemos considerar su cuerpo de fracciones y dentro de éste el subconjunto:

$$\overline{\mathbb{K}}(\mathcal{C}) = \left\{ \frac{g}{h} : g, h \text{ formas del mismo grado en } \Gamma(\mathcal{C}), h \neq 0 \right\}$$

cuyos elementos llamaremos funciones meromorfas en $\mathcal{C}$. Dentro del cuerpo de funciones meromorfas en $\mathcal{C}$ se encuentra el subcuerpo de funciones $\mathbb{K}-$racionales dado por:

$$\mathbb{K}(\mathcal{C}) = \left\{ \frac{g}{h} : g, h \text{ formas } \mathbb{K}-\text{racionales del mismo grado en } \Gamma(\mathcal{C}), h \neq 0 \right\}$$

Definición 1.8. Sea $\mathcal{C}$ la curva definida por F (donde $F \in \overline{\mathbb{K}}[X,Y,Z]$ es un polinomio homogéneo irreducible) y $f = \overline{G}/\overline{H}$ una función meromorfa no nula en $\mathcal{C}$, donde G y H son polinomios homogéneos del mismo grado ($\overline{G}$ y $\overline{H}$ son las clases módulo F de dichos polinomios). Si $P \in \mathbb{P}^2$ definimos el orden de P en $\mathcal{C}$ como:

$$ord_P(f) = I(P, F \cap G) - I(P, F \cap H)$$

donde $I(P, F \cap G)$ denota el índice de intersección de F con G en P (ver pág. 37 y 54 de [**15**]) que es una medida de la multiplicidad de la intersección de F con G, por ejemplo, si

ambas curvas se cortan transversalmente en P ese índice vale 1. Dicho índice solo depende de P, F y f (y no de los polinomios G y H escogidos para representar a f).

Se puede demostrar que en el caso que $ord_P(f) \geq 0$ su valor en P está bien definido y no depende del representante elegido para escribir a P, denotamos dicho valor por $f(P)$ además $f(P) = 0$ solo en el caso que $ord_P(f) > 0$.

Definición 1.9. Con las mismas notaciones que en la definición anterior, tenemos dos casos especiales a destacar:

- Si $ord_P(f) = -n < 0$ decimos que f tiene en P un polo de orden n.
- Si $ord_P(f) = n > 0$ decimos que f tiene en P un cero de orden n.

Observación 1.10. El hecho que $\overline{G}$ y $\overline{H}$ sean no nulas, como F es irreducible, es equivalente a pedir que G y H no tengan componentes comunes con F, luego tanto $I(P, F \cap G)$ como $I(P, F \cap H)$ son naturales para cada $P \in \mathbb{P}^2$. Además F y G no pueden tener infinitas raíces comunes al no tener componentes comunes (es consecuencia directa de Bezout, pero puede verse mucho más elementalmente por ejemplo en la pág. 9 de [**15**]) así que $I(P, F \cap G) = 0$ para todo $P \in \mathbb{P}^2$ salvo una cantidad finita de puntos (las raíces comunes de F y G), la misma conclusión vale con F y H, por lo tanto toda función meromorfa en $\mathcal{C}$ no nula solo puede tener un número finito de ceros y de polos en $\mathbb{P}^2$.

De hecho, usando Bezout podemos decir un poco más, que la suma de los ordenes de los ceros y polos contados con multiplicidades da 0. En efecto, con las notaciones anteriores, dicha suma viene dada por:

$$\sum_{P \in \mathcal{C}} ord_P(f) = \sum_{P \in \mathcal{C}} I(P, F \cap G) - \sum_{P \in \mathcal{C}} I(P, F \cap H) = gr(F)gr(G) - gr(F)gr(H) =$$
$$= gr(F)(gr(G) - gr(H)) = 0$$

1.1.1. Espacios de Riemann-Roch. Una idea interesante para estudiar las curvas es a través de sus funciones meromorfas, la idea es elegir una cierta cantidad finita de puntos de la curva $P_1, P_2, \ldots, P_m \in \mathcal{C}$ y considerar el conjunto de las funciones f que cumplan con las restricciones $ord_{P_i}(f) \geq n_i$ para ciertos n_i enteros prefijados (si $n_i = n > 0$ estamos pidiendo que f tenga un cero en P de orden al menos n_i, si $n_i = -n < 0$ que si llega a tener polo en P_i su orden no supere a n y si $n_i = 0$ que no tenga polos en P_i). El conjunto de tales funciones junto con la función nula forman un espacio vectorial de dimensión finita (los espacios de Riemann-Roch asociados a la curva $\mathcal{C}$) cuyo estudio nos brindarán información escencial de la curva $\mathcal{C}$. La noción de divisor en una curva $\mathcal{C}$ permite una formulación más elegante de los resultados, así que comenzemos definiendo esta noción.

Definición 1.11. Un divisor D en una curva $\mathcal{C}$ es una suma formal de puntos de la curva, $D = \sum_{P \in \mathcal{C}} n_P P$ donde los $n_P \in \mathbb{Z}$ son todos nulos salvo una cantidad finita. Se conviene en que pueden omitirse aquellos términos que corresponden a puntos P con $n_P = 0$, si $n_P = 0$ para todo $P \in \mathcal{C}$ escribimos $D = 0$ y lo llamamos divisor nulo. Al conjunto de todos los divisores de la curva los denotaremos por $Div(\mathcal{C})$.

Se observa que $Div(\mathcal{C})$ tiene estructura natural de grupo abeliano definiendo la suma coordenada a coordenada y un orden dado por $D = \sum_{P \in \mathcal{C}} n_P P \geq D' = \sum_{P \in \mathcal{C}} n'_P P$ siempre que $n_P \geq n'_P$ para todo $P \in \mathcal{C}$ (que es lo mismo que decir que $D - D' \geq 0$). Una

importante cantidad asociada a un divisor es lo que llamamos su grado.

Definición 1.12. Si $D = \sum_i n_i P_i \in Div(\mathcal{C})$ entonces definimos su grado como $\deg(D) = \sum_i n_i$.

Se observa que el grado $\deg : Div(\mathcal{C}) \to \mathbb{Z}$ es un epimorfismo de grupos ordenados.

En el caso que la curva $\mathcal{C}$ este definida sobre $\mathbb{K}$ entonces la acción de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ en $\mathbb{P}^2$ se puede restringir a una acción en $\mathcal{C}$ (puesto que si $P \in \mathcal{C} \Rightarrow F(\sigma(P)) = \sigma(F(P)) = 0$ (la segunda igualdad es porque F tiene coeficientes en $\mathbb{K}$) $\Rightarrow \sigma(P) \in \mathcal{C}$). Para $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ y $D = \sum_i n_i P_i \in Div(\mathcal{C})$ definimos $\sigma(D) = \sum_i n_i \sigma(P)$ (donde la acción de $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ en $\mathcal{C}$ es la acción en $\mathbb{P}^2$ restringida), así que para curvas $\mathbb{K}-$racionales tenemos que $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ actua en el conjunto de divisores $Div(\mathcal{C})$ en la forma que acabamos de mencionar.

Definición 1.13. Un divisor $D \in Div(\mathcal{C})$ se dice que es $\mathbb{K}-$racional o definido sobre $\mathbb{K}$ si $\sigma(D) = D$ para todo $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ (obs: esto no implica que su soporte $sop(D) = \{P \in \mathcal{C} : n_p \neq 0\}$ esté contenido en $\mathbb{K}$).

Ahora definiremos una clase distinguida de divisores que vienen asociados a funciones meromorfas.

Definición 1.14. Sea f una función meromorfa no nula en la curva $\mathcal{C}$, definimos su divisor de ceros y polos como:

$$div(f) = \sum_{P \in \mathcal{C}} ord(P) P$$

Es efectivamente un divisor, pues como mencionamos antes (Obs. 1.10), toda función meromorfa tiene una cantidad finita de ceros y polos. Al conjunto de dichos divisores los llamaremos divisores principales.

Además como toda función meromorfa no nula tiene la misma cantidad de ceros que de polos contados con multiplicidades, los divisores principales tienen todos grado cero. Observemos que los divisores de grado cero son un subgrupo del grupo de divisores de una curva.

Ahora ya tenemos todas las notaciones necesarias para definir en forma elegante los espacios de Riemann-Roch.

Definición 1.15 (Espacios de Riemann-Roch.)**.** Sea $\mathcal{C}$ una curva y $D \in Div(\mathcal{C})$ definimos el espacio de Riemann-Roch asociado al divisor D como el conjunto:

$$\mathcal{L}(D) = \{f \in \overline{\mathbb{K}}(\mathcal{C}) : div(f) + D \geq 0\} \cup \{0\}$$

Para cuando el divisor D está definido sobre $\mathbb{K}$ tenemos también la versión $\mathbb{K}-$racional de dichos espacios:

$$\mathcal{L}_{\mathbb{K}}(D) = \{f \in \mathbb{K}(\mathcal{C}) : div(f) + D \geq 0\} \cup \{0\}$$

Observemos que si $D = \sum_{P\in\mathcal{C}} n_P P$ tenemos que los n_P son todos ceros salvo para una cantidad finita de puntos $P \in \mathcal{C}$, si $n_P = n > 0$ entonces le estamos pidiendo a f que tenga un cero de orden al menos n en P mientras que si $n_P = -n < 0$ le estamos pidiendo que si llega a tener polo en P su orden no supere a n. A partir de la observación no es difícil ver que los espacios de Riemann-Roch asociados son espacios vectoriales. Es importante observar que para el caso de que el divisor D tenga grado negativo el espacio $\mathcal{L}(D) = \{0\}$ (en efecto, si $\mathcal{L}(D)$ tuviese alguna función meromorfa no nula f tendríamos que $0 = \deg(div(f)) \geq \deg(-D)$ y por lo tanto $\deg(D) \geq 0$). Un resultado importante es que para cada divisor D, el espacio vectorial $\mathcal{L}(D)$ es de dimensión finita (cuya dimensión lo denotaremos $\ell(D)$) y de hecho verifican el Teorema de Riemann-Roch:

Teorema 1.16 (Riemann-Roch)**.** *Existe un divisor $W \in Div(\mathcal{C})$ y un natural g (llamado* **género** *de la curva) tal que para todo divisor $D \in Div(\mathcal{C})$ se cumple que:*

$$\ell(D) = \deg(D) + \ell(W - D) - g + 1$$

Una prueba de este Teorema puede verse por ejemplo en la página 108 de [**15**].

Nota: En el caso que el divisor D está definido sobre $\mathbb{K}$ entonces puede probarse que $dim(\mathcal{L}_{\mathbb{K}}(D)) = \ell(D)$, es decir, se puede encontrar una base de $\mathcal{L}(D)$ formada por funciones meromorfas en $\mathcal{C}$ definidas sobre $\mathbb{K}$ (ver [**35**] pág.36).

1.1.2. El género de una curva. Observemos que para divisores D tales que $\deg(D) > \deg(W)$ entonces $\deg(W - D) < 0$ y por lo tanto $\ell(W - D) = 0$. Luego en virtud de Riemann-Roch se tiene que $\ell(D) = \deg(D) - g + 1$ para divisores D con grado suficientemente grande (de hecho para $\deg(D) > -(W - D)$) luego el género g está univocamente determinado.

Para el caso particular de curvas planas, cuando el polinomio F que define la curva $\mathcal{C}$ es no singular (su gradiente nunca se anula) puede probarse que $g = \frac{(n-1)(n-2)}{2}$ donde $n = \deg(F)$. Cuando F es singular pero todos sus puntos múltiples son ordinarios (sin tangentes múltiples) entonces el género de la curva puede calcularse por $g = \frac{(n-1)(n-2)}{2} - \sum_{P\in\mathcal{C}} \frac{m_P(m_P-1)}{2}$ donde m_P es la multiplicidad del punto P (ver [**15**] Proposición 5, página 102).

Otra forma de calcular el género es a través de cubrimientos, para ello introduciremos los mapas racionales entre curvas no singulares. Comenzamos recordando los conceptos de singularidad, anillo local y uniformizantes.

Definición 1.17. Si $\mathcal{C}$ es una curva definida por una curva F, un punto singular de la curva es un punto $P \in \mathcal{C}$ que verifica $\nabla F(P) = 0$. Si la curva $\mathcal{C}$ no posee puntos singulares se dice que la curva es no singular o suave.

1.1.3. Anillo local, uniformizante, grado de un mapa racional. Si $\mathcal{C}$ es una curva y $P \in \mathcal{C}$ se define el anillo local de $\mathcal{C}$ en P como el conjunto de funciones $f \in \mathbb{K}(\mathcal{C})$ definidas en P y es denotado por $\mathcal{O}_P(\mathcal{C})$. El anillo local $\mathcal{O}_P(\mathcal{C})$ es efectivamente un anillo local en el sentido que posee un único ideal maximal el cual es denotado por $M_P(\mathcal{C})$, dicho ideal

está formado por las funciones que se anulan en P, las cuales son los elementos no invertibles de $\mathcal{O}_P(\mathcal{C})$ (por detalles ver [**15**] página 21).

Cuando P es un punto no singular de la curva $\mathcal{C}$ el anillo local $\mathcal{O}_P(\mathcal{C})$ resulta ser un anillo de valuación discreta (y por lo tanto $M_P(\mathcal{C})$ es un ideal principal), a un generador de $M_P(\mathcal{C})$ se le llama uniformizante local de $\mathcal{C}$ en P (o simplemente uniformizante). Toda función $f \in \mathcal{O}_P(\mathcal{C})$ se escribe como $f = ut^n$ con $u(P) \neq 0$, t una uniformizante local y $n \in \mathbb{N}$, donde n está unívocamente determinado y se denota por $ord_P(f)$ (por detalles ver [**15**] página 34). Si f tiene un polo en P entonces $1/f \in \mathcal{O}_P(\mathcal{C})$ y se define $ord_P(f) = -ord_P(1/f)$; esta definición coincide con la dada anteriormente usando el índice de intersección (ver [**15**] página 40).

Definición 1.18. Si $\mathcal{C}$ es una curva no singular, un mapa polinomial es una función $\phi = [p_1 : p_2 : p_3] : \mathcal{C} \to \mathbb{P}^2$ donde p_1, p_2 y $p_3 \in \mathbb{K}(\mathcal{C})$, si $P \in \mathcal{C}$ y t es una uniformizante en P entonces definimos $\phi(P) = [t^{-n}p_1(P) : t^{-n}p_2(P) : t^{-n}p_3(P)]$ donde $n = \text{mín}\{ord_P(p_1), ord_P(p_2), ord_P(p_3)\}$, dicho valor no depende de la uniformizante escogida.

Definición 1.19. Un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre dos curvas no singulares[1] $\mathcal{C}_1$ y $\mathcal{C}_2$, es un mapa polinomial que verifica que $\phi(P) \in \mathcal{C}_2$ para todo $P \in \mathcal{C}_1$.

Una remarcable propiedad de dichos mapas es que o bien son constantes o sobreyectivos. En el caso que el mapa $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ sea sobreyectivo este induce un morfismo no nulo $\phi^* : \mathbb{K}(C_2) \to \mathbb{K}(C_1)$ entre los cuerpos de funciones, dado por $\phi^*(f) = f \circ \phi$ y por ende una extensión de cuerpos $\phi^*\mathbb{K}(C_2) \subset \mathbb{K}(C_1)$.

Definición 1.20. El grado de un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre dos curvas no singulares se define como $\deg(\phi) = [\phi^*\mathbb{K}(\mathcal{C}_2) : \mathbb{K}(\mathcal{C}_1)]$ (observemos que esta extensión es finita por ser ambos cuerpos finitamente generados y tener grado de trascendencia 1 sobre $\mathbb{K}$).

Considerando la clausura separable de $\phi^*\mathbb{K}(\mathcal{C}_2)$ en $\mathbb{K}(\mathcal{C}_1)$, que denotaremos por $\phi^*\mathbb{K}(\mathcal{C}_2)^{sep}$ podemos factorizar nuestra extensión como una parte separable $\phi^*\mathbb{K}(\mathcal{C}_2) \subset \phi^*\mathbb{K}(\mathcal{C}_2)^{sep}$ y una parte puramente inseparable $\phi^*\mathbb{K}(\mathcal{C}_2)^{sep} \subset \mathbb{K}(\mathcal{C}_1)$.

Definición 1.21. El grado de separabilidad de un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre dos curvas no singulares se define como $\deg_s(\phi) = [\phi^*\mathbb{K}(\mathcal{C}_2)^{sep} : \phi^*\mathbb{K}(\mathcal{C}_2)]$ y el grado de inseparabilidad como $deg_i(\phi) = [\mathbb{K}(\mathcal{C}_1) : \phi^*\mathbb{K}(\mathcal{C}_2)^{sep}]$.

Observemos que $\deg(\phi) = \deg_s(\phi)\deg_i(\phi)$ y que en el caso de característica 0 no hay inseparabilidad y por lo tanto $\deg_i(\phi) = 1$ mientras que en el caso de característica $p > 0$ se tiene que $\deg_i(\phi) = p^k$ para algún $k \in \mathbb{N}$ (Corolario A.5 del Apéndice).

[1]Para curvas con puntos singulares también se definen los mapas racionales, pero estos pueden no estar definidos en todos los puntos, en estos casos la condición que hay que pedirle es que $\phi(P) \in \mathcal{C}_2$ para todo $P \in \mathcal{C}_1$ en donde ϕ está definida.

Definición 1.22. Un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre curvas no singulares se dice que es separable si $\deg_i(\phi) = 1$ y puramente inseparable cuando $\deg_s(\phi) = 1$ (o sea, cuando la extensión de cuerpos que genera es separable o puramente inseparable respectivamente).

Más adelante, cuando hablemos de isogenias, veremos más geométricamente que significado tienen los grados de separabilidad e inseparabilidad. Por último la noción de isomorfismo.

Definición 1.23 (Isomorfismo)**.** Un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre curvas no singulares se dice que es un isomorfismo si es biyectivo y su inversa $\phi^{-1} : \mathcal{C}_2 \to \mathcal{C}_1$ es un mapa racional. Si existe un isomorfismo entre dos curvas se dice que las curvas son isomorfas.

Un isomorfismo entre dos curvas no singulares siempre induce un isomorfismo entre los cuerpos de funciones correspondientes. El hecho de que un mapa racional sea biyectivo no asegura que su inversa lo sea (un ejemplo es el morfismo de Frobenius que veremos más adelante). No obstante, lo que si vale es que todo mapa de grado 1 entre curvas no singulares resulta ser un isomorfismo, lo cual puede verse como consecuencia de un isomorfismo de categorías que hablaremos a continuación (Cor 2.4.1 [**35**]).

1.1.4. Isomorfismo categórico. Comenzemos recordando la definición más general de curvas.

Definición 1.24 (Curvas en general)**.** Una hipersuperficie (proyectiva) $\mathcal{H}$ es el conjunto de ceros en $\mathbb{P}^n = \mathbb{P}^n(\overline{\mathbb{K}})$ de un polinomio homogéneo irreducible $F \in \overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]$. Un conjunto algebraico (proyectivo) es una intersección finita de hipersuperficies. Un conjunto algebraico $\mathcal{V}$ es una variedad algebraica si no es unión de dos conjuntos algebraicos propios no vacios (equivalentemente si el ideal de $\overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]$ formados por aquellos polinomios que se anulan en el conjunto algebraico es un ideal primo). Si $\mathcal{V}$ es una variedad algebraica se definen, el anillo de polinomios sobre $\mathcal{V}$ como $\Gamma(\mathcal{V}) = \overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]/I(\mathcal{V})$, el cuerpo de funciones meromorfas en $\mathcal{V}$ como $\overline{\mathbb{K}}(\mathcal{V}) = \left\{\frac{g}{h} : g, h \text{ formas } \overline{\mathbb{K}}-\text{racionales del mismo grado en } \Gamma(\mathcal{C}), h \neq 0\right\}$ y la dimensión de la variedad algebraica $\mathcal{V}$ como el grado de trascendencia de la extensión $\overline{\mathbb{K}} \subset \overline{\mathbb{K}}(\mathcal{V})$. Una curva es una variedad algebraica de dimensión 1 (esta definición coincide con la dada para curvas planas en el caso en que $n = 2$).

Todos los conceptos vistos antes para curvas planas se generalizan para curvas algebraicas en general.

La extensión de cuerpos inducida por un mapa entre curvas no singulares (no necesariamente planas) establece un isomorfimo de categorías (ver el libro de Silverman [**35**], Teo. 2.4 por más detalles y referencias) entre la categoría que tiene como objetos curvas no singulares definidos sobre $\mathbb{K}$ y como flechas mapas racionales no constantes definidos sobre $\mathbb{K}$ y la categoría cuyos objetos son extensiones de cuerpo $\mathbb{L}|\mathbb{K}$ de grado de trascendencia 1 tales que $\mathbb{L} \cap \overline{\mathbb{K}} = \mathbb{K}$ y cuyas flechas son los $\mathbb{K}$-morfismos. De ese modo el cuerpo $\phi^*(\mathbb{K}(\mathcal{C}_2))^{sep}$ resulta ser un cuerpo de funciones $\mathbb{K}(\mathcal{C})$ para alguna curva no singular $\mathcal{C}$ y el isomorfismo anterior nos brinda una factorización de ϕ:

$$\begin{array}{ccc} \mathbb{K}(\mathcal{C}_1) & & \mathcal{C}_1 \\ \uparrow{\scriptstyle p.i} & & \downarrow{\scriptstyle \phi_1} \\ \mathbb{K}(\mathcal{C}_2)^{sep} = \mathbb{K}(\mathcal{C}) & \rightsquigarrow & \mathcal{C} \\ \uparrow{\scriptstyle sep} & & \downarrow{\scriptstyle \phi_2} \\ \mathbb{K}(\mathcal{C}_2) & & \mathcal{C}_2 \end{array}$$

de donde todo mapa ϕ factoriza como $\phi = \phi_2 \circ \phi_1$ donde ϕ_2 es separable y ϕ_1 puramente inseparable. Sacaremos más provecho de este isomorfismo cuando veamos los teoremas de factorización para isogenias en la sección siguiente.

1.1.5. Ramificación. Consideremos un mapa $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre curvas no singulares, P un punto de la curva $\mathcal{C}_1$ y $t_{\phi(P)}$ una uniformizante en $\phi(P)$ para la curva $\mathcal{C}_2$. Observemos que $\phi^* t_{\phi(P)}(P) = t_{\phi(P)}(\phi(P)) = 0$ por definición de uniformizante, lo cual implica que $\phi^* t_{\phi(P)} \in M_P(\mathcal{C}_1)$ pero no necesariamente va a ser una uniformizante en P, cuando esto sucede decimos que ϕ es no ramificado en P. Definimos ramificación:

Definición 1.25. Con las notaciones de antes, se define el índice de ramificación de ϕ en P como $e_\phi(P) = ord_P(\phi^* t_{\phi(P)})$. Decimos que el mapa ϕ es no ramificado cuando $e_\phi(P) = 1$ para todo $P \in \mathcal{C}_1$ (o sea, cuando no hay ramificación).

Geométricamente el grado representa la cantidad de preimágenes de un punto si contamos cada preimagen tantas veces como lo indica su ramificación (ver [**35**] Prop.2.6, página 28).

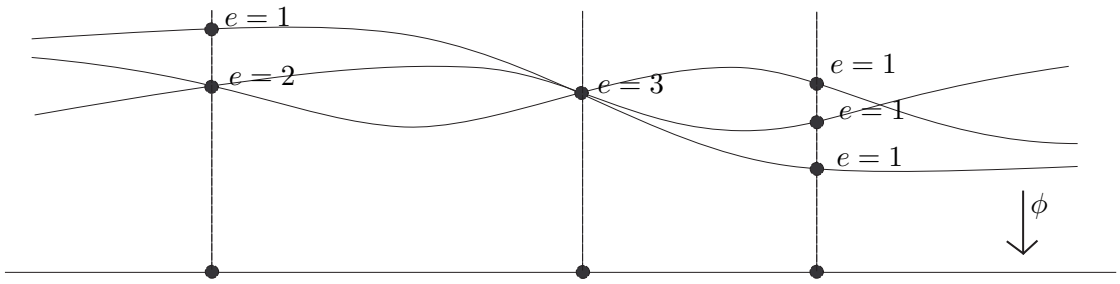


FIGURA 1. Cubrimiento (o mapa) ramificado de grado 3

1.1.6. Fórmula de Hurwitz. Una interesante conexión entre mapas racionales entre dos curvas no singulares y sus géneros viene dado por la famosa fórmula de Hurwitz.

Teorema 1.26 (Fórmula de Hurwitz)**.** *Si $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ es un mapa racional separable y no constante, entre dos curvas no singulares de géneros g_1 y g_2 respectivamente se cumple que:*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in \mathcal{C}_1} (e_\phi(P) - 1)$$

con igualdad si y solo si la característica del cuerpo es 0 o la característica es $p > 0$ y p no divide a ningún $e_\phi(P)$ (ver [**35**] *Teorema 5.9, página 41).*

Vamos ahora a concentrarnos de aquí en más en el caso que nos interesa que son las curvas de género 1.

1.2. Curvas Elípticas.

Definición 1.27. Una curva elíptica definida sobre $\mathbb{K}$ es una pareja $(\mathcal{C}, \mathcal{O})$ donde $\mathcal{C}$ es una curva no singular $\mathbb{K}-$racional de género 1 y $\mathcal{O}$ un punto $\mathbb{K}-$racional de la curva $\mathcal{C}$.

Por ejemplo si $\mathcal{C}$ es una curva plana definida por un polinomio homogéneo no singular $F(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$ (o sea por los ceros de $F^*(X,Y,Z) = Z^3F(\frac{X}{Z}, \frac{Y}{Z})$ en $\mathbb{P}^2$) de tercer grado entonces, por la observación hecha al principio de *1.1.2*, su género será $(3-1)(3-2)/2 = 1$ y tomando por ejemplo el punto $\mathcal{O} = [0:1:0] \in \mathcal{C}$ resulta que $(\mathcal{C}, \mathcal{O})$ es una curva elíptica. De hecho toda curva elíptica es isomorfa a una de esa forma, como observaremos más adelante, recordando porque.

Observación 1.28. Nos resultará útil observar que si la curva elíptica $(\mathcal{C}, \mathcal{O})$ está definida por un polinomio cúbico no singular F como mencionamos arriba entonces las funciones coordenadas $x = X/Z$ e $y = Y/Z$ tienen un polo de orden 2 y 3 en $\mathcal{O} = [0:1:0]$ respectivamente y ningún otro polo.)

Demostración: Observemos que los posibles polos de x e y solo pueden darse en los ceros de Z, pero el sistema:

$$\begin{cases} Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0 \\ Z = 0 \end{cases}$$

tiene como solución $Z = X = 0$ y por lo tanto el único cero de Z es $[0:1:0] = \mathcal{O}$.

Calculamos ahora los respectivos índices de intersección de X, Y y Z con $\mathcal{C}$ en el punto $\mathcal{O}$:

$I(\mathcal{O}, X \cap F) = I((0,0), X \cap Z + a_1XZ + a_3Z^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3) = 1$

$I(\mathcal{O}, Y \cap F) = 0 \quad$ pues $\mathcal{O} \notin Y$

$I(\mathcal{O}, Z \cap F) = I((0,0), Z \cap Z + a_1XZ + a_3Z^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3) = I((0,0), Z \cap -X^3) = 3$

Finalmente podemos calcular los órdenes que queríamos:

$ord_{\mathcal{O}}(x) = I(\mathcal{O}, X \cap F) - I(\mathcal{O}, Z \cap F) = -2$

$ord_{\mathcal{O}}(y) = I(\mathcal{O}, Y \cap F) - I(\mathcal{O}, Z \cap F) = -3$

□

Corolario 1.29. *Se verifica que* $\{1, x\}$ *es base de* $\mathcal{L}(2\mathcal{O})$ *y que* $\{1, x, y\}$ *es base de* $\mathcal{L}(3\mathcal{O})$.

Demostración: Consecuencia directa de la proposición anterior y el Teorema de Riemann-Roch.

Para el caso especial de curvas de género 1 el teorema de Riemann-Roch nos dice que $\ell(D) - \ell(W - D) = \deg(D)$ donde el divisor W tiene grado $2g - 2 = 0$ (Corolario de la Proposición 8 de [**15**] página 107). Por lo tanto si $\deg(D) \geq 1$ tenemos que $\deg(W - D) = \deg(W) - \deg(D) \leq -1 < 0$ y por lo tanto $\ell(W - D) = 0$ así que se da la

igualdad $\ell(D) = \deg(D)$ siempre que $\deg(D) > 0$.

Teorema 1.30 (Forma Normal de Weierstrass.)**.** *Si $E/\mathbb{K}$ es una curva elíptica con punto distinguido $\mathcal{O} \in E(\mathbb{K})$ entonces existen $f, g \in \mathbb{K}(E)$ tal que el mapa $\phi : E \to \mathbb{P}^2$ dado por $\phi = [f : g : 1]$ define un isomorfismo de $E/\mathbb{K}$ en una cúbica no singular $\mathcal{C} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ con $a_1, a_3, a_2, a_4, a_6 \in \mathbb{K}$ cumpliendo además que $\phi(\mathcal{O}) = [0 : 1 : 0]$.*

Demostración: Como $\ell(\mathcal{O}) = \deg(\mathcal{O}) = 1 \Rightarrow$ el espacio de Riemann-Roch asociado al divisor $\mathcal{O}$ está formado por las constantes, luego no hay funciones con un único polo simple en $\mathcal{O}$.

Como $\ell(2\mathcal{O}) = \deg(2\mathcal{O}) = 2 \Rightarrow$ existe una base $\{1, f\} \to_b \mathcal{L}(2\mathcal{O})$ donde podemos elegir $f \in \mathbb{K}(E)$ dado que el divisor $2\mathcal{O}$ es $\mathbb{K}-$racional.

Como $\ell(3\mathcal{O}) = \deg(3\mathcal{O}) = 3 \Rightarrow \exists$ una base $\{1, f, g\} \to_b \mathcal{L}(3\mathcal{O})$ con $g \in \mathcal{L}(3\mathcal{O}) \setminus \mathcal{L}(2\mathcal{O})$ luego g tiene un único polo triple en $\mathcal{O}$ (puedo elegir $g \in \mathbb{K}(E)$ puesto que el divisor $3\mathcal{O}$ está definido sobre $\mathbb{K}$).

Como $\ell(6\mathcal{O}) = \deg(6\mathcal{O}) = 6$ y $A = \{1, f, g, f^2, fg, f^3, g^2\} \subset \mathcal{L}(6\mathcal{O})$ debe ser un conjunto linealmente dependiente sobre $\overline{K}$. Al ser $6\mathcal{O}$ un divisor $\mathbb{K}-$racional y el conjunto A estar formado por funciones $\mathbb{K}-$racionales, se puede probar de hecho que el conjunto A resulta ser también un conjunto linealmente dependiente sobre $\mathbb{K}$ (Siverman [**35**],Lema 5.8.1.). Luego existen $A_1, A_2, \ldots, A_7 \in \mathbb{K}$ no todos nulos tales que:

$$A_1 + A_2f + A_3g + A_4f^2 + A_5fg + A_6f^3 + A_7g^2 = 0$$

Observemos que $A_6A_7 \neq 0$ pues si uno de ellos fuese nulo, la ecuación de arriba nos queda una combinación lineal nula de funciones con polos de distinto orden en $\mathcal{O}$ y por lo tanto el resto de los coeficientes también serían nulos contradiciendo nuestra suposición. Cambiando las funciones f y g por $-A_6A_7f$ y $A_6^2A_7g$ respectivamente (lo cual no afecta el orden de ceros y polos, ni tampoco la $\mathbb{K}-$racionalidad) nos queda:

$$A_1 - A_2A_6A_7f + A_3A_6^2A_7g + A_4A_6^2A_7^2f^2 - A_5A_6^3A_7^2fg - A_6^4A_7^3f^3 + A_7^3A_6^4g^2 = 0$$

dividiendo entre $A_6^4A_7^3$ de ambos lados y despejando términos nos queda una ecuación de dependencia lineal de la forma:

$$g^2 + a_1fg + a_3g = f^3 + a_2f^2 + a_4f + a_6$$

con $a_1, a_3, a_2, a_4, a_6 \in \mathbb{K}$.

Luego el mapa $\phi = [f : g : 1] : E \to \mathbb{P}^2$ define un morfismo de curvas algebraicas entre E y la cúbica $\mathcal{C} : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. Si t es una uniformizante local de E en $\mathcal{O}$ tenemos que $\phi(\mathcal{O}) = [t^3f(\mathcal{O}) : t^3g(\mathcal{O}) : t^3(\mathcal{O})] = [0 : 1 : 0]$ puesto que f tiene un polo de orden 2 en $\mathcal{O}$ y g un polo de orden 3.

Para probar que este mapa ϕ es un isomorfismo observemos primero que $\deg(\phi) = 1$, en efecto, considerando el mapa $\alpha : [x : 1] : E \to \mathbb{P}^1$ ($\mathbb{P}^1$ visto como curva plana de ecuación $Z = 0$) resulta $\alpha^{-1}([0 : 1]) = \{\mathcal{O}\}$ (por ser el único polo) y $e_\alpha(\mathcal{O}) = 2$ (pues coincide con el orden de $\mathcal{O}$ como polo de x) así que $\deg(\alpha) = \sum_{P \in \alpha^{-1}(Q)} e_\alpha(P) = e_\alpha(\mathcal{O}) = 2$ (tomando $Q = [0 : 1] \in \mathbb{P}^1$ en la fórmula de Hurwitz) y como $\alpha^*(\mathbb{K}(\mathbb{P}^1)) = \alpha^*(\mathbb{K}(X)) = \mathbb{K}(x)$

resulta que $[\mathbb{K}(E) : \mathbb{K}(x)] = 2$. De forma análoga resulta que $[\mathbb{K}(E) : \mathbb{K}(y)] = 3$, de donde $[\mathbb{K}(E) : \mathbb{K}(x, y)] = 1$ por dividir a ambos índices y como $\phi^*(\mathbb{K}(\mathcal{C})) = \mathbb{K}(x, y)$ resulta que $\deg(\phi) = 1$.

Si la cúbica $\mathcal{C}$ fuese no singular sería posible construir un isomorfismo $\psi : \mathcal{C} \to \mathbb{P}^1$ (Proposición 1.6 página 53 de [**35**]), usando que el grado de la composición es el producto de los grados tendríamos el mapa $\psi \circ \phi : E \to \mathbb{P}^1$ que es un mapa de grado 1 entre curvas no singulares y por lo tanto un isomorfismo lo cual se contradice con que $\mathbb{P}^1$ tiene género 0.

□

Forma corta o reducida. Vimos que cuando la curva elíptica está definida sobre $\mathbb{K}$ siempre es posible encontrar un isomorfismo a una curva elíptica $(\mathcal{C}, [0 : 1 : 0])$ dada por una ecuación de Weiestrass con coeficientes en $\mathbb{K}$. Para el caso que $car(\mathbb{K}) \neq 2, 3$ se puede construir además, un isomorfismo (de hecho un cambio lineal de coordenadas) entre una curva elíptica $(\mathcal{C}, [0 : 1 : 0])$ dada por una ecuación de Weierstrass a una curva elíptica $(\mathcal{C}', [0 : 1 : 0])$ donde $\mathcal{C}'$ está dada por una ecuación de la forma $\mathcal{C}' : Y^2 = X^3 + aX + b$ con $a, b \in \mathbb{K}$ ([**32**], Cap.1.3.3.) que llamaremos ecuación reducida de la curva. Para una curva escrita en forma reducida, la no singularidad es equivalente a que $\Delta = -16(4a^3+27b^2) \neq 0$.

De ahora en más, cuando necesitemos probar resultados manipulando las fórmulas explícitas, vamos a enunciar el resultado general pero veremos las pruebas para el caso de característica distinta de 2 y 3 usando las ecuaciones cortas.

1.2.1. El j-invariante e isomorfismos. Una importante cantidad asociada a una curva elíptica viene dada por el j-invariante:

Definición 1.31. Sea $(E, \mathcal{O})$ una curva elíptica y $\mathcal{C} : Y^2 = X^3 + aX + b$ una forma corta para la curva elíptica E. Definimos el $j-$invariante de E como:

$$j(E) = 4 \cdot \frac{1728a^3}{4a^3 + 27b^2} = \begin{cases} \frac{6912}{4+27(\frac{b^2}{a^3})} & \text{si } a \neq 0 \\ 0 & \text{si } a = 0 \end{cases}$$

Veamos que no depende de la ecuación reducida escogida (la cual no es única), más aún, veremos que solo depende de la clase de isomorfimo de E. Comenzemos observando que si $\mathcal{C}_1 : Y^2 = X^3 + a_1X + b_1$ es una forma corta para una curva elíptica E_1 y $\mathcal{C}_2 : Y^2 = X^3 + a_2X + b_2$ es una forma corta para E_2 donde E_1 y E_2 son isomorfas, entonces dicho isomorfismo induce un isomorfismo entre $\mathcal{C}_1$ y $\mathcal{C}_2$, por lo tanto el hecho que el j-invariante solo depende de la clase de isomorfismo (y en particular no depende de la forma corta escogida) se desprende del siguiente resultado.

Teorema 1.32. *Si $\mathcal{C}_1 : Y^2 = X^3 + a_1X + b_1$ y $\mathcal{C}_2 : Y^2 = X^3 + a_2X + b_2$ son dos curvas elípticas isomorfas y $\phi = [f : g : 1] : \mathcal{C}_1 \to \mathcal{C}_2$ un isomorfismo entonces existe $u \in \overline{K}$ tal que:*

$$\begin{cases} f = u^2x \\ g = u^3y \end{cases}$$

y en ese caso se cumple la siguiente relación entre los coeficientes de $\mathcal{C}_1$ y $\mathcal{C}_2$:

$$\begin{cases} a_2 = u^4a_1 \\ b_2 = u^6b_1 \end{cases}$$

Corolario 1.33. *Si $\mathcal{C}_1$ y $\mathcal{C}_2$ son dos curvas elípticas escritas en forma reducida entonces $j(\mathcal{C}_1) = j(\mathcal{C}_2)$.*

Demostración del Corolario: Con las notaciones del teorema, el hecho de que $\mathcal{C}_1$ y $\mathcal{C}_2$ sean isomorfas implica que o bien $a_1 = a_2 = 0$ (puesto que $u \neq 0$) o bien $b_1^2/a_1^3 = (u^3b_2)^2/(u^2a_2)^3 = b_2^2/a_2^3$ lo cual implica la igualdad de sus j-invariante.

Demostración del Teorema: El isomorfismo de curvas $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ induce un isomorfismo entre el cuerpo de funciones $\phi^* : \mathbb{K}(\mathcal{C}_2) \to \mathbb{K}(\mathcal{C}_1)$. Si llamamos x_2 e y_2 a las funciones coordenadas de $\mathcal{C}_2$ tenemos que $\phi^*(x_2) = x_2(\phi) = f \in \mathbb{K}(\mathcal{C}_1)$ y $\phi^*(y_2) = y_2(\phi) = g \in \mathbb{K}(\mathcal{C}_1)$ por lo tanto f y g tienen en $\phi^{-1}(\mathcal{O}) = \mathcal{O}$ polos de orden 2 y 3 respectivamente y ningún otro polo (si P fuese otro polo de f ó g entonces $\phi(P)$ sería otro polo de x_2 ó y_2, pero el único polo de x_2 e y_2 es $\mathcal{O}$) así que $f \in \mathcal{L}(2\mathcal{O})$ y $g \in \mathcal{L}(3\mathcal{O})$.

Llamando x e y las funciones coordenadas de $\mathcal{C}_1$, en virtud del Corolario 1.29 tenemos que:

$$\begin{cases} f = ax + b \quad \text{con } a \neq 0 \\ g = my + nx + s \quad \text{con } m \neq 0 \end{cases} \tag{1}$$

donde $a, b, m, n, s \in \mathbb{K}$.

Como $\phi(\mathcal{C}_1) = \mathcal{C}_2$ entonces las funciones $f, g \in \mathbb{K}(\mathcal{C}_1)$ deben verificar $g^2 = f^3 + a_2 f + b_2$ sustituyendo f y g de las ecuaciones (1) y agrupando términos nos queda:

$$my^2 = a^3x^3 - 2mnxy + (3a^2b - n^2)x^2 - 2msy + (3ab^2 + a_2a - 2ns)x + (b^3 + a_2b + b_2 - s^2)$$

Por otra parte, por la ecuación que define $\mathcal{C}_1$ debe cumplirse que $m^2y^2 = m^2x^3 + a_1m^2x + b_1m^2$ y como el conjunto $\{1, x, y, x^2, xy, x^3\}$ es linealmente independiente (por tener polos de distinto orden en $\mathcal{O}$) debe cumplirse el sistema:

$$\begin{cases} \boxed{m^2 = a^3} \\ -2mn = 0 \Rightarrow \boxed{n = 0} \text{ pues } m \neq 0 \\ 3a^2b - n^2 = 0 \Rightarrow \boxed{b = 0} \text{ pues } n = 0 \text{ y } a \neq 0 \\ -2ms = 0 \Rightarrow \boxed{s = 0} \text{ pues } m \neq 0 \\ 3ab^2 + a_2a - 2ns = a_1m^2 \Rightarrow \boxed{a_2a = a_1m^2} \text{ pues } b = n = 0 \\ b^3 + a_2b + b_2 - s^2 = b_1m^2 \Rightarrow \boxed{b_2 = b_1m^2} \text{ pues } b = s = 0 \end{cases}$$

De la primer ecuación, como 2 y 3 son coprimos existe $u \in \overline{K}$ tal que $m = u^3$ y $a = u^2$ con $u \neq 0$ (pues $am \neq 0$) sustituyendo en las dos últimas ecuaciones nos queda:

$$a_2u^2 = a_1u^6 \Rightarrow \boxed{a_2 = a_1u^4}$$
$$b_2 = b_1u^6 \Rightarrow \boxed{b_2 = b_1u^6}$$

que nos da la relación entre los coeficientes de ambas curvas.

Sustituyendo los valores de $m = u^3, a = u^2, b = n = s = 0$ en la ecuación (1) nos queda que:

$$\begin{cases} f = u^2x \\ g = u^3y \end{cases}$$

como queríamos probar.

□

Como observamos, el teorema anterior mostraba que el j-invariante solo depende de la clase de isomorfismo, veamos de hecho que es un clasificador de las clases de isomorfismo (sobre $\overline{\mathbb{K}}$) de una curva elíptica.

Teorema 1.34. *Dos curvas elípticas son isomorfas (sobre $\overline{\mathbb{K}}$) si y solo si poseen el mismo j-invariante.*

Demostración: Ya vimos que el j-invariante solo dependia de la clase de isomorfismo, consideremos ahora dos curvas elípticas E y E' con $j(E_1) = j(E_2)$, sean $\mathcal{C} : Y^2 = X^3 + aX + b$ y $\mathcal{C}' : Y^2 = X^3 + a'X + b'$ formas reducidas para E y E' respectivamente (para $car(\mathbb{K}) = 2$ o 3 trabajamos con la ecuación de Weiestrass completa y el resultado puede verificarse en forma parecida, supondremos para esta prueba que $car(\mathbb{K}) \neq 2, 3$), por lo tanto $E \simeq \mathcal{C}$ y $E' \simeq \mathcal{C}'$.

Observemos primero que $a = 0 \Leftrightarrow j(E) = 0 \Leftrightarrow j(E') = 0 \Leftrightarrow a' = 0$ y en este caso ambos b y b' deben ser no nulos por la no singularidad, tomando cualquier $u \in \overline{\mathbb{K}}$ tal que $u^6 = \frac{b}{b'}$ nos queda que $\mathcal{C} : Y^2 = X^3 + u^6 b'$ dividiendo ambos lados por u^6 nos queda la ecuación para $\mathcal{C} : (u^{-3}Y)^2 = (u^{-2}X)^3 + b'$ así que $\mathcal{C} \simeq \mathcal{C}'$ (con isomorfismo $\phi(x, y) = (u^{-2}x, u^{-3}y)$) lo cual implica $E \simeq E'$.

Para el caso $b = 0$ tenemos que $b = 0 \Leftrightarrow j(E) = 1728 \Leftrightarrow j(E') = 1728 \Leftrightarrow b' = 0$ y $aa' \neq 0$ por la no singularidad, en este caso tomando cualquier $u \in \overline{\mathbb{K}}$ tal que $u^4 = \frac{a}{a'}$ nos queda que $\mathcal{C} : Y^2 = X^3 + u^4 a' X$ dividiendo ambos lados por u^6 nos queda la ecuación para $\mathcal{C} : (u^{-3}Y)^2 = (u^{-2}X)^3 + a'(u^{-2}X)$ así que $\mathcal{C} \simeq \mathcal{C}'$ (con isomorfismo $\phi(x, y) = (u^{-2}x, u^{-3}y)$) lo cual implica $E \simeq E'$.

Y por último, si $ab \neq 0$ (que implica $a' \neq 0$ por la primera observación) podemos considerar la función $f : \overline{\mathbb{K}} - \{-4/27\} \to \overline{\mathbb{K}}$ dada por $f(x) = \frac{6912}{4+27x}$ que es inyectiva (recordar que estamos en el caso $car(\mathbb{K}) \neq 2, 3$) y dado que b^2/a^3 y b'^2/a'^3 son distintos de $-4/27$ (puesto que $\Delta(\mathcal{C})$ y $\Delta(\mathcal{C}')$ son distintos de cero) tenemos que:

$$f\left(\frac{b^2}{a^3}\right) = j(E_1) = j(E_2) = f\left(\frac{b'^2}{a'^3}\right) \Rightarrow \frac{b^2}{a^3} = \frac{b'^2}{a'^3}$$

De la última igualdad, dado que $b \neq 0$, resulta que $\left(\frac{a}{a'}\right)^3 = \left(\frac{b}{b'}\right)^2$ y al ser 2 y 3 coprimos entonces existe (y es único) $v \in \overline{\mathbb{K}}$ tal que $\frac{a}{a'} = v^2$ y $\frac{b}{b'} = v^3$. Tomando cualquier $u \in \overline{\mathbb{K}}$ tal que $u^2 = v$ nos queda que $\mathcal{C} : Y^2 = X^3 + u^4 a' + u^6 b'$ dividiendo ambos lados por u^6 nos queda la ecuación para $\mathcal{C} : (u^{-3}Y)^2 = (u^{-2}X)^3 + a'(u^{-2}X) + b'$ así que $\mathcal{C} \simeq \mathcal{C}'$ (con isomorfismo $\phi(x, y) = (u^{-2}x, u^{-3}y)$) lo cual implica que $E \simeq E'$ culminando así la prueba.

□

Observación 1.35. El Teorema anterior puede expresarse como:

$j : \left\{E/\overline{\mathbb{K}} \text{ curva elíptica (mód } \overline{\mathbb{K}} - \text{isomorfismo)}\right\} \longrightarrow \overline{\mathbb{K}}$ está bien definida y es inyectiva

Veamos de hecho que es sobreyectivo, y más aún, veremos que toda curva elíptica está definida sobre la extensión generada por su j-invariante.

Teorema 1.36. *Sea $\mathbb{K}$ un cuerpo de característica distinta de 2 y 3 (el teorema vale en general pero hay que modificar brevemente la prueba [ver por ejemplo* [**35**] *Prop.1.4 c, pág.50])*

1. *Para cada $j \in \overline{\mathbb{K}}$ existe una curva elíptica $\mathcal{C}/\overline{\mathbb{K}}$ con $j(\mathcal{C}) = j$.*
2. *Dada una curva elíptica $E/\overline{\mathbb{K}}$ con j-invariante igual a j, existe una curva elíptica $\mathcal{C}$ en forma reducida con coeficientes en $\mathbb{K}(j)$ isomorfa a E (i.e. toda curva elíptica E está definida, salvo isomorfismo, sobre $\mathbb{K}(j(E))$).*

Demostración: Para la primer parte basta exibir para cada $j \in \overline{\mathbb{K}}$ una curva elíptica $\mathcal{C}_j$ con j-invariante igual a j:

Para $j = 0$ definimos $\mathcal{C}_j : Y^2 = X^3 + 1$ es no singular pues $\Delta = -2^4\, 3^3 \neq 0$.

Para $j = 1728$ definimos $\mathcal{C}_j : Y^2 = X^3 + X$ es no singular pues $\Delta = -2^6 \neq 0$.

Para $j \neq 0, 1728$ busquemos una curva de la forma $\mathcal{C}_j : Y^2 = X^3 + aX + a$ donde a debe verificar:

$$\frac{6912}{4 + \frac{27}{a}} = j \Rightarrow a = \frac{27j}{4(1728 - j)}$$

Tomando ese valor de a su discriminante queda $\Delta = -16a^2(4a + 27)$, como $j \neq 0$ y $car(\mathbb{K}) \neq 3$ tenemos que $a \neq 0$, por otra parte tenemos que:

$$4a + 27 = \frac{27j}{1728 - j} + 1 = \frac{2^6 3^6}{1728 - j} \neq 0 \quad \text{puesto que } car(\mathbb{K}) \neq 2, 3$$

por lo tanto $\Delta \neq 0$ y por lo tanto $\mathcal{C}_j$ es una curva elíptica con j-invariante j.

Para la segunda parte del Teorema basta observar que si E es una curva elíptica con $j(E) = j$ entonces $E \simeq \mathcal{C}_j$ por tener el mismo j-invariante y claramente $\mathcal{C}_j$ está en forma reducida y tiene sus coeficientes en $\mathbb{K}(j)$.

□

Observación 1.37. Dado que E está definida sobre $\mathbb{K}$ (salvo $\overline{\mathbb{K}}$-isomorfismos) si y solo si $j(E) \in \mathbb{K}$, tenemos una correspondencia biunívoca dada por el mapa:

$$j : \left\{E/\mathbb{K} \text{ curva elíptica (mód } \overline{\mathbb{K}} - \text{isomorfismo})\right\} \longrightarrow \mathbb{K}$$

Observemos que dos curvas $\mathbb{K}$-racionales pueden ser $\overline{\mathbb{K}}$-isomorfas pero no $\mathbb{K}$-isomorfas, esto ocurre cuando los isomorfismos que llevan una a la otra no están definidos sobre $\mathbb{K}$, esto nos lleva al concepto de twist.

1.2.2. Twist de Curvas Elípticas.

Definición 1.38. Sean $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$ curvas elípticas decimos que son twist una de la otra si son $\overline{\mathbb{K}}$-isomorfas pero no son $\mathbb{K}$-isomorfas.

Mientras que el j-invariante distingue clases de isomorfismos sobre $\overline{\mathbb{K}}$ pueden haber varias curvas que no son $\mathbb{K}$-isomorfas con el mismo j-invariante como veremos a continuación.

Teorema 1.39. *Sea $\mathcal{C} : Y^2 = X^3 + aX + b$ una curva elíptica con $a, b \in \mathbb{K}$ y con $j(\mathcal{C}) \notin \{0, 1728\}$. Sea $v \in \mathbb{K}^* \setminus \mathbb{K}^{*2}$ entonces la curva*

$$\mathcal{C}_v : vY^2 = X^3 + aX + b$$

es una curva elíptica twist de la curva $\mathcal{C}$ (a tales twist los llamaremos twist cuadráticos). Además estos son los únicos twists de la curva $\mathcal{C}$ salvo $\mathbb{K}$-isomorfismos y dos de tales twists $\mathcal{C}_{v_1}$ y $\mathcal{C}_{v_2}$ son $\mathbb{K}$-isomorfos si y solo si $v_1 \equiv v_2 \pmod{\mathbb{K}^{*2}}$.

Demostración: Recordemos que si $\mathcal{C} : Y^2 = X^3 + aX + b$ y $\mathcal{C}' : Y^2 = X^3 + a'X + b'$ son dos curvas elípticas isomorfas con j-invariante distinto de 0 y 1728 entonces el isomorfismo entre ellas viene dado por $\phi(x, y) = (u^2x, u^3y)$ donde $u \in \overline{\mathbb{K}}$ verifica $u^4 = \frac{a'}{a}$ y $u^6 = \frac{b'}{b}$, de donde se deduce que $u^2 = \frac{u^6}{u^4} = \frac{ab'}{a'b} \in \mathbb{K}^*$ (recordar que el j-invariante distinto de 0 y 1728 implica que los coeficientes de la curva sean no nulos). Dadas las dos curvas $\mathcal{C}$ y $\mathcal{C}'$ los únicos dos posibles valores de u son opuestos en signo por lo tanto ambos isomorfismos entre $\mathcal{C}$ y $\mathcal{C}'$ están definidos sobre $\mathbb{K}$ o ninguno de los dos lo están, así que para que $\mathcal{C}'$ sea twist de $\mathcal{C}$ esta última debe ser de la forma $\mathcal{C}' : Y^2 = X^3 + \alpha^2 aX + \alpha^3 b$ donde $\alpha = u^2 \in \mathbb{K}$ no debe ser un cuadrado en $\mathbb{K}$ (o lo que es lo mismo, $u \notin \mathbb{K}$).

En resumen, todas las curvas twist de $\mathcal{C}$ deben ser de la forma $\mathcal{C}_\alpha : Y^2 = X^3 + a\alpha^2 X + b\alpha^3$ donde $\alpha \in \mathbb{K}$ no es un cuadrado, en tal caso solo hay dos isomorfismos entre ambas curvas y ambos están definidos en una extensión cuadrática de $\mathbb{K}$ (que es $\mathbb{K}(\sqrt{\alpha})$). Observemos además que $\mathcal{C}_\alpha$ es $\mathbb{K}$-isomorfa a la curva de ecuación $(\alpha^2 Y)^2 = (\alpha X)^3 + a\alpha^2(\alpha X) + b\alpha^3$ que no es otra que el twist de $\mathcal{C}$ por α (basta dividir ambos lados de la igualdad por α^3).

Para probar la última parte del Teorema consideremos v_1 y v_2 en $\mathbb{K}$ ninguno de ellos nulo ni cuadrado perfecto. Si $v_1 \equiv v_2 \pmod{\mathbb{K}^{*2}}$ entonces $v_2 = c^2 v_1$ con $c \in \mathbb{K}^*$ y tenemos $\mathcal{C}_{v_1} : v_1 Y^2 = X^3 + aX + b$ es $\mathbb{K}$-isomorfa a $v_1(cY)^2 = X^3 + aX + b$ que es la ecuación de $\mathcal{C}_{v_2}$.

Para probar el recíproco supongamos que $\mathcal{C}_{v_1}$ es $\mathbb{K}$-isomorfa a $\mathcal{C}_{v_2}$. Como $\mathcal{C}_{v_1}$ es $\mathbb{K}$-isomorfa a $\mathcal{C}'_{v_1} : Y^2 = X^3 + av_1^2 X + bv_1^3$ y $\mathcal{C}_{v_2}$ es $\mathbb{K}$-isomorfa a $\mathcal{C}'_{v_2} : Y^2 = X^3 + av_2^2 X + bv_2^3$ por transitiva resulta que las curvas $\mathcal{C}'_{v_1}$ y $\mathcal{C}'_{v_2}$ son $\mathbb{K}$-isomorfas. En virtud del Teorema 1.32, existe $u \in \overline{\mathbb{K}}$ tal que $u^4 = \frac{av_2^2}{av_1^2}$ y $u^6 = \frac{bv_2^3}{bv_1^3}$ y por lo observado al principio u debe estar en $\mathbb{K}$ para que el isomorfimo entre ambas curvas esté definida sobre $\mathbb{K}$, dividiendo la segunda ecuación por la primera obtenemos $u^2 = \frac{v_2}{v_1}$ y por lo tanto $v_1 \equiv v_2 \pmod{\mathbb{K}^{*2}}$.□

Para el caso $j = 0$, si $\mathcal{C} : Y^2 = X^3 + b$ y $\mathcal{C}' : Y^2 = X^3 + b'$ con b y b' en $\mathbb{K}^*$ son twist sobre $\mathbb{K}$, entonces los isomorfismos entre ellas serán de la forma $\phi(x, y) = (u^2x, u^3y)$ donde $u \in \overline{\mathbb{K}}$ verifica $u^6 = \frac{b'}{b} \in \mathbb{K}$ y $u \notin \mathbb{K}$ (de lo contrario serían $\mathbb{K}$-isomorfas) y por lo tanto $b \not\equiv b' \pmod{\mathbb{K}^{*6}}$. Recíprocamente, si $b \equiv b' \pmod{\mathbb{K}^{*6}}$ entonces $b' = u^6 b$ para algún $u \in \mathbb{K}^*$ y el mapa $\phi(x, y) = (u^2x, u^3y)$ resultaría un $\mathbb{K}$-isomorfismo entre las curvas $\mathcal{C} : Y^2 = X^3 + b$ y $\mathcal{C}' : Y^2 = X^3 + b'$, así que serían $\mathbb{K}$-isomorfas (y por lo tanto no serían twist una de la otra). En resumen, en este caso tenemos tantos twists como clases en $\mathbb{K}^*/\mathbb{K}^{*6}$ (donde $b\mathbb{K}^{*6} \mapsto Y^2 = X^3 + b$ (mód $\mathbb{K}$-isomorfismos) sería la correspondencia entre clases módulo potencias sextas y twist salvo $\mathbb{K}$-isomorfismos).

Para el caso $j = 1728$, si $\mathcal{C} : Y^2 = X^3 + aX$ y $\mathcal{C}' : Y^2 = X^3 + a'X$ son isomorfas con a y a' en $\mathbb{K}^*$ son twist sobre $\mathbb{K}$, entonces los isomorfismos entre ellas serán de la forma

$\phi(x,y) = (u^2x, u^3y)$ donde $u \in \overline{\mathbb{K}}$ verifica $u^4 = \frac{a'}{a}$ y $u \notin \mathbb{K}$ (de lo contrario serían $\mathbb{K}$-isomorfas) y por lo tanto $a \not\equiv a'$ (mód $\mathbb{K}^{*4}$). Recíprocamente, si $a \equiv a'$ (mód 4) entonces $a' = u^4a$ para algún $u \in \mathbb{K}^*$ y el mapa $\phi(x,y) = (u^2x, u^3y)$ resultaría un $\mathbb{K}$-isomorfismo entre las curvas $\mathcal{C} : Y^2 = X^3 + aX$ y $\mathcal{C}' : Y^2 = X^3 + a'X$ y no serían twist una de la otra. En resumen, en este caso tenemos tantos twists como clases en $\mathbb{K}^*/\mathbb{K}^{*4}$ (donde $a\mathbb{K}^{*4} \mapsto Y^2 = X^3 + aX$ (mód $\mathbb{K} - isomorfismos$) sería la correspondencia entre clases módulo potencias cuartas y twist salvo $\mathbb{K}$-isomorfismos).

Nos será de especial interés las curvas definidas sobre un cuerpo finito $\mathbb{K} = \mathbb{F}_q$ donde $q = p^m$ con p primo y supondremos para simplificar que $p \neq 2$ y $p \neq 3$. En algunas ocasiones el Teorema anterior continua valiendo aún para $j = 0$ o $j = 1728$.

Observación 1.40. El Teorema anterior sigue siendo válido cuando $j = 0$ siempre que $q \equiv -1$ (mód 6) y para $j = 1728$ siempre que $q \equiv -1$ (mód 4).

Demostración: Recordemos que el grupo multiplicativo $\mathbb{K}^*$ es cíclico de orden $q-1$. Si $q \equiv -1$ (mód 6) entonces $mcd(q-1, 3) = 1$ y por lo tanto todo elemento es un cubo perfecto (i.e. $\mathbb{K}^{*6} = \mathbb{K}^{*2}$) y en virtud del comentario previo tenemos una biyección entre $\mathbb{K}^*/\mathbb{K}^{*2}$ y los twist salvo $\mathbb{K}$-isomorfismo dado por $b\mathbb{K}^{*2} \mapsto Y^2 = X^3 + b$ (mód $\mathbb{K} - isomorfismos$). Si $q \equiv -1$ (mód 4) entonces $mcd(q-1, 4) = 2$ y por lo tanto todo cuadrado es también una potencia cuarta (i.e. $\mathbb{K}^{*4} = \mathbb{K}^{*2}$) y en este caso la biyección entre $\mathbb{K}^*/\mathbb{K}^{*2}$ y los twist salvo $\mathbb{K}$-isomorfismo viene dada por $a\mathbb{K}^{*2} \mapsto Y^2 = X^3 + aX$ (mód $\mathbb{K} - isomorfismos$). □

Cabe observar que si bien en estos casos solo tenemos twist cuadráticos (en el sentido que el isomorfismo entre las curvas twist está definido en una extensión de grado 2 del cuerpo base), estos no son necesariamente de la forma del Teorema, pues por ejemplo si $q \equiv -1$ (mód 4) entonces para todo $\nu \in \mathbb{K}^*$ existe $\mu \in \mathbb{K}^*$ tal que $\nu^2 = \mu^4$ (porque como ya vimos todo cuadrado es potencia cuarta en este caso) así que $\nu Y^2 = X^3 + aX \simeq (\nu^2 Y)^2 = (\nu X)^3 + a\nu^2(\nu X) \simeq Y^2 = X^3 + a\mu^4 X \simeq (\mu^3 Y)^2 = (\mu^2 X)^3 + a\mu^4(\mu^2 X) \simeq Y^2 = X^3 + aX$ donde todos los isomorfismos están definidos sobre $\mathbb{K}$ así que para este caso $\nu Y^2 = X^3 + aX$ siempre es $\mathbb{K}$-isomorfo a $Y^2 = X^3 + aX$, es fácil verificar que esto implica automáticamente que la cantidad de puntos sobre $\mathbb{F}_q$ es exactamente $q+1$. Para el caso en que $j = 1728, q \equiv -1$ (mód 6) entonces para todo $\nu \in \mathbb{K}^*$ existe $\mu \in \mathbb{K}^*$ tal que $\nu = \mu^3$ (porque en este caso vimos que todos son cubos) así que $Y^2 = X^3 + \nu b \simeq (\nu Y)^2 = (\mu X)^3 + \nu b \simeq \nu Y^2 = X^3 + b$ así que en este caso todos los twist cuadráticos son como en el Teorema anterior.

Este caso en realidad corresponde al llamado caso supersingular; curvas supersingulares son débiles a los efectos del logaritmo discreto así que no nos va a interesar este caso (en el final de este capítulo hablaremos un poco más sobre este punto).

Por último nos toca observar que pasa para el caso que nos queda, que es cuando $j = 0$ y $q \equiv 1$ (mód 6) y $j = 1728$ y $q \equiv 1$ (mód 4).

Observación 1.41. En el caso $j = 0$ y $q \equiv 1$ (mód 6) tenemos exactamente 6 twist salvo $\mathbb{K}$-isomorfismos y en el caso $j = 1728$ y $q \equiv 1$ (mód 4) tenemos exactamente 4 twist salvo $\mathbb{K}$-isomorfismos.

Demostración: Basta recordar que en el caso $j = 0, q \equiv 1 \pmod 6$ habian tantos twist como $\#\mathbb{F}_q^*/\mathbb{F}^{*6}$ y este cardinal es 6 puesto que $\mathbb{F}_q^*$ es cíclico y $6|q-1$ mientras que en el caso $j = 1728, q \equiv 1 \pmod 4$ habian tantos twist como $\#\mathbb{F}_q^*/\mathbb{F}_q^{*4}$ y este cardinal es 4 puesto que $\mathbb{F}_q^*$ es cíclico y $4|q-1$. □

En el Capítulo 3 (Lema (3.5)), probaremos que para el caso ordinario (que es el que nos interesa a los efectos del logaritmo discreto) curvas que son twist una de la otra tienen distinto cardinal sobre $\mathbb{F}_q$. Por lo tanto para este caso se cumple que el j-invariante junto con la cantidad de puntos sobre $\mathbb{F}_q$ clasifican las clases de $\mathbb{F}_q$-isomorfismos de curvas elípticas.

1.2.3. Estructura de grupo, isomorfismo con el grupo de Picard y consecuencias. Recordemos que las curvas elípticas poseen estructura de grupo abeliano definida geométricamente por el método de las cuerdas y las tangentes (ver por ejemplo [**32**]). Veamos ahora la versión algebraica de dicho grupo a través del grupo de divisores, recordemos que la estructura de grupo estaba caracterizada por la propiedad de que $P \oplus Q \oplus R = \mathcal{O}$ si y solo si P, Q y R están alineados. Comenzemos definiendo el grupo de Picard.

Definición 1.42. Sea $\mathcal{C}/\mathbb{K}$ una curva elíptica, $Div(\mathcal{C})$ su grupo de divisores. Denotemos por $Div^0(\mathcal{C})$ el subgrupo de los divisores de grado 0 y $Div^{princ}(\mathcal{C})$ al subgrupo de divisores principales (recordar que los divisores principales tienen grado 0). Entonces el grupo de Picard reducido de $\mathcal{C}$ viene dado por:

$$Pic^0(\mathcal{C}) = \frac{Div^0(\mathcal{C})}{Div^{princ}(\mathcal{C})}$$

Observación 1.43. Para P_1, P_2 y P_3 son puntos de $(\mathcal{C}(\mathbb{K}), \mathcal{O})$ se tiene:

$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \leftrightarrow P_1, P_2, P_3$ alineados $\leftrightarrow div(r) = P_1 + P_2 + P_3 - 3\mathcal{O}$ donde r es la recta

$$\text{que pasa por } P_1 \text{ y } P_2 \leftrightarrow P_1 + P_2 + P_3 - 3\mathcal{O} \equiv 0 \pmod{Div^{princ}} \leftrightarrow$$
$$(P_1 - \mathcal{O}) + (P_2 - \mathcal{O}) + (P_3 - \mathcal{O}) \equiv 0 \pmod{Div^{princ}}$$

En particular:

$$P \oplus (-P) \oplus \mathcal{O} = \mathcal{O} \Rightarrow (P - \mathcal{O}) + ((-P) - \mathcal{O}) \equiv 0 \pmod{Div^{princ}}$$

En vista de dicha observación tenemos bien definido un morfismo de grupos:

$$\varphi : \mathcal{C}(\overline{\mathbb{K}}) \to Pic^0(\mathcal{C}) \quad / \quad P \mapsto P - \mathcal{O}$$

Veamos que dicho morfismo es efectivamente un isomorfismo.

Proposición 1.44. *El mapa φ definido anteriormente es biyectivo.*

Demostración: Veamos primero la inyectividad, sea $P \in \mathcal{C}(\overline{\mathbb{K}})$ tal que $P - \mathcal{O} \equiv 0 \pmod{Div^{princ}}$ entonces $\exists r \in \overline{\mathbb{K}}(\mathcal{C})$ tal que $div(r) = P - \mathcal{O}$ pero como no hay funciones sobre $\mathcal{C}$ con un único polo de orden 1 en $\mathcal{O}$ (pues $\ell(\mathcal{O}) = 1 \Rightarrow \mathcal{L}(\mathcal{O}) = \overline{K}$) se tiene que $P = \mathcal{O}$ y $r \equiv 0$.

Ahora la sobreyectividad, dado $D \in Div^0(\mathcal{C})$, queremos ver que $\exists P \in \mathcal{C}(\overline{\mathbb{K}})$ tal que $D \equiv P - \mathcal{O}$ (mód Div^{princ}) o equivalentemente queremos encontrar $P \in \mathcal{C}$ tal que $D + \mathcal{O} \equiv P$ (mód Div^{princ}).

Consideremos el espacio de Riemann-Roch $\mathcal{L}(D + \mathcal{O})$ cuya dimensión es $\ell(D + \mathcal{O}) = \deg(D+\mathcal{O}) = 1$ por lo tanto existe una función no nula $f \in \mathcal{L}(D+\mathcal{O})$ como $div(f)+D+\mathcal{O} \geq 0$ y $\deg(div(f) + D + \mathcal{O}) = 1$ entonces $div(f) + D + \mathcal{O} = P$ para algún punto $P \in \mathcal{C}$ como queríamos probar.

□

Ahora definiremos nuestro principal objeto de estudio para atacar el problema del logaritmo discreto que son las isogenias.

Definición 1.45 (Isogenias)**.** Si $\mathcal{C}_1$ y $\mathcal{C}_2$ son curvas elípticas sobre $\mathbb{K}$, llamaremos isogenia a cualquier mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ que preserve la estructura de grupo. Decimos que la isogenia está definida sobre $\mathbb{K}$ si es un mapa $\mathbb{K}$-racional.

Una de las principales consecuencias del isomorfismo entre el grupo de la curva elíptica con su grupo de Picard es que facilita muchísimo varios resultados que de otra manera serían más complicados de probar. Por ejemplo el siguiente resultado sobre isogenias que será de gran importancia para nuestro estudio.

Teorema 1.46. *Todo mapa racional entre curvas elípticas $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ tal que $\phi(\mathcal{O}_1) = \mathcal{O}_2$ (donde $\mathcal{O}_1$ y $\mathcal{O}_2$ son los puntos distinguidos de $\mathcal{C}_1$ y $\mathcal{C}_2$, neutros para la estructura de grupo) es una isogenia.*

Demostración: (idea) Un mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ induce un mapa lineal $\phi_* : Div^0(\mathcal{C}_1) \to Div^0(\mathcal{C}_2)$ dado por $\phi_*(\sum_P n_P P) = \sum_P n_P \phi(P)$, este mapa verifica que lleva divisores principales en divisores principales ([**35**], pág.34 por detalles y referencias) por lo tanto induce un morfismo entre el grupo de Picard de ambas curvas definido por la propiedad $\phi_*(P) = \phi(P)$.

Para ver que $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ induce un morfismo de grupo entre ambas curvas alcanza verificar la conmutatividad del siguiente diagrama:

$$\begin{array}{ccc} \mathcal{C}_1 & \xrightarrow{\phi} & \mathcal{C}_2 \\ \varphi_1 \downarrow & & \downarrow \varphi_2 \\ Pic^0(\mathcal{C}_1) & \xrightarrow{\phi_*} & Pic^0(\mathcal{C}_2) \end{array}$$

donde $\varphi_1 : \mathcal{C}_1 \to Pic^0(\mathcal{C}_1)$ y $\varphi_2 : \mathcal{C}_2 \to Pic^0(\mathcal{C}_2)$ son los isomorfismos que llevan $P \mapsto P - \mathcal{O}_i$ (mód $Div^{princ}(\mathcal{C}_i)$) para $i = 1, 2$ respectivamente.

En efecto, para todo $P \in \mathcal{C}_1$ se tiene:

$$\phi_* \circ \varphi(P) = \phi_*(\varphi(P)) = \phi_*(P - \mathcal{O}_1) = \phi(P) - \phi(\mathcal{O}_1) = \phi(P) - \mathcal{O}_2 = \varphi_2(\phi(P)) = \varphi_2 \circ \phi(P)$$

□

En la próxima sección definiremos algunos conceptos básicos sobre las isogenias y algunas propiedades elementales.

2. Hechos básicos sobre Isogenias.

Aunque muchos de los resultados que expondremos aquí valen para curvas elípticas sobre cualquier cuerpo $\mathbb{K}$, nos centraremos en el caso que más nos importa que es cuando $\mathbb{K} = \mathbb{F}_q$ con $q = p^r$ siendo p (primo) su característica. Varios de los resultados en donde usaremos las ecuaciones explícita de la curva, enunciaremos el teorema general y haremos la prueba para cuando $p \neq 2, 3$ usando la forma reducida, aunque puede hacerse en general usando la ecuación de Weiestrass completa. En esta sección entonces nuestras curvas elípticas las supondremos dadas en forma reducida $E : Y^2 = X^3 + aX + b$ con $4a^3 + 27b^2 \neq 0$ (y con punto distinguido $\mathcal{O} = [0 : 1 : 0]$).

Desde ahora en más, usaremos las siguientes notaciones para denotar al conjunto de isogenias entre dos curvas elípticas (definidas sobre un cuerpo finito o no).

Notación 1.47. Sean $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$ dos curvas elípticas, denotaremos por:

$$\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2 : \phi \text{ isogenia}\}$$

Si $E/\mathbb{K}$ es una curva elíptica denotaremos al conjunto de sus endomorfismos como:

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

Para denotar al conjunto de las isogenias o endomorfismos que están definidos sobre el cuerpo base $\mathbb{K}$ usaremos $\mathrm{Hom}_{\mathbb{K}}(E_1, E_2)$ y $\mathrm{End}_{\mathbb{K}}(E)$.

Cuando queramos restringirnos a isogenias de cierto grado ℓ fijo (como en el siguiente capítulo) entonces notaremos por $\mathrm{Hom}_\ell(E_1, E_2)$ al conjunto de isogenias de grado ℓ (o ℓ-isogenias) que van de E_1 a E_2.

2.1. Los mapas $[m]$ y el Endomorfismo de Frobenius ϕ_q.

Una importante familia de endomorfismos de una curva elíptica lo constituyen los m-mapas y para el caso de cuerpos con característica finita (especialmente nos interesan los cuerpos finitos $\mathbb{F}_q$) tenemos además un endomorfismo disntinguido que es el endomorfismo de Frobenius.

Definición 1.48. Se denota por $[m] : E \to E$ el mapa multiplicación por m (o m-mapa):

$$[m](P) = \underbrace{P \oplus P \oplus \ldots \oplus P}_{m \text{ veces}}$$

No es difícil ver que los mapas $[m] : P \mapsto mP$ son de hecho endomorfismos en E, recordemos que con un sencillo argumento geométrico es posible obtener fórmulas explícitas para la duplicación y la suma de puntos y que estas son de hecho funciones racionales de los coeficientes de los puntos ([**32**] pág.23). Por ejemplo para $m = 2$ y $P \in E(\overline{\mathbb{K}})$ teníamos que:

$$[2](P) = \begin{cases} [0:1:0] & \text{si } P = \mathcal{O} \text{ o } P = (x, y) \text{ con } y = 0. \\ \left(\frac{\phi_2(x)}{(2y)^2}, \frac{\omega_2(x)}{(2y)^3}\right) = [2y\phi_2(x) : \omega_2(x) : 8y^3] & \text{si } P = (x, y) \text{ con } y \neq 0. \end{cases}$$

donde los polinomios ϕ_2 y ω_2 vienen dados por:

$$\begin{cases} \phi_2(x) = x^4 - 2ax^2 - 8bx + a^2 \\ \omega_2(x) = x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2 \end{cases}$$

Observemos de hecho que la última expresión para [2] es válida para todo $P \in E(\overline{\mathbb{K}})$, para $P = \mathcal{O}$ como ϕ_2 y ω_2 tienen polo de orden 8 y 12 respectivamente (pues x tiene polo de orden 2 en $\mathcal{O}$) e y tiene polo de orden 3 en $\mathcal{O}$ tenemos que:

$$[2y\phi_2(x) : \omega_2(x) : 8y^3](\mathcal{O}) = \left[\frac{2\phi_2}{y^3} : \frac{\omega_2}{y^4} : \frac{8}{y}\right](\mathcal{O}) = [0:1:0] = \mathcal{O}$$

Y para $P = (x_0, 0) \in E$ tenemos que:

$$[2y\phi_2(x) : \omega_2(x) : 8y^3](P) = [0 : \omega_2(x_0) : 0]$$

Luego nos queda verificar solo que $\omega_2(x_0) \neq 0$, observemos que el hecho que $y(P) = 0$ implica $x_0^3 + ax_0 + b = 0$ y así que alcanza verificar que los polinomios $\omega_2(x)$ y $x^3 + ax + b$ no tienen raices en común. Si $b = 0$ entonces $a \neq 0$ (pues $4a^3 + 27b^2 \neq 0$) y se chequea directamente que ninguna de las raices de $x^3 + ax = 0$ anula a ω_2. Para el caso que $b \neq 0$ el resultado se desprende del siguiente conjunto de ecuaciones:

$$\omega_2(x) = (x^3{+}4ax{+}19b)(x^3{+}ax{+}b){-}(9a^2x^2{+}27abx{+}a^3{+}27b^2)$$
$$9a^3(x^3{+}ax{+}b) = (ax{-}3b)(9a^2x^2{+}27abx{+}a^3{+}27b^2){+}(4a^3{+}27b^2)(2ax{+}3b)$$
$$8a^3(x^3{+}ax{+}b) = (4a^2x^2{-}6abx{+}4a^3{+}9b^2)(2ax{+}3b){-}b(4a^3{+}27b^2)$$

Al ser $4a^3 + 27b^2 \neq 0$ si x_0 fuese una raíz común de $\omega_2(x)$ y $x^3 + ax + b$ esto implicaría que $b = 0$ contradiciendo nuestra suposición. Concluimos que:

$$[2] = \left(\frac{\phi_2(x)}{(2y)^2}, \frac{\omega_2(x)}{(2y)^3}\right)$$

es un endomorfismo de E definido sobre $\mathbb{K}$ (el cuerpo base de E).

Usando un razonamiento por inducción usando la duplicación y la fórmula de la suma de puntos, puede probarse que en general se tiene (en [**35**], pág. 105, se da una guía para una prueba por inducción):

$$[m](P) = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right)$$

donde las funciones ϕ_m y ω_m se escriben en función de las $(\psi_n)_{n\geq 0}$ como:

$$\begin{cases} \phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\ 4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \end{cases}$$

Y las funciones $(\psi_n)_{n\geq 0}$ se definen de forma inductiva:

$$\begin{cases} \psi_0 = 0 \\ \psi_1 = 1 \\ \psi_2 = 2y \\ \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2 \\ \psi_4 = 4y(x^6 + 5ax^4 + 20bx^2 - 5a^2x^2 - 4abx - 8b^2 - a^3) \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad \text{para } m \geq 2 \\ 2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \quad \text{para } m \geq 3 \end{cases}$$

A los polinomios ψ_m se los conoce como los polinomios de m-división (que juegan un papel importante en la construcción de isogenias de curva elípticas definidas sobre cuerpos finitos). Se puede probar que para m par resulta que $\phi_m, \omega_m \in \overline{\mathbb{K}}[x]$ y $\psi_m \in y\overline{\mathbb{K}}[x]$ mientras

que para m impar se tiene que $\psi_m, \phi_m \in \overline{\mathbb{K}}[x]$ y $\omega_m \in y\overline{\mathbb{K}}[x]$. Con respecto a los grados como polinomios resulta que ψ_m^2 es un polinomio en x (sustituyendo y^2 por x^3+ax+b) de grado m^2-1 si m no divide a la característica de $\mathbb{K}$, mientras que ϕ_m es un polinomio en x de grado m^2 y dichos polinomios son coprimos en $\overline{\mathbb{K}}[x]$ ([**35**], Ej.3.7, pág.105).

2.1.1. Puntos de m-torsión y separabilidad de los mapas $[m]$. Observemos que $[m] = [\phi_m\psi_m : \omega_m : \psi_m^3]$ y al no tener ψ_m y ω_m puntos en común (si $P_0 = (x_0, y_0)$ fuese tal que $\psi_m(P_0) = \omega_m(P_0) = 0$, como $\omega_m^2 = \phi_m^3 + a\phi_m\psi_m^4 + b\psi_m^6$ entonces x_0 sería una raíz común de ϕ_m y ψ_m^2 contradiciendo la coprimidad), resulta que los puntos $P = (x, y) \in \ker([m])$ son justamente los que verifican $\psi_m(x, y) = 0$.

Usando la acción del pullback en el diferencial invariante se prueba que $[m]$ es separable si y solo si $p \nmid m$ (donde $p > 0$ es la característica del cuerpo), la teoría involucrada y los detalles de este resultado en particular se encuentra en el libro de Silverman [**35**], Capítulo 3.5. en especial el Corolario 5.5.

Otra propiedad importante de los mapas $[m]$ que se obtiene como consecuencia de la dualidad (repasaremos las principales propiedades de la dualidad en la sección 2.3.4), es que su grado es $\deg([m]) = m^2$, así que para el caso en que $p \nmid m$ (o sea cuando $[m]$ es separable) resulta que $\#ker([m]) = m^2$.

Otra consecuencia del resultado anterior es el teorema de estructura para la parte de m-torsión $E[m] = \ker([m])$ cuando m es coprimo con la característica, en efecto, si $E[m] \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$ con $m_1|m_2|\ldots|m_k$ tenemos que $E[m/m_k] = m_kE[m] = \{\mathcal{O}\} \Rightarrow m_k = m$ y como $m_1m_2\ldots m_k = m$ resulta $k = 2, m_1 = m_2 = m$ por lo tanto:

$$E[m] \simeq \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}} \qquad \text{siempre que } m \text{ no divida a la característica de } \mathbb{K}$$

Para el caso en que $m = p^t$ con $p = car(\mathbb{K})$ como consecuencia de la dualidad se tiene que $E[p^t] \simeq \{\mathcal{O}\}$ para todo t o $E[p^t] \simeq \mathbb{Z}/p^t\mathbb{Z}$ para todo t según el dual del Frobenius $\widehat{\phi_p}$ sea separable o no respectivamente ([**35**],Cor.6.4., pág.89).

2.1.2. $\mathrm{End}(E)$ *como* $\mathbb{Z}$*-módulo.* Observemos que al ser los polinomio de m-división ϕ_m y ω_m no nulos en E resulta que los m-mapas son no nulos, en particular tenemos una inyección

$$\mathbb{Z} \hookrightarrow \mathrm{End}(E), \quad m \mapsto [m]$$

El conjunto $\mathrm{End}(E)$ con la suma y composición resulta entonces un anillo de característica 0. Cuando $\mathbb{Z} \subsetneq \mathrm{End}(E)$ decimos que $E/\mathbb{K}$ tiene multiplicación compleja, la nomenclatura proviene de la teoría de curvas elípticas complejas, que visto como toros complejos corresponde a multiplicaciones por complejos no reales ([**32**] Cáp. 2).

2.1.3. El mapa de Frobenius. Para el caso de curvas elípticas sobre cuerpos finitos siempre tienen multiplicación compleja, pues tienen un endomorfismo distinguido (el endomorfismo de Frobenius) que definiremos a continuación. En esta parte supondremos que $\mathbb{K}$ es un cuerpo perfecto de característica p y q una potencia de p.

Definición 1.49. Sea $E/\mathbb{K}$ una curva elíptica dada por ecuación reducida $E : Y^2 = X^3 + aX + b$, $q = p^t$ y definimos la curva $E^{(q)} : Y^2 = X^3 + a^qX + b^q$. El mapa de Frobenius

viene dado por

$$\phi_q : E \to E^{(q)}, \quad (x, y) \mapsto (x^q, y^q)$$

(observemos que si $\mathbb{K} = \mathbb{F}_q$ entonces $E^{(q)} = E$ y ϕ_q resulta un automorfismo de E).

Observemos de hecho que la curva $E^{(q)}$ es una curva elíptica pues su discriminante $-16(4a^{3q} + 27b^{2q}) = -16(4a^3 + 27b^2)^q \neq 0$ pues E es no singular. Que $\phi_q(E) = E^{(q)}$ puede verse fácilmente, en efecto, si $(x, y) \in E(\overline{\mathbb{K}})$ se tiene que $y^2 = x^3 + ax + b$ luego

$$(y^q)^2 = (y^2)^q = (x^3 + ax + b)^q = (x^q)^3 + a^q x^q + b^q$$

Observemos además que si $E/\mathbb{K}$ (es decir, si $a, b \in \mathbb{K}$) entonces ϕ_q es de hecho un automorfismo (pues $a^q = a$ y $b^q = b$).

Respecto a la extensión de cuerpos inducida por el Frobenius $\phi = \phi_q$, usando que $\mathbb{K}$ es perfecto no es difícil ver que $\phi^*(\mathbb{K}(E^{(q)})) = \mathbb{K}(E)^q$ y por lo tanto ϕ es puramente inseparable, al serlo la extensión $\mathbb{K}(E)^q \subset \mathbb{K}(E)$ (ver Prop.A.6 del Apéndice).

Un poco más difícil es ver que $\deg(\phi_q) = q$, la clave es un resultado sobre uniformizantes que prueba que el cuerpo de funciones $\mathbb{K}(E)$ de una curva elíptica es una extensión finita separable de $\mathbb{K}(t)$, para toda uniformizante t en algún punto P de E (Prop.1.4, pág.22 de [**35**]). Considerando una uniformizante $t = t_P$ resulta que por un lado $\mathbb{K}(E)^q(t) \subset \mathbb{K}(E)$ es separable (por ser una subextensión de la extensión separable $\mathbb{K}(t) \subset \mathbb{K}(E)$) y por otro puramente inseparable (por ser una subextensión de la extensión puramente inseparable $\mathbb{K}(E)^q \subset \mathbb{K}(E)$) así que debe darse la igualdad $\mathbb{K}(E)^q(t) = \mathbb{K}(E)$. Por otra parte el grado del elemento primitivo t de la extensión (puramente inseparable) $\mathbb{K}(E)^q \subset \mathbb{K}(E)$ debe tener grado divisor de q (ver Prop.A.6 del Apéndice), para probar que su grado es exactamente q basta probar que $t^{\frac{q}{p}} \notin \mathbb{K}(E)^q$, en caso contrario, si $t^{\frac{q}{p}} = f^q$ con $f \in \mathbb{K}(E)$ entonces $q/p = ord_P(t^{\frac{q}{p}}) = ord_P(f^q) = q\ ord_P(f)$ lo cual implica $ord_P(f) \notin \mathbb{Z}$ lo cual es absurdo, por lo tanto t tiene grado q, lo cual implica que la extensión $\mathbb{K}(E)^q \subset \mathbb{K}(E)$ tiene grado q.

En esta misma sección veremos algunas propiedades que hacen del Frobenius un mapa sumamente relevante, veremos de hecho que es el causable de la parte no separable de una isogenia en el sentido que toda isogenia no separable se factoriza por un Frobenius (en la subsección que habla de Factorización de Isogenias). También juega un papel fundamental en el trabajo de Kohel (que hablaremos en el próximo capítulo), para reconocer la $\mathbb{F}_q$-racionalidad de curvas elípticas.

2.2. Grado de Isogenias. En 1.1.3 dimos las definiciones de grado de un mapa racional entre curvas, así como del grado de separabilidad e inseparabilidad, que se aplican al caso particular de isogenias. La estructura de grupo de una curva elíptica hace que muchas propiedades locales sean independientes del punto P en virtud de los mapas translación (que no son isogenias por no dejar fijo el origen pero si son isomorfismos como mapa racionales).

El resultado principal lo establece el Teo.4.10, pág.76 de [**35**], que dice que la cantidad de preimágenes no depende del punto $Q \in E_2$ y esta coincide con el grado de separabilidad del mapa ϕ y que la ramificación tampoco depende del punto $P \in E_1$ y esta coincide con

el grado de inseparabilidad del mapa ϕ.

Proposición 1.50. *Sea $\phi : E_1 \to E_2$ una isogenia entre dos curvas elípticas E_1 y E_2 se tiene:*

i) $\deg_s(\phi) = \#\phi^{-1}(Q)\ \forall Q \in E_2$.
ii) $\deg_i(\phi) = e_\phi(P)\ \forall P \in E_1$.

Idea de la Demostración:

i) Sean Q y Q' puntos en E_2 y sea $P_0 \in \phi^{-1}(Q' - Q)$ entonces el mapa $P \mapsto P + P_0$ resulta claramente una biyección entre $\phi^{-1}(Q)$ y $\phi^{-1}(Q')$, esto pruba que la cantidad de preimágenes es independiente del punto $Q \in E_2$. La Prop.2.6, pág.28 de [**35**] establece que la igualdad $\deg_s(\phi) = \phi^{-1}(Q)$ es válida para mapas racionales entre curvas no singulares pero podría fallar en finitos casos, la homogeneidad que acabamos de ver implica que nunca falla.

ii) Sean P y P' puntos en E_1, las translaciones son isomorfismos, por lo tanto inducen un isomorfismo entre los anillos locales vía composición en particular preserva órdenes (es decir $ord_P(f) = ord'_p(f \circ \tau_{P-P'})$ donde τ es el mapa translación). Sean $Q = \phi(P), Q' = \phi(P')$ y tomamos como uniformizantes t_Q y $t_{Q'} = t_Q \circ \tau_{Q-Q'}$ en Q y Q' respectivamente. Entonces $\phi^* t'_Q = t_Q \circ \tau_{Q-Q'} \circ \phi = t_Q \circ \phi \circ \tau_{P-P'} = \phi^* t_Q \circ \tau_{P-P'}$ por lo tanto $e_\phi(P) = ord_P(\phi^* t_P) = ord_{P'}(\phi^* t_{P'}) = e_\phi(P')$. Llamemos $e = e_\phi(P)$ para cualquier $P \in E_1$, usando que $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$ (Prop.2.6, pág.28 de [**35**]) y que $\#\phi^{-1}(Q) = \deg_s(\phi)$ resulta que $\deg_s(\phi) \cdot e = \deg(\phi)$ y por lo tanto $e = \deg_i(\phi)$.

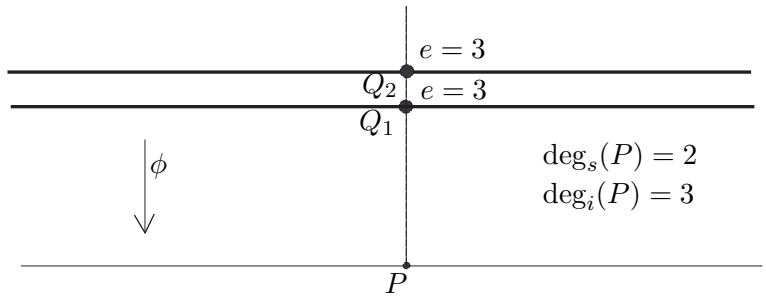


FIGURA 2. Comportamiento homogéneo del grado de una isogenia entre curvas elípticas debido a su estructura de grupo.

2.3. Teoremas de Factorización. En esta subsección repasaremos los resultados más relevantes que refieren a factorización de isogenias incluyendo la construcción de la isogenia dual.

2.3.1. Factorización por Frobenius. En 1.1.4 vimos que todo mapa racional $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ entre curvas no singulares factorizaba como $\phi = \phi_2 \circ \phi_1$ donde $\phi_1 : \mathcal{C}_1 \to \mathcal{C}$ es un mapa puramente inseparable y $\phi_2 : \mathcal{C} \to \mathcal{C}_2$ es un mapa separable. Para el caso en que el mapa ϕ sea una isogenia entre dos curvas elípticas $\mathcal{C}_1$ y $\mathcal{C}_2$ se puede dar una descripción más explícita de dicha factorización.

En efecto, recordemos que el cuerpo de funciones $\mathbb{K}(\mathcal{C})$ de la curva no singular $\mathcal{C}$ (a priori no sabemos que se trate de una curva elíptica) correspondia con la clausura separable de $\mathbb{K}(\mathcal{C}_2)$ en $\mathbb{K}(\mathcal{C}_1)$ por lo tanto la extensión $\mathbb{K}(\mathcal{C}) \subset \mathbb{K}(\mathcal{C}_1)$ es una extensión finita puramente inseparable por lo tanto su grado debe ser $q' = p^r$, potencia de la característica del cuerpo $\mathbb{K}$ y $\mathbb{K}(\mathcal{C}_1)^{q'} \subset \mathbb{K}(\mathcal{C})$ (Prop.A.7 del Apéndice). Por otra parte, como vimos anteriormente la extensión $\mathbb{K}(\mathcal{C}_1)^{q'} \subset \mathbb{K}(\mathcal{C}_1)$ tiene grado q' y es la inducida por el endomorfismo de Frobenius $\phi_{q'} : \mathcal{C}_1 \to \mathcal{C}_1^{(q)}$, así que comparando grados resulta $\mathbb{K}(\mathcal{C}) = \mathbb{K}(\mathcal{C}_1)^{q'}$ que por el isomorfismo functorial resulta que $\mathcal{C} = \mathcal{C}_1^{(q')}$ y $\phi_1 = \phi_{q'} = \phi_p^r$ es la potencia r-ésima del Frobenius elevar a la p.

$$\begin{array}{ccc} \mathbb{K}(\mathcal{C}_1) & & \mathcal{C}_1 \\ \uparrow{\scriptstyle p.i} & & \downarrow{\scriptstyle \phi_1=\phi_{q'}=\phi_p^r} \\ \mathbb{K}(\mathcal{C}) = \mathbb{K}(\mathcal{C}_1)^{q'} = \mathbb{K}(\mathcal{C}_1^{(q')}) & \rightsquigarrow & \mathcal{C} = \mathcal{C}_1^{(q')} \\ \uparrow{\scriptstyle sep} & & \downarrow{\scriptstyle \phi_2} \\ \mathbb{K}(\mathcal{C}_2) & & \mathcal{C}_2 \end{array}$$

En resumen, cuando el cuerpo $\mathbb{K}$ tiene característica p (nos interesa especialmente el caso cuando $\mathbb{K} = \mathbb{F}_q$ un cuerpo finito con $q = p^n$ elementos) la parte inseparable de una isogenia corresponde siempre a una potencia del Frobenius ϕ_p, en muchos casos esto nos permite restringirnos a isogenias separables y jugará un papel importante en el posterior desarrollo. Cuando el cuerpo $\mathbb{K}$ tiene característica 0 entonces toda extensión resulta separable y la descomposición anterior queda trivial.

2.3.2. Factorización por inclusión de kernel. Observemos que si una isogenia $\psi : E \to E'$ factoriza como producto de dos isogenias $\psi = \lambda \circ \phi$ entonces necesariamente debe cumplirse que $\ker(\psi) \supset \ker(\phi)$. Esta condición también es suficiente cuando ϕ es separable.

Proposición 1.51. *Si $\phi : E_1 \to E_2$ es separable y $\psi : E_1 \to E_3$ es tal que $\ker(\psi) \supset \ker(\phi)$ entonces existe una isogenia $\lambda : E_2 \to E_3$ tal que el diagrama:*

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi \ sep} & E_2 \\ & \searrow^{\psi} & \downarrow{\scriptstyle \lambda} \\ & & E_3 \end{array} \qquad \textit{conmuta, es decir, se cumple que } \psi = \lambda\phi.$$

Demostración: Recordemos que cada isogenia induce un mapa entre los cuerpos de funciones, es clave entonces entender mejor dicha extensión de cuerpos y para ello estudiamos que pasa con los automorfismos que dejan fijo el cuerpo base (para usar Teoría de Galois).

En primer lugar observemos que si $T \in \ker(\phi)$ y $\tau_T : E_1 \to E_1$ es el mapa translación por T entonces este mapa induce un automorfismo en el cuerpo de funciones $\tau_T^* : \mathbb{K}(E_1) \to \mathbb{K}(E_1)$ dada por $f \mapsto f \circ \tau_T$ que verifica que para toda $g \in \phi^*(\mathbb{K}(E_2))$ se cumple $\tau_T^*(g) = g$. En efecto, $g = h \circ \phi$ para algún $h \in \mathbb{K}(E_2)$ y por lo tanto $\tau_T^*(g) = g \circ \tau_T = h \circ \phi \circ \tau_T = h \circ \phi = g$ (para la penúltima igualdad se usa que $T \in \ker(\phi)$). Así que $\tau_T^* \in Aut(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2))$

para todo $T \in \ker(\phi)$.

De hecho es fácil ver que valores distintos de T inducen morfismos distintos en $\mathbb{K}(E_1)$ (basta evaluar en las funciones coordenadas) y que son todos (mirando cardinalidad), detalles pueden verse en [**35**] Teo.4.10, pág.76. Así que resulta:

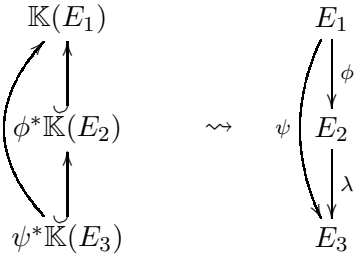
$$Aut(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2)) = \{\tau_T^* : T \in \ker(\phi)\}$$

En el caso que ϕ sea separable se cumple la cadena de igualdades:

$$[\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2)] = \deg(\phi) = \deg_s(\phi) = \#\ker(\phi) = \#Aut(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2))$$

y por lo tanto, en este caso, la extensión resulta ser de Galois.

Ahora bien, la inclusión de kerneles $\ker(\phi) \subset \ker(\psi)$ implica la inclusión $\mathrm{Gal}(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2)) \subset Aut(\mathbb{K}(E_1)/\psi^*\mathbb{K}(E_3))$ así que todo elemento $\tau_T \in \mathrm{Gal}(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2))$ deja fijo los elementos del cuerpo $\psi^*\mathbb{K}(E_3)$ así que por Teoría de Galois se tiene la inclusión $\psi^*\mathbb{K}(E_3) \subset \phi^*\mathbb{K}(E_2)$ que corresponde (por el isomorfismo functorial) a una isogenia $\lambda : E_2 \to E_3$ obteniendo la factorización deseada:



□

Esta proposición tiene un importante corolario.

Corolario 1.52. *Si $\phi : E_1 \to E_2$ separable con $\ker(\phi) = K \Rightarrow \phi$ es única, salvo isomorfismo, con esa propiedad.*

Demostración: En efecto, si $\psi : E_1 \to E_3$ es otra isogenia con $\ker(\psi) = K$ la proposición anterior nos brinda la existencia de dos isogenias $\lambda : E_2 \to E_3$ y $\mu : E_3 \to E_2$ que verifican $\psi = \lambda\phi$ y $\phi = \mu\psi \Rightarrow \psi = \lambda\mu\psi$ y $\phi = \mu\lambda\phi$, que por la sobreyectividad de las isogenias se tiene $\lambda\mu = 1_{E_3}$ y $\mu\lambda = 1_{E_2}$.

□

Observación 1.53. El mapa $T \mapsto \tau_T^*$ resulta un isomorfismo entre $\ker(\phi)$ y su imagen $\{\tau_T^* : T \in \ker(\phi)\}$, cuando ϕ es separable vimos que este conjunto coincide con $\mathrm{Gal}(\mathbb{K}(E_1)/\phi^*\mathbb{K}(E_2))$ así que resulta isomorfo como grupo a $\ker(\phi)$.

2.3.3. La Curva cociente. De hecho, dada la curva elíptica E_1 y un subgrupo finito N de E_1 siempre existe una isogenia separable $\phi : E_1 \to E_2$ con $\ker(\phi) = N$. Este resultado es nuevamente consecuencia del isomorfismo functorial, considerando la extensión $\mathbb{K}(E_1)^{N^*} \subset \mathbb{K}(E_1)$ que resulta ser Galois finita, por una de las equivalencias del Teorema de correspondencia de Galois (ver Teo.2.10.A del Apéndice), donde $N^* = \{\tau_P^* : P \in N\}$; al ser finita, $\mathbb{K}(E_1)^{N^*}$ tiene grado de trascendencia 1 sobre $\mathbb{K}$ y por lo tanto es el cuerpo

de funciones de una curva no singular E_2, la correspondencia nos asegura la existencia de un mapa racional no constante $\phi : E_1 \to E_2$:

$$\begin{array}{ccc} \mathbb{K}(E_1) & & E_1 \\ \uparrow & & \downarrow \phi \\ \mathbb{K}(E_1)^{N^*} = \mathbb{K}(E_2) & \rightsquigarrow & E_2 \end{array}$$

Se prueba que ϕ es no ramificado chequeando que para todo $Q \in E_2$ se tiene que $\#\phi^{-1}(Q) = \deg(\phi)$ [Prop 2.6 y Cor 2.7 Silverman] y luego como consecuencia directa de la fórmula de Hurwitz para el género se deduce que E_2 tiene género 1 y por lo tanto ϕ resulta una isogenia tomando como punto distinguido de E_2 el punto $\phi(\mathcal{O}_{E_1})$ (por detalles ver [**35**], Prop.4.12, pág.78).

La curva E_2 queda determinada salvo isomorfismo según el corolario anterior y se la denota por E_1/K (su grupo de puntos será isomorfo al grupo E_1/K). Más aún, si la curva E_1 y K están definidos sobre $\mathbb{K}$ entonces la curva cociente E_1/K también estará definida sobre el cuerpo base $\mathbb{K}$ ([**35**], Remark 4.13.2, pág.78).

2.3.4. La isogenia dual. Tal vez una de las consecuencias más importantes de los teoremas de factorización es la existencia de la isogenia dual (que también puede verse de alguna manera como otro teorema de factorización sobre los mapas $[m]$).

Comenzemos observando que si $\phi : E_1 \to E_2$ es una isogenia no nula, con $|\ker(\phi)| = m$ entonces por el Teorema de Lagrange, para todo $P \in \ker(\phi)$ tenemos que $mP = 0$ por lo tanto se tiene la inclusión de kerneles $\ker(\phi) \subset \ker([m]) = E_1[m]$. En el caso que ϕ sea separable, el Teorema de factorización por inclusión de kernel nos asegura la existencia de una isogenia $\widehat{\phi} : E_2 \to E_1$ tal que hace conmutar el diagrama:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ & \searrow^{[m]} & \downarrow \widehat{\phi} \\ & & E_1 \end{array}$$

Teorema 1.54. *(Isogenia dual). Para toda isogenia $\phi : E_1 \to E_2$ no nula con $|\ker(\phi)| = m$, existe una única isogenia $\widehat{\phi} : E_2 \to E_1$ tal que $\widehat{\phi} \circ \phi = [m]$.*

Demostración: Primero se observa que si existe es única, pues si $\widehat{\phi}_1$ y $\widehat{\phi}_2$ fueran dos isogenias duales para ϕ entonces $(\widehat{\phi}_1 - \widehat{\phi}_2)\phi = 0$ pero al ser ϕ no nula (y por lo tanto sobreyectiva) se tiene que $\widehat{\phi}_1 = \widehat{\phi}_2$.

Para la existencia separamos en casos. El caso en que ϕ es separable es consecuencia directa del Teorema de factorización por inclusión de kernel como acabamos de ver. Para el caso en que $\phi = \phi_p$ el p-Frobenius, primero se chequea que el mapa $[p]$ no es separable y por el Teorema de factorización por Frobenius tenemos que $[p] = \psi \circ \phi_p^s$ con ψ separable y $s > 1$ (pues $[p]$ es no separable) de modo que podemos tomar $\widehat{\phi} = \psi \circ \phi_p^{s-1}$. Luego se chequea sencillamente que si $\widehat{\phi}$ y $\widehat{\psi}$ son isogenias duales para ϕ y ψ respectivamente, entonces $\widehat{\psi} \circ \widehat{\phi}$ es una isogenia dual para $\phi \circ \psi$, el resultado general se sigue nuevamente del Teorema de descomposición por Frobenius pues toda isogenia ϕ no nula puede factorizarse

como $\phi = \psi \circ \phi_p^s$ con ψ separable y ϕ_p el p-Frobenius (más detalles pueden verse en [**35**],Teo.6.1,pág.84).

□

De esta forma tenemos un operador dualidad tal que a cada isogenia ϕ le hace corresponder su isogenia dual $\widehat{\phi}$. Culminaremos esta sección enunciando las principales propiedades de este operador dualidad.

Proposición 1.55 (Propiedades de la dualidad)**.** *Sean E_1, E_2 y E_3 curvas elípticas, entonces se cumple.*

1. (Aditividad) $\widehat{\phi+\psi} = \widehat{\phi} + \widehat{\psi} \qquad \forall \phi, \psi \in \mathrm{Hom}(E_1, E_2)$.
2. (Anticonmutatividad) $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi} \qquad \forall \phi \in \mathrm{Hom}(E_1, E_2), \psi \in Hom(E_2, E_3)$.
3. (Idempotencia) $\widehat{\widehat{\phi}} = \phi \qquad \forall \phi \in \mathrm{Hom}(E_1, E_2)$.
4. ($\mathbb{Z}$-invariancia) $\widehat{m} = m \quad \forall m \in \mathbb{Z}$.

La demostración puede verse en ([**35**], Teo.6.2, pág 86). Observemos que la anticonmutatividad es inmediata de verificar pues $(\widehat{\phi}\circ\widehat{\psi})\circ(\psi\circ\phi) = \widehat{\phi}\circ(\widehat{\psi}\circ\psi)\circ\phi = \widehat{\phi}\circ[\deg(\psi)]\circ\phi = [\deg(\psi)]\widehat{\phi}\circ\phi = [\deg(\psi)][\deg(\phi)] = [\deg(\psi\circ\phi)]$. La $\mathbb{Z}$-invariancia se deduce de la aditividad, utilizando que $\widehat{m+1} = \widehat{m} + \widehat{1}$ y que $\widehat{1} = 1$ que es directo de verificar. La idempotencia se deduce de la $\mathbb{Z}$-invariancia, como $\widehat{\phi}\circ\phi \in \mathbb{Z} \Rightarrow \widehat{\phi}\circ\phi = \widehat{\widehat{\phi}\circ\phi} = \widehat{\phi}\circ\widehat{\widehat{\phi}}$ de donde $\phi = \widehat{\widehat{\phi}}$ (observemos que vale la cancelativa pues $\alpha\beta = 0 \Rightarrow \deg(\alpha)\deg(\beta) = \deg(\alpha\beta) = 0$ luego uno de los mapas tiene grado nulo así que debe ser el mapa nulo y por lo tanto $\alpha = 0$ o $\beta = 0$). Luego la única parte no inmediata es la aditividad donde puede consultarse en la referencia anterior.

3. Curvas ordinarias y supersingulares.

El objetivo de esta sección es mostrar que para el caso de curvas elípticas sobre un cuerpo finito $\mathbb{F}_p$ solo hay dos posibilidades para $\mathrm{End}(E)$ y es que sea isomorfo (como anillo) o bien a un orden en un cuerpo cuadrático imaginario (caso ordinario), o bien a un orden en un álgebra de cuaterniones (caso supersingular). Comenzaremos enunciando un teorema de estructura para $\mathrm{End}(E)$ que será probado en las siguientes dos secciones.

Teorema 1.56 (Estructura de $\mathrm{End}(E)$)**.** *Sea $E/\mathbb{K}$ una curva elíptica y $\mathrm{End}(E)$ su anillo de endomorfismos, se cumplen las siguientes dos propiedades:*

i) $\mathrm{End}(E)$ *es un $\mathbb{Z}-$módulo libre de rango a lo sumo* 4.
ii) *Posee una antiinvolución $\phi \mapsto \widehat{\phi}$ que cumple $\phi\widehat{\phi} \in \mathbb{Z}^+$ para toda isogenia no nula $\phi \in \mathrm{End}(E)$.*

3.1. Estructura de $\mathrm{End}(E)$ como $\mathbb{Z}-$módulo.

En esta parte probaremos la primer parte del teorema de estructura, es decir, que $\mathrm{End}(E)$ es un $\mathbb{Z}-$módulo de rango $r \leq 4$. Probaremos algo un poco más general, que si E_1 y E_2 son curvas elípticas sobre un cuerpo $\mathbb{K}$ entonces $\mathrm{Hom}(E_1, E_2)$ como $\mathbb{Z}-$módulo es libre de rango a lo sumo 4.

La idea principal es conseguir una inmersión de $\mathrm{Hom}(E_1, E_2)$ en un $\mathbb{Z}$-módulo más grande. Quien jugará el papel de ese $\mathbb{Z}$-módulo más grande será $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ donde $T_\ell(E)$ es el ℓ-módulo de Tate de la curva elíptica E que definiremos a continuación.

Definición 1.57. Sea $E[\ell^n]$ el conjunto de puntos de ℓ^n-torsión de la curva elíptica E, donde ℓ es un primo que no divide a la característica de $\mathbb{K}$, definimos el ℓ-módulo de Tate de E como:

$$T_\ell(E) = \varprojlim E[\ell^n]$$

donde el limite inverso se hace respecto de los ℓ-mapas $E[\ell^{n+1}] \to E[\ell^n] : P \mapsto \ell P$.

Es decir, un elemento $P \in T_\ell(E)$ es una sucesión infinita $P = (P_1, P_2, P_3, \ldots)$ donde $P_i \in E[\ell^i]$ y $\ell P_{i+1} = P_i$ para todo $i \in \mathbb{Z}^+$.

Describir la estructura del ℓ-módulo de Tate es muy sencillo: como ℓ no divide a la característica de $\mathbb{K}$ tenemos para la parte de ℓ^n-torsión el isomorfismo $E[\ell^n] \simeq \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$. Cada punto de $E[\ell^n]$ tiene ℓ^2 levantados a $E[\ell^{n+1}]$, en efecto, el kernel del mapa $\pi_n : E[\ell^{n+1}] \to E[\ell^n] : P \mapsto \ell P$ es justamente $E[\ell]$, los puntos de ℓ-torsión, su cardinal es $\#E[\ell] = \#\left(\frac{\mathbb{Z}}{\ell\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}}\right) = \ell^2 = \#E[\ell^{n+1}]/\#E[\ell^n]$ por lo tanto π_n es sobreyectiva y cada elemento de $E[\ell^n]$ tiene ℓ^2 levantados a $E[\ell^{n+1}]$. Observemos además que si $\{P', Q'\}$ es un generador (como $\mathbb{Z}$-módulo) de $E[\ell^n]$ entonces todo levantado $\{P, Q\}$ es un generador de $E[\ell^{n+1}]$, en efecto, si $X \in E[\ell^{n+1}]$ entonces $\ell X \in E[\ell^n]$ por lo tanto existen $\alpha, \beta \in \mathbb{Z}$ tales que $\ell X = \alpha P' + \beta Q'$; por definición de levantado $P' = \ell P$ y $Q' = \ell Q$ así que cancelando ℓ tenemos que $X = \alpha P + \beta Q$ como queriamos probar.

Tomando P_1 y Q_1 tales que $E[\ell] = \frac{\mathbb{Z}}{\ell\mathbb{Z}}P_1 \oplus \frac{\mathbb{Z}}{\ell\mathbb{Z}}Q_1$ y $P, Q \in T_\ell(E)$ tales que $P = (P_1, \ldots)$ y $Q = (Q_1, \ldots)$, por lo visto anteriormente $E[\ell^n] = \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}P_n \oplus \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}Q_n$ y los isomorfismos $\sigma_n : E[\ell^n] \to \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ dado por $aP_n \oplus bQ_n \mapsto (a, b)$ inducen un isomorfismo de grupos $\sigma = (\sigma_n)_{n\geq 1}$ entre $T_\ell(E)$ y $\varprojlim \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$ que a su vez es isomorfo a $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ (vía $((\alpha_n, \beta_n))_{n\geq 1} \mapsto ((\alpha_n)_{n\geq 1}, (\beta_n)_{n\geq 1})$).

Para $\lambda = (\lambda_1, \lambda_2, \ldots) \in \mathbb{Z}_\ell$ y $P = (P_1, P_2, \ldots) \in T_\ell(E)$ podemos definir el producto $\lambda P = (\lambda_1 P_1, \lambda_2 P_2, \ldots)$, es directo verificar que esta sucesión resulta coherente con respecto al ℓ-mapa y por lo tanto $\lambda P \in T_\ell(E)$, de hecho esta operación le da estructura de $\mathbb{Z}_\ell$-módulo a $T_\ell(E)$ y el mapa σ resulta no solo ser un isomorfismo de grupos sino también un morfismo de $\mathbb{Z}_\ell$-módulos.

Ahora vamos a determinar los morfismos entre los ℓ-módulos de Tate de dos curvas elípticas.

Comenzemos por observar que si tenemos una isogenia $\phi \in \mathrm{Hom}(E_1, E_2)$ y si $P \in E_1[\ell^n]$ entonces $\phi(P) \in E_2[\ell^n]$ (pues $\ell\phi(P) = \phi(\ell P) = \phi(\mathcal{O}_1) = \mathcal{O}_2$), luego cada $\phi \in \mathrm{Hom}(E_1, E_2)$ induce un mapa $\phi_{\ell,n} : E_1[\ell^n] \to E_2[\ell^n]$ entre los puntos de ℓ^n-torsión de una y otra curva dado por $\phi_{\ell,n}(P) = \phi(P)$. Así que el mapa $\phi_\ell = (\phi_{\ell,n})_{n\geq 1}$ define un mapa entre los ℓ-módulo de Tate de una y otra curva. En efecto, si $P = (P_1, P_2, \ldots) \in T_\ell(E_1)$ entonces $\ell\phi_{\ell,n+1}(P_{n+1}) = \ell\phi(P_{n+1}) = \phi(\ell P_{n+1}) = \phi(P_n) = \phi_{\ell,n}(P_n)$ y por lo tanto $\phi_\ell(P) = (\phi_{\ell,n}(P_n))_{n\geq 1} \in T_\ell(P)$.

Definición 1.58. Un morfismo entre los ℓ-módulos de Tate de dos curvas elípticas $E_1/\mathbb{K}$ y $E_2/\mathbb{K}$ es un mapa

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

inducido por una isogenia $\phi \in \mathrm{Hom}(E_1, E_2)$ como mostramos anteriormente. Al conjunto de morfismos entre los ℓ-módulo de Tate de E_1 y E_2 lo notaremos por $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$.

El mapa $\Psi_\ell : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ dado por $\phi \mapsto \phi_\ell$ induce una estructura natural de anillo en $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ de forma que ese mapa resulta un morfismo de anillos (en particular de $\mathbb{Z}$-módulos). No es difícil verificar que ψ_ℓ es inyectivo, en efecto, $\phi_\ell \equiv 0$ implica que $E[\ell^n] \subset \ker(\phi)\ \forall n \geq 1$, luego $\phi \equiv 0$ por tener kernel infinito.

Así que conseguimos una inyección de $\mathbb{Z}$-módulos:

$$\Psi_\ell : \mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$

lamentablemente este último módulo es de dimensión infinita como $\mathbb{Z}$-módulo (pues por cardinalidad, $\mathbb{Z}_\ell$ lo es). Por suerte no todo está perdido, tenemos que $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \cong M_{2\times 2}(\mathbb{Z}_\ell)$ (eligiendo una $\mathbb{Z}_\ell$-base para cada uno de los módulos de Tate) que tiene dimensión 4 pero como $\mathbb{Z}_\ell$-módulo. Como $rango_{\mathbb{Z}}(\mathrm{Hom}(E_1, E_2)) \leq rango_{\mathbb{Z}_\ell}(\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell)$ (Corolario C.5 del Apéndice) alcanzaría probar que $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ está inmerso como $\mathbb{Z}_\ell$-módulo en $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ que tiene $\mathbb{Z}_\ell$-rango igual a 4.

Teorema 1.59. *La función Ψ_ℓ anteriormente descripta, se extiende a $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ de la siguiente forma:*

$$\Psi_\ell : \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$$
$$\sum_m \phi^{(i)} \otimes \lambda_i \mapsto \sum_m \lambda_i \phi_\ell^{(i)}$$

Esta extensión continua siendo inyectiva y además resulta un morfismo de $\mathbb{Z}_\ell$-módulos.

Probaremos previamente un resultado sobre módulos finitamente generados como lema.

Lema 1.60. *Si $M \subset \mathrm{Hom}(E_1, E_2)$ es un $\mathbb{Z}-$submódulo finitamente generado entonces el $\mathbb{Z}-$submódulo $M^{div} = \{x \in \mathrm{Hom}(E_1, E_2) : nx \in M \text{ para algún } n \in \mathbb{Z}\}$ también es finitamente generado.*

Demostración del Lema. Recordemos que $\mathrm{Hom}(E_1, E_2)$ es libre de torsión como $\mathbb{Z}-$módulo por lo tanto también lo será M y al ser finitamente generado entonces $M = m_1\mathbb{Z} \oplus m_2\mathbb{Z} \oplus \ldots \oplus m_t\mathbb{Z}$ con $m_i \in M$. Por los teoremas de extensión de generadores y conjuntos l.i. del producto tensorial (ver apéndice), tenemos $M \hookrightarrow M \otimes \mathbb{R} = m_1\mathbb{R} \oplus m_2\mathbb{R} \oplus \ldots \oplus m_t\mathbb{R} \cong \mathbb{R}^t$ (el isomorfismo como espacio vectorial). Veamos que la inyección natural $\iota : M \hookrightarrow M \otimes \mathbb{R}$ dada por $\iota(m) = m \otimes 1$ se extiende a $\iota : M^{div} \hookrightarrow M \otimes \mathbb{R}$. Si $x \in M^{div}$ y $n \in \mathbb{Z}^+$ es tal que $nx \in M$ definimos $\iota(x) = nx \otimes 1/n \in M \otimes \mathbb{R}$. Esta extensión está claramente bien definida puesto que si $x \in M^{div}$ y $n, m \in \mathbb{Z}^+$ son tales que $nx, mx \in M$ se tiene que:

$$nx \otimes 1/n = mnx \otimes 1/nm = mx \otimes 1/m$$

Además si $x, y \in M^{div}$ son tales que $\iota x = \iota y$ entonces $nx \otimes 1/n = my \otimes 1/m$ (donde $n, m \in \mathbb{Z}^+$ son tales que $nx, my \in M$), multiplicando por mn de ambos lados nos queda que $mnx \otimes 1 = nmy \otimes 1$ así que $mnx = nmy$ (ver apéndice) y como $\mathrm{Hom}(E_1, E_2)$ es libre de torsión tenemos que $x = y$, claramente esa inmersión es un morfismo de $\mathbb{Z}-$módulos.

Como $M < \mathrm{Hom}(E_1, E_2)$ entonces la restricción de la forma cuadrática deg define una forma cuadrática en M, por el teorema de extensión de módulos cuadráticos (ver apéndice) esa forma cuadrática se extiende a una $\mathbb{R}-$forma cuadrática $\widehat{\deg} : M \otimes \mathbb{R} \to \mathbb{R}$, que resulta una función continua considerando en $M \otimes \mathbb{R}$ la topología heredada de $\mathbb{R}^t$ a través del isomorfismo (ver apéndice).

Al estar $M^{div} \subset \mathrm{Hom}(E_1, E_2)$ entonces $\deg(x) \in \mathbb{Z}^+$ para todo $x \in M^{div}, x \neq 0$ por lo tanto $\widehat{\deg}^{-1}(-\infty, 1)$ es un abierto de $\mathbb{R}^t = M \otimes \mathbb{R}$ que corta a M^{div} solo en 0, por lo tanto M^{div} es un subgrupo discreto de $\mathbb{R}^t$ y por lo tanto es finitamente generado como $\mathbb{Z}-$módulo.

□

Demostración del Teorema. Para ver que se extiende a un morfismo de $\mathbb{Z}-$módulos dado por la fórmula de arriba, alcanza observar que el mapa $\mathrm{Hom}(E_1, E_2) \times \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2))$ dado por $(\phi, \lambda) \mapsto \phi_\ell \lambda$ es $\mathbb{Z}-$bilineal y equilibrada lo cual es inmediato de verificar. Una vez que sabemos que el mapa Ψ_ℓ está bien definido también es inmediato verificar que es un morfismo de $\mathbb{Z}_\ell-$módulos, solo hace falta chequear la inyectividad.

Tomemos $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ tal que $\phi_\ell \equiv 0$, queremos probar que $\phi \equiv 0$. Sea $\phi = \sum_{i=1}^n \phi_i \otimes \lambda_i = \sum_{i=1}^n \lambda_i \phi_i$ con la identificación usual, donde los $\phi_i \in \mathrm{Hom}(E_1, E_2)$ y $\lambda_i \in \mathbb{Z}_\ell$ para $i = 1, 2, \ldots, n$. Consideremos $M = \sum_{i=1}^n \mathbb{Z}\phi_i$ ($\mathbb{Z}-$módulo finitamente generado de $\mathrm{Hom}(E_1, E_2)$), se tiene que $\phi \in M \otimes \mathbb{Z}_\ell$. Además M^{div} es finitamente generado (por Lema) y libre (por ser $\mathbb{Z}-$submódulo de $\mathrm{Hom}(E_1, E_2)$ que es libre), por lo tanto:

$$M^{div} = \mathbb{Z}\psi_i \oplus \mathbb{Z}\psi_2 \oplus \ldots \oplus \mathbb{Z}\psi_t \qquad \text{con } \psi_1, \psi_2, \ldots, \psi_t \text{ li}/\mathbb{Z}$$

Como $\phi \in M \otimes \mathbb{Z}_\ell \subset M^{div} \otimes \mathbb{Z}_\ell = \mathbb{Z}_\ell\psi_1 \oplus \mathbb{Z}_\ell\psi_2 \oplus \ldots \oplus \mathbb{Z}_\ell\psi_t$ (ver apéndice, propiedad de extensión de base del producto tensorial), así que podemos escribir:

$$\phi = \alpha_1\psi_1 + \alpha_2\psi_2 + \ldots + \alpha_t\psi_t, \quad \alpha_i \in \mathbb{Z}_\ell$$

queremos probar que $\alpha_i = 0$ para $i = 1, 2, \ldots, t$.

Sea $r \in \mathbb{Z}^+$ y sean $a_1, a_2, \ldots, a_t \in \mathbb{Z}$ tales que $a_i \equiv \alpha_i \pmod{\ell^r}$ $\forall i : 1 \leq i \leq t$ (por ejemplo tomar $a_i = r$-ésima coordenada de α_i).

Por la linealidad de Ψ_ℓ tenemos que $\phi_\ell = \alpha_1(\psi_1)_\ell + \alpha_2(\psi_2)_\ell + \ldots + \alpha_t(\psi_t)_\ell$.

Para todo $P \in E[\ell^r]$ el mapa ϕ_ℓ coincide con $a_1(\psi_1)_\ell + a_2(\psi_2)_\ell + \ldots + a_t(\psi_t)_\ell = \eta_\ell$ donde $\eta = a_1\psi_1 + a_2\psi_2 + \ldots + a_t\psi_t \in \mathrm{Hom}(E_1, E_2)$.

Como $\phi_\ell \equiv 0 \Rightarrow \eta(P) = 0 \ \forall P \in E[\ell^r] \Rightarrow ker[\ell^r] \subset ker\eta$ siendo $[\ell^r]$ separable pues $\ell \not| car(\mathbb{K})$ así que por el Teorema de Factorización por inclusión de kernel, existe $\lambda : E_1 \to E_2$ tal que η factoriza como $\eta = \lambda \circ [\ell^r]_{E_1} = [\ell^r] \circ \lambda = \ell^r\lambda \in M$ lo cual implica que $\lambda \in M^{div}$ y por lo tanto:

$$\lambda = b_1\psi_1 + b_2\psi_2 + \ldots + b_t\psi_t \qquad b_i \in \mathbb{Z}$$

Como $\psi_1, \psi_2, \ldots, \psi_t$ son l.i sobre $\mathbb{Z}$ entonces $a_i = \ell^r b_i$ para $i = 1, 2, \ldots, t$ así que $\alpha_i \equiv a_i \equiv 0 \pmod{\ell^r}$, $1 \leq i \leq t$. Es decir, la $r-$ésima coordenada de $\alpha_i = 0$ para todo $r \in \mathbb{Z}^+$, $i = 1, 2, \ldots, t \Rightarrow \alpha_i = 0$ para $i = 1, 2, \ldots, t$ y por lo tanto $\phi = 0$ como queríamos probar.

□

Observación 1.61. El monomorfismo de $\mathbb{Z}_\ell-$módulos dado por el teorema anterior prueba que $rango_{\mathbb{Z}_\ell}\operatorname{Hom}(E_1,E_2)\otimes\mathbb{Z}_\ell \leq rango_{\mathbb{Z}_\ell}(\operatorname{Hom}(T_\ell(E_1),T_\ell(E_2))) = 4$ y como el $\mathbb{Z}-$rango de $\operatorname{Hom}(E_1,E_2)$ no puede superar al $\mathbb{Z}_\ell-$rango de $\operatorname{Hom}(E_1,E_2)\otimes\mathbb{Z}_\ell$ se deduce que $\operatorname{Hom}(E_1,E_2)$ es finitamente generado como $\mathbb{Z}-$módulo (con rango a lo sumo 4). Como consecuencia de esto último tenemos la igualdad $rango_{\mathbb{Z}}(\operatorname{Hom}(E_1,E_2)) = rango_{\mathbb{Z}_\ell}(\operatorname{Hom}(E_1,E_2)\otimes\mathbb{Z}_\ell)$ (Corolario C.5 del Apéndice).

Corolario 1.62. *El anillo* $\operatorname{Hom}(E_1,E_2)$ *es un* $\mathbb{Z}-$*módulo libre de rango a lo sumo* 4 *(lo cual prueba la primer parte del Teorema de estructura para* $\operatorname{Hom}(E_1,E_2)$*).*

3.2. Antiinvolución en $\operatorname{End}(E)$**.** Comenzemos recordando la definición de involución.

Definición 1.63. Sean R y R' dominios integrales de característica 0, una anti-involución de R en R' es una función$\widehat{\ }\colon R\to R'$ que verifica las siguientes tres propiedades:

i) (Linealidad) Para todo $x,y\in R$ y $\alpha,\beta\in\mathbb{Z}$ se cumple que $\widehat{\alpha x+\beta y} = \alpha\widehat{x}+\beta\widehat{y}$.
ii) (Anticonmutatividad) Para todo $x,y\in R$ se cumple que $\widehat{xy} = \widehat{y}\widehat{x}$.
iii) (Idempotencia) Para todo $x\in R$ se cumple que $\widehat{\widehat{x}} = x$.

Decimos que R posee una anti-involución cuando existe una anti-involución$\widehat{\ }\colon R\to R$.

Si E_1 y E_2 son dos curvas elípticas, la dualidad de isogenias define una involución de $\operatorname{Hom}(E_1,E_2)$ en $\operatorname{Hom}(E_2,E_1)$. Recordemos las propiedades de la dualidad enunciadas en la Prop.1.55, observamos que la dualidad cumple la anticonmutatividad e idempotencia. Observemos además que $\widehat{\alpha\widehat{x}} = \widehat{x}\widehat{\alpha} = \alpha\widehat{x}$ donde en la última igualdad se uso la $\mathbb{Z}$-invariancia y la conmutatividad de escalares, esto junto con la aditividad implican linealidad.

En el caso particular que $E_1 = E_2 = E$ tenemos que la dualidad define una antiinvolución en el anillo $\operatorname{End}(E)$.

3.3. Implicancia del Teorema de Estructura. Veamos ahora que solo hay tres posibilidades para $\operatorname{Hom}(E_1,E_2)$ donde E_1 y E_2 son dos curvas elípticas sobre un cuerpo $\mathbb{K}$. El objetivo de esta sección es probar el siguiente teorema:

Teorema 1.64. *Si* R *es un dominio integral de característica* 0 *con las propiedades:*

i) R *es un* $\mathbb{Z}-$*módulo libre de rango a lo sumo* 4*.*
ii) R *posee una ani-involución* $\alpha\mapsto\widehat{\alpha}$ *tal que para todo* $\alpha\in R^*$ *se cumple que* $\alpha\widehat{\alpha}\in\mathbb{Z}^+$*.*

Entonces se tienen las siguientes posibilidades para R*:*

a) $R\cong\mathbb{Z}$*.*
b) $R\cong\mathcal{O}$*, un orden en un cuerpo cuadrático imaginario.*
c) $R\cong\Sigma$*, un orden en un álgebra de cuaterniones.*

Recordemos algunas definiciones.

Definición 1.65 (Orden sobre una $\mathbb{Q}-$álgebra.)**.** Si $\mathcal{K}$ es una $\mathbb{Q}-$álgebra (no necesariamente conmutativa) de dimensión finita (como $\mathbb{Q}-$espacio vectorial), un orden $\mathcal{O}$ en $\mathcal{K}$ es un subanillo de $\mathcal{K}$ que como $\mathbb{Z}-$módulo es libre y finitamente generado y satisface además que $\mathcal{O}\otimes\mathbb{Q}=\mathcal{K}$ (es decir, existe una $\mathbb{Z}-$base $\{r_1,r_2,\ldots,r_t\}$ de R tal que $R=\mathbb{Z}r_1\oplus\mathbb{Z}r_2\oplus\ldots\oplus\mathbb{Z}r_t$ y $\mathcal{K}=\mathbb{Q}r_1\oplus\mathbb{Q}r_2\oplus\ldots\oplus\mathbb{Q}r_t$).

Definición 1.66 (Álgebra de Cuaterniones.)**.** Un álgebra de cuaterniones es un álgebra de la forma:

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

con las reglas multiplicativas:

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

Definición 1.67 (Norma y traza.)**.** Si R es un dominio integral con una anti-involución que verifica las hipótesis del teorema anterior, para $r\in R$ definimos la traza $Tr(r)=r+\widehat{r}$ y la norma $N(r)=r\widehat{r}$.

Proposición 1.68. *Se tiene las siguientes propiedades respecto la traza y la norma:*

i) *La traza $Tr:R\to\mathbb{Z}$ es una función $\mathbb{Z}-$lineal y la norma $N:R\to\mathbb{Z}$ es multiplicativa.*
ii) *La traza y la norma se extienden a $Tr:R\otimes\mathbb{Q}\to\mathbb{Q}$ y $N:R\otimes\mathbb{Q}\to\mathbb{Q}$ de forma que la traza es $\mathbb{Q}-$lineal y la norma sigue siendo multiplicativa.*

Demostración: Para la primera parte comenzemos observando que $N(\alpha)=\alpha\widehat{\alpha}\in\mathbb{Z}$ por hipótesis y con respecto a la traza tenemos:

$$N(\alpha-1)=(\alpha-1)\widehat{(\alpha-1)}=(\alpha-1)(\widehat{\alpha}-1)=\alpha\widehat{\alpha}-(\alpha+\widehat{\alpha})+1=N(\alpha)-Tr(\alpha)+1$$

y por lo tanto $Tr(\alpha)=N(\alpha)-N(\alpha-1)+1\in\mathbb{Z}$.

Ahora la linealidad de la traza, si $n,m\in Z$ y $\alpha,\beta\in R$ se tiene:

$$Tr(n\alpha+m\beta)=(n\alpha+m\beta)+\widehat{(n\alpha+m\beta)}=n\alpha+m\beta+n\widehat{\alpha}+m\widehat{\beta}=n(\alpha+\widehat{\alpha})+m(\beta+\widehat{\beta})$$
$$=nTr(\alpha)+mTr(\beta)$$

Respecto la norma, para $\alpha,\beta\in R$ se tiene:

$$N(\alpha\beta)=(\alpha\beta)\widehat{\alpha\beta}=\alpha(\beta\widehat{\beta})\widehat{\alpha}=\alpha\widehat{\alpha}\beta\widehat{\beta}=N(\alpha)N(\beta)$$

Para ver la segunda parte, basta ver que la anti-involución puede extenderse a $R\otimes\mathbb{Q}$ (o sea ha de verificarse $\widehat{qx}=q\widehat{x},\widehat{x+y}=\widehat{x}+\widehat{y},\widehat{xy}=\widehat{y}\widehat{x}$ y $\widehat{\widehat{x}}=x$ para todo $x,y\in R\otimes\mathbb{Q}$ y $q\in\mathbb{Q}$) y que además para todo $x\in R\otimes\mathbb{Q}$ se verifique $x\widehat{x}\in\mathbb{Q}$. Una vez que tengamos extendida la anti-involución cumpliendo las propiedades anteriormente descritas entonces definimos para $x\in R\otimes Q$, $Tr(x)=x+\widehat{x}$ y $N(x)=x\widehat{x}$. Luego, argumentando como en la parte anterior, se tiene que $Tr:R\otimes\mathbb{Q}\to\mathbb{Q}$ es $\mathbb{Q}-$lineal y $N:R\to\mathbb{Q}$ es multiplicativa y claramente extienden la traza y norma de R.

La función $R\times\mathbb{Q}\to R\otimes\mathbb{Q}$ dada por $(r,q)\mapsto\widehat{r}\otimes q$ es bilineal y balanceada, por lo tanto define un morfismo $\mathbb{Z}-$lineal en $R\otimes\mathbb{Q}$ que será nuestra anti-involución que verifica $\widehat{r\otimes q}=\widehat{r}\otimes q$. Recordemos que al ser $\mathbb{Q}$ el cuerpo de fracciones de $\mathbb{Z}$ todo elemento de $R\otimes\mathbb{Q}$ es de la forma $r\otimes q$ con $r\in R$ y $q\in Q$ (ver apéndice) así que facilmente se verifican

las propiedades, sean $x = r_1 \otimes q_1 \neq 0, y = r_2 \otimes q_2, a \in Z^*$ tales que $aq_1, aq_2 \in \mathbb{Z}$ y $q \in Q$ (si $x = 0$ se verifican trivialmente) se tiene:

i) $\widehat{qx} = \widehat{r_1 \otimes qq_1} = \widehat{r_1} \otimes qq_1$

ii) $\widehat{x+y} = (aq_1r_1 + aq_2r_2) \otimes \frac{1}{a} = aq_1\widehat{r_1 + aq_2r_2} \otimes \frac{1}{a} = (aq_1\widehat{r_1} + aq_2\widehat{r_2}) \otimes \frac{1}{a} = \widehat{r_1} \otimes q_1 + \widehat{r_2} \otimes q_2$
$= \widehat{x} + \widehat{y}$

iii) $\widehat{xy} = r_1\widehat{r_2 \otimes q_1}q_2 = \widehat{r_1r_2} \otimes q_1q_2 = \widehat{r_2}\widehat{r_1} \otimes q_1q_2 = (\widehat{r_2} \otimes q_2)(\widehat{r_1} \otimes q_1) = \widehat{yx}$

iv) $\widehat{\widehat{x}} = \widehat{\widehat{r_1} \otimes q_1} = \widehat{\widehat{r_1}} \otimes q_1 = r_1 \otimes q_1 = x$

Y por último:

v) $x\widehat{x} = (r_1 \otimes q_1)(\widehat{r_1} \otimes q_1) = r_1\widehat{r_1} \otimes q_1^2 = n \otimes q_1^2 = q_1^2 n \in \mathbb{Q}^+$

donde $n = r_1\widehat{r_1} \in \mathbb{Z}^+$ lo cual culmina la prueba.

□

Demostración del Teorema 1.56. Consideremos la $\mathbb{Q}-$álgebra $\mathcal{K} = R \otimes \mathbb{Q}$ y recordemos que $dim_{\mathbb{Q}}(\mathcal{K}) = rango_{\mathbb{Z}}(R) \leq 4$ (ver apéndice). Si el $\mathbb{Z}-$rango de R es 1 tenemos $R \cong \mathbb{Z}$ que es una de las posibilidades, así que supondremos de aquí en más, que el $\mathbb{Z}-$rango de R es mayor que 1 y por lo tanto $\mathcal{K}$ tendrá dimensión al menos 2 como $\mathbb{Q}-$espacio vectorial.

Consideremos la traza, la norma y la anti-involución en $\mathcal{K}$ inducida por la anti-involución en R como en la proposición anterior. Observemos que para todo $\alpha \in \mathcal{K}$ se tiene:

$$(X - \alpha)(X - \widehat{\alpha}) = X^2 - Tr(\alpha)X + N(\alpha) \in \mathbb{Q}[X]$$

por lo tanto, todo elemento de $\mathcal{K}$ tiene grado 2 sobre $\mathbb{Q}$ (recordemos que como $\mathcal{K}$ puede ser no conmutativo, $\mathcal{K}$ no es necesariamente un cuerpo cuadrático). De lo anterior se concluye además que si $\alpha \in \mathcal{K}$ es no nulo con $Tr(\alpha) = 0$ tenemos que $\alpha^2 = -N(\alpha) \in \mathbb{Q}^-$.

Sea $\alpha \in \mathcal{K}, \alpha \notin \mathbb{Q}$, podemos suponer que $Tr(\alpha) = 0$ (en caso contrario tomamos $\beta = \alpha - \frac{1}{2}Tr(\alpha) \notin \mathbb{Q}$ pues $\alpha \notin \mathbb{Q}$ y $Tr(\alpha) \in \mathbb{Q}$ y $Tr(\beta) = Tr(\alpha) - Tr(\frac{1}{2}Tr(\alpha)) = Tr(\alpha) - 2 \cdot \frac{1}{2}Tr(\alpha) = 0$).

Si $\mathcal{K} = \mathbb{Q}(\alpha)$, como $Tr(\alpha) = 0$ y $\alpha \neq 0$ (pues $\alpha \notin \mathbb{Q}$) por la observación previa $\alpha^2 < 0$ y por lo tanto $\mathcal{K}$ es un cuerpo cuadrático imaginario y R es un orden en $\mathcal{K}$.

Si $\mathcal{K} \neq \mathbb{Q}(\alpha)$ tomemos $\gamma \in \mathcal{K}, \gamma \notin \mathbb{Q}(\alpha)$. Observemos que para cualquier $r \in \mathbb{Q}$ tenemos que $\beta = \gamma - \frac{1}{2}Tr(\gamma) - r\alpha \notin \mathbb{Q}(\alpha)$ (pues $\gamma \notin \mathbb{Q}(\alpha)$ y $\frac{1}{2}Tr(\gamma) + r\alpha \in \mathbb{Q}(\alpha)$) y además $Tr(\beta) = Tr(\gamma) - 2 \cdot \frac{1}{2}Tr(\gamma) - rTr(\alpha) = 0$. Queremos que $Tr(\alpha\beta) = 0$, como:

$$Tr(\alpha\beta) = Tr(\alpha\gamma) - \frac{1}{2}Tr(\gamma)Tr(\alpha) - rTr(\alpha^2)$$

dado que $Tr(\alpha^2) = 2\alpha^2 \neq 0$ (pues $\alpha^2 \in \mathbb{Q}$ y $\alpha \neq 0$) podemos elegir r tal que $Tr(\alpha\beta) = 0$.

Resumiendo tenemos que $\alpha, \beta \in \mathcal{K}$ verifican $\alpha^2 < 0, Tr(\alpha) = 0, \beta \notin \mathbb{Q}(\alpha), Tr(\beta) = 0, Tr(\alpha\beta) = 0$ lo cual implica que $\alpha^2 < 0, \beta^2 < 0$ y $\alpha\beta = -\widehat{\alpha\beta} = -\widehat{\beta}\widehat{\alpha} = -(-\beta)(-\alpha) = -\beta\alpha$ (donde en la primera igualdad se usó que $Tr(\alpha\beta) = 0$ y en la tercera que $Tr(\alpha) = 0$ y $Tr(\beta) = 0$) y por lo tanto:

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q} \subset \mathcal{K}$$

es un álgebra de cuaterniones. Vamos a probar que $\mathcal{K} = \mathbb{Q}[\alpha, \beta]$.

Como $\mathcal{K}$ es un $\mathbb{Q}-$espacio vectorial de dimensión a lo sumo 4, alcanza probar que $\{1, \alpha, \beta, \alpha\beta\}$ es l.i. sobre $\mathbb{Q}$. Sean $a, b, c, d \in \mathbb{Q}$ tales que $a + b\alpha + c\beta + d\alpha\beta = a + b\alpha + \beta(c + d\alpha) = 0$, como $\beta \notin \mathbb{Q}[\alpha]$ esto implica que $a + b\alpha = 0$ y $c + d\alpha = 0$, como $\alpha \notin \mathbb{Q}$ esto implica $a = b = 0$ y $c = d = 0$ como queríamos probar.

□

3.4. Caso de curvas elípticas sobre un cuerpo finito $\mathbb{F}_q$. Denotemos como antes $\mathbb{F}_q$ el cuerpo finito de $q = p^s$ elementos con p primo y sea $E/\mathbb{F}_q$ una curva elíptica; veremos que en dicho caso el endomorfismo de Frobenius $\phi = \phi_q$ vive efectivamente en una extensión cuadrática de $\mathbb{Q}$ y por lo tanto $\mathrm{End}(E)$ resulta estrictamente mayor que $\mathbb{Z}$.

3.4.1. La ecuación característica del Frobenius. Recordemos primero que la norma del Frobenius $N(\phi) = \deg(\phi) = q$ (Sección.2.1.3).

Por otra parte en el Cor.5.5, pág.83 de [**35**] se prueba usando un criterio de separabilidad vía diferenciales (Prop.4.2, pág.35 de [**35**]) que los mapa $m + n\phi$ son separables para $m, n \in \mathbb{Z}$ tales que $p \not| m$ y en particular el mapa $\phi - 1$ resulta separable. Aceptando eso calculemos la traza del Frobenius, observamos primero que:

$$P = (x, y) \in ker(\phi - 1) \Leftrightarrow \phi(P) = (x^q, y^q) = (x, y) \Leftrightarrow P \in E(\mathbb{F}_q)$$

y por lo tanto, en virtud de la separabilidad de $\phi - 1$ se tiene que $\deg(\phi - 1) = \#ker(\phi - 1) = \#E(\mathbb{F}_q)$.

Ahora utilizamos la relación $tr(\phi) = N(\phi) - N(\phi - 1) + 1$ vista en la demo. de la Prop.1.69 (pág.40), donde $N = \deg$ y nos queda:

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

donde t es la traza del Frobenius. En resumen, nos queda que $N(\phi) = \widehat{\phi}\phi = q \in \mathbb{Z}$ y $t = tr(\phi) = \widehat{\phi} + \phi = q + 1 - \#E(\mathbb{F}_q) \in \mathbb{Z}$ por lo tanto ϕ (y $\widehat{\phi}$) es raíz del polinomio mónico con coeficientes enteros:

$$X^2 - tX + q = 0$$

que se conoce como ecuación característica del Frobenius.

3.4.2. Forma cuadrática deg *y el Teorema de Hasse.* Comenzemos observando que el par $(\mathrm{End}(E), \deg)$ resulta un grupo cuadrático (definición D.2 del Apéndice), para ello hay que ver que $\deg : E \to \mathbb{Z}$ resulta una forma cuadrática. Como $\deg(-\phi) = \deg(-1)\deg(\phi) = \deg(\phi)$ falta probar la propiedad de bilinealidad, sea entonces $\langle \phi, \psi \rangle = \deg(\phi+\psi) - \deg(\phi) - \deg(\psi)$ y observemos que (Cor.6.8., pág.88 [**35**]):

$$\langle \phi, \psi \rangle = \widehat{(\phi + \psi)}(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = \widehat{\phi}\psi + \widehat{\psi}\phi$$

donde se ha identificado como es usual los mapas $[m]$ con los enteros (vía la inyección $m \mapsto [m]$). De la ecuación anterior es fácil verificar la linealidad respecto a cualquiera de sus dos variables usando la linealidad de la dualidad (sección 3.2). Como además $\deg(\phi) \geq 0$ para todo $\phi \in \mathrm{End}(E)$ con igualdad si y solo si $\phi = 0$, la forma cuadrática deg resulta una forma cuadrática definida positiva y en particular es válida la desigualdad de Cauchy-Schwarz (Teorema D.5 del Apéndice).

Teorema 1.69 (Teorema de Hasse)**.** *La traza de Frobenius cumple* $|t| \leq 2\sqrt{q}$.

Demostración: . Aplicando la desigualdad de Cauchy-Schwarz con el Frobenius ϕ y la identidad 1 nos queda:

$$|\langle \phi, 1 \rangle| \leq 2\sqrt{\deg(\phi)}\sqrt{\deg(1)} = 2\sqrt{q}$$

la conclusión se obtiene observando que $\langle \phi, 1 \rangle = -\langle \phi, -1 \rangle = -(deg(\phi - 1) - \deg(\phi) - 1) = t$

□

Observemos además que si $q = p^s$ con s impar entonces q no puede ser un cuadrado perfecto y la desigualdad será estricta en Cauchy-Schwarz, en ese caso vemos que el polinomio característico de Frobenius (el que aparece en la ecuación característica del Frobenius) tiene discriminante:

$$\Delta = t^2 - 4q = (|t| - 2\sqrt{q})(|t| + 2\sqrt{q}) < 0$$

por la desigualdad de Cauchy-Schwarz y por lo tanto $\mathrm{End}(E)$ será estrictamente mayor que $\mathbb{Z}$ en este caso.

Para el otro caso, cuando $q = p^s$ con $s = 2h$ par, puede darse el caso que la traza del Frobenius $t^2 = 4q$ (cuando $t = 2p^h$) y por la ecuación característica del Frobenius resulta que $\phi = t/2 = p^h \in \mathbb{Z}$ (obs. $p^h = \sqrt{q}$). Este caso de hecho ocurre a veces, pero solamente para el caso supersingular (ver [**22**],Teo.4.10) que es cuando $\mathrm{End}(E)$ resulta un álgebra de cuaterniones, en este caso el Problema del Logaritmo Discreto (PLD) puede transferirse al PLD sobre un cuerpo finito $(\mathbb{F}^*_{q^s}, .)$ con $s \leq 6$ en donde el Index Calculus resuelve el PLD en tiempo subexponencial (la transferencia vale en contextos más generales, pero en el caso de curvas elípticas supersingulares se prueba que la extensión de $\mathbb{F}_q$ de grado a lo sumo 6). Tal ataque es conocido como Frey-Ruck attack, por más detalles puede consultarse en [**17**] o [**10**].

Para algunos casos de curvas ordinarias también se conocen ataques eficientes para el Problema del Logaritmo Discreto (PLD) pero no se conocen ataques generales para este caso. Como nuestro principal interés es estudiar el PLD, podemos restringirnos entonces al caso ordinario.

Capítulo 2

El grafo de Isogenias

En el capítulo previo hemos cubierto gran parte de los preliminares generales, en este capítulo nos centraremos en un objetivo específico que es definir y mostrar las principales propiedades del grafo de j-invariantes y ℓ-isogenias (o simplemente grafo de ℓ-isogenias) donde ℓ será un primo distinto de p, la característica del cuerpo $\mathbb{F}_q$. Dicho grafo será denotado de ahora en más como $\mathcal{G}_{q,N,\ell}$, para ciertos parámetros q, N y ℓ que definiremos a continuación.

El grafo $\mathcal{G}_{q,N,\ell}$ jugará un papel clave en el algorimo de autoreducibilidad aleatoria que trataremos en el capítulo siguiente, el cual es motivador de este trabajo, así que comenzaremos por definir dicho objeto.

1. El grafo de isogenias.

Consideremos un cuerpo finito $\mathbb{F}_q$ de característica p, un entero $N \in \mathcal{I}_q = [q+1-2\sqrt{q}, q+1-2\sqrt{q}]$ en el intervalo de Hasse tal que exista al menos una curva elíptica ordinaria[1] $E/\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = N$ y un primo $\ell \neq p$.

1.1. Definición del grafo de isogenias. Comenzaremos describiendo en primer lugar el conjunto de vértices V del grafo $\mathcal{G}_{q,N,\ell}$, los vértices del grafo vendrán dados por $\mathbb{F}_q$-clases de isomorfismo de curvas elípticas $E/\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = N$, es decir:

$$V = \{[E]_{\mathbb{F}_q} : E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N\}$$

donde $[E]_{\mathbb{F}_q}$ denota la $\mathbb{F}_q$-clase de isomorfismo de la curva elíptica $E/\mathbb{F}_q$.

En otras palabras, los vértices están representados por $\mathbb{F}_q$-clases de isomorfismos de curvas elípticas definidas sobre $\mathbb{F}_q$ que contengan por lo menos algún representante con exactamente N puntos $\mathbb{F}_q$-racionales. Observemos que si $E' \in [E]_{\mathbb{F}_q}$, donde $[E]_{\mathbb{F}_q}$ es un vértice, entonces es claro que E' está definida sobre $\mathbb{F}_q$ (pues E y el isomorfismo entre E y E' lo está) y que $\#E'(\mathbb{F}_q) = N$ (pues el isomorfismo entre E y E' induce un isomorfismo de grupos entre $E(\mathbb{F}_q)$ y $E'(\mathbb{F}_q)$). Por lo tanto cualquier representante de la clase verifica $E'/\mathbb{F}_q$ y $\#E'(\mathbb{F}_q) = N$.

Recordemos que el j-invariante clasifica $\overline{\mathbb{F}_q}$-clases de isomorfismos de curvas elípticas, por lo tanto tenemos bien definida la función $[E]_{\mathbb{F}_q} \mapsto j(E)$ (que también llamaremos j) dado que curvas $\mathbb{F}_q$-isomorfas son en particular $\overline{\mathbb{F}_q}$-isomorfas. El recíproco no es cierto debido a la existencia de twists (ver Sección 1.2.2), por lo tanto no es claro que $j : V \to \mathbb{F}_q$

[1] Casi siempre va a existir alguna curva con esa propiedad, salvo unos pocos casos bien determinados, en virtud del Teorema de Waterhouse (Teoremas 9.10.11 y 9.11.2 de [**19**]).

sea inyectiva (recordar que $E/\mathbb{F}_q \Rightarrow j(E) \in \mathbb{F}_q$).

En el próximo capítulo (más precisamente en el Corolario 3.6) probaremos que si para $E/\mathbb{F}_q$ definimos $j_q(E) = (j(E), \#E(\mathbb{F}_q))$ entonces esta función j_q es un clasificador de $\mathbb{F}_q$-clases de isomorfismo, es decir, para E_1 y E_2 curvas elípticas definidas sobre $\mathbb{F}_q$ se cumple que existe un isomorfismo definido sobre $\mathbb{F}_q$ entre ellas si y solo si $j_q(E_1) = j_q(E_2)$. En consecuencia, si dos vértices $[E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q} \in V$ tienen el mismo j-invariante entonces $j(E_1) = j(E_2)$, pero como $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ resulta que $j_q(E_1) = j_q(E_2)$ y por lo tanto $[E_1]_{\mathbb{F}_q} = [E_2]_{\mathbb{F}_q}$, o sea, tenemos la siguiente proposición.

Proposición 2.1. *La función $V \to \mathbb{F}_q$ dada por $[E]_{\mathbb{F}_q} \mapsto j(E)$ es inyectiva.*

Esa proposición nos permite indexar los vértices de V con elementos de $\mathbb{F}_q$ sin ambigüedad (en el sentido que a vértices distintos corresponden elementos distintos) a través del j-invariante, así que en general cuando usemos que $V \subset \mathbb{F}_q$, estaremos usando la identificación anterior por medio del j-invariante (muchas veces resulta más conveniente representar los vértices como elementos de $\mathbb{F}_q$ en lugar de $\mathbb{F}_q$-clases de isomorfismo de curvas elípticas).

Antes de pasar a describir el conjunto de aristas, vamos a definir una relación de equivalencia entre isogenias.

Definición 2.2. Dos isogenias $\phi_1 : E \to E_1$ y $\phi_2 : E \to E_2$ son equivalentes si existe un isomorfismo $\psi : E_1 \to E_2$ tal que $\phi_2 = \psi\phi_1$.

Observemos que no estamos pidiendo que las isogenias ni el isomorfismo estén definidos sobre $\mathbb{F}_q$. Vamos a denotar por $\sim$ a la relación anterior, que es fácil observar que es una relación de equivalencia. Un criterio útil para decidir cuando dos isogenias son equivalentes lo da el siguiente resultado.

Proposición 2.3. *Sean $\phi_1 : E \to E_1$ y $\phi_2 : E \to E_2$ dos isogenias. Se tiene que $\phi_1 \sim \phi_2 \Leftrightarrow \ker(\phi_1) = \ker(\phi_2)$ y $\deg(\phi_1) = \deg(\phi_2)$.*

Demostración. El directo es evidente mientras que el recíproco es consecuencia del Corolario 1.52 para el caso en que las isogenias ϕ_1 y ϕ_2 sean separables. Para el caso no separable comenzemos observando que:

$$\deg_i(\phi_1) = \frac{\deg(\phi_1)}{\#\ker(\phi_1)} = \frac{\deg(\phi_2)}{\#\ker(\phi_2)} = \deg_i(\phi_2)$$

donde hemos usado que el grado de separabilidad es el cardinal del kernel y el grado es el producto del grado de separabilidad por el de inseparabilidad. Si denotamos por $t = \deg_i(\phi_k)$ para $k = 1, 2$ entonces las isogenias factorizan como $\phi_k = \psi_k \circ f_p^t$ para $k = 1, 2$ donde f_p es el p-Frobenius y ψ_k es una isogenia separable (Sección 2.3.1 del Capítulo 1). Ahora como $\psi_1 : E^{(p^t)} \to E_1$ y $\psi_2 : E^{(p^t)} \to E_2$ son isogenias separables y $\ker(\psi_1) = \ker(\psi_2)$, caemos en el caso separable y tenemos que $\psi_1 = \eta\psi_2$ donde $\eta \in Aut(E_2)$ y por lo tanto $\phi_1 = \psi_1 \circ f_p^t = \eta\psi_2 \circ f_p^t = \eta\phi_2$ lo cual implica que $\phi_1 \sim \phi_2$. □

Observación 2.4. La hipótesis de que las isogenias tengan el mismo grado es fundamental, pues para cualquier isogenia ϕ resulta que $\ker(\phi) = \ker(\phi \circ f_p)$ (donde f_p es el

p-Frobenius) pero $\phi \nsim \phi \circ f_p$ (pues $\deg(\phi \circ f_p) = p\deg(\phi) > \deg(\phi)$).

Ahora vamos a definir las aristas del grafo $\mathcal{G}_{q,N,\ell}$, que será en realidad un multigrafo (es decir, cada arista tiene asociada una multiplicidad).

Si $[E_1]_{\mathbb{F}_q}$ y $[E_2]_{\mathbb{F}_q}$ son dos vértices de $\mathcal{G}_{q,N,\ell}$, decimos que están conectados si $\mathrm{Hom}_\ell(E_1, E_2) \neq \varnothing$, en este caso definimos la multiplicidad de la arista como $\#\frac{\mathrm{Hom}_\ell(E_1,E_2)}{\sim}$ donde $\sim$ es la relación de equivalencia entre isogenias definida anteriormente.

Para ver que la definición anterior tiene sentido debemos probar que si E_1' y E_2' son curvas elípticas isomorfas sobre $\mathbb{F}_q$ a E_1 y E_2 respectivamente entonces $\mathrm{Hom}_\ell(E_1, E_2) \neq \varnothing \Leftrightarrow \mathrm{Hom}_\ell(E_1', E_2') \neq \varnothing$ y $\#\frac{\mathrm{Hom}_\ell(E_1,E_2)}{\sim} = \#\frac{\mathrm{Hom}_\ell(E_1',E_2')}{\sim}$; esto se obtiene como consecuencia directa de la siguiente proposición.

Proposición 2.5. *Sean E_1 y E_2 curvas elípticas, entonces $\#\mathrm{Hom}_\ell(E_1, E_2)$ y $\#\frac{\mathrm{Hom}_\ell(E_1,E_2)}{\sim}$ son finitos y solo dependen de la clase de isomorfismo de E_1 y E_2.*

Demostración. Para ver la finitud, en virtud de la proposición anterior, alcanzaria con ver que solo hay una cantidad finita de posibilidades para el kernel de una ℓ-isogenia $\phi : E_1 \to E_2$. Dicho kernel será un subgrupo de orden ℓ de $E_1[\ell]$ que es finito como observamos en la Sección 2.1.1 del Capítulo 1 y por lo tanto solo habrá un número finito de posibilidades (en la Prop.2.23 se da una versión más precisa de este resultado).

Ahora consideremos dos curvas elípticas E_1' y E_2' tales que existen isomorfismos $\psi_i : E_i \to E_i'$ para $i = 1, 2$. Para demostrar la proposición alcanza con construir una biyección $F : \mathrm{Hom}_\ell(E_1, E_2) \to \mathrm{Hom}_\ell(E_1', E_2')$ que preserve la relación de equivalencia. La función vendrá dada por $F(\phi) = \psi_2\phi\psi_1^{-1}$ es claro que está bien definida (es decir, preserva el grado) y que es biyectiva, vamos a ver que preserva la relación de equivalencia. Si $\phi_1 \sim \phi_2$ entonces existe $\psi \in Aut(E_2)$ tal que $\phi_2 = \psi\phi_1$, por lo tanto $F(\phi_2) = F(\psi\phi_1) = \psi_2\psi\phi_1\psi_1 = \psi_2\psi\psi_2^{-1}\psi_2\phi_1\psi_1 = (\psi_2\psi\psi_2^{-1})F(\phi_1) \sim F(\phi_1)$ como queríamos probar. □

Definición 2.6. Sea $e = ([E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q})$ una arista del grafo de isogenias $\mathcal{G}_{q,N,\ell}$. Definimos la multiplicidad de la arista e como $mult_\ell(e) = \#\frac{\mathrm{Hom}_\ell(E_1,E_2)}{\sim}$. Para simplificar notación definimos $mult_\ell(E_1, E_2) = mult_\ell([E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q})$.

La siguiente cuestión es respecto si el grafo de ℓ-isogenias puede considerarse como grafo no dirigido, vamos a ver que la respuesta es afirmativa en casi todos los casos.

Proposición 2.7. *Supongamos que $p \neq 2, 3$ y sea $([E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q})$ una arista de $\mathcal{G}_{q,N,\ell}$ tal que $j(E_i) \neq 0, 1728$ para $i = 1, 2$. Entonces $mult_\ell(E_1, E_2) = mult_\ell(E_2, E_1)$.*

Demostración. Sean $\phi, \psi \in \mathrm{Hom}_\ell(E_1, E_2)$, observemos que

$$\phi \sim \psi \Leftrightarrow \exists \eta \in Aut(E_2) : \phi = \eta\psi \Leftrightarrow \phi \in Aut(E_2)\psi$$

Por otro lado, si $j(E_2) \neq 0, 1728$, como $car(\mathbb{K}) = p \neq 2, 3$ resulta que $\#Aut(E_2) = 2$ y por lo tanto $Aut(E_2) = \{1, -1\}$.

Luego resulta que $\phi \sim \psi \Leftrightarrow \phi \in \{\psi, -\psi\}$.

En este caso, como $Aut(E_2) \subset \mathbb{Z}$, la dualidad pasa al cociente, es decir, queda bien definida

$$\wedge : \frac{\mathrm{Hom}_\ell(E_1, E_2)}{\sim} \to \frac{\mathrm{Hom}_\ell(E_2, E_1)}{\sim}$$

como función de clases. En efecto, si $\phi_1 \sim \phi_2 \Rightarrow \phi_1 = \pm\phi_2 \Rightarrow \widehat{\phi_1} = \pm\widehat{\phi_2} \Rightarrow \widehat{\phi_1} \sim \widehat{\phi_2}$. Del hecho que $\widehat{\widehat{\phi}} = \phi$ para todo $\phi \in \mathrm{Hom}_\ell(E_2, E_1)$ se deduce la sobreyectividad de la dualidad también a nivel de clases, por lo tanto tenemos que:

$$mult_\ell(E_1, E_2) \geq mult_\ell(E_2, E_1)$$

siempre que $j(E_2) \notin \{0, 1728\}$. En el caso que también $j(E_1) \notin \{0, 1728\}$ entonces vale la otra desigualdad y por lo tanto en este caso se deduce la igualdad $mult_\ell(E_1, E_2) = mult_\ell(E_2, E_1)$. □

Esta proposición nos permite considerar al grafo de isogenias $\mathcal{G}_{q,N,\ell}$ como grafo no dirigido para el caso en que el conjunto de vértices no contenga los j-invariantes 0 y 1728. Generalmente esta es la filosofia adoptada, suponer que se está trabajando en el caso genérico y tratar al grafo $\mathcal{G}_{q,N,\ell}$ como grafo no dirigido (como por ejemplo en el artículo de Jao-Miller-Venkatesan [**24**]).

Observación 2.8. Para toda arista $e = ([E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q})$ de $\mathcal{G}_{q,N,\ell}$ se tiene que $mult_\ell(E_1, E_2) \cdot \#Aut(E_2) = mult_\ell(E_2, E_1) \cdot \#Aut(E_1)$.

Demostración. De la prueba de la proposición anterior se tiene que

$$\frac{\mathrm{Hom}_\ell(E_1, E_2)}{\sim} = \{Aut(E_2)\psi : \psi \in \mathrm{Hom}_\ell(E_1, E_2)\}$$

luego, por propiedad de relación de equivalencia podemos escribir

$$\mathrm{Hom}_\ell(E_1, E_2) = \biguplus_{i+1}^{t} Aut(E_2)\psi \qquad \text{donde } t = mult_\ell(E_1, E_2)$$

de donde $\#\,\mathrm{Hom}_\ell(E_1, E_2) = t \cdot \#Aut(E_2)$ y por lo tanto $mult_\ell(E_1, E_2) \cdot \#Aut(E_2) = \#\,\mathrm{Hom}_\ell(E_1, E_2)$. De la misma forma resulta que $mult_\ell(E_2, E_1) \cdot \#Aut(E_1) = \#\,\mathrm{Hom}_\ell(E_2, E_1)$ y usando la involución canónica resulta que $\#\,\mathrm{Hom}_\ell(E_1, E_2) = \#Hom_\ell(E_2, E_1)$ y por lo tanto $mult_\ell(E_1, E_2) \cdot \#Aut(E_2) = mult_\ell(E_2, E_1) \cdot \#Aut(E_1)$. □

Comentario 2.9 (sobre otra posible definición para el grado[2])**.** Observemos que en realidad la proposición 2.7 es consecuencia de la observación anterior dado que $\#Aut(E) = 2$ siempre que $j(E) \neq \{0, 1728\}$. Otra definición alternativa para el grado (multiplicidad) de una arista podría ser $mult_\ell(E_1, E_2) \cdot \#Aut(E_2)$ en lugar de $mult_\ell(E_1, E_2)$ y de esa forma el grafo de isogenias puede considerarse como grafo no dirigido siempre, incluso que hayan j-invariantes 0 o 1728, con esa definición alternativa para la multiplicidad continuan valiendo las propiedades expansoras que serán probadas en la sección 4.2 y por lo tanto cualquiera de las dos definiciones para el grado son igualmente útiles para nuestro propósito. Continuando con la línea clásica vamos a continuar usando la primer definición para el grado.

[2]Cuidado de no confundir! Cuando nos refiramos al grado de una arista del grafo de isogenias, nos estaremos refiriendo siempre a su multiplicidad como arista del grafo, nunca al grado de las isogenias que representan la arista.

Definición 2.10 (Grafo de ℓ-isogenias)**.** El grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ es el grafo cuyo conjunto de vértices V viene dado por las clases de $\mathbb{F}_q$-isomorfismo de curvas elípticas E con $\#E(\mathbb{F}_q) = N$ y conjunto de aristas $E \subset V^2$ donde $([E_1]_{\mathbb{F}_q}, [E_2]_{\mathbb{F}_q}) \in E \Leftrightarrow$ existe una ℓ-isogenia $\phi : E_1 \to E_2$, la multiplicidad de dicha arista viene dado por $mult_\ell(E_1, E_2) = \#\frac{\mathrm{Hom}_\ell(E_1,E_2)}{\sim}$.

Comentario 2.11 (sobre cálculo eficiente de la multiplicidad de una arista)**.** Con respecto a como calcular efectivamente la multiplicidad de una arista para el grafo $\mathcal{G}_{q,N,\ell}$, una forma posible es a través de un polinomio simétrico con coeficientes enteros $\phi_\ell \in \mathbb{Z}[X, Y]$ llamado polinomio modular, que tiene la propiedad que dada una curva elíptica $E_1/\mathbb{F}_q$ entonces:

$$\{j \in \overline{\mathbb{F}_q} : \phi_\ell(j(E_1), j) = 0\} = \{j(E_2) : E_2 \text{ es } \ell\text{-isógena a } E_1\}$$

Además la multipliciadad de la raíz $j(E_2)$ coincide justamente con la multiplicidad de la arista $(j(E_1), j(E_2))$ en el grafo $\mathcal{G}_{q,N,\ell}$. Más detalles y referencias sobre el polinomio modular, así como métodos para calcularlo, serán dadas en el próximo capítulo (más precisamente en la sección 4.2).

Asociados a los grafos de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$, tenemos los grafos $S_{N,q,B}$ que definiremos a continuación.

Definición 2.12 (El grafo de isogenias $S_{N,q,B}$)**.** Consideremos un entero positivo $B \geq 2$ y sea $L(B) = \{\ell : \ell \text{ es primo}, \ell \leq B\}$. Entonces se define el grafo de isogenias $S_{N,q,B}$ como

$$S_{N,q,B} = \bigcup_{\ell \in L(B)} \mathcal{G}_{q,N,\ell}$$

es decir su conjunto de vértices coincide con el conjunto de vértices de $\mathcal{G}_{q,N,\ell}$ (que no depende del primo ℓ tomado), mientras que dos vértices j_1 y j_2 están conectados en $S_{N,q,B}$ si y solo si existe un primo $\ell \leq B$ tal que j_1 y j_2 están conectados en el grafo $\mathcal{G}_{q,N,\ell}$, en cuyo caso definimos la multiplicidad de la arista $e = (j_1, j_2)$ como:

$$mult(e) = \sum_{\ell \in L(B)} \#\frac{\mathrm{Hom}_\ell(E_1, E_2)}{\sim}$$

donde E_1 y E_2 son curvas elípticas definidas sobre $\mathbb{F}_q$ con $\#E_i(\mathbb{F}_q) = N$ y $j(E_i) = j_i$ para $i = 1, 2$. Vamos a suponer que los grafos $\mathcal{G}_{q,N,\ell}$ son no dirigidos suponiendo que no contienen los j-invariantes 0 o 1728 (observe que el conjunto de vértices de $\mathcal{G}_{q,N,\ell}$ no depende de ℓ) y de esa forma el grafo $S_{N,q,B}$ resulta no dirigido.

Respecto a la conectividad del grafo $S_{N,q,B}$ observemos que a medida que B crece, los grafos $S_{N,q,B}$ (fijados N y q) tendrán cada vez más aristas (en el mismo conjunto de vértices) y es de esperarse que en algún momento se llegue a un grafo conexo. Este hecho puede verse como consecuencia del siguiente Teorema de Tate.

Teorema 2.13 (Tate)**.** *Sean E_1, E_2 dos curvas elípticas sobre $\mathbb{F}_q$, entonces existe una isogenia definida sobre $\mathbb{F}_q$ entre ellas si y solo si $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*

Demostración: Vamos a ver en detalle una de las implicancias (la parte fácil) y dar una idea y referencias para la otra implicancia. La dirección fácil es el directo, suponemos que existe una isogenia $\varphi : E_1 \to E_2$ definida sobre $\mathbb{F}_q$ y queremos probar que las curvas

elípticas poseen el mismo cardinal sobre $\mathbb{F}_q$, o equivalentemente que el Frobenius para E_1 y E_2 tiene la misma ecuación característica (dado que la traza del Frobenius de E es $q+1-\#E(\mathbb{F}_q)$). Sea $x^2-tx+q=0$ la ecuación característica del endomorfismo de q-Frobenius π en E_1, como φ está definida sobre $\mathbb{F}_q$ entonces $\varphi\pi=\pi\varphi$, luego si $Q\in E_2$ consideramos $P\in E_1$ tal que $\varphi(P)=Q$ (recordar que toda isogenia no nula es sobreyectiva) y se tiene:

$$(\pi^2-t\pi+q)Q=(\pi^2-t\pi+q)\varphi(P)=\varphi\left((\pi^2-t\pi+q)P\right)=\varphi(\mathcal{O})=\mathcal{O}$$

donde en la segunda igualdad se usó que φ es una isogenia que conmuta con π, luego el Frobenius π tiene la misma ecuación característica en E_2 lo cual implica, como mencionamos anteriormente, que $\#E_1(\mathbb{F}_q)=\#E_2(\mathbb{F}_q)$.

Para el recíproco, siguiendo la línea de la demostración del artículo de D.Charles [**7**], podemos utilizar una técnica llamada Levantamiento de Deuring (que enunciaremos a continuación) que nos permite llevar el problema a un problema de curvas elípticas complejas (toros complejos) donde es más fácil de atacar, y de esa forma probar la existencia de una isogenia $\varphi:E_1\to E_2$ definida sobre $\mathbb{F}_q$ (en realidad prueba que está definida sobre $\mathbb{F}_q$ salvo $\overline{\mathbb{F}_q}$-isomorfismo, pero esto nos alcanza para nuestros propósitos). Por detalles y referencias puede verse el artículo [**7**] que mencionamos anteriormente.

□

Teorema 2.14 (Levantamiento de Deuring)**.** *Dada una pareja $(\widehat{E}/\mathbb{F}_p,\widehat{\varphi})$ donde $\widehat{E}$ es una curva elíptica ordinaria definida sobre $\mathbb{F}_p$ y $\widehat{\varphi}\in\mathrm{End}(\widehat{E})$ entonces existe una tripleta $(E/\mathbb{L},\varphi,\wp)$ donde E es una curva elíptica definida sobre un cuerpo de números $\mathbb{L}$ (el ring class field del orden $\mathcal{O}=\mathrm{End}(\widehat{E})$), $\varphi\in\mathrm{End}(E)$ y $\wp$ un primo de $\mathbb{L}$ encima de p (o sea $\wp|p$) tal que E y φ reducen a $\widehat{E}$ y $\widehat{\varphi}$ respectivamente, módulo $\wp$.*

Demostración: La demostración es un poco técnica y requiere varios prerrequisitos por lo que no será expuesta aquí, la demostración puede encontrarse en el libro de Lang [**27**], en el Capítulo 13, Teoremas 12 y 14.

□

Corolario 2.15 (del Teorema de Tate)**.** *El grafo $S_{N,q,B}$ es conexo para B suficientemente grande.*

Demostración: (Basada en el Teorema 25.1.2 de [**19**]) Todos los grafos $S_{N,q,B}$ tienen en común el mismo conjunto de vértices $V=\{[E]_{\mathbb{F}_q}:E/\mathbb{F}_q,\#E(\mathbb{F}_q)=N\}$. Como consecuencia de la Proposición 2.1 resulta que $\#V\leq q$ en particular V es un conjunto finito y basta probar que para cualquier par de vértices v y v' existe un $B=B(v,v')$ tal que v y v' son conectables por camino en $S_{N,q,B}$ (luego tomando por ejemplo B_0 como el máximo de los $B(v,v')$ con $(v,v')\in V^2$, resulta que $S_{N,q,B}$ será conexo para todo $B\geq B_0$).

Sean entonces v y v' dos vértices de V y sean E y E' representantes de v y v' respectivamente tales que E y E' están definidos sobre $\mathbb{F}_q$ y $\#E(\mathbb{F}_q)=\#E'(F_q)=N$. Por el Teorema de Tate, sabemos que existe una isogenia $\psi:E\to E'$ de grado n definida sobre $\mathbb{F}_q$, en el sentido que el subgrupo $\ker(\phi)<E(\overline{\mathbb{F}}_q)$ es $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-invariante.

Primero podemos factorizar a $\psi=\phi\circ f_p^r$ donde $\phi:E_0\to E'$ es una isogenia separable ($E_0=E^{p^r}$ la curva que surge de elevar a la p^r todos los coeficientes del polinomio definidor

de la curva E) y f_p en el morfismo de Frobenius (ver Cap.1 Sec.2.3.1). En primer lugar tenemos el camino de isogenias:

$$E \xrightarrow{f_p} E^{(p)} \xrightarrow{f_p} \cdots \xrightarrow{f_p} E^{(p^r)} = E_0$$

Cada una de las curvas $E^{(p^i)}$ está definida sobre $\mathbb{F}_q$ (pues $E/\mathbb{F}_q$ y $E^{(p^i)}$ es elevar los coeficientes de E a la potencia p^i) y además todas tienen el mismo cardinal N sobre $\mathbb{F}_q$, dado que el morfismo de Frobenius induce una biyección $f_p : E^{(p^{i-1})}(\mathbb{F}_q) \to E^{(p^i)}(\mathbb{F}_q)$ (con inversa $f_{q/p}$), por lo tanto cada una de la curvas $E^{(p^i)}$ están en V (en realidad sus clases) para $1 \leq i \leq r$ y están conectadas en $\mathcal{G}_{q,N,p}$ (en particular en $S_{q,N,B}$ para $B \geq p$). Ahora solo resta probar que E_0 y E' son conectables en $S_{N,q,B}$ para algún B adecuado.

Podemos suponer que no existe $m > 1$ tal que $E[m] \subset \ker(\phi)$, en caso contrario podemos tomar el mayor $n \in \mathbb{Z}^+$ tal que $E[n] \subset \ker(\phi)$ y en virtud de la Proposición 1.51 (dado que $[n]$ es separables y $E[n] = \ker([n])$) es posible factorizar $\phi = \psi \circ [n]$ donde $\psi : E_0 \to E'$ es una isogenia, que será también separable (pues ϕ lo es) y definida sobre $\mathbb{F}_q$ (pues $E_0/\mathbb{F}_q$ y $j(E/\ker(\psi)) = j(E') \in \mathbb{F}_q$), por lo tanto bastaria con remplazar ϕ por ψ.

Descomponemos ahora $\deg(\phi) = \ell_1\ell_2 \dots \ell_t$ donde ℓ_i son primos (no necesariamente distintos) para $i = 1, 2, \dots, t$ (recordar que $\deg(\phi) = \#\ker(\phi)$ dado que ϕ es separable).

Por el Teorema de Cauchy, podemos tomar $P_1 \in \ker(\phi)$ de orden ℓ_1, veamos que $\langle P_1 \rangle$ está definido sobre $\mathbb{F}_q$: Consideremos $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, como $\sigma(P) \subset \sigma(\ker(\phi)) = \ker(\phi)$ (pues ϕ está definida sobre $\mathbb{F}_q$) tenemos que $\langle P, \sigma(P) \rangle \subset \ker(\phi)$.

Pero $\ell_1\sigma(P_1) = \sigma(\ell_1 P_1) = \sigma(\mathcal{O}) = \mathcal{O}$ por lo tanto $\langle P, \sigma(P) \rangle \subsetneq E[\ell_1]$ (la inclusión estricta es porque estamos suponiendo que $E[\ell_1] \nsubseteq \ker(\phi)$) luego, dado que el orden de $E[\ell_1]$ es ℓ_1^2 ($\ell_1 \neq p$ pues ϕ es separable), por Lagrange el subgrupo $\langle P, \sigma(P) \rangle$ tiene orden p y por lo tanto $\sigma(P) \in \langle P \rangle$ (es decir, $\langle P_1 \rangle$ está definido sobre $\mathbb{F}_q$).

Luego aplicando nuevamente la Proposición 1.51 podemos factorizar $\phi : E_0 \to E'$ como:

$$E_0 \xrightarrow{\phi_1} E_0/\langle P_1 \rangle = E_1 \xrightarrow{\phi_1'} E'$$

Observemos que la separabilidad de ϕ implica la separabilidad de ϕ_1'. Además como $\langle P_1 \rangle$ está definido sobre $\mathbb{F}_q$ entonces E_1 también (escogiendo un representante adecuado de la clase de isomorfismo) y luego también lo estará ϕ_1' (pues $j(E_1/\ker(\phi_1')) = j(E') \in \mathbb{F}_q$) y $\deg(\phi_1') = \ell_2\ell_3 \dots \ell_t$. Podemos repetir el mismo argumento hecho para ϕ con ϕ_1' y así sucesivamente, obteniendo al final un camino de isogenias:

$$E_0 \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_t} E_t = E'$$

donde cada ϕ_i es una ℓ_i-isogenia definida sobre $\mathbb{F}_q$ (en el sentido que su kernel está definido sobre $\mathbb{F}_q$) y por construcción cada curva E_i estará definida sobre $\mathbb{F}_q$ y además $\#E_i(\mathbb{F}_q) = N$ por la parte fácil del Teorema de Tate. De esa manera la cadena de isogenias anterior induce (tomando clases) un camino en el grafo $S_{q,N,B}$ para $B \geq B_0 := \max\{\ell_i : 1 \leq i \leq t\}$ que conecta $[E_0]_{\mathbb{F}_q}$ con $[E']_{\mathbb{F}_q}$. Por lo tanto para $B \geq \max\{B_0, p\}$ las curvas E y E' estarán conectadas en $S_{N,q,B}$ como queríamos probar.

□

Observación 2.16. En la demostración hemos usado el término "isogenia definida sobre $\mathbb{F}_q$" para referirnos a una isogenia $\phi : E \to E'$ donde E y $\ker(\phi)$ están definidos sobre $\mathbb{F}_q$, esto implica que $\phi(x, y) = \psi \circ \phi_0$ donde ψ es un $\overline{F}_q$-isomorfismo y $\phi_0(x, y) = (f_1(x, y), f_2(x, y))$ donde f_1, f_2 son mapas racionales (por eso a veces es usado el término "isogenia definida sobre $\mathbb{F}_q$ salvo $\mathbb{F}_q$-isomorfismo", cuando queremos recalcar esa diferencia). En el capítulo 3 (el principal de este trabajo), la construcción eficiente de dicho camino de isogenias jugará un papel clave, pero vamos a necesitar además que nuestras isogenias induzcan funciones $\phi : E(\mathbb{F}_q) \to E'(\mathbb{F}_q)$ y para eso necesitamos un poco más, necesitaremos que las isogenias estén compuestas por mapas racionales por lo tanto será necesaria una pequeña modificación en nuestro argumento para crear una versión implementable.

Observación 2.17. En la versión implementable que haremos en el siguiente capítulo vamos a restringirnos al caso en que $q = p$ primo, en este caso el morfismo de Frobenius resulta un endomorfismo y en este caso la igualdad $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ implica que E y E' serán isógenas por una isogenia separable (en virtud del Teorema de Tate y de la Proposición 1.51). En este caso podría omitirse la primer parte de la demostración del Corolario resultando que E y E' conectables para $B \geq B_0$ (en lugar de máx$\{B_0, p\}$), realmente esto es lo que ocurre para este caso, el B que hace que $S_{N,q,B}$ sea conexo es mucho menor que p (cuando $p = q$), esto es clave para que el algoritmo de reducibilidad aleatoria sea eficiente.

En la sección 4 de este capítulo, generalizaremos este resultado (sobre la conectividad de $S_{N,q,B}$) mostrando que en realidad resulta ser un grafo expansor (restringiendonos a cierto subconjunto), que informalmente quiere decir que podemos llegar de un vértice a otro con caminatas al azar con probabilidad no despreciable.

Comentario 2.18 (sobre el grado $S_{N,q,B}$)**.** Una pregunta natural que surge aquí es porque restringirnos a isogenias de grados primos y porque considerar solo aquellas cuyo grado está acotado por cierto B, en otras palabras porque el grafo $S_{N,q,B}$ resulta un objeto interesante de estudiar. Una respuesta parcial a esta pregunta es que, como mencionamos antes, tener un algoritmo que nos permita pasar de una curva a otra por medio de isogenias, será clave para el algoritmo de reducibilidad aleatoria del próximo capítulo y la complejidad de computar una isogenia aumenta a medida que el kernel se vuelve más grande, por esa razón tener una isogenia descompuesta en isogenias de grado pequeño parece ser ventajoso (lo cual justificaria también la cota B) y la máxima descomposición posible se obtiene con isogenias de grado primo (por el Corolario 2.15). Otra razón es que resulta más fácil reconocer curvas que se relacionan por una isogenia de kernel cíclico (a través del polinomio modular) que por una que no lo es, y las isogenias de grado primo necesariamente tienen kernel cíclico.

1.2. Niveles del grafo de isogenias. En su tesis de doctorado, Kohel observó que los anillos de endomorfismos de dos curvas elípticas ordinarias ℓ-isógenas (con ℓ primo) están relacionados por inclusión, en función de esto clasificó las aristas del grafo de isogenia según el tipo de inclusión dándole estructura adicional al grafo de ℓ-isogenias (particionando los vértices en niveles). En esta subsección desarrollaremos el concepto de niveles en el grafo de isogenias y en la siguiente subsección hablaremos más sobre los distintos tipo de isogenias, en función del nivel de salida y el de entrada.

Primeramente, para poder hablar de inclusión entre los anillos de endomorfismo de dos curvas elípticas tenemos que poder ver dichos anillos dentro de un mismo espacio ambiente. Comenzaremos observando que si dos curvas elípticas son isógenas entonces sus anillos de endomorfismos son ordenes para el mismo cuerpo cuadrático imaginario.

En efecto, consideremos una curva elíptica ordinaria E y sea $\varphi : E \to E'$ una isogenia. Sea $\mathcal{O} = \mathrm{End}(E)$ el anillo de endomorfismo de E, que por ser ordinaria resulta ser un orden en un cuerpo cuadrático imaginario $\mathbb{K}$. Por propiedad de órdenes resulta que $\mathbb{K} = \mathcal{O} \otimes \mathbb{Q}$ y se tiene la siguiente inmersión:

$$\iota : \mathcal{O}' = \mathrm{End}(E') \hookrightarrow \mathbb{K} : \psi \mapsto \widehat{\varphi}\psi\varphi \otimes n^{-1} \qquad \text{donde } n = \deg(\varphi)$$

es sencillo probar de hecho que esta inmersión no depende de la isogenia φ ([**25**],pág.44).

Consideremos de esta manera un grafo de isogenias $S_{N,q,B}$ y su conjunto de vértices $V = \{[E]_{\mathbb{F}_q} : E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N\}$ (que no depende de B), escojamos una curva de cada clase $E_0, E_1, \ldots, E_h$ tal que $E_i/\mathbb{F}_q$ y $\#E_i(\mathbb{F}_q) = N$ para $i = 0, 1, \ldots, h$. Por el Teorema de Tate, todas esas curvas son isógenas así que podemos considerar para cada i, $1 \leq i \leq h$ una isogenia $\varphi_i : E_0 \to E_i$ y sus respectivas inmersiones inducidas $\iota_i : \mathcal{O}_i \to \mathbb{K}$ (que no dependen de la elección de la isogenia) donde $\mathcal{O}_i = \mathrm{End}(E_i)$ y $\mathbb{K} = End(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$; o sea, todas los anillos de endomorfismos podemos verlos inmersos dentro del mismo cuerpo cuadrático imaginario $\mathbb{K}$ y de esa forma la inclusión $\mathcal{O}_i \subseteq \mathcal{O}_j$ será entendida como $\iota_i(\mathcal{O}_i) \subseteq \iota_j(\mathcal{O}_j)$.

Comentario 2.19 (consideraciones prácticas)**.** En la práctica, o sea, en el momento de implementar, no es necesario calcular explícitamente las inmersiones ι para decidir si un anillo de endomorfismo está contenido en otro. Recordemos que dados dos órdenes $\mathcal{O}$ y $\mathcal{O}'$ dentro de un mismo cuerpo cuadrático imaginario $\mathbb{K}$ entonces $\mathcal{O} \subset \mathcal{O}'$ si y solo si $d_{\mathcal{O}'} | d_{\mathcal{O}}$ (donde $d_{\mathcal{O}'}$ y $d_{\mathcal{O}}$ son los discriminantes de $\mathcal{O}'$ y $\mathcal{O}$ respectivamente), luego el tipo de inclusión está determinado por la relación de divisibilidad entre sus discriminantes.

Para terminar esta subsección observemos que a curvas isomorfas les corresponde el mismo tipo de órden, en efecto, si $\eta : E \to E'$ es un isomorfismo entre dos curvas elípticas entonces dicho isomorfismo induce un isomorfismo $\mathrm{End}(E') \to \mathrm{End}(E)$ dado por $\varphi \mapsto \widehat{\eta}\varphi\eta$ (es un cálculo directo verificar que es un isomorfismo de anillos). De esa forma el tipo de anillo de endomorfismo, solo va a depender de la clase de isomorfismo de una curva elíptica y entonces a cada clase $v = [E]_{\mathbb{F}_q} \in V$ (que representa un vértice del grafo $S_{N,q,B}$) podemos asociarle su orden $\mathcal{O}_v = \mathrm{End}(E)$. Esta correspondencia no será en general inyectiva, de forma que a varios vértices les puede corresponder el mismo orden (o sea tienen el mismo tipo de anillo de endomorfismo), luego podemos particionar al conjunto V según el tipo de anillo de endomorfismo, formando lo que Kohel llamó de niveles.

Definición 2.20. (Niveles del grafo de isogenias). Un nivel del grafo de isogenia $S_{N,q,B}$ es una clase de equivalencia de vértices, donde dos vértices v_1 y v_2 son equivalentes si y solo si $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$, donde $\mathcal{O}_v$ es el orden asociado al vértice v (es decir $\mathrm{End}(E) \simeq \mathcal{O}_v \ \forall E \in v$).

1.3. Isogenias ascendentes, descendentes y horizontales. Supongamos que $E/\mathbb{F}_q$ es una curva elíptica ordinaria y $\varphi : E \to E'$ una ℓ-isogenia, con ℓ primo. Observemos primero que si $\alpha \in \mathcal{O} = \mathrm{End}(E)$ entonces, denotando por $\mathcal{O}' = \mathrm{End}(E')$ se tienen las

igualdades $\ell^2\alpha = \ell\alpha\ell = (\widehat{\varphi}\varphi)\alpha(\widehat{\varphi}\varphi) = \widehat{\varphi}(\varphi\alpha\widehat{\varphi})\varphi \in \widehat{\varphi}\mathcal{O}'\varphi$ de donde se obtiene la inclusión:

$$\mathbb{Z} + \ell^2\mathcal{O} \subseteq \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi$$

Por otra parte, para todo $\beta \in \mathcal{O}'$ resulta que $\widehat{\varphi}\beta\varphi \in \mathcal{O}$ y por lo tanto $\mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq \mathcal{O}$, que junto con la inclusión anterior resulta en la siguiente cadena de inclusiones:

$$\mathbb{Z} + \ell^2\mathcal{O} \subseteq \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq \mathcal{O}$$

Respecto al índice de la inclusión $\mathbb{Z} + \ell^2\mathcal{O} \subseteq \mathcal{O}$, observemos que $[\mathcal{O}_\mathbb{K} : \mathcal{O}] = f \Rightarrow \mathcal{O} = Z + f\omega_\mathbb{K}\mathbb{Z} \Rightarrow \mathbb{Z} + \ell^2\mathcal{O} = \mathbb{Z} + \ell^2 f\omega_\mathbb{K}\mathbb{Z} \Rightarrow [\mathcal{O}_\mathbb{K} : \mathbb{Z} + \ell^2\mathcal{O}] = \ell^2 f$ de donde $[\mathcal{O} : \mathbb{Z} + \ell^2\mathcal{O}] = \ell^2$, que como ℓ es primo tenemos solo 3 posibilidades para los índices de las inclusiones en la cadena anterior. En función de estas posibilidades Kohel determina las posibilidades para la inclusiones entre los anillos de endomorfismos de dos curvas ℓ-isogenias.

Proposición 2.21. *(Prop.21, pág.44 de* [**25**]*) Sean E y E' dos curvas elípticas definidas sobre $\mathbb{F}_q$, ℓ-isogenias (ℓ primo, $\ell \neq p$), con anillos de endomorfismo $\mathcal{O}$ y $\mathcal{O}'$ respectivamente y sea $\varphi : E \to E'$ una ℓ-isogenia definida sobre $\mathbb{F}_q$. Entonces, denotando por $\subseteq_i$ a una inclusión de índice i, se tienen* 3 *posibilidades:*

- $\mathbb{Z} + \ell^2\mathcal{O} \subseteq_\ell \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq_\ell \mathcal{O} \Rightarrow \mathcal{O} = \mathcal{O}'$.
- $\mathbb{Z} + \ell^2\mathcal{O} \subseteq_1 \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq_{\ell^2} \mathcal{O} \Rightarrow \mathcal{O}' \subseteq \mathcal{O}$ *y* $[\mathcal{O} : \mathcal{O}'] = \ell$.
- $\mathbb{Z} + \ell^2\mathcal{O} \subseteq_{\ell^2} \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi \subseteq_1 \mathcal{O} \Rightarrow \mathcal{O} \subseteq \mathcal{O}'$ *y* $[\mathcal{O}' : \mathcal{O}] = \ell$.

Demostración: En primer lugar podemos ver ambos órdenes inmersos en el mismo cuerpo cuadrático imaginario $\mathbb{K}$ como vimos en la subsección anterior.

Recordemos que el orden de conductor f en $\mathbb{K}$ viene dado por $\mathcal{O} = \mathbb{Z} + f\omega_\mathbb{K}\mathbb{Z}$ donde $\omega_\mathbb{K} = \frac{d_\mathbb{K} + \sqrt{d_\mathbb{K}}}{2}$ ($d_\mathbb{K}$ el discriminante del cuerpo $\mathbb{K}$), luego si $\mathcal{O}$ es el orden de conductor f entonces $\mathbb{Z} + k\mathcal{O}$ es el orden de conductor kf. Llamemos f el conductor de $\mathcal{O}$ y f' el conductor de $\mathcal{O}'$, entonces el conductor de $\mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi = \mathbb{Z} + \ell\mathcal{O}'$ es $\ell f'$.

Denotando por $\mathcal{O}_\mathbb{K}$ el orden maximal, la proposición se sigue de la relación:

$$\ell f' = [\mathcal{O}_\mathbb{K} : \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi] = [\mathcal{O}_\mathbb{K} : \mathcal{O}] \cdot [\mathcal{O} : \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi] = [\mathcal{O} : \mathbb{Z} + \widehat{\varphi}\mathcal{O}'\varphi] \cdot f$$

En efecto, en el primer caso se tiene que $\ell f' = \ell f \Rightarrow f' = f \Rightarrow \mathcal{O}' = \mathcal{O}$, en el segundo caso $\ell f' = \ell^2 f \Rightarrow f' = \ell f \Rightarrow \mathcal{O}' \subseteq_\ell \mathcal{O}$ y en el tercer caso $\ell f' = f \Rightarrow \mathcal{O} \subseteq_\ell \mathcal{O}'$.

□

En función de las posibilidades anteriores se dice que una ℓ-isogenia $\varphi : E \to E'$ es ascendente, descendente u horizontal según $[\mathcal{O} : \mathcal{O}'] = \ell, [\mathcal{O}' : \mathcal{O}] = \ell$ u $\mathcal{O} = \mathcal{O}'$ respectivamente.

Con respecto al grafo de ℓ-isogenias tiene sentido hablar de aristas ascendentes, descendentes u horizontales dado que el anillo de endomorfismo de una curva elíptica $E/\mathbb{F}_q$ solo depende de la clase de isomorfismo (sobre $\overline{\mathbb{F}}_q$).

Definición 2.22. Sean $\varphi : E \to E'$ una arista del grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$. Decimos que φ es ascendente, descendente u horizontal según se tenga $\mathcal{O} \subsetneq \mathcal{O}', \mathcal{O}' \subsetneq \mathcal{O}$ u $\mathcal{O} = \mathcal{O}'$ respectivamente ($\mathcal{O}$ y $\mathcal{O}'$ denota los anillos de endomorfismos de E y E' respectivamente).

1.4. Cantidad de ℓ-isogenias y el piso de racionalidad. Para ir comprendiendo mejor el grafo de ℓ-isogenias, comenzemos acotando el grado de los vértices.

Proposición 2.23. *Sea $E/\mathbb{F}_q$ curva elíptica ordinaria fija y ℓ primo.*

1. *Si $\ell \neq p$ entonces existen exactamente $\ell+1$ isogenias $\phi : E \to E'$ de grado ℓ (salvo isomorfismos y no necesariamente definidas sobre $\mathbb{F}_q$).*

2. *Si $\ell = p$ entonces existen exactamente 2 isogenias (salvo isomorfismo), una puramente inseparable dada por el Frobenius $\phi_p : E \to E^{(p)}$ y la otra es separable y viene dada por la isogenia dual del Frobenius $\widehat{\phi_p} : E \to E^{(q/p)}$ (en este caso ambas están definidas sobre $\mathbb{F}_q$).*

Demostración:

1. Para el caso en que $\ell \neq p$ recordemos que dado $K < E = E(\overline{\mathbb{F}_q})$ con $\#K = \ell$, salvo isomorfismo existe una única isogenia separable $\phi : E \to E/K$ con $\ker(\phi) = K$ entonces hay que ver cuantas posibilidades hay para K (es decir, cuantos subgrupos de orden ℓ tiene E). Observemos que si $K < E, \#K = \ell$ entonces $K \subset E[\ell]$ (Lagrange) donde $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ (Cap.1, Sec.2.1.1, pág.28). Si hubiesen t subgrupos de orden ℓ, como todos ellos deben ser cíclicos (pues ℓ es primo), todo punto salvo $\mathcal{O}$ de $E[\ell]$ tiene orden ℓ y dos de tales subgrupos se intersectan trivialmente (Lagrange) entonces $t(\ell-1) = \ell^2 - 1$ de donde $t = \ell + 1$.

2. Para el caso $\ell = p$ hay que considerar además la posibilidad de que la isogenia no sea separable. Recordemos que toda isogenia $\phi : E \to E'$ factoriza como $\phi = \psi \circ \phi_p^r$ donde ψ es separable y ϕ_p Frobenius. Igualando grados resulta que $p = \deg(\psi)p^r$ y por lo tanto $r = 0$ o $r = 1$. Si $r = 1$ (que es el caso en que ϕ no sea separable) tenemos que ψ resulta ser un isomorfismo y por lo tanto $\phi \sim \phi_p$. Si $r = 0$ entonces ϕ resulta ser separable y su clase de equivalencia queda determinada por su kernel, como E es ordinaria resulta que $E[p]$ es cíclico de orden p (Teorema 3.1, Cap.5 de [**35**]) y por lo tanto tenemos una única isogenia separable que va a estar definida sobre $\mathbb{F}_q$ (pues su kernel $E[p]$ es $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-invariante). Analizando con más detalle se puede obtener una descripción más explícita del mapa separable, para curvas elípticas ordinarias, el dual del Frobenius es separable (implícito en la prueba del Corolario 6.4 del Cap.3 de [**35**] y Teorema 3.1 del Cap.5 de [**35**]), si $E/\mathbb{F}_q$ entonces $E^{(q)} = E$ luego el p-Frobenius en $E^{(q/p)}$ tiene como imagen la curva $E^{(q)} = E$ y su dual $\overline{\phi}_p : E \to E^{(q/p)}$ es una isogenia de grado p separable y como vimos anteriormente, es la única p-isogenia separable partiendo de E salvo equivalencia.

□

Observación 2.24. El salvo isomorfismo de la proposición anterior significa salvo isomorfismos de E', es decir, si $\phi : E \to E'$ y $\nu : E' \to E'$ es un isomorfismo, entonces a ϕ y a $\nu \circ \phi$ las contamos como iguales.

Corolario 2.25. *El grado máximo de los vértices del grafo de ℓ-isogenias es $\ell+1$.*

Demostración: Dada una curva elíptica $E/\mathbb{F}_q$, de las ℓ +1 curvas isógenas pueden haber algunas cuyo j-invariantes no esté en $\mathbb{F}_q$, por lo tanto, cuando tomemos clases para formar el grafo de ℓ-isogenias dichas isogenias no serán contadas y el grado de los vértices en el grafo $\mathcal{G}_{q,N,\ell}$ podría llegar a ser menor estricto que $\ell+1$ (siempre será menor o igual).

□

Observemos que todos los vértices del grafo de ℓ-isogenia $\mathcal{G}_{q,N,\ell}$ contienen, por definición, alguna curva $E/\mathbb{F}_q$ y $\#E(\mathbb{F}_q) = N$ y por tanto su anillo de endomorfismo $\mathcal{O} = \mathrm{End}(E)$ contiene al morfismo de Frobenius $\pi = \pi_q$ (es decir, el morfismo π_q será un endomorfismo puesto que como cada coeficiente de E está en $\mathbb{F}_q$ permanece invariante al ser elevado a la q), como vimos antes, el endomorfismo de Frobenius π verifica la ecuación característica del Frobenius $X^2 - tX + q = 0$ donde $t = q + 1 - N$ y el N es el mismo para cada vértice. En resumen, tenemos el siguiente resultado:

Proposición 2.26. *Los anillos de endomorfismo de las curvas del grafo de isogenia $\mathcal{G}_{q,N,\ell}$ (ó $S_{N,q,B}$ ya que los vértices son los mismos) corresponden con órdenes $\mathcal{O}$ tales que $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}}$, donde π verifica $X^2 - (q + 1 - N)X + q = 0$ (que corresponde con el endomorfismo de Frobenius) y $\mathcal{O}_{\mathbb{K}}$ es el orden maximal. Como consecuencia la cantidad de niveles en el grafo de isogenias resulta a lo sumo[3] la cantidad de órdenes que contienen al orden $\mathbb{Z}[\pi]$; o sea, está acotado superiormente por la cantidad de divisores del conductor de Frobenius $f_\pi = [\mathcal{O}_k : \mathbb{Z}[\pi]]$.*

Demostración: La primera parte ya la vimos. Para la segunda se usa simplemente que si $\mathcal{O}$ es un orden en el cuerpo imaginario $\mathbb{Q}[\pi]$, entonces $\mathcal{O}$ contiene a $\mathbb{Z}[\pi]$ si y solo si su conductor $f = [\mathcal{O}_K : \mathcal{O}]$ divide al conductor de π.

□

Ahora definiremos algunas nomenclaturas que son comunes (y otras quizás no tanto) en la literatura.

Definición 2.27 (Piso de racionalidad)**.** Decimos que una curva $E/\mathbb{F}_q$ está en el piso de racionalidad cuando se verifica la igualdad $\mathrm{End}(E) = \mathbb{Z}[\pi]$, donde π denota el q-Frobenius. En el grafo de isogenias $S_{N,q,B}$ decimos que un vértice $v = [E]_{\mathbb{F}_q}$ está en el piso de racionalidad si E lo está (claramente no depende del representante), o sea, en virtud de la Proposición 2.26, el piso de racionalidad corresponde al nivel más pequeño (si ordenamos los niveles por inclusión).

La siguiente observación es consecuencia directa de la Proposición 2.26 y la definición de isogenia descendente.

Observación 2.28. Si $E/\mathbb{F}_q$ está en el piso de racionalidad, entonces (su clase) no posee aristas descendentes en el grafo de isogenias $S_{N,q,B}$ (donde $N = \#E(\mathbb{F}_q)$).

Definición 2.29 (Superficie o cráter)**.** Decimos que una curva $E/\mathbb{F}_q$ está en la superficie (o cráter[4]) cuando se verifica la igualdad $\mathrm{End}(E) = \mathcal{O}_{\mathbb{K}}$. En el grafo de isogenias $S_{N,q,B}$ decimos que un vértice $v = [E]_{\mathbb{F}_q}$ está en la superficie si E lo está (claramente no depende del representante), o sea, en virtud de la Proposición 2.26, la superficie corresponde al

[3]El "a lo sumo" es porque podrían haber órdenes $\mathcal{O}$ con $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}}$ tal que no exista ningún vértice $j(E)$ en el grafo $\mathcal{G}_{q,N,\ell}$ tal que $\mathrm{End}(E) = \mathcal{O}$. Esto en realidad nunca sucede como quedará claro una vez visto el Teorema de Kohel (Teorema 2.38), de modo que la cantidad de niveles coincide con la cantidad de órdenes intermedios entre $\mathbb{Z}[\pi]$ y $\mathcal{O}$, o sea la cantidad de divisores del conductor del Frobenius.

[4]El nombre viene de que cuando dibujamos el grafo de isogenias para el caso no degenerado, ordenando por altura los niveles, el grafo de ℓ-isogenias tiene forma de cráter (ver el ejemplo mostrado en la sección siguiente).

nivel más grande (si ordenamos los niveles por inclusión).

El análogo a la Observación 2.28 sería:

Observación 2.30. Si $E/\mathbb{F}_q$ está en la superficie, entonces (su clase) no posee aristas ascendentes en el grafo de isogenias $S_{N,q,B}$ (donde $N = \#E(\mathbb{F}_q)$).

Las definiciones anteriores respecto del grafo de isogenias $S_{N,q,B}$ varian ligeramente cuando queremos estudiar localmente el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$.

Definición 2.31 (Piso de racionalidad respecto de ℓ)**.** Decimos que una curva $E/\mathbb{F}_q$ está en el piso de racionalidad respecto de ℓ cuando se verifica $\nu_\ell([\mathcal{O}_\mathbb{K} : \mathrm{End}(E)]) = \nu_\ell([\mathcal{O}_\mathbb{K} : \mathbb{Z}[\pi])$, donde π denota el q-Frobenius y ν_ℓ la valuación ℓ-ádica (o sea $\nu_\ell(n)$ es el exponente de ℓ en la descomposición factorial de n). En el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ decimos que un vértice $v = [E]_{\mathbb{F}_q}$ está en el piso de racionalidad (respecto de ℓ) si E lo está (claramente no depende del representante).

Observación 2.32. Si $E/\mathbb{F}_q$ está en el piso de racionalidad respecto de ℓ, entonces (su clase) no posee aristas descendentes en el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ (donde $N = \#E(\mathbb{F}_q)$).

Definición 2.33 (Superficie o cráter respecto de ℓ)**.** Decimos que una curva $E/\mathbb{F}_q$ está en la superficie (o cráter) respecto de ℓ, cuando $\nu_\ell(\mathrm{End}(E)) = \nu_\ell(\mathcal{O}_\mathbb{K})$. En el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ decimos que un vértice $v = [E]_{\mathbb{F}_q}$ está en la superficie si E lo está (claramente no depende del representante).

Observación 2.34. Si $E/\mathbb{F}_q$ está en la superficie, entonces (su clase) no posee aristas ascendentes en el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ (donde $N = \#E(\mathbb{F}_q)$).

Definición 2.35 (Caso degenerado o genérico y caso no degenerado)**.** Decimos que el grafo de ℓ-isogenias es degenerado (ó genérico) cuando $\ell \nmid [\mathcal{O}_\mathbb{K} : \mathbb{Z}[\pi]]$, en ese caso (en virtud de la Proposición 2.21) todas las aristas en el grafo $\mathcal{G}_{q,N,\ell}$ serán horizontales (es en realidad el caso más importante para nosotros). Cuando $\ell \mid [\mathcal{O}_\mathbb{K} : \mathbb{Z}[\pi]]$ decimos que el grafo $\mathcal{G}_{q,N,\ell}$ es no degenerado.

Definición 2.36 (Grado vector y grado)**.** En el grafo $\mathcal{G}_{q,N,\ell}$ usaremos la notación $Gr(E) = (gr_a(E), gr_h(E), gr_d(E))$ para indicar que la cantidad de ℓ-isogenias ascendentes $\phi : E \to E'$ es $gr_a(E)$, la cantidad de ℓ-isogenias horizontales $\phi : E \to E'$ es $gr_h(E)$ y la cantidad de ℓ-isogenias descendentes $\phi : E \to E'$ es $gr_d(E)$ (las isogenias son contadas al menos de equivalencia). El grado simplemente será denotado por $gr(E) = gr_a(E) + gr_h(E) + gr_d(E)$.

1.5. El Teorema de Kohel. El objetivo de esta subsección es obtener una fórmula explícita para el grado vector. Comenzaremos probando un lema sobre órdenes en cuerpos cuadráticos imaginarios que nos será de utilidad.

Lema 2.37. *Sean* $\tau \in \mathbb{C} \setminus \mathbb{R}$ *y* $\mathrm{End}(\tau) = \{\alpha \in \mathbb{C} : \alpha\langle 1, \tau\rangle \subseteq \langle 1, \tau\rangle\}$ *(donde* $\langle x, y\rangle = x\mathbb{Z}+y\mathbb{Z}$ *es el* $\mathbb{Z}$*-módulo generado por* x *e* y*). Supogamos que* $\mathrm{End}(\tau) = \mathcal{O}$ *un orden en un cuerpo cuadrático imaginario y que* τ *verifica una ecuación* $a\tau^2 + b\tau + c = 0$ *con* $a, b, c \in \mathbb{Z}$ *y* $mcd(a, b, c) = 1$ *entonces* $d_{\mathcal{O}} = b^2 - 4ac$ *(donde* $d_{\mathcal{O}}$ *denota el discriminante del orden* $\mathcal{O}$*).*

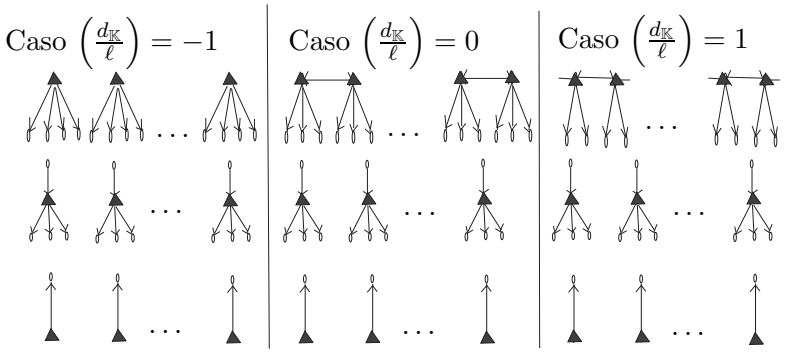
Demostración: Se pueden verificar las cuentas directamente aunque la forma más corta es hacer uso del Teorema 7.7 de ([**11**], pág.137), si consideramos la forma cuadrática $f(x, y) = ax^2 + bxy + cy^2$ que será primitiva (pues $mcd(a, b, c) = 1$) y definida positiva ($a \neq 0$ pues $\tau \notin \mathbb{R}$ así que $\tau = \frac{-b+\sqrt{D}}{2a} \in \mathrm{End}(\tau) = \mathcal{O} \subset \mathbb{K}$ con $\mathbb{K}$ cuerpo cuadrático imaginario y por lo tanto $D = b^2 - 2ac < 0$), el Teorema 7.7 de ([**11**]) nos dice que el $\mathbb{Z}$-módulo $a\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z} = a\langle 1, \tau\rangle$ es un ideal (fraccionario) propio del orden $\mathcal{O}_D$ de discriminante $D \Rightarrow \mathrm{End}(\tau) = \{\alpha \in \mathbb{C} : \alpha \cdot a\langle 1, \tau\rangle \subseteq \langle 1, \tau\rangle\} = \mathcal{O}_D$ y por lo tanto $\mathcal{O} = \mathcal{O}_D$ el orden de discriminante D.

□

Teorema 2.38 (Kohel [**25**])**.** *Sea* E *una curva elíptica con* $j(E) \in \mathbb{F}_q$ *y* ℓ *un primo distinto de* p*, entonces en el caso no degenerado se tiene que:*

$$Gr(E) = \begin{cases} \left(0, 1 + \left(\frac{d_{\mathbb{K}}}{\ell}\right), \ell - \left(\frac{d_{\mathbb{K}}}{\ell}\right)\right) & \text{si } E \text{ está en la superficie} \\ (1, 0, \ell) & \text{si } E \text{ está en la zona media} \\ (1, 0, 0) & \text{si } E \text{ está en el piso} \end{cases}$$

Mientras que en el caso degenerado solo hay aristas horizontales y se tiene que $gr(E) = 1 + \left(\frac{d_{\mathbb{K}}}{\ell}\right)$.



Demostración (basada en la prueba del Teo.4, Apéndice 11.5 de [**16**]*):* Sea $E/\mathbb{F}_q$ con anillo de endomorfismo $\mathrm{End}(E) = \mathcal{O}$ un orden en un cuerpo cuadrático imaginario, si denotamos por $\mathcal{O}_{\mathbb{K}}$ y $\mathbb{Z}[\pi]$ el orden maximal y el orden generado por el frobenius $\pi \in \mathrm{End}(E)$ tenemos las inclusiones $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\mathbb{K}}$.

Usando el levantamiento de Deuring obtenemos una curva elíptica compleja $E/\mathbb{L}$ ($\mathbb{L}$ un cuerpo de números) con anillo de Endomorfismo $\mathcal{O}$, componiendo con un isomorfismo de ser necesario podemos suponer que $E = \mathbb{C}/\Lambda$ con $\Lambda = \langle 1, \tau\rangle$ (todo toro complejo puede llevarse a esa forma a través de una rotohomotecia), además por Lema 2.37 τ verifica una ecuación de la forma $A\tau^2 + B\tau + C = 0$ con $A, B, C \in \mathbb{Z}$ con $mcd(A, B, C) = 1$ y $discr(\mathcal{O}) = D = B^2 - 4AC$.

La idea va a ser probar el resultado para $E = \mathbb{C}/\Lambda$, luego reduciendo obtenemos el resultado para una curva en la clase de isomorfismos de E y de esa forma determinamos el grado vector para el j-invariante de E en el grafo de ℓ-isogenias correspondiente.

Consideremos las isogenias $\phi_i : \frac{\mathbb{C}}{\Lambda} \to \frac{\mathbb{C}}{\Lambda_i}$ dadas por $z + \Lambda \mapsto z + \Lambda_i$ donde $\Lambda_0 = \langle \frac{1}{\ell}, \tau \rangle$ y $\Lambda_k = \langle 1, \frac{\tau+k}{\ell} \rangle$ para $k = 1, 2, \ldots, \ell$ son superláttices de Λ de índice ℓ (no es difícil de verificar que $\Lambda \subset \Lambda_k$ para $0 \leq k \leq \ell$ y que los mapas $\frac{\Lambda_0}{\Lambda} \to \frac{\mathbb{Z}}{\ell\mathbb{Z}} : \frac{a}{\ell} + b\tau + \Lambda \mapsto a \pmod{\ell}$ y $\frac{\Lambda_k}{\Lambda} \to \frac{\mathbb{Z}}{\ell\mathbb{Z}} : a + \left(\frac{\tau+i}{\ell} b + \Lambda\right) \mapsto b \pmod{\ell}$ para $1 \leq k \leq \ell$ están bien definidos y son biyectivos).

Para probar que las curvas elípticas $E_i = \frac{\mathbb{C}}{\Lambda_i}$ son un conjunto de representantes de las curvas ℓ-isógenas a E salvo isomorfismo recordamos que el kernel de una isogenia determina la clase de isomorfismo de la isogenia (y por lo tanto de la curva de llegada) y como hay $\ell + 1$ de tales clases (Prop.2.23) alcanza con probar que las isogenias ϕ_i tienen todas kerneles distintos.

En efecto, como $ker(\phi_i) = \frac{\Lambda_i}{\Lambda}$ para probar que $\frac{\Lambda_0}{\Lambda} \neq \frac{\Lambda_i}{\Lambda}$ observemos que $\frac{1}{\ell} + \Lambda \notin \{n + m\left(\frac{\tau+k}{\ell}\right) + \Lambda\}$ pues si $\frac{1}{\ell} - \left(n + m\left(\frac{\tau+k}{\ell}\right)\right) = \frac{1-mi-n\ell}{\ell} - \frac{m}{\ell}\tau \in \Lambda = \mathbb{Z} + \tau\mathbb{Z}$ con $m, n \in \mathbb{Z}$ como $\{1, \tau\}$ es ℓ.i. sobre $\mathbb{R}$ entonces $mi \equiv 1 \pmod{\ell}$ y $m \equiv 0 \pmod{\ell}$ lo cual es imposible. Con un razonamiento similar para ver que $\frac{\Lambda_i}{\Lambda} \neq \frac{\Lambda_j}{\Lambda}$ con $1 \leq i < j \leq \ell$ basta observar que $\frac{\tau+i}{\ell} - \left(n + m\left(\frac{\tau+j}{\ell}\right)\right) = \frac{i-mj-n\ell}{\ell} + \frac{1-m}{\ell}\tau \in \Lambda$ con $m, n \in \mathbb{Z} \Rightarrow \begin{cases} m \equiv 1 \pmod{\ell} \\ i \equiv mj \pmod{\ell} \end{cases} \Rightarrow i \equiv j \pmod{\ell}$ lo cual es absurdo puesto que $1 \leq i < j \leq \ell$.

Ahora veamos cuantas isogenias de cada tipo hay según $\mathrm{End}(E_i)$ (o lo que es lo mismo, según su discriminante D_i) descartando las isogenias descendentes en el caso que E esté en el piso de racionalidad (ya que las curvas de llegadas corresponderian a j-invariantes que no están en $\mathbb{F}_q$ por la observación 2.32).

Observemos que $E_0 \simeq \frac{\mathbb{C}}{\langle 1, \ell\tau \rangle}$ donde $A(\ell\tau)^2 + B\ell(\ell\tau) + \ell^2 C = 0$ y dado que $mcd(A, B, C) = 1$ resultan tres posibilidades para $d = mcd(A, B\ell, \ell^2 C) = 1, \ell$ o ℓ^2. Como $(B\ell)^2 - 4A(\ell^2 C) = \ell^2 D$ resulta que $D_0 = \ell^2 D$ si $d = 1$ (isogenia descendente), $D_0 = D$ si $d = \ell$ (isogenia horizontal) o $D_0 = \frac{D}{\ell^2}$ si $d = \ell^2$ (isogenia ascendente).

Para $1 \leq k \leq \ell$ tenemos que $E_k = \frac{\mathbb{C}}{\langle 1, \frac{\tau+k}{\ell} \rangle}$ donde $x = \frac{\tau+k}{\ell}$ verifica $A(\ell x - k)^2 + B(\ell x - k) + C = A\ell^2 x^2 - (2Ak - B)\ell x + (Ak^2 - Bk + C) = 0$ y dado que $mcd(A, B, C) = 1 \Rightarrow mcd(A, 2Ak - B, Ak^2 - Bk + C) = 1 \Rightarrow d = mcd(A\ell^2, (2Ak - B)\ell, Ak^2 - Bk + C) = 1, \ell$ o ℓ^2. Como $((2Ak - B)\ell)^2 - 4(A\ell^2)(Ak^2 - Bk + C) = \ell^2 D$ resulta que $D_k = \ell^2 D$ si $d = 1$ (isogenia descendente), $D_k = D$ si $d = \ell$ (isogenia horizontal) o $D_k = \frac{D}{\ell^2}$ si $d = \ell^2$ (isogenia ascendente).

Denotemos por $f(k) = Ak^2 - Bk + C$ y analizemos primero el caso no degenerado $(\ell | [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\pi]])$:

I) Caso en que E esté en la superficie: Vamos a separar aquí 5 casos, cada caso representará una posibilidad para el símbolo de Legendre $\left(\frac{d_{\mathbb{K}}}{\ell}\right)$. Recordemos que $D = [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]^2 d_{\mathbb{K}}$

que como $\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$ pues E está en la superficie resulta que $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = \left(\frac{D}{\ell}\right)$.

Caso 1) $A \neq \dot{\ell}, \left(\frac{D}{\ell}\right) = -1$ (corresponde a $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = -1$):

En este caso $mcd(A, B\ell, \ell^2 C) = 1$ por lo que $E \to E_0$ es descendente. Como $\left(\frac{D}{\ell}\right) = -1$ el polinomio f no posee raices módulo ℓ por lo tanto para $1 \leq k \leq \ell$ resulta que $f(k) \neq \dot{\ell}$ lo cual implica que $mcd(A\ell^2, (2Ak - B)\ell, f(k)) = 1$ y por lo tanto todas las isogenias $E \to E_k$ serán también descendentes para $k = 1, 2, \ldots, \ell$.

Caso 2) $A \neq \dot{\ell}, \left(\frac{D}{\ell}\right) = 0$ (corresponde a $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 0$):

Al igual que el caso anterior $E \to E_0$ será descendente, pero esta vez el polinomio f tiene raíz doble $\frac{B}{2A}$ módulo ℓ (usamos aquí también que $\ell \neq 2$). Sea k_0 el único entero k con $1 \leq k \leq \ell$ tal que $k \equiv \frac{B}{2A} \pmod{\ell}$.

Si $k \neq k_0, 1 \leq k \leq \ell$ entonces $f(k) \neq \dot{\ell}$ así que $mcd(A\ell^2, (2Ak - B)\ell, f(k)) = 1$ y las isogenias $E \to E_k$ serán descendentes también (hay $\ell - 1$ valores de k).

Si $k = k_0$ entonces $mcd(A\ell^2, (2Ak_0 - B)\ell, f(k_0)) = \ell$ o ℓ^2 pero el segundo caso implicaría una isogenia ascendente desde E lo cual es imposible si E está en la superficie por lo tanto $mcd(A\ell^2, (2Ak_0 - B)\ell, f(k_0)) = \ell$ y $E \to E_{k_0}$ será horizontal.

Caso 3) $A \neq \dot{\ell}, \left(\frac{D}{\ell}\right) = 1$ (corresponde a $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$):

También aquí como $A \neq \dot{\ell}$ la isogenia $E \to E_0$ será descendente. Esta vez el polinomio f tendrá dos raices simples módulo ℓ (pues $\ell \neq 2$) que llamaremos k_1 y k_2 con $1 \leq k_1 < k_2 \leq \ell$.

Para $k \neq k_1, k_2$, $1 \leq k \leq \ell$ tenemos que $f(k) \neq \dot{\ell}$ y como vimos en el caso anterior las correspondientes isogenias $E \to E_k$ serán descendentes (hay $\ell - 2$ valores de k).

Por otra parte $mcd(A\ell^2, (2Ak_i - B)\ell, f(k_i)) = \ell$ o ℓ^2 para $i = 1, 2$ pero el segundo caso implica la existencia de una isogenia ascendente desde E que está en la superficie por lo tanto $mcd(A\ell^2, (2Ak_i - B)\ell, f(k_i)) = \ell$ y las isogenias $E \to E_{k_i}$ será horizontales para $i = 1, 2$.

Caso 4) $A = \dot{\ell}, B \neq \dot{\ell}$ (corresponde a $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$) ya que $D \equiv B^2 \pmod{\ell}$ y $B \neq \dot{\ell}$):

En este caso $mcd(A, B\ell, \ell^2 C) = \ell$ por lo que $E \to E_0$ será horizontal. El polinomio $f(k) = -Bk + C \pmod{\ell}$, como $B \neq \dot{\ell}$ tendrá una única raíz módulo ℓ, llamemos k_0' a la única raíz módulo ℓ en el conjunto $\{1, 2, \ldots, \ell\}$.

Si $k \neq k_0'$, $1 \leq k \leq \ell$ entonces $f(k) \neq \dot{\ell}$ y las correspondientes isogenias $E \to E_k$ serán descendentes (hay $\ell - 1$ valores de k).

Si $k = k_0'$ como $mcd(A\ell^2, (2Ak_0' - B)\ell, f(k_0')) = \ell$ o ℓ^2 y no hay isogenias ascendentes desde E, deducimos como en los casos anteriores que $E \to E_{k_0'}$ es horizontal.

Caso 5) $A = \dot{\ell}, B = \dot{\ell}$ (corresponde a $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 0$):

En este caso $mcd(A, B\ell, \ell^2 C) = \ell$ o ℓ^2 pero el segundo caso implica que $E \to E_0$ sea ascendente, lo cual es imposible si E está en la superficie, así que en este caso $E \to E_0$ resulta horizontal.

Como $mcd(A, B, C) = 1$ resulta que $C \neq \dot{\ell}$ así que $f(k) \equiv C \not\equiv 0 \pmod{\ell}$ $\forall k = 1, 2, \ldots, \ell$ y por lo tanto $mcd(A\ell^2, (2Ak - B)\ell, f(k)) = 1$ y $E \to E_k$ resultan ser todas descendentes para $1 \leq k \leq \ell$.

En resumen, juntando los 5 casos anteriores resulta que

$$Gr(E) = \begin{cases} (0, 0, \ell + 1) & \text{si } \left(\frac{d_{\mathbb{K}}}{\ell}\right) = -1 \\ (0, 1, \ell) & \text{si } \left(\frac{d_{\mathbb{K}}}{\ell}\right) = 0 \\ (0, 2, \ell - 1) & \text{si } \left(\frac{d_{\mathbb{K}}}{\ell}\right) = -1 \end{cases}$$

Ambos casos pueden resumirse en $Gr(E) = \left(0, 1 + \left(\frac{d_{\mathbb{K}}}{\ell}\right), \ell - \left(\frac{d_{\mathbb{K}}}{\ell}\right)\right)$.

II) Caso en que E esté en la zona media: Comenzemos observando que de los 5 casos discutidos para el caso anterior, los casos 1,3 y 4 implican $\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$ (puesto que $\ell \nmid D = [\mathcal{O}_K : \mathcal{O}]^2 d_{\mathbb{K}}$) y por lo tanto no pueden darse en este caso.

Caso 2) $A \neq \dot{\ell}, \left(\frac{D}{\ell}\right) = 0$: El mismo argumento que usamos para el caso en que E estaba en la superficie sirve para probar que las isogenias $E \to E_k$ son todas descendentes para $k \neq k_0$, donde k_0 es el único entero $1 \leq k_0 \leq \ell$ que verifica $k_0 \equiv \frac{B}{2A} \pmod{\ell}$.

Para $k = k_0$ el argumento aquí es un poco distinto, como E no está en la superficie resulta que $\ell | [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$ lo cual implica que $\ell^2 | D = [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]^2 d_{\mathbb{K}}$ así que $4Af(k_0) = (2Ak_0 - B)^2 - D = \dot{\ell}^2$ (ya que $k_0 \equiv \frac{B}{2A} \pmod{\ell} \Rightarrow 2ak_0 - B = \dot{\ell}$). Como $A \neq \dot{\ell}$ y $\ell \neq 2$ resulta que $f(k_0) = \dot{\ell}$ lo cual implica que $mcd(A\ell^2, (2Ak_0 - B)\ell, f(k_0)) = \ell^2$ y por lo tanto la isogenia $E \to E_{k_0}$ será ascendente.

Caso 5) $A = \dot{\ell}, B = \dot{\ell}$: Recordemos que en este caso teniamos que $C \neq \dot{\ell}$ ya que $mcd(A, B, C) = 1$, además como $\ell | [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$ entonces $\ell^2 | D = [\mathcal{O}_K : \mathcal{O}]^2 d_{\mathbb{K}}$ y como $\ell | B$ tenemos que $\ell^2 | B^2 - D = 4AC$. Como $\ell \neq 2$ y $\ell \nmid C$ resulta que $\ell^2 | A$ y por lo tanto $mcd(A, B\ell, \ell^2 C) = \ell^2$ lo cual implica que la isogenia $E \to E_0$ será ascendente.

Por otra parte, al igual que en el caso en que E estaba en la superficie, como $f(k) \equiv C \not\equiv 0 \pmod{\ell}$ $\forall k = 1, 2, \ldots, \ell$ todas las demás isogenias $E \to E_k$ resultan descendentes para $1 \leq k \leq \ell$.

En resumen, para el caso en que E se encuentre en la zona media se tendrá en todos los casos $Gr(E) = (1, 0, \ell)$.

III) Caso en que E esté en el piso de racionalidad: Este caso es igual al caso anterior pero con la diferencia que debemos descartar las isogenias descendentes. Los casos 1,3 y 4 no pueden darse, mientras que los casos 2 y 5 dan lugar a una única isogenia ascendente, por lo tanto en este caso tenemos siempre que $Gr(E) = (1, 0, 0)$.

Así que reuniendo todos los resultados para el caso no degenerado obtenemos los valores para $Gr(E)$ que nos dice el Teorema.

Para el caso degenerado, es decir, cuando $\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathbb{Z}[\pi]]$ vale el mismo análisis que hicimos para el caso no degenerado cuando E estaba en la superficie (es decir, cuando $\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$) excepto que esta vez debemos descartar las isogenias descendentes. De esta manera todas las aristas resultan horizontales y $gr(E) = \left(\frac{D}{\ell}\right)+1$. Este caso será de especial importancia para nosotros.

□

2. Una implementación en Sage del grafo de ℓ-isogenias.

Es esta sección usaremos la información sobre el grado-vector de los vértices del grafo $\mathcal{G}_{q,N,\ell}$ (Teorema de Kohel) para poder implementar un ejemplo en Sage de un grafo de ℓ-isogenias. La implementación del ejemplo está basada en el artículo de Fouquet y Morain [**14**], pero considerando la posibilidad de que aparezcan aristas múltiples.

Vamos a suponer que los j-invariante 0 y 1728 no formen parte de nuestro grafo de $\mathcal{G}_{q,N,\ell}$ para poder suponer que nuestro grafo es no dirigido[5], en este caso identificamos cada arista con su dual y no hay ambigüedad en hacer esto.

Partiremos entonces de una curva $E/\mathbb{F}_p$ calculamos su cardinal[6] $N = \#E(F_p)$, escogemos un primo $\ell \neq p$ y nuestro objetivo será calcular la componente conexa de $v = [E]_{\mathbb{F}_p}$ en el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$. En nuestro ejemplo vamos a tomar la curva $E : Y^2 = X^3 + 7478X + 1649$ en el cuerpo finito $\mathbb{F}_{10009}$:

```
> E=EllipticCurve(GF(10009),[7478,1649])
> E.cardinality()
10057
```

Como $\#E(\mathbb{F}_{10009}) = 10057$, su $\mathbb{F}_q$-clase será un vértice del grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ con $N = 10057, q = 10009$ y en principio ℓ un primo diferente de 10009 cualquiera.

Como mencionamos al inicio de la sección anterior, una buena forma de representar los vértices del grafo $\mathcal{G}_{q,N,\ell}$ es a través de su j-invariante y eso es lo que haremos, comenzaremos por calcular el j-invariante de nuestra curva de ejemplo.

[5]En caso contrario igual podríamos suponerlo cambiando la definición de grado (Comentario 2.9).

[6]Existen varios algoritmos eficientes para el cálculo de $\#E(\mathbb{F}_p)$, el más clásico es el Algoritmo de Schoof, pero hay versiones más eficientes. Para más información puede verse el Cap.IV del libro [**10**].

```
> E.j_invariant()
  83
```

Ahora precisamos poder calcular a partir de un vértice del grafo $\mathcal{G}_{q,N,\ell}$, representado por un j-invariante, todos sus j-invariantes vecinos y a través de cuantas aristas (clase de equivalencia de ℓ-isogenias) se conecta. Como mencionamos en la sección anterior, una forma de lograrlo es usando el polinomio modular $\phi_\ell(x,y)$ que tiene la propiedad de que si j' es una raíz con múltiplicidad m de $\phi_\ell(x,j)$ entonces la arista (j,j') aparece en el grafo $\mathcal{G}_{q,N,\ell}$ con multiplicidad m. Existe mucha literatura relacionada a la computación del polinomio modular, lo cual está lejos de ser un problema trivial. En el próximo capítulo volveremos a ese punto, pero por el momento imaginemos que tenemos dado el polinomio modular $\phi_\ell \pmod q$.

Para nuestro ejemplo vamos a elegir $\ell = 3$ (el polinomio modular $\phi_3(x,y)$ lo extrajimos de [**25**], Cáp.3, pág.27), lo definimos como polinomio en el anillo $\mathbb{F}_{10009}[x,y]$.

```
> R2.⟨x,y⟩= GF(10009)[ ]
```
> phi3=$x^4+y^4+1855425871872000000000x+452984832000000x^2+36864000x^3+1855425871872000000000y-770845966336000000xy+8900222976000x^2y-1069956x^3y+452984832000000y^2+8900222976000xy^2+2587918086x^2y^2+2232x^3y^2+36864000y^3-1069956xy^3+2232x^2y^3-x^3y^3$

Por lo dicho anteriormente, ahora no tenemos dificultad en calcular los j-invariantes vecinos de un j-invariante j_0 dado en el grafo $\mathcal{G}_{q,N,\ell}$, simplemente hacemos $y = j_0$ en el polinomio $\phi_3(x,y)$ y calculamos las raices en $\mathbb{F}_q$ del nuevo polinomio (en una variable) que nos queda. Implementamos esa sencilla rutina en Sage:

Algoritmo 1. Cálculo de los vecinos de un j-invariante en el grafo de ℓ-isogenias.

Entrada: Un vértice j de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil$=\phi_\ell \pmod q$.
Salida: Una lista de parejas (j',m') donde $mult_\ell(j,j') = m'$ en el grafo $\mathcal{G}_{q,N,\ell}$.

```
1. def vecinos(j,phil):
2.     F= phil.base_ring()
3.     R1.⟨x⟩= F[ ]
4.     p=phil.subs(y=j)
5.     p=R1(p)
6.     return p.roots()
```

En nuestro ejemplo nos queda:

```
> vecinos(83, phi3)
> [(6038,1),(2930,1),(2907,1),(2631,1)]
```

Nos será de utilidad definir una función altura que distinga niveles, otorgaremos al nivel más bajo con respecto de ℓ altura $h = 0$ (que corresponde al piso de racionalidad respecto de ℓ) y queremos que cuando exista una ℓ isogenia ascendente desde el j-invariante j_1 hasta el j-invariante j_2 entonces $h(j_2) = h(j_1) + 1$. Es fácil verificar que la siguiente función altura cumple con los requisitos.

Definición 2.39 (Altura)**.** : Si $E/\mathbb{F}_q$ una curva elíptica ordinaria, definimos su altura (con respecto de ℓ) como $h(E) = \nu_\ell([\mathrm{End}(E) : \mathbb{Z}[\pi]])$ (donde ν_ℓ es la valuación ℓ-ádica).

Observación 2.40. Dado que si $\phi : E_1 \to E_2$ es una isogenia ascendente entonces $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell$ y como $[\mathrm{End}(E_2) : \mathbb{Z}[\pi]] = [\mathrm{End}(E_2) : \mathrm{End}(E_1)] \cdot [\mathrm{End}(E_1) : \mathbb{Z}[\pi]]$ tomando valuación ℓ-ádica resulta $h(E_2) = h(E_1) + 1$.

Observación 2.41. Dado que dos curvas isomorfas tienen anillo de endomorfismos isomorfos (y por lo tanto le corresponden el mismo orden), entonces la altura es en realidad una función de su j-invariante. De esa manera podemos hablar de altura de un j-invariante.

Vamos a ver ahora como calcular la altura; comenzamos con la observación de que usando la función "vecinos" es fácil distinguir cuando una curva (ó j-invariante) tiene altura 0 (o sea cuando está en el piso de racionalidad respecto de ℓ).

En efecto, como consecuencia del Teorema de Kohel tenemos para el caso no degenerado que $h(j) = 0 \Leftrightarrow gr(j) = 1$ (ver Definición 2.36) mientras que en el caso degenerado todas las curvas se encuentran en el piso de racionalidad y $gr(E) = 0, 1$ o 2. En el caso no degenerado se tiene además que $gr(E) = \ell + 1 \geq 3$ (para cualquier ℓ primo) cuando E no está en el piso de racionalidad, o sea en cualquier caso podemos garantizar que el j-invariante j está en el piso si $gr(E) < 3$.

La otra observación fundamental para implementar un algoritmo para calcular la altura es que o bien $h(j) = 0$ o bien existe un único j' adyacente a j tal que $h(j') = h(j) - 1$ (es decir, existe entre sus vecinos una única isogenia descendente, esto es también consecuencia directa del Teorema de Kohel), podemos aprovechar esa observación para crear una cadena de isogenias descendentes hasta una curva del piso de racionalidad y midiendo el largo de dicha cadena obtenemos la altura. Definiremos por conveniencia previamente una función auxiliar piso que detecte cuando una lista de j-invariantes tenga algun j-invariante del piso de racionalidad respecto de ℓ.

Algoritmo 2. Para detectar cuando una lista contiene un j-invariante en el piso de racionalidad respecto de ℓ. Usa como subrutina la función vecinos.

Entrada: Una lista L de j-invariantes de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil $= \phi_\ell \pmod q$.
Salida: True si L contiene un j-invariante del piso y False en caso contrario.

```
1. def piso(L,phil):
2.     for j in L:
3.        gr = sum([x[1] for x in vecinos(j,phil)])
4.        if gr<3:
5.           return True
6.     return False
```

Algoritmo 3. Cálculo de la altura de un j-invariante.
Usa como subrutina las funciones vecinos y piso.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil= ϕ_ℓ (mód q).
Salida: La altura $h(E)$.

```
1. def altura(j,phil):
2.     A=[j]
3.     m=0
4.     while piso(A,phil)==False:
5.        m=m+1
6.        B=[ ]
7.        for x in A:
8.           B=B+vecinos(x,phil)
9.        A=[b[0] for b in B]
10.    return m
```

Observemos que en el m-ésimo paso del algoritmo anterior la lista B estará formada por todos aquellos j-invariantes que están a distancia menor o igual a m del j-invariante inicial j, luego por la observación previa, para $m < h(j)$ existirá un único j-invariante $j_m \in B$ tal que $h(j_m) = h(j) - m$ y los demás elementos de la lista B tendrán altura mayores. El algoritmo para la primera vez que encuentra un j-invariante con altura $h = 0$, en ese momento el contador m nos indica cuantos pasos necesitamos para llegar al piso por lo que en esa instancia $m = h(j)$.

Computamos la altura para el ejemplo que estabamos considerando que correspondia al j-invariante $j = 83$ en el grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ con $N = 10057, \ell = 3$ y $q = 10009$:

```
> altura(83,phi3)
  1
```

El Teorema de Kohel (para un ℓ fijo) nos dice que cada j-invariante j contiene un único j-invariante j_m en la superficie tal que se puede llegar desde j hasta j_m por un camino de aristas ascendentes. El Algoritmo 4 nos da dicho j-invariante, analizaremos dicho algoritmo.

Observemos que en cada iteración del while (punto 3.), comparamos la altura de j con la de cada uno de sus vecinos hasta encontrar un vecino con altura mayor o igual a la de j. En caso de no encontrarlo es porque j ya estaba en la superficie. Si lo encontramos hay dos posibilidades: Si el vecino tiene la misma altura de j entonces j está en la superficie (pues aristas horizontales en $\mathcal{G}_{q,N,\ell}$ solo son posibles entre vértices de la superficie con respecto de ℓ), caso contrario cambiamos nuestro j por otro j-invariante por encima y repetimos el proceso.

Para nuestro ejemplo computamos $max(83, phi3) = 2631$ donde $altura(2631, phi3) = 2$, esto nos dice que estamos en un caso no degenerado y que nuestro grafo de ℓ-isogenias tendrá exactamente 3 niveles que corresponde a $h = 0, 1$ y 2.

Algoritmo 4. Cálculo de un j-invariante en la superficie por encima de un j-invariante dado. Usa como subrutina las funciones sup, vecinos y altura.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil$=\phi_\ell$ (mód q).
Salida: El único j-invariante j_m en la superficie por encima de j.

```
1. def max(j,phil):
2.     Fin=False
3.     while Fin==False:
4.        V=vecinos(j,phil)
5.        l=len(V)
6.        h=altura(j,phil)
7.        i=0
8.        while altura(V[i][0],phil)<h and i<l-1:
9.           i=i+1
10.       if i<l-1:
11.          if altura(V[i][0],phil)==h:
12.             Fin=True
13.          else:
14.             j=V[i][0]
15.       if i==l-1:
16.          if altura(V[i][0],phil)<=h:
17.             Fin=True
18.          else:
19.             j=V[i][0]
20.    return j
```

Ahora queremos un algoritmo que dado un vértice (j-invariante) del grafo $\mathcal{G}_{q,N,\ell}$, calcule todas los vértices de la superficie de la componente conexa de j. Primero aplicamos la función max para obtener un vértice a por encima de j, luego consideramos todas las posibilidades para su grado horizontal $grh(a)$ (por el Teorema de Kohel este número solo puede ser $0, 1$ o 2 y no depende de la curva de la superficie que tomemos), teniendo las posibilidades de vértice aislado, loop o ciclo (compuesto de dos o más vértices). A la función calculada por nuestro algoritmo llamaremos de "superficie".

Por comodidad definiremos previamente la función auxiliar vecinoshor que nos da una lista de los j-invariantes vecinos a un j-invariante dado, que se encuentran en la misma altura (que será una lista vacia salvo tal vez en el caso que el j-invariante se encuentre en la superficie).

Algoritmo 5. Cálculo de vecinos horizontales. Usa como subrutina las funciones vecinos y altura.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil$=\phi_\ell$ (mód q).
Salida: Una lista con los vecinos de j que estén conectados horizontalmente con j.

```
1. def vecinoshor(j,phil):
2.     L=[ ]
3.     h= altura(j,phil)
4.     for x in vecinos(j,phil):
5.        if altura(x[0],phil)==h:
6.           L=L+[x]
7.     return L
```

Algoritmo 6. Cálculo del subgrafo inducido por los vértices de la componente conexa que está en la superficie. Usa como subrutina la función vecinoshor.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil= ϕ_ℓ (mód q).
Salida: Una lista L=[S, ES] donde S es una lista con los vértices de la componente conexa que contiene a j y que están en la superficie y ES es una lista con las aristas entre los elementos de S.

```
1. def superficie(j,phil):
2.     a=max(j,phil)
3.     L=[a]
4.     Vh=vecinoshor(a,phil)
5.     grh=sum([v[1] for v in Vh])
6.     if grh==0:
7.        return [L,[]]
8.     if gh==1:
9.        e=[a, Vh[0][0]]
10.       return [e,[e]]
11.    if gr==2 and len(Vh)==1 and Vh[0][0]==a:
12.       e= [a,a]
13.       return [[a],[e,e]]
14.    if gr==2 and len(Vh)==1 and Vh[0][0]!=a:
15.       return [[a,Vh[0][0]],[[a,Vh[0][0]],[Vh[0][0],a]]]
16.    if gr==2 and len(Vh)>1:
17.       L=L+[Vh[0][0]]
18.       while L[len(L)-1]!=a:
19.          y=L[len(L)-2]
20.          for x in vecinoshor(L[len(L)-1],phil):
21.             if x[0]!=y:
22.                L=L+[x[0]]
23.       e=[[L[i],L[i+1]] for i in [0..len(L)-2]]
24.       return [L[0:len(L)-1], e]
```

Comentemos un poco sobre este último algoritmo. Como dijimos antes, hay tres posibilidades para la superficie (vértice aislado, loop o ciclo), analizemos con detalle dichas posibilidades. El algoritmo comienza tomando un vértice a en la superficie por encima de j y calculando $grh(a)$ que puede ser $0, 1$ y 2. En el caso que $grh(a) = 0$ entonces a no tiene conexiones horizontales y corresponde claramente al caso de vértice aislado, si $grh(a) = 1$ entonces tenemos una única arista (a, b). Además en este caso se tiene necesariamente que $a \neq b$ por la siguiente observación.

Observación 2.42. Si $\phi : E \to E$ es una ℓ-isogenia (con ℓ-primo) entonces ϕ y $\widehat{\phi}$ no son equivalentes (y en consecuencia la presencia de loops implica $grh(E) \geq 2$).

Demostración: Por la Proposición 2.3, basta probar que ϕ y $\widehat{\phi}$ tienen distinto kernel. En el caso $\ell = p$ es porque como vimos en la demostración de la Prop.2.3 una es separable y la otra no. En el caso $\ell \neq p$ tenemos que $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, sean P y Q en $E(\overline{\mathbb{F}}_q)$ tal que $\langle P\rangle = \ker(\phi)$ y $E[\ell] = \langle P\rangle \oplus \langle Q\rangle$.

Como $Q \notin \langle P\rangle$ (y por lo tanto $\phi(Q) \neq \mathcal{O}$) pero $\phi(Q) \in E[\ell]$ (pues $\ell Q = \mathcal{O} \Rightarrow \ell\phi(Q) = \phi(\ell Q) = \phi(\mathcal{O}) = \mathcal{O}$), entonces $\phi(Q) = iP + jQ$ con $j \not\equiv 0$ (mód ℓ). Luego

$\mathcal{O} = \ell Q = \widehat{\phi}\phi(Q) = i\widehat{\phi}(P) + j\widehat{\phi}(Q)$, por lo tanto si $\widehat{\phi}(P) = \mathcal{O}$ tendríamos que $\widehat{\phi}(Q) = 0$ (puesto que $j \not\equiv 0 \pmod{\ell}$) lo cual sería una contradicción. De esa forma $\widehat{\phi}(P) \neq 0$ lo cual implica $\langle P\rangle \cap \ker(\widehat{\phi}) = \{0\}$ (pues $\#\langle P\rangle = \ell$ primo). Luego $\ker(\phi) \neq \ker(\widehat{\phi})$ (en realidad no es difícil de ver que $\ker(\widehat{\phi}) = \langle Q\rangle$) y por lo tanto ϕ y $\widehat{\phi}$ son no equivalentes.

□

Por último tenemos el caso en que $grh(a) = 2$; en este caso la superficie resultará un (multi)grafo 2-regular conexo y por lo tanto puede ser un loop (doble), un arista doble entre dos vértices distintos o un ciclo de largo $t \geq 3$.

Computamos el algoritmo que nos da la superficie para nuestro ejemplo:

```
> [S, ES] = superficie(83, phi3)
> S ; ES
  [2631, 9171, 1157, 5711, 8992, 8578, 8077]
  [[2631,9171],[9171,1157],[1157,5711],[5711,8992],[8992,8578],
  [8578,8077],[8077,2631]]
```

La primer lista corresponde a los vértices que se encuentran en la superficie de la componente conexa del grafo de ℓ-isogenia que contiene a nuestro j-invariante $j = 83$, la segunda a sus conexiones.

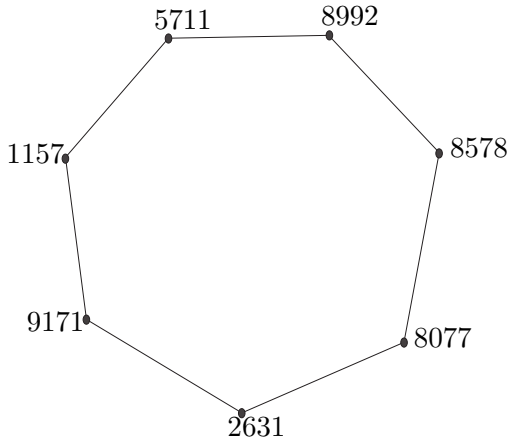


FIGURA 1. Resultado de superficie(83,phi3).

Para calcular la componente conexa de un j-invariante, la idea será pararnos en cada curva de la superficie y calcular el árbol colgante que tiene como nodo principal dicho j-invariante, por comodidad definiremos una función auxiliar vecinosdes, que es análoga a vecinoshor pero esta vez nos quedamos con aquellos vecinos que están a una altura inferior (acompañado de su multiplicidad de conexión).

Algoritmo 7. Cálculo de vecinos descendentes. Usa como subrutina las funciones altura y vecinos.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil= ϕ_ℓ (mód q).
Salida: Una lista con los vecinos de j que estén conectados horizontalmente con j.

```
1. def vecinosdes(j,phil):
2.     L=[ ]
3.     h= altura(j,phil)
4.     for x in vecinos(j,phil):
5.        if altura(x[0],phil)<h:
6.           L=L+[x]
7.     return L
```

Algoritmo 8. Cálculo del árbol colgante de un j-invariante. Usa como subrutina las funciones piso y vecinosdes.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil= ϕ_ℓ (mód q).
Salida: El subgrafo E=[D,ED] inducido por los vértices que están por debajo[7] de j (incluyendo j), donde D es el conjunto de vértices y ED sus conexiones.

```
1. def arbol(j,phil):
2.     N=[[j],[ ],[j]]
3.     while not piso(N[2],phil):
4.        N2=[ ]
5.        for x in N[2]:
6.           for y in vecinosdes(x,phil):
7.              N[0]=N[0]+[y[0]]
8.              N[1]=N[1]+y[1]*[[x,y[0]]]
9.              N2 = N2+[y[0]]
10.       N[2]=N2
11.    return N[0:2]
```

Recordemos que para nuestro ejemplo teníamos $max(83, phi3) = 2631$, calculamos entonces el árbol colgante con nodo principal $j = 2631$ obteniendo:

```
> [V,E]=arbol(2631,phi3)
> V ; E
[2631,3527,83,8123,2146,1353,6038,2930,2907]
[[2631, 3527], [2631, 83], [3527, 8123], [3527, 2146], [3527, 1353],
[83, 6038], [83, 2930], [83, 2907]]
```

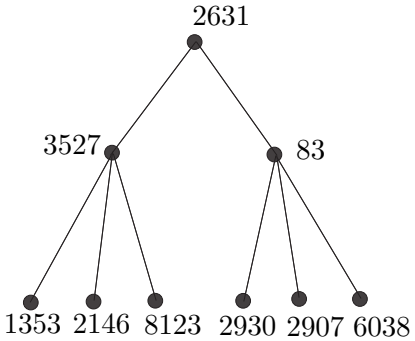


FIGURA 2. Resultado de arbol(83,phi3).

Finalmente podemos implementar el algoritmo que calcula la componente conexa de un j-invariante dado, utilizamos la función *superficie* para obtener la parte de la superficie de dicha componente conexa y luego con la función *arbol* aplicada a cada vértice de la superficie obtenemos la componente conexa deseada.

Algoritmo 9. Cálculo de una componente conexa del grafo de ℓ-isogenias.
Usa como subrutina las funciones superficie y arbol.

Entrada: Un j-invariante de $\mathcal{G}_{q,N,\ell}$ y el polinomio ℓ-modular phil= ϕ_ℓ (mód q).
Salida: La componente conexa del grafo de ℓ-isogenias que contiene a j.

```
1. def grafoisogenias(j,phil):
2.     E=[[ ],[ ]]
3.     S=superficie(j,phil)
4.     for v in S[0]:
5.        [A,EA]=arbol(v,phil)
6.        E[0]=E[0]+A
7.        E[1]=E[1]+EA
8.     E[1]=E[1]+S[1]
9.     return E
```

Lo calculamos para nuestro ejemplo concreto ($j = 83$ y $(q, N, \ell) = (10009, 10057, 3)$):

```
> [V,E]=grafoisogenias(83,phi3)
> V
  [2631, 3527, 83, 8123, 2146, 1353, 6038, 2930, 2907, 9171, 9968, 7994,
  8734, 3965, 1071, 8030,6430, 2689, 1157, 9295, 7251, 7793, 7508, 2500,
  7964, 5521, 5334, 5711, 6484, 3656, 5946, 2391,1472, 9336, 1969, 1438,
  8992, 4091, 667, 9218, 8351, 6770, 9599, 2392, 1898, 8578, 6085, 1978,
  7518, 3480, 1578, 8143, 3665, 1380, 8077, 8798, 2403, 9241, 7657, 996,
  9143, 7146, 3218]
> E
  [[2631, 3527], [2631, 83], [3527, 8123], [3527, 2146], [3527, 1353],
  [83, 6038], [83, 2930], [83, 2907], [9171, 9968], [9171, 7994],
  [9968,8734], [9968, 3965], [9968, 1071], [7994, 8030], [7994, 6430],
  [7994,2689], [1157, 9295], [1157, 7251], [9295, 7793], [9295, 7508],
  [9295,2500], [7251, 7964], [7251, 5521], [7251, 5334], [5711, 6484],
  [5711,3656], [6484, 5946],[6484, 2391], [6484, 1472], [3656, 9336],
  [3656,1969], [3656, 1438], [8992, 4091], [8992, 667],[4091, 9218],
  [4091,8351], [4091, 6770], [667, 9599], [667, 2392], [667, 1898],
  [8578,6085],[8578, 1978], [6085, 7518], [6085, 3480], [6085, 1578],
  [1978,8143], [1978, 3665], [1978, 1380],[8077, 8798], [8077, 2403],
  [8798,9241], [8798, 7657], [8798, 996], [2403, 9143], [2403, 7146],
  [2403,3218], [2631, 9171], [9171, 1157], [1157, 5711], [5711, 8992],
  [8992,8578], [8578, 8077],[8077, 2631]]
```

Al grafo de ℓ-isogenias se le suele llamar grafo volcán de ℓ-isogenias, porque justamente para este caso (no degenerado y $\left(\frac{D}{\ell}\right) = 1$) cada componente conexa puede ser dibujada en forma de volcán y al conjunto de vértices de la superficie suele llamarse de volcán.

Estos algoritmos requieren como precomputación el polinomio modular $\phi_\ell(X, Y)$ módulo p, donde p es la característica de $\mathbb{F}_q$. La computación de dichos polinomios no es tarea

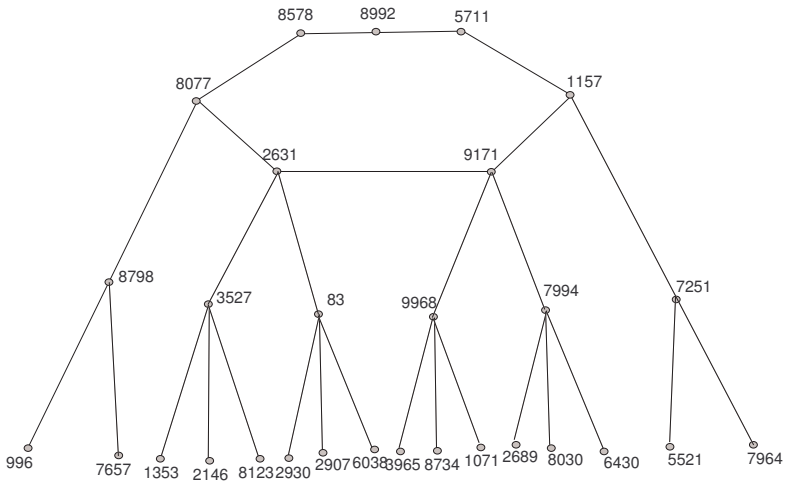


FIGURA 3. Resultado de grafoisogenias(83,phi3).

trivial, hay muchos artículos al respecto y varios resultados nuevos. Se comentará más sobre este punto en el próximo capítulo.

A lo que refiere al problema principal que es el de implementar un algoritmo de autoreducibilidad aleatoria, uno de los ingredientes claves es la realización de una caminata al azar en el grafo de isogenias $S_{N,q,B}$ (unión de todos los grafos de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$, para $\ell \leq B$ primo), claramente no es necesario calcular todo el grafo de isogenias para realizar dicha caminata (lo cual sería muy costoso).

En el artículo de Jao-Miller-Venkatesan [**24**], es probado que la familia de grafos $S_{N,q,B}$ posee buenas propiedades expansoras (en un sentido que explicitaremos más adelante), asumiendo una cierta generalización de la hipótesis de Riemann (GRH), lo cual es escencial para probar (condicionalmente a GRH) que el algoritmo de autoreducibilidad aleatoria puede computarse en tiempo polinomial. Este será el tema de la sección 4.

3. El grafo de isogenias y el grafo de clases de ideales.

Una importante herramienta para el estudio del grafo de isogenias es una correspondencia entre este y cierto grafo de Cayley de clases de ideales. En esta sección daremos una idea de dicha correspondencia que es usada en la sección siguiente para estudiar las propiedades expansoras del grafo de ℓ-isogenias y será usada en la primer parte del algoritmo de autoreducibilidad aleatoria que implementaremos en el siguiente capítulo.

3.1. Curvas complejas generadas por ideales de un orden de un cuerpo cuadrático imaginario.

Recordemos que el grafo de ℓ-isogenias está separado por niveles que corresponden a ordenes en un cuerpo cuadrático imaginario $\mathcal{O}$ así que vamos a concentrar nuestra atención a un nivel $\mathcal{O}$ particular.

Consideremos un ideal $\mathfrak{a}$ propio de $\mathcal{O}$, es decir, un Z-módulo de rango 2 tal que su anillo de multiplicación compleja $\mathrm{End}(\mathfrak{a}) = \{x \in \mathbb{C} : x\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}$ (estos corresponden a

los ideales invertibles en el grupo de ideales fraccionarios del orden $\mathcal{O}$) ([**11**], cap.7).

Si $\mathbb{K}$ es el cuerpo cuadrático que contiene a $\mathcal{O}$, como es imaginario de grado 2 (sobre $\mathbb{Q}$), su único automorfismo no trivial coincide con la conjugación compleja y por lo tanto $N(x) = x\overline{x} = ||x||^2$ (donde $||\ ||$ denota la norma euclidea), es un resultado clásico que $N(\mathcal{O}_{\mathbb{K}}) \subset \mathbb{Z}$ y por lo tanto $D(0,1) \cap \mathcal{O}_K = \{0\}$ (donde $D(0,1)$ es el disco abierto unidad con centro en el origen), así que $\mathcal{O}_{\mathbb{K}}$ resulta un subgrupo aditivo discreto de $\mathbb{C}$ y por lo tanto un látice. En particular todo suborden $\mathcal{O}$ y todo ideal fraccionario $\mathfrak{a}$ de cualquier orden $\mathcal{O}$ serán látices (ya que son subgrupos de $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{Z}$-rango igual a 2).

Ahora supongamos que tenemos un orden $\mathcal{O}$ dado, a cada ideal propio $\mathfrak{a}$ de $\mathcal{O}$ le podemos asociar una curva elíptica compleja $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ (ya que como observamos anteriormente $\mathfrak{a}$ es un látice). Recordemos que los endomorfismos de $E_{\mathfrak{a}}$ vienen dados por multiplicación por escalar, es decir, son de la forma $x + \mathfrak{a} \mapsto \alpha x + \mathfrak{a}$ donde $\alpha \in \mathbb{C}$ es tal que $\alpha\mathfrak{a} \subseteq \mathfrak{a}$. Como es usual, asociando el mapa multiplicación por α con el complejo α, el anillo de endomorfismo de la curva elíptica $E_{\mathfrak{a}}$ resulta $\mathrm{End}(E_{\mathfrak{a}}) = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}$ (la última igualdad es porque el ideal $\mathfrak{a}$ de $\mathcal{O}$ es propio).

3.2. Clases de isomorfismo de curvas elípticas y el grupo de Picard de un orden. Supongamos que tenemos una curva elíptica $\mathbb{C}/\mathfrak{a}$ como en la parte anterior, donde $\mathfrak{a}$ es un ideal propio del orden $\mathcal{O}$. A cada ideal propio $\mathfrak{c}$ podemos asociarle la isogenia $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathfrak{c}^{-1}$ dada por $x + \mathfrak{a} \mapsto x + \mathfrak{a}\mathfrak{c}^{-1}$ ($\mathfrak{c}^{-1}$ es el ideal fraccionario inverso del ideal $\mathfrak{c}$ en el grupo de los ideales propios[8] del orden $\mathcal{O}$, como $\mathfrak{c} \subset \mathcal{O} \Rightarrow \mathfrak{c}^{-1} \supset \mathcal{O}$ y por lo tanto el mapa anterior está bien definido). Observemos además que:

$$\frac{\mathfrak{a}\mathfrak{c}^{-1}}{\mathfrak{a}} \simeq \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{c}} \simeq \frac{\mathcal{O}}{\mathfrak{c}}$$

y por lo tanto el grado de la isogenia asociada al $\mathcal{O}$-ideal propio $\mathfrak{c}$ será $\#\frac{\mathcal{O}}{\mathfrak{c}} = N(\mathfrak{c})$, o sea la norma del ideal $\mathfrak{c}$.

Recíprocamente, dada una curva elíptica compleja $\mathbb{C}/\Lambda$ con $\mathrm{End}(\mathbb{C}/\Lambda) = \mathcal{O}$ como látices homotéticos dan lugar al mismo anillo de endomorfismo entonces el Teorema 10.14 de ([**11**], pág.209) nos dice que Λ será homotético a un ideal fraccionario propio de $\mathcal{O}$, de hecho a un ideal propio ya que todo $\mathcal{O}$-ideal fraccionario es homotético a un $\mathcal{O}$-ideal y por lo tanto $\mathbb{C}/\Lambda \simeq \mathbb{C}/\mathfrak{a}$ donde $\mathfrak{a}$ es un $\mathcal{O}$-ideal propio.

Proposición 2.43. *Si $\phi : \frac{\mathbb{C}}{\Lambda} \to \frac{\mathbb{C}}{\Lambda'}$ es una ℓ-isogenia entre las curvas elípticas $\frac{\mathbb{C}}{\Lambda}$ y $\frac{\mathbb{C}}{\Lambda'}$, ambas con anillo de endomorfismo el mismo orden $\mathcal{O}$ de un cuerpo cuadrático imaginario entonces existen ideales propios $\mathfrak{a}$ y $\mathfrak{c}$ tales que $\frac{\mathbb{C}}{\Lambda} \simeq \frac{\mathbb{C}}{\mathfrak{a}}$ y $\frac{\mathbb{C}}{\Lambda'} \simeq \frac{\mathbb{C}}{\mathfrak{a}\mathfrak{c}^{-1}}$. Además si $\psi_1 : \frac{\mathbb{C}}{\Lambda} \to \frac{\mathbb{C}}{\mathfrak{a}}$ y $\psi_2 : \frac{\mathbb{C}}{\Lambda'} \to \frac{\mathbb{C}}{\mathfrak{a}\mathfrak{c}^{-1}}$ son isomorfismos, entonces la isogenia $\psi_2\phi\psi_1^{-1} : \frac{\mathbb{C}}{\mathfrak{a}} \to \frac{\mathbb{C}}{\mathfrak{a}\mathfrak{c}^{-1}}$ vendrá dada por $x+\mathfrak{a} \mapsto x+\mathfrak{a}\mathfrak{c}^{-1}$ (o sea la isogenia asociada al ideal propio $\mathfrak{c}$, en particular $N(\mathfrak{c}) = \ell$).*

Demostración: Como vimos antes, el hecho de que las curvas elípticas $\mathbb{C}/\Lambda$ y $\mathbb{C}/\Lambda'$ tengan como anillo de multiplicación compleja el mismo orden $\mathcal{O}$ implica la existencia de $\mathcal{O}$-ideales propios $\mathfrak{a}$ y $\mathfrak{b}$ e isomorfismos $\psi_1 : \mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}$ y $\psi_2' : \mathbb{C}/\Lambda' \to \mathbb{C}/\mathfrak{b}$. Supongamos que el mapa $\psi_2'\phi\psi_1^{-1} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}$ viene dado por $z + \mathfrak{a} \mapsto \alpha z + \mathfrak{b}$ donde $\alpha \in \mathbb{C}$ verifica $\alpha\mathfrak{a} \subset \mathfrak{b}$ entonces de hecho $\alpha \in \mathbb{K}$ (pues $\alpha\mathfrak{a} \subset \mathfrak{b} \Rightarrow \alpha \in \mathfrak{b}\mathfrak{a}^{-1} \subset \mathbb{K}$) y la inclusión de $\mathcal{O}$-ideales

[8]Recordar que un ideal I de $\mathcal{O}$ es propio si $\mathrm{End}(I) = \mathcal{O}$.

fraccionarios propios $\alpha\mathfrak{a} \subset \mathfrak{b}$ implica la existencia de un $\mathcal{O}$-ideal propio $\mathfrak{c}$ tal que $\alpha\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ lo cual implica que $\alpha^{-1}\mathfrak{b} = \mathfrak{a}\mathfrak{c}^{-1}$. Consideremos ahora el isomorfismo $\psi_2'' : \mathbb{C}/\mathfrak{b} \to \mathbb{C}/\alpha^{-1}\mathfrak{b}$ dado por $z + \mathfrak{b} \mapsto \alpha^{-1}z + \alpha^{-1}\mathfrak{b}$ y definimos $\psi_2 = \psi_2''\psi_2'$.

$$\begin{array}{ccccc} \mathbb{C}/\Lambda & \xrightarrow[\simeq]{\psi_1} & \mathbb{C}/\mathfrak{a} & & \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \cdot\alpha} & \searrow & \\ \mathbb{C}/\Lambda' & \xrightarrow[\simeq]{\psi_2'} & \mathbb{C}/\mathfrak{b} & \xrightarrow[\simeq]{\cdot\alpha^{-1}} & \mathbb{C}/\mathfrak{a}\mathfrak{c}^{-1} \end{array}$$

Finalmente chequeamos $\psi_2\phi\psi_1^{-1}(z+\mathfrak{a}) = \psi''(\psi_2'\phi\psi_1^{-1}(z+\mathfrak{a})) = \psi''(\alpha z+\mathfrak{b}) = z+\alpha^{-1}\mathfrak{b} = z + \mathfrak{a}\mathfrak{c}^{-1}$ como queríamos.

□

3.3. Grafo de isogenias como grafo de Cayley de clases de ideales de un orden. Volvamos ahora al grafo de ℓ-isogenias $\mathcal{G}$ y consideremos un nivel fijo, llamemos $\mathcal{O}$ al orden asociado a dicho nivel. Usando el Teorema de Levantamiento de Deuring obtenemos un isomorfismo con un grafo cuyos vértices son clases de isomorfismos de curvas elípticas complejas, todas con anillo de endomorfismo isomorfo a $\mathcal{O}$ y dos clases están relacionadas si existe una ℓ-isogenia entre un representante de cada clase.

Por lo visto en las subsecciones previas, toda clase de isomorfismo de curvas elípticas complejas contendrá alguna curva de la forma $\mathbb{C}/\mathfrak{a}$ donde $\mathfrak{a}$ es un $\mathcal{O}$-ideal propio y si $\mathbb{C}/\mathfrak{c}$ es otra curva de la misma clase (con $\mathfrak{c}$ otro $\mathcal{O}$-ideal propio) de isomorfismo entonces los ideales $\mathfrak{a}$ y $\mathfrak{c}$ son homotéticos como látices y por lo tanto son equivalentes módulos ideales principales, es decir $[\mathfrak{a}] = [\mathfrak{c}]$ en $C(\mathcal{O})$ el grupo de clases de ideales del orden $\mathcal{O}$, de esa manera cada una de estas clases de isomorfismo de curvas complejas tendrá asociado un único elemento del grupo de clases de ideales $C(\mathcal{O})$.

Además vimos en la Prop. 2.43 que dadas dos clases de isomorfismos entre las cuales existe una ℓ-isogenia entre un representante de cada clase entonces es posible encontrar una isogenia $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{b}$ asociada al ideal $\mathfrak{a}\mathfrak{b}^{-1}$ (si $\mathfrak{b} = \mathfrak{a}\mathfrak{c}^{-1} \Rightarrow \mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$) de norma ℓ. Si $\mathbb{C}/\mathfrak{a}' \simeq \mathbb{C}/\mathfrak{a}$ y $\mathbb{C}/\mathfrak{b}' \simeq \mathbb{C}/\mathfrak{b}$ entonces existen $x, y \in \mathbb{K}$ tales que $\mathfrak{a}' = x\mathfrak{a}$ y $\mathfrak{b}' = y\mathfrak{b}$ entonces $\mathfrak{a}'\mathfrak{b}'^{-1} = xy^{-1} \cdot \mathfrak{a}\mathfrak{b}^{-1}$ que es equivalente al ideal $\mathfrak{a}\mathfrak{b}^{-1}$ módulo ideales principales por lo tanto a cada arista que conecta dos clases se le puede asociar un único elemento de $C(\mathcal{O})$ dado por $[\mathfrak{a}][\mathfrak{b}]^{-1}$.

Si consideramos la función que a la clase de isomorfismo que contiene a $\mathbb{C}/\mathfrak{a}$ le corresponde $[\mathfrak{a}] \in C(\mathcal{O})$ obtenemos un isomorfismo con un grafo cuyo conjunto de vértice es $C(\mathcal{O})$ el grupo de clases de ideales del orden $\mathcal{O}$ y dos vértices $[\mathfrak{a}]$ y $[\mathfrak{b}]$ están conectados si y solo si existen representantes $x \in [\mathfrak{a}]$ e $y \in [\mathfrak{b}]$ tal que $N(xy^{-1}) = \ell$, dado que $[xy^{-1}] = [\mathfrak{a}][\mathfrak{b}]^{-1}$, otra forma de decirlo es que dos clases $[\mathfrak{a}]$ e $[\mathfrak{b}]$ están relacionadas si la clase $[\mathfrak{a}][\mathfrak{b}]^{-1}$ contiene un ideal de norma ℓ o sea, las aristas son todas de la forma $\{[\mathfrak{a}], [\mathfrak{a}][\mathfrak{c}]\}$ para $[\mathfrak{c}] \in S = \{\mathcal{I} \in C(\mathcal{O}) : \mathcal{I}^{-1}$ contenga un ideal de norma $\ell\}$ (recordar que como $[\mathfrak{a}][\mathfrak{a}^{-1}] = [\mathfrak{a}\mathfrak{a}^{-1}] = [\mathcal{O}] = \mathbf{1}$ entonces $[\mathfrak{a}]^{-1} = [\mathfrak{a}^{-1}]$).

Para cada B fijo vamos a considerar la unión de los grafos de ℓ-isogenias para cierto nivel $\mathcal{O}$ también fijo donde ℓ recorre todos los primos menores que B, que denotaremos por $\mathcal{G}_{q,N,\ell}(\mathcal{O})$ a ese grafo. Por la correspondencia previa, este grafo resulta isomorfo a un

grafo de clases de ideales con aristas de la forma $\{[\mathfrak{a}], [\mathfrak{a}][\mathfrak{c}]\}$ para $[\mathfrak{c}] \in S = \{\mathcal{I} \in C(\mathcal{O}) : \mathcal{I}^{-1}$ contenga un ideal de norma primo $\leq B\}$, el Teorema de la Cota de Minkowski nos asegura que a partir de un B el conjunto S será un generador del grupo de clases de ideales de $C(\mathcal{O})$ y nos queda el grafo de Cayley asociado al grupo $C(\mathcal{O})$ y generador S (en particular resultará un grafo conexo).

4. Expansividad del Grafo de Isogenias.

En esta sección analizaremos las propiedades expansivas del grafo de isogenias, las cuales jugarán un papel fundamental en el algoritmo de autoreducibilidad aleatoria que veremos en el capítulo siguiente.

4.1. Relación entre los grados y propiedades espectrales con respecto a la expansividad. Consideraremos para un orden $\mathcal{O}$, los grafos

$$S_{n,q,B}(\mathcal{O}) = \bigcup_{\substack{\ell \leq B \\ \ell \text{ primo}}} \mathcal{G}_{q,N,\ell}(\mathcal{O})$$

donde $\mathcal{G}_{q,N,\ell}(\mathcal{O})$ es el nivel $\mathcal{O}$ del grafo de ℓ-isogenias $\mathcal{G}_{q,N,\ell}$ como en la sección previa. Los grafos $S_{N,q,B}(\mathcal{O})$ son grafos regulares y a medida que B crece también lo hace el grado de sus vértices. El siguiente resultado clásico de Teoría de Grafos nos será de utilidad.

Proposición 2.44. *Sea G un grafo k-regular con h vértices, A su matriz de adyacencia y supongamos que el único vector propio asociado al valor propio 1 son los múltiplos del vector constante $\mathbf{1} = (1, 1, \ldots, 1)$. Supongamos además que existe $c < k$ tal que para todo otro valor propio λ se verifica $|\lambda| \leq c$. Consideremos además $x \in V$ y $S \subset V$. Entonces todo camino al azar de largo $r \geq r_0 = \frac{\log\left(\frac{2h}{\sqrt{|S|}}\right)}{\log\left(\frac{k}{c}\right)}$ que comienze en x terminará en un punto de S con probabilidad $P \geq \frac{|S|}{2h}$.*

Demostración: Dada una ordenación de los vértices $V = \{v_1, v_2, \ldots, v_h\}$, tenemos una correspondencia natural entre vectores de $\mathbb{R}^h$ y funciones en $L^2(V)$, de esa manera A resulta un operador autoadjunto en el espacio de Hilbert $L^2(V)$, haremos uso de esa correspondencia.

Para r fijo, denotemos por $C_S(x, r)$ la cantidad de caminos de largo r que parten de x y terminan en S. Como la cantidad de caminos al azar de largo r que parten de x es k^r (pues el grafo es k-regular) entonces la probabilidad de que un camino al azar partiendo de x termine en S será $P = \frac{C_S(x,r)}{k^r}$.

Recordemos que $(A^r)_{ij}$ nos da la cantidad de caminos de largo desde v_i hasta v_j y por lo tanto, para $x = v_i$ resulta que $A^r\chi_x$ es la columna i-ésima de A^r, luego $A^r\chi_x(y)$ nos da la cantidad de caminos de largo r que parten de y y terminan en x (que es lo mismo que contar los caminos de largo r que empiezan en x y terminan en y ya que el grafo en no dirigido). Por otra parte se observa que $\langle \chi_S, f \rangle = \sum_{v \in S} f(v)$ luego se tiene la fórmula:

$$C_S(x, r) = \langle \chi_S, A^r\chi_x \rangle$$

Llamemos $W = \mathbf{1}\mathbb{R}$ y $\mathcal{P}$ la proyección ortogonal sobre W, tenemos que $\mathcal{P}(\chi_S) = \langle \chi_S, \mathbf{1}\rangle \frac{\mathbf{1}}{||\mathbf{1}||^2} = \frac{|S|}{h}\mathbf{1}$ y $\mathcal{P}(\chi_x) = \langle \chi_x, \mathbf{1}\rangle \frac{\mathbf{1}}{||\mathbf{1}||^2} = \frac{1}{h}\mathbf{1}$ y de esa forma conseguimos la descomposición ortogonal:

$$\chi_S = \frac{|S|}{h}\mathbf{1} + u \quad \text{y} \quad \chi_x = \frac{1}{h}\mathbf{1} + v$$

con $\langle u, \mathbf{1}\rangle = \langle v, \mathbf{1}\rangle = 0$. Como $A\mathbf{1} = k\mathbf{1} \Rightarrow A^r\mathbf{1} = k^r\mathbf{1} \Rightarrow A^r\chi_x = \frac{k^r}{h}\mathbf{1} + A^r v$ y como A es autoadjunta también resulta $\langle A^r v, \mathbf{1}\rangle = 0$.

Sustituyendo arriba nos queda que $C_S(x, r) = \frac{|S|}{h}k^r + \langle u, A^r v\rangle$ y por lo tanto

$$P = \frac{|S|}{h} + \frac{\langle u, A^r v\rangle}{k^r}$$

A continuación acotamos $|\langle u, A^r v\rangle|$:

$$|\langle u, A^r v\rangle| \leq ||u||\cdot||A^r v|| = ||u||\cdot||A^r|_{W^\perp} v|| \leq ||u||\cdot||A^r|_{W^\perp}||\cdot||v|| \leq ||A|_{W^\perp}||\cdot||v|| \leq c^r||u||\cdot||v||$$

donde la primer desigualdad es por Cauchy-Schwarz y la última es porque por hipótesis W es el subespacio propio asociado al valor propio k y como A es autoadjunta entonces los valores propios de $A|_{W^\perp}$ son los de A excepto k y vale la cota de la hipótesis.

Finalmente usando Pitágoras tenemos que $||u|| \leq ||\chi_S|| = \sqrt{|S|}$ y $||w|| \leq ||\chi_x|| = 1$, sustituyendo en la última desigualdad obtenemos la cota $|\langle u, A^r v\rangle| \leq c^r\sqrt{|S|}$. Para que $P \leq \frac{|S|}{2h}$ alcanza con que

$$\frac{c^r\sqrt{|S|}}{k^r} \leq \frac{|S|}{2h}$$

lo cual es equivalente a que $\left(\frac{c}{k}\right)^r \leq \frac{\sqrt{|S|}}{2h} \Leftrightarrow \left(\frac{k}{c}\right)^r \geq \frac{2h}{\sqrt{|S|}} \Leftrightarrow r\log\left(\frac{k}{c}\right) \geq \log\left(\frac{2h}{\sqrt{|S|}}\right)$ y como $k > c$ esto último equivale a que $r \geq \frac{\log\left(\frac{2h}{\sqrt{|S|}}\right)}{\log\left(\frac{k}{c}\right)} = r_0$. Por lo tanto fijando de antemano un $r \geq r_0$ si realizamos una caminata al azar de largo r entonces la probabilidad de caer en un punto de S será de al menos $\frac{|S|}{2h}$ donde h es la cantidad de vértices total del grafo.

□

4.2. Propiedades espectrales del grafo de isogenias. Como vimos en el Teorema anterior, las propiedades expansivas del grafo de isogenias están relacionadas con la separación espectral (más precisamente entre el primer valor propio y los restantes).

En esta parte daremos un resumen de las ideas que aparecen en el artículo de Jao, Miller y Venkatesan [**24**] sobre el Teorema de separación de autovalores del grafo de isogenias. Los autores utilizan principalmente resultados de formas modulares y series θ y en esa parte del artículo ([**24**], secciones 4 y 5) se referencia principalmente al libro de Iwaniec [**23**] en lo referente a resultados sobre formas modulares. Otra referencia más introductoria sobre formas modulares (donde aparecen todas las definiciones requeridas para comprender esta sección) es el libro de Diamond y Shurman [**12**].

Para demostrar propiedades espectrales del grafo de isogenias se utiliza el isomorfismo con el grafo de Cayley de clases de ideales y las propiedades espectrales se demuestran para este último, asumiendo la Hipótesis de Riemann Generalizada (GRH). Recordemos

que los vértices del grafo de clases de ideales $\mathcal{H}$ viene dado por un conjunto de representantes $\mathcal{V} = \{\alpha_1, \alpha_2, \ldots, \alpha_h\}$ del grupo de clases de ideales de un orden en un cuerpo cuadrático imaginario $\mathcal{O}$ y las aristas entre dos vértices α_i y α_j son representadas por $\mathcal{O}$-ideales propios β tales que $\beta\alpha_i \equiv \alpha_j$ módulo ideales principales. Además el grado de la isogenia corresponde con la norma del ideal β, de modo que restringirnos a isogenias de grado ℓ equivale a restringirnos a los ideales β de norma ℓ.

La idea es encontrar una base de autovectores simultaneos para las matrices $M(n)$ cuya entrada ij nos da la cantidad de aristas entre α_i y α_j en el grafo $\mathcal{H}$ restringiendo las aristas a ideales de norma n, esto se consigue utilizando teoría de formas modulares. Una vez conseguido esto, lo siguiente es expresar los autovalores en función de ciertas sumas que involucran los caracteres del grupo de clases de ideales $Cl(\mathcal{O})$, cada autovalor corresponde con un caracter, luego utilizando teoría analítica de números y formas modulares se consigue una cota no trivial para la suma de caracteres que determinan los autovalores, asumiendo la Hipótesis de Riemann Generalizada.

Consideremos entonces para cada $n \in \mathbb{Z}$ la matriz $M(n)$, su entrada ij la denotaremos por $M_{\alpha_i,\alpha_j}(n)$ y viene dada por:

$$M_{\alpha_i,\alpha_j}(n) = \{\beta \lhd \mathcal{O} : \beta\alpha_i \equiv \alpha_j, N(\beta) = n\}$$

donde $\equiv$ denota equivalencia de ideales módulo ideales principales.

Consideremos la función generatriz $\sum_{n=1}^{\infty} M_{\alpha_i,\alpha_j}(n)q^n$ que encapsula de alguna forma toda la información del grafo de clases de ideales. Reescribamos dicha función generatriz de una forma más conveniente.

Primero observemos que si $\beta \lhd \mathcal{O}$ es un $\mathcal{O}$-ideal propio tal que $\beta\alpha_j \equiv \alpha_i$ entonces existe un $\mathcal{O}$-ideal fraccionario principal $(z) = z\mathcal{O}$ que verifica $(z)\alpha_i = \alpha_j\beta$ y resulta que $N(\beta) = N((z)\alpha_i\alpha_j^{-1}) = \frac{N(z)}{N(\alpha_i^{-1}\alpha_j)}$. Además $(z) = \alpha_i^{-1}\alpha_j\beta \subset \alpha_i^{-1}\alpha_j$ pues $\beta \subset \mathcal{O}$.

Recíprocamente, cada $\mathcal{O}$-ideal principal propio $(z) \subset \alpha_i^{-1}\alpha_j$ determina un $\mathcal{O}$-ideal propio $\beta = z\alpha_i\alpha_j^{-1}$ que verifica $\beta\alpha_j \equiv \alpha_i$.

Así que podemos reescribir la función generatriz original en la forma:

$$\sum_{n=1}^{\infty} M_{\alpha_i,\alpha_j}(n)q^n = \sum_{\substack{\beta \lhd \mathcal{O} \\ \beta\alpha_j \equiv \alpha_i}} q^{N(\beta)} = \sum_{(z) \subset \alpha_i^{-1}\alpha_j} q^{\frac{N(z)}{N(\alpha_i^{-1}\alpha_j)}} = \frac{1}{e} \sum_{z \in \alpha_i^{-1}\alpha_j} q^{\frac{N(z)}{N(\alpha_i^{-1}\alpha_j)}}$$

Donde e es el número de unidades del orden $\mathcal{O}$ (se usa que $(z) = (z') \Leftrightarrow z = uz'$ con u unidad).

Fijando una $\mathbb{Z}$-base del ideal $\alpha_i^{-1}\alpha_j$, la función $z \mapsto \frac{N(z)}{N(\alpha_i^{-1}\alpha_j)}$ resulta una forma cuadrática ([**11**], pág.141) y por lo tanto la última suma que aparece es una serie θ que la

denotaremos por $\theta_{\alpha_i^{-1}\alpha_j}(q) = \sum_{z\in\alpha_i^{-1}\alpha_j} q^{\frac{N(z)}{N(\alpha_i^{-1}\alpha_j)}}$, que resulta ser una forma modular holomorfa[9], de peso 1 para $\Gamma_0(|D|)$, donde $D = discr(\mathcal{O})$ ([**24**], sección 4.2 - [**23**], Teo.10.9.).

La idea para la diagonalización simultanea es considerar la matriz $A_q = \sum_{n\geq 1} M(n)q^n$ para cada $|q| < 1$, y diagonalizar simultaneamente todas las $M(n)$ equivale a diagonalizar simultaneamente todas las matrices A_q (encontrando una base de vectores propios, que no dependan de q)[10].

Se consideran entonces los caracteres del grupo de clase de ideales[11] de $\mathcal{O}$, que son interpretados como vectores de $\mathbb{C}^h$ vía evaluación en los α_i (es decir, identificamos χ con el vector columna cuya coordenada i-ésima es $\chi(\alpha_i)$ y las matrices $M(n)$ como operadores que actuan en $\mathcal{L}^2(\mathcal{V})$ obteniendo:

$$(A_q\chi)(\alpha_i) = \frac{1}{e}\sum_{j=1}^{h}\theta_{\alpha_i^{-1}\alpha_j}(q)\chi(\alpha_j) = \frac{1}{e}\sum_{j=1}^{h}\theta_{\alpha_j}(q)\chi(\alpha_i\alpha_j) = \frac{1}{e}\left(\sum_{j=1}^{h}\theta_{\alpha_j}(q)\chi(\alpha_j)\right)\chi(\alpha_i)$$

Lo cual implica que:

$$(eA_q)\chi = \theta_\chi(q)\chi \tag{2}$$

donde $\theta_\chi(q) = \sum_{j=1}^{h}\theta_{\alpha_j}(q)\chi(\alpha_j)$ sería entonces, el valor propio de eA_q asociado al vector propio χ. Observemos además que como cada $\theta_{\alpha_i}(q) \in \mathcal{M}_1(\Gamma_0(|D|))$ para cada $i = 1, 2, \ldots, h$ entonces $\theta_\chi \in \mathcal{M}_1(\Gamma_0(|D|))$. De hecho el conjunto $\{\theta_\chi : \chi \text{ caracter de } Cl(\mathcal{O})\}$ resulta una base de forma modulares formada por autoformas para los operadores de Hecke (sus elementos son conocidos como funciones θ de Hecke) (por detalles y referencias [**24**], pág.31).

Si desarrollamos $\theta_\chi = \sum_{n=1}^{\infty} a_n(\chi)q^n$ y comparamos coeficientes de q^n en la ecuación (2) resulta que $eM(n)\chi = a_n(\chi)\chi$. El grafo de isogenia $S_{N,q,B} = \bigcup_{\ell\leq B}\mathcal{G}_{q,N,\ell}$ donde los índices ℓ de la unión varian en el conjunto de primos menores que B, que tiene matriz de adyacencia $\sum_{\ell\leq B} M(\ell)$ con vectores propios los caracteres χ. Además se tiene que

$$\sum_{\ell\leq B} M(\ell)\chi = \frac{1}{e}\sum_{\ell\leq B} a_\ell(\chi)\chi$$

por lo que el valor propio asociado al valor propio χ es $\lambda_\chi = \frac{1}{e}\sum_{\ell\leq B} a_p(\chi)$.

Haciendo cuenta con ideales JMV prueban que $a_n(\chi) = \sum_{\mathfrak{a}:N(\mathfrak{a})=n}\chi(\mathfrak{a})$ donde $\mathfrak{a}$ varia en los ideales enteros de norma n ([**24**] pág.31), de forma que el valor propio asociado al caracter χ puede expresarse en función de ideales como:

$$\lambda_\chi = \frac{1}{e}\sum_{\ell\leq B}\sum_{\substack{\mathfrak{a}\lhd\mathcal{O}_{\mathbb{K}}:\\ N(\mathfrak{a})=\ell}}\chi(\mathfrak{a}) \tag{3}$$

[9]Con respecto a la variable s donde $q = e^{2s\pi i}$

[10]Los valores propios por otra parte, van a tener necesariamente que depender de q

[11]O sea, homomorfismos de grupo $\chi : Cl(\mathcal{O}) \to \mathbb{C}^*$ donde $Cl(\mathcal{O})$ es el grupo de clases de ideales del orden $\mathcal{O}$.

Como $|\chi(\mathfrak{a})| \leq 1\ \forall \mathfrak{a} \lhd \mathcal{O}_{\mathbb{K}}$, el autovalor de norma máxima se obtiene para $\chi = 1$ el caracter trivial y este corresponde por lo tanto al autovalor trivial. Entonces el problema se resume en encontrar una buena cota para los autovalores λ_χ para χ caracter no trivial y es aquí donde JMV utilizan la Hipótesis de Riemann Generalizada (GRH) que es una análogo a la Hipótesis de Riemann pero para las L-series de Dirichlet[12] $L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ y dice que si $L(\chi, s) = 0$ con $0 < Re(s) < 1$ entonces $Re(s) = \frac{1}{2}$. La parte más difícil para encontrar una cota no trivial, bajo la GRH, para los autovalores no triviales, consiste en probar el siguiente resultado (Lema 4.1. de [**24**]):

Proposición 2.45. *Sea $D < 0$ y $\mathcal{O}$ es el orden cuadrático de discriminante D. Si χ es un caracter no trivial del grupo de clases de ideales del orden $\mathcal{O}$ entonces la Hipótesis de Riemann Generalizada para $L(s, \chi)$ implica que $\lambda_\chi = O(\sqrt{B}\log(|BD|))$ con una constante absoluta implicada*[13]*.*

La demostración es complicada y utiliza Teoría analítica de números incluyendo formas modulares, el hilo de la demostración y referencias se encuentran en [**24**], principalmente la sección 5.

En la siguiente subsección veremos como de la proposición anterior y el Teorema 2.44 se obtiene la propiedad expansora de los grafos de isogenias.

4.3. El Teorema de expansividad de JMV para el grafo de isogenias. Antes de enunciar y probar la propiedad expansora para los grafos de isogenias, analizaremos con un poco más de cuidado el enunciado de la proposición 2.45.

Si llamamos $\mathcal{D} = \{D : D = discr(\mathcal{O})$ para algún orden $\mathcal{O}$ de un cuerpo cuadrático imaginario$\}$ entonces para $B \in \mathbb{Z}^+, D \in \mathcal{D}$ y χ un caracter del grupo de clases de ideales de $\mathcal{O}$, teniamos el autovalor $\lambda_\chi = \lambda_\chi(B, D)$ dado por la ecuación (3). Entonces la proposición 2.45 nos dice que asumiendo GRH, existe una constante K independiente de B y D tales que

$$\frac{\text{máx}_{\chi \neq \chi_{triv}}\, \lambda_\chi(B, D)}{\sqrt{B}\log(|BD|)} < K$$

para todo $D \in \mathcal{D}$ y $B > 1$. Por simplicidad de ahora en más definiremos $\lambda^* = \text{máx}\{|\lambda_\chi| :$ χ caracter no trivial$\}$.

Ahora, para $0 < \beta < 1$ a cada grafo de isogenias $S_{N,q,B}(\mathcal{O})$ podemos asociarle un número (que llamaremos de gap ponderado) dado por $g_\beta = \frac{\lambda^*}{\lambda_{triv}^\beta}$ donde λ^* es el segundo mayor valor propio en módulo y λ_{triv} el valor propio predominante (que coincide con el grado del grafo regular $S_{N,q,B}(\mathcal{O})$). Dado que el orden $\mathcal{O}$ queda unívocamente determinado por su discriminante $D = discr(\mathcal{O})$ el gap ponderado puede verse como función de N, q, B y D, es decir $g_\beta = g_\beta(N, q, B, D)$.

[12]Al igual que la función Zeta de Riemann, esta serie converge para $Re(s) > 1$ y se extiende por prologanción analítica a todo el plano complejo, salvo polos aislados.

[13]Recordar que $f = O(g)$ significa que el cociente $\frac{|f|}{g}$ permanece acotado por cierta constante, en nuestro caso dicha constante es independiente de B y de D.

Fijado q, tenemos finitas posibilidades para N (pues $|q+1-N| \leq 2\sqrt{q}$ por la desigualdad de Hasse) y también para D (pues $D|t^2-4q$ donde $t = q+1-N$ por contener al orden asociado la frobenius), diremos que un par (N, D) es adimisible para q si el grafo de isogenias $S_{N,q,B}$ contiene un nivel asociado al órden de discriminante D (que obviamente no depende de B). Llamaremos $\mathcal{A}(q)$ al conjunto de todos los pares (N, D) admisibles para q.

Fijamos un $\delta > 0$ y establescamos $B(q) = (\log(q))^{2+\delta}$, definimos entonces

$$g_{\beta,\delta}(q) = \max_{(N,D)\in\mathcal{A}(q)} g(N, q, B(q), D)$$

o sea, el mayor gap ponderado posible para los autovalores de cualquier grafo de isogenia $S_{N,q,B,D}$ fijado el q y $B = B(q)$. La siguiente proposición (que como veremos es un corolario del Teorema 2.45) nos dá un resultado sobre el gap ponderado para los grafos de isogenias, que será clave para probar la propiedad expansora para los grafos de isogenia.

Proposición 2.46. *Para cada $\delta > 0$ existe un $\beta \in (\frac{1}{2}, 1)$ tal que la función $g_{\beta,\delta}$ es acotada (vista como función de la variable q)*[14]*.*

Demostración: Sean $\delta > 0$ y $B = (\log(q))^{2+\delta}$. Consideremos un grafo de isogenias $S_{N,q,B}(\mathcal{O})$ con autovalor principal λ_{triv}, en virtud de la ecuación (3), para el caracter trivial se tiene que:

$$\lambda_{triv} = \frac{1}{e}\#\{\mathfrak{a} \lhd \mathcal{O}_{\mathbb{K}} : N(\mathfrak{a}) = \ell, \text{ para algún primo } \ell \leq B\}$$

Si existe un ideal $\mathfrak{a}$ de norma $N(\mathfrak{a}) = \ell$, entonces ℓ descompone o ramifica (que corresponde con $\left(\frac{\ell}{D}\right) = 1$ y $\ell|D$ respectivamente, donde D es el discriminante de $\mathcal{O}_K$), cuando descompone lo hace en dos ideales ($\mathfrak{a}$ e $\overline{\mathfrak{a}}$) por lo tanto

$$\lambda_{triv} = \frac{1}{e} \cdot (2\pi_d(B) + \pi_r(B)) \geq \frac{2\pi_d(B)}{e}$$

donde $\pi_d(B)$ y $\pi_r(B)$ son la cantidad de primos $\ell \leq B$ que descomponen y ramifican en $\mathbb{K}$ respectivamente.

Como la densidad de los primos que descomponen en un cuerpo cuadrático es $\frac{1}{2}$ (Teorema de densidad de Cebotarev) resulta que $2\pi_d(B)$ es asintótico a $\pi(B)$ y por lo tanto también será asintótico a $\frac{B}{\log(B)}$ por el Teorema de los números primos. En particular, existe $q_0 > 0$ tal que

$$\lambda_{triv} \geq \frac{B}{2e\log(B)}$$

para $q \geq q_0$ (pues la desigualdad vale para B suficientemente grande y $B \to \infty$ cuando $q \to \infty$).

Ahora, en virtud de la proposición 2.45, resulta natural intentar acotar superiormente la cantidad $B^{1/2}\log(|BD|)$. Para comenzar recordemos que como todo nivel $\mathcal{O}$ admisible para el grafo $S_{N,q,B}$ debe contener al orden asociado al frobenius, cuyo discriminante es

[14]Este resultado es el que en el artículo [**24**] de Jao,Miller y Venkatesan, lo expresan como $\lambda_\chi = O(\lambda_{triv}^\beta)$.

$t^2 - 4q < 0$ (donde $t = q + 1 - N$ es la traza del frobenius) se tiene que $|D| \leq |t^2 - 4q| = 4q - t^2 \leq 4q$, luego:

$$B^{\frac{1}{2}} \log(|BD|) \leq B^{\frac{1}{2}} \log|4Bq| = B^{\frac{1}{2}} \left(\log(|4B|) + \log(q)\right). \tag{4}$$

Ahora bien, por órdenes existe $q_1 > 0$ tal que $\log(|4B|) \leq B^{\frac{1}{2+\delta}}$ para $q \geq q_1$ (puesto que $B \to \infty$ cuando $q \to \infty$) y como $B = (\log(q))^{2+\delta} \Rightarrow \log(q) = B^{\frac{1}{2+\delta}}$, sustituyendo en (4) se tiene:

$$B^{\frac{1}{2}} \log(|BD|) \leq B^{\frac{1}{2}} \left(B^{\frac{1}{2+\delta}} + B^{\frac{1}{2+\delta}}\right) = 2B^{\frac{1}{2}+\frac{1}{2+\delta}} \tag{5}$$

Luego para cualquier $\beta > \frac{1}{2} + \frac{1}{2+\delta}$, existe $q_2 = q_2(\beta) > 0$ tal que $B^{\frac{1}{2}+\frac{1}{2+\delta}} < \left(\frac{B}{2e\log(B)}\right)^{\beta}$ para todo $q \geq q_2$ (puesto que $(2e)^{\beta} \cdot (\log(B))^{\beta} < B^{\beta-(\frac{1}{2}+\frac{1}{2+\delta})}$ para B suficientemente grande), como $\frac{1}{2} + \frac{1}{2+\delta} < 1$ es posible escoger $\beta < 1$. sustituyendo en (5) resulta que:

$$B^{\frac{1}{2}} \log(|BD|) \leq 2\left(\frac{B}{2e\log(B)}\right)^{\beta} \leq 2\lambda_{triv}^{\beta}$$

para $q \geq \text{máx}\{q_0, q_1, q_2\}$. Para $q < \text{máx}\{q_0, q_1, q_2\}$ solo hay un número finito de posibilidades para D y por lo tanto un número finito posible de valores para $B^{\frac{1}{2}} \log(|BD|)$ (recordar que $B = (\log(q))^{2+\delta}$), por lo tanto se puede afirmar que $B^{\frac{1}{2}} \log(|BD|) = O(\lambda_{triv}^{\beta})$ y luego por la proposición 2.45 resulta que $\lambda^* = O(\lambda_{triv})$ para cualquier grafo de isogenias $S_{N,q,B}(\mathcal{O})$ lo cual implica que $g_\beta(q)$ es una función acotada de q.

□

Por último enunciaremos y probaremos a partir de la proposición anterior el Teorema de expansividad de JMV para el grafo de isogenias.

Teorema 2.47. *Existen polinomios $p(x)$ y $q(x)$ (independientes de N y q) tal que para $B = p(\log(q))$ y $r_0 = g(\log(q))$, se tiene que fijando $r \geq r_0$, un vértice v, un conjunto de vértices S del grafo $S_{N,q,B}(\mathcal{O})$ entonces todo camino al azar de largo r que comienze en v terminará en S con probabilidad $P \geq \frac{h}{2|S|}$, donde h es el número de vértices del grafo $S_{N,q,B}(\mathcal{O})$.*

Demostración: Fijemos $\delta \in \mathbb{Z}^+$ y consideremos el polinomio $p_0(x) = x^{2+\delta}$, como vimos en la proposición anterior, tomando β tal que $\frac{1}{2} + \frac{1}{2+\delta} < \beta < 1$ resulta que $\lambda^* = O(\lambda_{triv})$. En virtud de la Proposición 2.44, basta probar que

$$\frac{\log\left(\frac{2h}{|S|^{\frac{1}{2}}}\right)}{\log\left(\frac{k}{c}\right)} \leq g(\log(q))$$

para algún polinomio g, donde h es la cantidad de vértices del grafo $S_{N,q,B}(\mathcal{O})$, $k = \lambda_{triv}$ es su grado y c es una cota superior para los autovalores no triviales, en este caso podemos tomar $c = \lambda^*$.

Por la proposición anterior, existe una constante $C > 0$ (independiente del grafo de isogenias escogido) tal que $c \leq Ck^{\beta}$ lo cual implica que $\frac{k}{c} \geq C^{-1}k^{1-\beta}$, pero $1 - \beta > 0$ y $k \geq \frac{B}{2e\log(B)} \to \infty$ cuando $q \to \infty$ (puesto que $B = (\log(q))^{2+\delta}$) así que tenemos $\frac{k}{c} > e$

para q suficientemente grande, digamos para todo $q \geq q_0$ (para cierto $q_0 > 0$), de donde:

$$\frac{\log\left(\frac{2h}{|S|^{\frac{1}{2}}}\right)}{\log\left(\frac{k}{c}\right)} \leq \frac{\log(2h)}{\log\left(\frac{k}{c}\right)} \leq \log(2h) \leq \log(2q) = \log(2) + \log(q) \leq 2\log(q)$$

para $q \geq q_0$. Esto prueba el Teorema para q suficientemente grande (mayor que q_0).

Para $q \leq q_0$ solo hay un número finito de grafos de isogenias de la forma $S_{N,q,B}(\mathcal{O})$ (donde $B = p(\log(q))$), cada uno de esos grafos tiene un número $\frac{\log(2h)}{\log\left(\frac{k}{c}\right)}$ asociado, consideremos una cota superior $M > 0$ para todos esos valores (que son una cantidad finita), o sea para $q \leq q_0$ tenemos:

$$\frac{\log\left(\frac{2h}{|S|^{\frac{1}{2}}}\right)}{\log\left(\frac{k}{c}\right)} \leq \frac{\log(2h)}{\log\left(\frac{k}{c}\right)} \leq M$$

En general tenemos que:

$$\frac{\log\left(\frac{2h}{|S|^{\frac{1}{2}}}\right)}{\log\left(\frac{k}{c}\right)} \leq 2\log(q) + M = g(\log(q))$$

tomando el polinomio $g(x) = 2x + M$.

Para terminar la prueba, solo falta ver que se verifica la hipótesis de separación espectral del Teorema 2.44 para primos pequeños (es decir cuando $q \leq q_0$). Para esta parte también debemos recurrir a otro teorema clásico de Teoría de grafos.

Teorema 2.48. *Sea G un (multi)grafo k-regular no dirigido.*

i) *La cantidad de componentes conexas de G coincide con la multiplicidad de k como autovalor de G.*
ii) *Si G es conexo y $-k$ es un autovalor de G entonces G es bipartito.*

La demostración de este Teorema puede encontrarse en el libro de Brouwer y Haemers [**6**], la primer parte es la Prop. 1.3.8 y la segunda la Prop. 3.4.1. Ahora concluiremos la prueba del Teorema 2.47 para q pequeño a partir de estos resultados de grafos.

Como todo ideal propio de un orden $\mathcal{O}$ en un cuerpo imaginario descompone como producto de ideales primos propios, usando la correspondencia vista en la sección 3 entre el grafo de isogenias $S_{N,q,B}$ restricto a un nivel $\mathcal{O}$ y el grafo de Cayley del grupo de clases de ideales de $\mathcal{O}$ con generadores clases de ideales que contengan algún ideal de norma menor que B, resulta que, para B suficientemente grande este grafo resultará conexo. Más aún, es posible (aunque bastante difícil) probar que cada clase de ideales debe contener algún ideal primo (Teoremas 7.7 y 9.12 del libro de Cox [**11**]), por lo tanto a partir de un B, cualquier par de vértices estará conectado por alguna arista, de modo que el grafo $S_{N,q,B}(\mathcal{O})$ no puede ser bipartito.

De esa forma, por el Teorema 2.48 se verifica la hipótesis de separación espectral para cualquier grafo $S_{N,q,B}(\mathcal{O})$ para B suficientemente grande. Como cada grafo $S_{N,q,B}$ tiene un número finito de niveles $\mathcal{O}$ y por cada q hay solo un número finito de posibilidades para N, entonces existe una constante $K > 0$ (solo dependiente de q_0) tal que para cualquier grafo

de isogenias $S_{N,q,B}(\mathcal{O})$ con $q \leq q_0$ se verifica la hipótesis de separabilidad para $B \geq K$.

Esto prueba entonces que el Teorema 2.47 vale (tanto para q grande como para q pequeño) con $p(x) = x^{2+\delta} + K$ y $g(x) = 2x + M$.

□

Capítulo 3

Algoritmo de Autoreducibilidad aleatoria

El objetivo de este capítulo es implementar un algoritmo de autoreducibilidad aleatoria como lo sugiere el artículo [**24**] de Jao-Miller-Venkatesan. Para comenzar repasaremos la noción de autoreducibilidad aleatoria en general probando como ejemplo y sobretodo para fijar ideas que el Problema del Logaritmo en un grupo cíclico de orden primo es autoreducible. En las siguientes secciones enfocaremos la atención a nuestro problema de interés que es la autoreducibilidad aleatoria aplicado al problema de determinar si curvas elípticas definidas sobre el mismo cuerpo finito y con la misma cantidad de puntos racionales poseen la misma dificultad respecto al Problema del Logaritmo Discreto.

1. Autoreducibilidad aleatoria en general.

Que un problema posea autoreducibilidad aleatoria significa que es posible construir algoritmos eficientes (por ejemplo de tiempo polinomial o subexponencial) capaces de reducir el problema de una instancia cualquiera dada a una instancia tomada al azar con cierta distribución.

Veremos una posible formalización de las propiedades que debe cumplir un algoritmo para garantizar la autoreducibilidad aleatoria de un problema. Probaremos como ejemplo que el PLD en un grupo de orden primo es autoreducible construyendo un algoritmo que verifique dichas propiedades.

Supongamos que queremos computar cierta función f que toma valores en un conjunto finito $\mathcal{A}$ cuyos elementos son llamados "instancias" (el conjunto $\mathcal{A}$ puede depender de algunos parámetros) y devuelve valores en un conjunto no necesariamente finito $\mathcal{B}$ (valores de salida). Supongamos que tenemos un conjunto finito $\mathcal{K}$ que llamamos conjunto comodín y que asociado a cada instancia $a \in \mathcal{A}$ tenemos un subconjunto $\mathcal{K}(a) \subset \mathcal{K}$.

Definición 3.1 (Autoreducibilidad aleatoria)**.** Un algoritmo de Autoreducibilidad aleatoria para el problema de computar la función f es la construcción de una pareja (Ran, Red) donde:

1. (La parte aleatoria) El algoritmo Ran es un algoritmo probabilístico que tiene asociado una función determinística
$$tr : \{(a,k) : a \in \mathcal{A}, k \in \mathcal{K}(a)\} \subset \mathcal{A} \times \mathcal{K} \to \mathcal{A}$$
llamada función de transición. Si $a \in \mathcal{A}$ es una instancia dada entonces $Ran(a) = (a', k)$ tales que:
   a) $k \in_R \mathcal{K}(a)$ con cierta distribución[1] tal que para cada $a_0 \in \mathcal{A}$ se tiene que $P\left(tr(a,k) = a_0\right) \geq \frac{1}{2A}$ donde $A = \#\mathcal{A}$.

[1]El símbolo $\in_R$ denota la relación de pertenencia usual, el subíndice R (que viene de "Random") es simplemente para recalcar el hecho de que ese elemento fué elegido al azar dentro del conjunto considerado.

   b) $a' = tr(a, k)$.
   c) Tanto la construcción del comodín k como la computación de $tr(a, k)$ se debe poder hacer en tiempo polinomial.
2. (La parte de reducibilidad) La función de reducción $Red : \mathcal{B} \times \mathcal{K} \to \mathcal{B} \cup \{\perp\}$ es una función que se debe poder computar en tiempo polinomial y que verifica la propiedad $Red\left(f\left(a'\right), k\right) = f(a)$, donde $a' = tr(a, k)$.

En concreto lo que hace *Ran* es cambiar una instancia dada a por una instancia al azar a' con distribución cercana a la uniforme, guardando además una información extra que es el comodín k, que luego, junto con el valor de $f(a')$ es usado por el algoritmo *Red* para calcular $f(a)$. Si justo nos topamos con un a' tal que $f(a')$ puede calcularse efectivamente entonces también podremos calcular efectivamente $f(a)$ a partir del algoritmo de autoreducibilidad aleatoria.

La condición *(a)* de la parte aleatoria puede relajarse (y en nuestro problema concreto lo vamos a necesitar) introduciendo el concepto de compatibilidad de una relación de equivalencia.

Definición 3.2. Sea $f : \mathcal{A} \to \mathcal{B}$ una función, una relación de equivalencia $\mathcal{R}$ se dice compatible con el problema de computar f si $a_1 \mathcal{R} a_2$ implica que computar $f(a_1)$ y $f(a_2)$ son problemas computacionalmente equivalentes (es decir, existe un algoritmo polinomial para calcular $f(a_1)$ a partir de conocer $f(a_2)$ y viceversa).

De esa manera podemos fijar de antemano una relación de equivalencia $\mathcal{R}$ compatible con el problema de computar f y cambiar la condición *(a)* por:

a') $k \in_R \mathcal{K}(a)$ con cierta distribución tal que para cada $[a_0] \in \mathcal{A}/\mathcal{R}$ se tiene que $P([tr(a, k)] = [a_0]) \geq \frac{1}{2r}$ donde $r = \#\mathcal{A}/\mathcal{R}$.

Estamos interesados especialmente en problemas relacionados con el Problema del logaritmo discreto (PLD) así que vamos a introducir una notación que nos será de utilidad:

Notación 3.3. Si G es un grupo de orden finito N denotamos por PLD_G a la función $PLD_G : G^2 \to \mathbb{Z} \cup \{\perp\}$ dada por

$$PLD_G(g, h) = \begin{cases} \text{mín}\{t \in \mathbb{N} : h = g^t\} & \text{si } \{t \in \mathbb{N} : h = g^t\} \neq \varnothing \\ \perp & \text{si } \{t \in \mathbb{N} : h = g^t\} = \varnothing \end{cases}$$

Observemos que en el caso que $\{t \in \mathbb{N} : h = g^t\} \neq \varnothing$ entonces denotando por t_0 al menor elemento de ese conjunto se tiene que $h = g^t \Leftrightarrow t \equiv t_0 \pmod{o(g)}$ (donde $o(g)$ es el orden de g). En particular, el conjunto de exponentes t tales que $h = g^t$ será en este caso $N\mathbb{Z}$-invariante, por eso a veces consideraremos como dominio de PLD_G a $\mathbb{Z}/N\mathbb{Z} \cup \{\perp\}$ (tomando clases) en lugar $\mathbb{Z} \cup \{\perp\}$.

Recordamos que el PLD en un grupo G consiste en dada una pareja $(g, h) \in G^2$ tal que $h \in \langle g \rangle$ computar algún $t \in \mathbb{Z}$ tal que $h = g^t$. En el caso que tengamos algoritmos eficientes para computar $|G|$ y los órdenes de los elementos, así como un método para determinar si $h \in \langle g \rangle$ para una pareja dada $(g, h) \in G^2$ entonces resolver el PLD en G es equivalente a computar la función PLD_G (si $t \in \mathbb{Z}$ es tal que $h = g^t$ y t_0 es el resto de

dividir t entre $o(g)$ entonces $t_0 = PLD_G(g,h)$).

1.1. Autoreducibilidad aleatoria del logaritmo discreto. Para fijar ideas vamos a probar autoreducibilidad aleatoria para el PLD en un grupo finito de orden primo, este ejemplo está sacado del libro de Galbraith [**19**] (Cap.2.1.4).

Como $|G| = p$ primo entonces todo elemento $g \neq e$ (donde e es el elemento neutro) tiene orden $o(g) = p$ y es un generador del grupo, por lo tanto dados $(g,h) \in G^2$ si $g \neq e$ entonces $h \in \langle g \rangle \ \forall h \in G$ y si $g = e$ entonces $h \notin \langle g \rangle$ salvo si $h = e$. Así que en este caso, podemos considerar como conjunto de instancias para el PLD en G al conjunto $\mathcal{A} = \mathcal{A}(G) = \{(g,h) : g \in G^*, h \in G\}$ (donde $G^* = G - \{e\}$) y el PLD consiste en computar $f = PLD_G : \mathcal{A} \to \mathbb{Z}/p\mathbb{Z}$ tal que $f(g,h) = b \Leftrightarrow h = g^b$.

Proposición 3.4. *El PLD en un grupo finito G de orden primo p es autoreducible.*

Demostración: Sea (g,h) una instancia particular y elegimos $(x,y) \in \{1,2,\ldots,p-1\} \times \{0,1,2,\ldots,p-1\}$ al azar con distribución uniforme. Calculamos $(g^x, h^x g^{xy})$, como cada par $(g_1,g_2) \in \mathcal{A}(G)$ proviene de exactamente un par (x,y) (del x tal que $g^x = g_1$ y del y tal que $g_1^y = g_2 h^{-x}$, aquí utilizamos que todo elemento distinto de e es generador lo cual es cierto pues G tiene orden primo) de esa manera construimos una instancia al azar uniformemente. Si tenemos la solución para la instancia que obtuvimos aleatoria $f(g^x, h^x g^{xy}) = a$ entonces $h^x g^{xy} = g^{xa} \Leftrightarrow h g^y = g^a$ (usamos que $p \nmid x$) $\Leftrightarrow h = g^{a-y}$ luego tenemos para la instancia original la solución $f(g,h) = a - y$.

□

La construcción de un algoritmo de autoreducibilidad aleatoria para el problema de computar una función $f : \mathcal{A}(G) \to \mathbb{Z}/p\mathbb{Z}$ que resuelva el PLD nos dice en algún sentido que la dificultad de computar el PLD en un grupo finito G fijo de orden primo es independiente de la instancia considerada.

Analizemos la demostración anterior en términos de la construcción de un algoritmo (Ran, Red):

Como conjunto de instancias tenemos $\mathcal{A} = G^* \times G$ y consideramos como relación de equivalencia en $\mathcal{A}$ la trivial ($[a] = \{a\}, \forall \mathcal{A}$), como conjunto de posibles salidas tenemos $\mathcal{B} = \mathbb{Z}/p\mathbb{Z}$ y la función $f : \mathcal{A} \to \mathbb{Z}/p\mathbb{Z}$ a computar es PLD_G, la que nos brinda el logaritmo discreto en el grupo G. El conjunto comodín en este caso viene dado por $\mathcal{K} = \{1,2,\ldots,p-1\} \times \{0,1,2,\ldots,p-1\}$ y el subconjunto de comodines asociado a cada instancia $a \in \mathcal{A}$ viene dado en este caso por $\mathcal{K}(a) = \mathcal{K}$.

La función de transición en este caso viene dada por $tr\left((g,h),(x,y)\right) = (g^x, h^x g^{xy})$.

Los comodines en este caso se eligen al azar uniformemente, suponemos siempre que tenemos un generador de números aleatorios con valores en un intervalo a especificar, donde cada valor de dicho intervalo es equiprobable, de esa forma, aplicando ese generador obtenemos $x \in_R \{1,2,\ldots,p-1\}$ e $y \in_R \{0,1,2,\ldots,p-1\}$ y calcular $(g^x, h^x g^{xy})$ se logra en tiempo polinomial usando el algoritmo de exponenciación binario (suponiendo que tenemos un algoritmo eficiente para computar las operaciones de grupo). De esa manera

el algoritmo $Ran(g,h) = ((g^x, h^x g^{xy}), (x,y))$ puede realizarse efectivamente.

Con respecto a la función de reducción, en este caso viene dada por $Red : \mathbb{Z}/p\mathbb{Z} \times \mathcal{K} \to \mathbb{Z}/p\mathbb{Z}, (a,(x,y)) = a - \overline{y}$ (donde $\overline{y} = y \pmod p$) que claramente puede efectuarse en tiempo polinomial (suponemos que el orden p del grupo G lo tenemos precomputado), si $a = f((g^x, h^x g^{xy}))$ entonces $h^x g^{xy} = g^{xa}$ como vimos en la demostración esto implica que $f(g,h) = a - y$ así que conociendo el comodín (x,y) es inmediato computar $a - y = Red(f((g^x, h^x g^{xy})), (x,y))$.

1.2. Curvas elípticas sobre $\mathbb{F}_q$ con el mismo cardinal. El trabajo de Jao-Miller-Venkatesan [**24**] es un resultado teórico motivado a responder la pregunta de si la dificultad del logaritmo discreto en una curva elíptica solo depende de su cardinal (que es lo que se hace en la práctica, se escoge una curva elíptica $E/\mathbb{F}_q$ y se calcula[2] $\#E(\mathbb{F}_q) = N$) y en función de este número se discrimina si una curva es buena o mala para fines criptográficos.

Específicamente se consideran 3 parámetros que son q (el orden del cuerpo finito de definición de las curvas), N de forma que exista al menos una curva ordinaria $E/\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = N$ y $\mathcal{O} = \mathrm{End}(E)$ el tipo de endomorfismo de la curva E (que queda determinado a través de su discriminante D). El conjunto de instancias en este caso será $\mathcal{A}(q,N,\mathcal{O}) = \{E/\mathbb{F}_q : \#E(\mathbb{F}_q) = N, \mathrm{End}(E) = \mathcal{O}\}$ y la función f a computar en este caso será $E \mapsto PLD_E$ para cada $E \in \mathcal{A}(q,N,\mathcal{O})$ (a la función f la notaremos como PLD).

Hay dos puntos a considerar, el primer punto es aclarar qué es tener una función (o devolver una función) PLD_E, tener una función significa tener un método eficiente para poder calcular su valor en cualquier instancia determinada. El segundo punto es respecto al concepto de eficiencia, qué significa ser eficiente, en este caso el conjunto de instancias $\mathcal{A}$ queda determinado por los tres parámetros N, q y $\mathcal{O}$ (o respectivamente su determinante D) como vimos previamente, dado que $N \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ y $D \leq d_\pi = t^2 - 4q \leq 4q^2$ (donde d_π es el discriminante del Frobenius y t su traza y la última desigualdad es porque $t = q+1-N$ también pertenece al intervalo de Hasse) se tiene que $N = O(q)$ y $D = O(q^2)$ y por lo tanto el largo de la entrada es $O(\log(q) + \log(q) + 2\log(q)) = O(\log(q))$.

Por las consideraciones anteriores diremos que un algoritmo con instancias en el conjunto $\mathcal{A}$ es eficiente si su costo es polinomial en $\log(q)$. Respecto la función PLD_E, cada instancia es una pareja de puntos de $E(\mathbb{F}_q)$ cuyo tamaño es del orden de $\log(q)$ así que una implementación eficiente de PLD_E también debe ser de costo polinomial en $\log(q)$.

La construcción de un algoritmo eficiente de autoreducibilidad aleatoria para este caso nos dice que la dificultad del Problema del Logaritmo Discreto en una curva elíptica $E/\mathbb{F}_q$ solo dependen del cuerpo de definición $\mathbb{F}_q$, del cardinal $N = \#E(\mathbb{F}_q)$ y del tipo de anillo de endomorfismo $\mathrm{End}(E)$, que es un paso en la dirección de probar que la dificultad del PLD en una curva elíptica definida sobre un cuerpo finito solo depende de su cardinal.

En este caso nos convendrá utilizar una relación de equivalencia en $\mathcal{A} = \mathcal{A}(q,N,\mathcal{O})$ compatible con el problema de computar f que sea distinta de la trivial. Para sacar provecho de los resultados de Jao-Miller-Venkatesan sobre las propiedades expansivas del grafo

[2]Hay buenos algoritmos para calcular $N = \#E(\mathbb{F}_q)$, por ejemplo el algoritmo de Schoof [**34**] que calcula N en tiempo polinomial y otras versiones mejoradas.

de isogenias vamos a definir la relación de equivalencia en $\mathcal{A}$ dada por $E_1 \sim E_2 \Leftrightarrow j(E_1) = j(E_2)$. Para poder usar esta relación en un algoritmo de autoreducibilidad aleatoria debemos probar que es compatible con el problema de computar f.

Probemos previamente el siguiente lema:

Lema 3.5. *Sean $E_1/\mathbb{F}_q$ y $E_2/\mathbb{F}_q$ dos curvas elípticas ordinarias definidas sobre $\mathbb{F}_q$. Supongamos que $j(E_1) = j(E_2)$ y que existe una isogenia $\phi : E_1 \to E_2$ definida sobre $\mathbb{F}_q$ entonces existe un isomorfismo $\psi : E_1 \to E_2$ definido sobre $\mathbb{F}_q$.*

Demostración: Para comenzar recordemos que dos curvas son isógenas sobre $\mathbb{F}_q$ si y solo si tienen la misma cantidad de puntos sobre $\mathbb{F}_q$ (Teorema de Isogenia de Tate) y observemos que si $E/\mathbb{F}_q$ y χ es el caracter cuadrático en $\mathbb{F}_q$ entonces el número de puntos sobre $\mathbb{F}_q$ para una curva elíptica $E : Y^2 = f(X)$ con $f(X) = X^3 + aX + b \in \mathbb{F}_q[X]$ está dado por:

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) \tag{6}$$

En efecto, si $\chi(f(x_0)) = 1$ este x_0 aporta $2 = 1+\chi(f(x_0))$ puntos $(x_0, \pm y_0) \in E(\mathbb{F}_q)$ (donde $y_0^2 = f(x_0)$), si $\chi(f(x_0)) = -1$ entonces aporta $0 = 1 + \chi(f(x_0))$ puntos y si $\chi(f(x_0)) = 0$ entonces aporta $1 = 1 + \chi(f(x_0))$ punto que es $(x_0, 0) \in E(\mathbb{F}_q)$ y el 1 de adelante es por el punto $\mathcal{O}$ del infinito. Observemos que reagrupando esta ecuación es equivalente a:

$$t = -\sum_{x \in \mathbb{F}_q} \chi(f(x)) \tag{7}$$

donde $t = q + 1 - \#E(\mathbb{F}_q)$ es la traza del Frobenius en la curva elíptica E.

El caso más sencillo es cuando $j = j(E_1) = j(E_2) \neq 0, 1728$ donde tenemos dos clases de $\mathbb{F}_q$-isomorfismo para curvas con $j(E) = j$ (Teo.1.39), consideramos un representante de cada clase $E : Y^2 = f(X)$ y $E_\nu : \nu Y^2 = f(X)$ donde $f(X) = X^3 + aX + b$ y $\nu \in \mathbb{F}_q^*/\mathbb{F}_q^{*2}$. Observemos que para cada $x \in \mathbb{F}_q$ si $\chi(f(x)) = 1$ entonces aporta $0 = 1 - \chi(f(x))$ puntos a $E_\nu(\mathbb{F}_q)$, si $\chi(f(x)) = -1$ aporta $2 = 1 - \chi(f(x))$ puntos a $E_\nu(\mathbb{F}_q)$ y si $\chi(f(x)) = 0$ aporta $1 = 1 - \chi(f(x))$ puntos a $E_\nu(\mathbb{F}_q)$ por lo tanto para el twist se tiene $\#E_\nu(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (1 - \chi(f(x)))$ y usando la ecuación (6) obtenemos que $\#E(\mathbb{F}_q) + \#E_\nu(\mathbb{F}_q) = 2(q+1)$. Ahora si tomamos $E_1/\mathbb{F}_q$ y $E_2/\mathbb{F}_q$ dos curvas elípticas ordinarias que verifiquen las hipótesis del lema, si estuviesen en distinta clase de $\mathbb{F}_q$-isomorfismo entonces una seria isomorfa sobre $\mathbb{F}_q$ a E y la otra a E_ν, supongamos que E_1 sea isomorfa sobre $\mathbb{F}_q$ a E y que E_2 lo sea a E_ν, dichos isomorfismos inducen isomorfismos de grupos sobre los puntos $\mathbb{F}_q$-racionales de donde $\#E_1(\mathbb{F}_q) = \#E(\mathbb{F}_q)$ y $\#E_2(\mathbb{F}_q) = \#E_\nu(\mathbb{F}_q)$, por el Teorema de Isogenias de Tate se tiene además que $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ por lo tanto $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = q+1$ contradiciendo que sean ordinarias (ver [**22**], Teorema 4.6).

El caso $j = 0$ o $j = 1728$ es un poco más complicado, la idea en ambos casos es utilizar la fórmula de la traza del Frobenius (7).

Para el caso $j = 0$, toda curva es de la forma $E : Y^2 = X^3 + b$ y se puede calcular explícitamente la traza obteniendo $t = \binom{3s}{2s} b^s$ donde $q = 6s + 1$ (el caso ordinario solo puede darse para $j = 0$ cuando $q \equiv 1 \pmod 6$). De esa forma, si $E_1 : Y^2 = X^3 + b_1$ y $E_2 : Y^2 = X^3 + b_2$ con $b_1, b_2 \in \mathbb{F}_q$ son dos curvas elípticas ordinarias que verifican las

hipótesis del Lema con $j(E_1) = j(E_2) = 0$, al ser $\mathbb{F}_q$-isógenas tienen la misma cantidad de puntos sobre $\mathbb{F}_q$ y por lo tanto la traza de sus Frobenius $t_1 = \binom{3s}{2s} b_1^s$ y $t_2 = \binom{3s}{2s} b_2^s$ coinciden. Esto último implica que $\left(\frac{b_2}{b_1}\right)^{\frac{q-1}{6}} = 1$, que a su vez implica que $\frac{b_2}{b_1} = u^6$ para algún $u \in \mathbb{F}_q^*$ y por el Teorema 1.32 las curvas E_1 y E_2 resultan isomorfas sobre $\mathbb{F}_q$.

Para el caso $j = 1728$, el caso ordinario solo puede darse cuando $q = 4s+1$ y las curvas elípticas para ese j-invariante son de la forma $E : Y^2 = X^3 + aX$. Con un cálculo explícito usando (7) resulta que $t = \binom{2s}{s} a^s$ y con un razonamiento análogo al anterior se llega a que dos curvas $E_1 : Y^2 = X^3 + a_1 X$ y $E_2 : Y^2 = X^3 + a_2 X$ isógenas sobre $\mathbb{F}_q$ deben cumplir $\left(\frac{a_2}{a_1}\right)^{\frac{q-1}{4}} = 1$ (por tener la misma traza de frobenius) de donde $\frac{a_2}{a_1} = u^4$ para algún $u \in \mathbb{F}_q^*$, luego, por el Teorema 1.32 las curvas E_1 y E_2 resultan isomorfas sobre $\mathbb{F}_q$.

Más detalles sobre las cuentas puede verse en [**22**] (Cap.4, Teo.4.14, pág.113).

□

Corolario 3.6. *Dos curvas elípticas ordinarias $E_1/\mathbb{F}_q$ y $E_2/\mathbb{F}_q$ son $\mathbb{F}_q$-isomorfas $\Leftrightarrow (j(E_1), \#E_1(\mathbb{F}_q)) = (j(E_2), \#E_2(\mathbb{F}_q))$.*

Proposición 3.7. *La relación de equivalencia en $\mathcal{A}$ determinada por el j-invariante es compatible con el problema de computar $f = PLD$.*

Demostración: Sean $E_1/\mathbb{F}_q$ y $E_2/\mathbb{F}_q$ dos curvas elípticas en $\mathcal{A}(q, N, \mathcal{O})$ con $j(E_1) = j(E_2) = j$, tenemos que ver que el problema de computar PLD_{E_1} puede reducirse eficientemente al problema de computar PLD_{E_2}.

Como $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = N$, las curvas elípticas E_1 y E_2 son $\mathbb{F}_q$-isógenas (Teorema de Isogenias de Tate) y al tener el mismo j-invariante resultan ser $\mathbb{F}_q$-isomorfas por el Lema 3.5. Si denotamos $E_i : Y^2 = X^3 + a_i X + b_i$ para $i = 1, 2$ entonces por el Teo.1.32 todo $\mathbb{F}_q$-isomorfismo $\phi : E_1 \to E_2$ es de la forma $(X, Y) \mapsto (u^2 X, u^3 Y)$ con $u \in \mathbb{F}_q$ (el Teorema dice que todo isomorfismo es de esa forma para algún $u \in \overline{\mathbb{F}_q}$, que esté definido sobre $\mathbb{F}_q$ implica que $u^2 \in \mathbb{F}_q$ y $u^3 \in \mathbb{F}_q$, lo cual implica $u \in \mathbb{F}_q$) verificando el sistema:

$$\begin{cases} a_2 = u^4 a_1 \\ b_2 = u^6 b_1 \end{cases} \tag{8}$$

donde además cada solución del sistema nos brinda un isomorfismo.

Resolviendo el sistema (8) (con incógnita u) podemos hallar explícitamente el isomorfismo $\phi : E_1 \to E_2$. Separamos en 3 casos, si $j \neq 0, 1728$ entonces $a_1 a_2 b_1 b_2 \neq 0$ y dividiendo tenemos que $u^2 = \frac{a_1 b_2}{a_2 b_1}$ así que el problema se reduce a resolver una raíz cuadrada en el cuerpo finito $\mathbb{F}_q$. Si $j = 0$ entonces $a_1 = a_2 = 0$ y $b_1 b_2 \neq 0$ así que la condición resulta en este caso $u^6 = \frac{b_2}{b_1}$ y el problema se reduce a resolver en este caso una raíz sexta en $\mathbb{F}_q$ (o equivalentemente una raíz cuadrada más una raíz cúbica). Si $j = 1728$ entonces $b_1 = b_2 = 0$ y $a_1 a_2 \neq 0$, la condición sobre $u \in \mathbb{F}_q$ queda $u^4 = \frac{a_2}{a_1}$ y el problema se reduce a la resolución de una raíz cuarta en $\mathbb{F}_q$ (o equivalentemente dos raices cuadradas).

Una vez construido el isomorfismo $\phi : E_1 \to E_2$, como está definido sobre $\mathbb{F}_q$, este induce un isomorfismo de grupos $\phi : E_1(\mathbb{F}_q) \to E_2(\mathbb{F}_q)$ dado por $\phi(x, y) = (u^2 x, u^3 y)$

que tiene una implementación eficiente (dado $(x,y) \in E_1(\mathbb{F}_q)$ computar $\phi(x,y)$ requiere apenas dos multiplicaciones en $\mathbb{F}_q$) al igual que su inversa $\phi^{-1}(x,y) = (u^{-2}x, u^{-3}y)$. Por lo tanto si queremos computar PLD_{E_2} en una instancia $(P',Q') \in E_2(\mathbb{F}_q)$ hallamos $(P,Q) = \phi^{-1}(P',Q')$, resolvemos $t = PLD_{E_2}(P,Q)$ y ese mismo valor verifica $Q' = (P')^t$ (pues los isomorfismos preservan el orden).

Ahora debemos ver que la reducción se puede llevar en forma eficiente. Como vimos, el costo computacional de la reducción es el de computar explícitamente un isomorfismo entre las dos curvas elípticas y este se resume en última instancia a algunos de estos tres problemas

- Cálculo de una raíz cuadrada sobre $\mathbb{F}_q$ (si $j \neq 0, 1728$).
- Cálculo de una raíz cuadrada y una raíz cúbica sobre $\mathbb{F}_q$ (si $j = 0$).
- Cálculo de dos raices cuadradas sobre $\mathbb{F}_q$ (si $j = 1728$).

Luego la reducción puede llevarse a cabo de forma eficiente ya que la extracción de raices cuadradas y cúbicas sobre cuerpos finitos puede hacerse en forma eficiente, como puede verse por ejemplo en [**31**] y [**10**] pág.221.

□

Ahora que tenemos la relación de equivalencia definida en $\mathcal{A}$ vamos a construir la pareja (Ran, Red) para implementar el algoritmo de autoreducibilidad aleatoria para el problema de computar $f = PLD$ en $\mathcal{A} = \mathcal{A}(q, N, \mathcal{O})$.

2. La parte Aleatoria.

El resultado Teórico clave para una eficiente implementación del algoritmo *Ran* es el que aparece en el artículo [**24**] de Jao-Miller-Venkatesan (Teo.1.1.) que es la existencia de dos polinomios $p(x)$ y $g(x)$ independientes de N y q tal que para $B = p(\log(q))$, el grafo $S_{N,q,B}(\mathcal{O})$ resulta un grafo expansor, en el sentido del Teorema 2.47, es decir, para cada par de vértices j y j' dados de $S_{N,q,B}(\mathcal{O})$, si tomamos un camino al azar de largo $r_0 = g(\log(q))$ comenzando en j entonces la probabilidad de que termine en j' es de al menos $\frac{1}{2h}$ donde h es la cantidad de vértices de $S_{N,q,B}(\mathcal{O})$.

2.1. Construcción de la función de transición. Antes de definir la función de transición para el algoritmo *Ran* vamos a definir nuestro conjunto $\mathcal{K}$ de comodines, en este caso nuestro conjunto de comodines $\mathcal{K}$ vendrá dado por todos los caminos $\{(E_0, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0})$ con $E_0 \in \mathcal{A} = \mathcal{A}(q, N, \mathcal{O})$ y $\varphi_i : E_{i-1} \to E_i$ isogenias definidas sobre $\mathbb{F}_q$ de grado primo $\ell \leq B$ para $1 \leq i \leq r_0$; donde $B = p(\log(q))$ y $r_0 = g(\log(q))$ son los del Teo.1.1. de [**24**] (como $E_0/\mathbb{F}_q$ y las isogenias ϕ_i están definidas sobre $\mathbb{F}_q$ para $1 \leq i \leq r_0$ entonces las curvas elípticas E_i estarán también definidas sobre $\mathbb{F}_q$ para $i = 1, 2, \ldots, r_0$). Para cada instancia $E \in \mathcal{A}$ definimos su conjunto de comodines asociados como aquellos caminos de isogenias que comienzan en E, es decir $\mathcal{K}(E) = \{(E_0, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0}) \in \mathcal{K} : E_0 = E\}$.

Para cada pareja (E,k) donde $E \in \mathcal{A}$ y $k = (E, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0}) \in \mathcal{K}(E)$ definimos la función de transición como $tr(E,k) = E_{r_0}$ (o sea, como la curva de llegada del camino k).

2.2. Construcción del comodín. Un aspecto sutil en la implementación del algoritmo *Ran* es la construcción del comodín y aquí entra en juego las propiedades expansivas

del Grafo de Isogenias (cuyos vértices está formado por j-invariantes).

Para comenzar *Ran* toma como entrada una instancia particular $E \in \mathcal{A}(q, N, \mathcal{O})$, calculamos a continuación su j-invariante $j(E) = j_0$, ese j-invariante será un vértice del grafo de isogenias (o grafo de j-invariantes) $S_{N,q,B}(\mathcal{O})$, que recordamos, sus vértices consisten en j-invariantes de curvas elípticas $E/\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = N$ y $\mathrm{End}(E) \simeq \mathcal{O}$ (donde $\mathcal{O}$ era un orden en un cuerpo cuadrático imaginario) y dos vértices $[E]$ y $[E']$ (donde $[E]$ es la clase de $\mathbb{F}_q$-isomorfismo de E) están conectados si E y E' son ℓ-isogenias, para algún primo impar ℓ menor que B y distinto de p (donde $B = p(\log(q))$ del Teorema de Jao-Miller-Venkatesan).

Observemos que al ser el j-invariante un caracterizador de la clase de isomorfismo, el conjunto de vértices del grafo $S_{N,q,B}(\mathcal{O})$ resulta ser exactamente el conjunto cociente del conjunto $\mathcal{A} = \mathcal{A}(q, N, \mathcal{O})$ por la relación de equivalencia dada por el j-invariante.

Navegamos ahora en el grafo de isogenias $S_{N,q,B}(\mathcal{O})$ realizando una caminata al azar de longitud $r_0 = g(\log(q))$, el Teorema 2.47 nos garantizaba que para un j' dado (vértice del grafo $S_{N,q,B}(\mathcal{O})$), la probabilidad de que el camino termine en j' es de al menos $\frac{1}{2h}$ donde $h = h_{\mathcal{O}}$ es la cantidad de vértices del grafo $\mathcal{G}_B(\mathcal{O})$ (que coincide con el número de clases del orden $\mathcal{O}$ como consecuencia del isomorfismo de grafos visto en el Cap.2.2). Si llamamos $(j_0 = j(E), j_1, j_2, \ldots, j_{r_0})$ al camino de j-invariantes obtenidos entonces construimos a partir de esta lista de j-invariantes una sucesión $E_0 = E, E_1, E_2, \ldots, E_{r_0}$ de curvas elípticas en $\mathcal{A}(q, N, \mathcal{O})$ tales que $j(E_i) = j_i$ y para cada $i = 1, 2, \ldots, r_0$ una isogenia $\varphi_i : E_{i-1} \to E_i$ definida sobre $\mathbb{F}_q$ de grado primo menor que $B = p(\log(q))$. El comodín que nos devuelve el algoritmo *Ran* en este caso será $(E_0, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0})$.

Veamos ahora que se verifica la propiedad *(a')* que debe verificar el algoritmo *Ran* respecto a la relación de equivalencia dada por el j-invariante. En efecto, aplicando la función de transición obtenemos $tr(E, k) = E_{r_0}$ que por construcción tiene j-invariante j_{r_0}, por lo visto anteriormente para un j' dado (que corresponde a una clase de equivalencia de $\mathcal{A}(q, N, \mathcal{O})$) la probabidad $Prob([E_{r_0}] = j') = Prob(j_{r_0} = j') \geq \frac{1}{2h}$ donde $h = \#\mathcal{A}/\sim$.

Finalmente debemos ver que se verifica la propiedad *(c)* del algoritmo *Ran*, es decir, que todo puede computarse eficientemente (polinomial en $\log(q)$). Es claro que la función de transición tr es eficiente así que solo queda ver que la cadena de curvas elípticas (el comodín) puede obtenerse en forma eficiente.

Uno comienza con una curva elíptica $E \in \mathcal{A}(q, N, \mathcal{O})$ y desea construir una cadena de isogenias

$$E_0 = E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{r_0}} E_{r_0}$$

cumpliendo con la condición que $j(E_i) = j_i$ para $0 \leq i \leq r_0$ (donde $(j_0 = j(E), j_1, j_2, \ldots, j_{r_0})$ se habia obtenido a partir de la caminata al azar), alcanza tener un algoritmo que dada una curva elíptica $E \in \mathcal{A}(q, N, \mathcal{O})$ y un j-invariante $j' \in \mathbb{F}_q$ tal que $\phi_\ell(j(E), j') = 0$ nos brinde una curva elíptica $E' \in \mathcal{A}(q, N, \mathcal{O})$ y una isogenia $\varphi : E \to E'$ definida sobre $\mathbb{F}_q$. Vamos a ver dos métodos para lograrlo, el primero está basado en las fórmulas de Vélu y se lo puede aplicar siempre, el segundo es a través del Algoritmo de Elkies que aunque es más eficiente que el anterior tiene algunas restricciones (no muy importantes).

2.2.1. Las fórmulas de Vélu. Antes de enunciar las fórmulas de Vélu observemos que dadas dos curvas elípticas $E_i : Y^2 = X^3 + a_iX + b_i, i = 1, 2$ sobre $\mathbb{F}_q$ dadas en forma reducida (suponemos $p \neq 2, 3$) se tiene que toda isogenia separable $\varphi : E_1 \to E_2$ definida sobre $\mathbb{F}_q$ puede expresarse en la forma

$$\varphi(x, y) = (\varphi_1(x), cy\varphi_1'(x)) \tag{9}$$

con $\varphi_1 \in \mathbb{F}_q[X]$ y $c \in \mathbb{F}_q$. En efecto, usando que $y^2 = x^3 + a_1x + b_1$ resulta que $\varphi(x, y) = (\varphi_1(x) + \varphi_2(x)y, \varphi_3(x) + \varphi_4(x)y)$ y usando que $-(x, y) = (x, -y)$ en E_1 (aquí usamos que está en forma corta) tenemos que $\varphi_2(x) = \varphi_3(x) = 0$. Para probar que $\varphi_4(x) = c\varphi_1'(x)$ se usa que φ es separable y se analiza la acción del pullback de φ en el diferencial invariante de E_2 (Teo.9.7.5. del libro de Galbraith [**19**]).

Una descripción mucho más detallada para cuando φ es una ℓ-isogenia con ℓ impar (que es el caso que nos interesa) aparece también en el libro de Galbraith [**19**] (Lema 9.6.13 pág.175, comentarios en pág.546, Corolario 25.1.8. pág.550):

$$\varphi(x, y) = \left(\frac{u(x)}{v(x)^2}, \frac{yw_1(x)}{v(x)^3}\right) \tag{10}$$

donde u y v son polinomios coprimos de grado ℓ y $\frac{\ell-1}{2}$ respectivamente y w_1 un polinomio con $gr(w_1) \leq 3(\ell - 1)/2$. Además el kernel de ϕ queda determinado por v como $\ker(\varphi) = \{\mathcal{O}_E\} \cup \{(x_p, \pm y_p) \in E\left(\overline{\mathbb{F}_q}\right) : v(x_p) = 0\}$ (observar que $y_p \neq 0$ pues $\ker(\varphi)$ no posee puntos de orden 2 ya que $\ell = \deg(\varphi)$ es impar).

La versión original de las fórmula de Vélu expresa la isogenia en términos de $E/\mathbb{F}_q$ y los puntos de un subgrupo finito $G < E(\overline{\mathbb{F}_q})$ que resulta ser el kernel de dicha isogenia ([**19**] Teo.25.1.6. pág.547) en su lugar usaremos la versión de Kohel [**25**] de las fórmulas de Vélu que expresa la isogenia en términos del polinomio definidor del kernel de la isogenia.

Teorema 3.8 (Fórmulas de Vélu.)**.** *Sea $E : Y^2 = X^3 + aX + b$ una curva elíptica definida sobre $\mathbb{F}_q$ y $G < E(\overline{\mathbb{F}_q})$ un subgrupo finito de orden impar $\ell = 2d + 1$. Si consideramos $G_1 \subset G$ tal que $G = \{\mathcal{O}\} \cup G_1 \cup \{-Q : Q \in G_1\}$ y consideramos el polinomio (definidor del kernel):*

$$\psi(x) = \prod_{Q \in G_1} (x - x_Q) = x^d - s_1x^{d-1} + s_2x^{d-2} + \ldots + (-1)^d s_d$$

donde s_i es el i-ésimo polinomio simétrico elemental en las raices de ψ (equivalentemente, en las x-coordenadas de los puntos de G sin repetición). Entonces existe una isogenia $\varphi : E \to E'$ con $\ker(\varphi) = G$ de la forma $\varphi(x, y) = \left(\frac{A(x)}{\psi^2(x)}, \frac{B(x,y)}{\psi^3(x)}\right)$ donde $A(x)$ y $B(x, y)$ son polinomios. Más concretamente

$$\varphi_1(x, y) = \frac{A(x)}{\psi^2(x)} = \ell x - 2s_1 - 4(x^3 + a + b)\left(\frac{\psi'(x)}{\psi(x)}\right)' - 2(3x^2 + 2b)\frac{\psi'(x)}{\psi(x)}$$

Demostración: Ver el libro de Galbraith [**19**], la demostración de la versión original se prueba en Teo.25.1.6. pág.547 y la versión de Kohel aparece como ejercicio guiado, a partir de la versión original, en la pág.552 ejercicios 25.1.17, 25.1.18, 25.1.19, 25.1.20.

□

Observación 3.9. Si G está definido sobre $\mathbb{F}_q$ entonces todo elemento $\sigma \in G = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ permuta los elementos de G, si $(x_0, y_0) \in G$ entonces $(x_0, -y_0) \in G$, además

como G tiene orden impar se tiene que $y_0 \neq 0$ y por lo tanto cada x-coordenada de un punto de G se repite exactamente dos veces. Luego G permuta las raices de ψ y por lo tanto $\psi \in \mathbb{F}_q[x]$. En particular $s_1 \in \mathbb{F}_q$ así que la fórmula para φ_1 muestra que la primer coordenada de φ es un polinomio en $\mathbb{F}_q[x]$ y usando (9) resulta $\varphi \in \mathbb{F}_q$ y por lo tanto E' está definida sobre $\mathbb{F}_q$.

El algoritmo para construir una pareja (E', φ) donde $E' \in \mathcal{A}(q, N, \mathcal{O})$ con $j(E') = j'$ a partir de una curva $E \in \mathcal{A}(q, N, \mathcal{O})$ y un j-invariante j' con $\phi_\ell(j(E), j') = 0$ usando la fórmula de Vélu sería computar primero ψ_ℓ, el polinomio de ℓ-división para E (Cap.1 Sección 2.1.) y calcular una raíz x_0 de ψ_ℓ (en alguna extensión de $\mathbb{F}_q$), luego hallar $P_0 = (x_0, y_0) \in E(\overline{\mathbb{F}_q})$ usando la ecuación de E, computar $\langle P_0 \rangle$ (el grupo cíclico generado por P_0) y verificar que esté definido sobre $\mathbb{F}_q$ usando el Frobenius.

Una forma de implementarlo es factorizar ψ_ℓ en $\mathbb{F}_q[x]$ y tomar un factor irreducible F y considerar la raíz $P_0 = \overline{x} \in \mathbb{F}_q[x]/(F)$ (la extensión será $\mathbb{F}_{q^t} = \mathbb{F}_q[x]/(F)$ donde $t = gr(F)$) y verificar que $\langle P_0 \rangle$ está definido sobre $\mathbb{F}_q$ trabajando con aritmética módulo F (podemos considerar solo factores irreducibles F con $gr(F) \leq \frac{\ell-1}{2}$ ya que si es mayor entonces $\langle P_0 \rangle$ no estará definido sobre $\mathbb{F}_q$ (Galbraith [**19**] pág.487). Una vez que conseguimos un subgrupo $G = \langle P_0 \rangle$ de orden ℓ podemos aplicar las fórmulas de Vélu para obtener la isogenia (en principio solo la primer coordenada φ_1 pero a partir de esta podemos hallar la segunda φ_2 usando (9) con $c = 1$, ver [**19**] Teo.25.1.6 pág.547, Ej.21.1.11 pág 550) y finalmente podemos hallar la curva elíptica buscando una combinación lineal $\varphi_2^2 = \varphi_1^3 + a'\varphi_1 + b'$ con $a', b' \in \mathbb{F}_q$ (sistema con 2 incógnitas).

Chequear si esa curva tiene j-invariante j', en caso contrario volver a repetir el procedimiento[3].

2.2.2. El Algoritmo de Elkies. Otra forma de calcular ℓ-isogenias cuando su grado es pequeño respecto la característica del cuerpo $\mathbb{F}_q$ es utilizando el Algoritmo de Elkies. Este algoritmo toma como entrada la curva elíptica de partida $E/\mathbb{F}_q$, el grado ℓ (primo impar) de la isogenia a hallar y el j-invariante $\widetilde{j}$ de la curva de llegada y devuelve el polinomio definidor del kernel de una ℓ-isogenia $\phi : E \to \widetilde{E}$ con $j(\widetilde{E}) = \widetilde{j}$.

Observemos que si queremos computar una ℓ-isogenia racional partiendo de una curva elíptica $E/\mathbb{F}_q$ usando las fórmulas de Vélu precisariamos computar primero un grupo de orden ℓ que esté definido sobre $\mathbb{F}_q$, mientras que usando el Algoritmo de Elkies solo se precisa un j-invariante en $\mathbb{F}_q$ de una curva ℓ-isógena a E (que puede obtenerse de forma particularmente fácil a través del polinomio modular $\phi_\ell(X, Y)$ (mód p) como comentamos en el capítulo anterior, pág.49). Por esa razón privilegiaremos en nuestra implementación el Algoritmo de Elkies frente a las fórmulas de Vélu. Lamentablemente el Algoritmo de Elkies tiene algunas restricciones como ser, $\ell < p-2$ (entonces no es aplicable para cuerpo de característica pequeña), $j(E) \neq 0, 1728$ y que el j-invariante de la curva de llegada no sea raíz múltiple de $\phi_\ell(j(E), x)$ (para esos casos podemos aplicar por ejemplo Vélu como mostramos anteriormente).

[3]En realidad podemos hacer algo diferente que es utilizar la fórmula de Vélu para obtener el j', esto puede afectar la aleatoriedad de la caminata al azar, cuando hablemos del costo de implementación de *Ran* y comentarios analizaremos esto con más detalles.

El pseudocódigo completo del Algoritmo de Elkies puede encontrarse en el libro de Galbraith [**19**], Algoritmo 28.

Como comentamos anteriormente, el algoritmo de Elkies no es aplicable para el caso de característica pequeña debido a la restricción de que $\ell < p - 2$. Para este caso puede emplearse otros métodos, por ejemplo el de Couveignes (ver [**19**] Cap25.2.3).

2.2.3. Costo de la implementación de Ran y comentarios. Vamos a analizar cada etapa de la construcción del algoritmo *Ran* para estimar los costos, junto con algunas consideraciones importantes a tener en cuenta en la implementación.

En primer lugar observemos que el costo del algoritmo es la de calcular el comodín (la cadena de isogenias) partiendo de una curva elíptica $E = E_0 \in \mathcal{A}(q, N, \mathcal{O})$. En primer lugar necesitamos almacenar una lista con los primeros primos ℓ hasta $B = p(\log(q))$ y tales que $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$[4], esto se puede realizar por ejemplo con el Algoritmo de la Criba de Eratóstenes que tiene complejidad $O(B^{1+\epsilon})$ (y por lo tanto polinomial en $\log q$) y luego para cada ℓ verificar que $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$ es de costo $O(\log(d_{\mathbb{K}})\log(\ell))$ donde $d_{\mathbb{K}} = O(q^2)$ (como vimos al inicio de la sección 1.2) resulta de costo polinomial y por lo tanto construir esta lista de primos tendrá también complejidad polinomial.

Otra lista a almacenar (la que lleva más trabajo) es para cada primo ℓ de la lista anterior computar los polinomios modulares $\phi_\ell \pmod p$ (p la característica) esta etapa se puede realizar por ejemplo con los algoritmos de Bröker, Lauter y Sutherland que tiene costo $O(\ell^{3+\epsilon}) = O(B^{3+\epsilon})$ para cada ℓ y por lo tanto polinomial (ver [**19**], pág.488). Una vez computada la tabla con las parejas (ℓ, ϕ_ℓ) estas son utilizadas para cualquiera de las instancias $E \in \mathcal{A}(q, N, \mathcal{O})$. No vamos a contar el costo de la construcción de dicha tabla en el costo del algoritmo *Ran* sino que vamos a suponer que ya la tenemos precomputada.

La primera etapa consta de la construcción de la cadena de j-invariantes, es preciso notar aquí que las aristas $\{j(E), j'\}$ del grafo de isogenias están ponderadas por la cantidad de clases de ℓ-isogenias que hay partiendo de E (para $\ell \leq B$) y llegando a una curva de j-invariante j'[5], por lo tanto cuando realizamos la caminata al azar hay que tenerlo en cuenta.

En nuestro caso elegimos un ℓ al azar (en la lista de primos $\ell \leq B, \left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$) y luego calculamos las raices de $\phi_\ell(j(E), x) = 0$ que correspondan a isogenias horizontales en el grafo de isogenias, que serán dos valores contados con multiplicidades (excepto para aquellos ℓ que dividen al conductor de $\mathcal{O}$ para los cuales no hay aristas horizontales) por el Teorema de Kohel (Cap2.1.4.) y luego elegimos una de las dos raices al azar obteniendo una pareja (ℓ, j'). El costo de computar $F(x) = \phi_\ell(j(E), x)$ (dados $\phi_\ell(y, x)$ y $j(E)$) es $O(\ell^{3+\epsilon}\log(q)^2)$ mientras que computar una raíz sobre $\mathbb{F}_q$ de F tiene costo $O(\ell^{2+\epsilon}\log(q)^3)$ ([**19**] Ex.25.2.2, pág.554) y como $\ell \leq B$ con $B = p(\log(q))$ este proceso tiene costo polinomial.

[4]En este caso todo ℓ nos brinda exactamente dos clases de isogenias

[5]Aquí hay un detalle cuando $j' = 0, 1728$ ver Galbraith [**19**] Remark 25.3.2, pág.558

Como la multiplicidad de j' en $\phi_\ell(j(E), x)$ coincide con la cantidad de clases de ℓ-isogenias desde E hasta una curva con j-invariante j' y fijado ℓ tenemos exactamente 2 posibilidades para j' (contada con multiplicidad), el método anterior nos otorga un j-invariante j' con la probabilidad adecuada (por la fórmula de probabilidad total)[6].

Una vez construida la cadena de j-invariantes y primos $[(\ell_1, j_1), \ldots, (\ell_{r_0}, j_{r_0})]$, vamos a ver como realizar el primer paso $E \xrightarrow{\varphi} E_1$ luego se repite el proceso $r_0 = g(\log(q))$ veces hasta llegar a una cadena de largo r_0. Tomamos j_1 y ℓ_1, si j_1 resulta una raíz doble de $\phi_{\ell_1}(j_0, x)$ o si $\ell_1 = 2$ entonces utilizamos las fórmulas de Vélu para construir (φ_1, E_1) donde E_1 es una curva elíptica con definida sobre $\mathbb{F}_q$ con $j(E_1) = j_1$ y $\varphi_1 : E \to E_1$ es una ℓ-isogenia también definida sobre $\mathbb{F}_q$, el costo de aplicar este método es de $O(\ell^2)$ ([**19**],Ex.25.1.21, pág.552). En caso de que j_1 sea una raíz simple de $\phi_{\ell_1}(j(E), x)$ entonces aplicamos el Algoritmo de Elkies cuyo costo es $O(\ell^2)$ ([**19**],Ex.25.2.4, pág.556). Ambos métodos son polinomiales en $\log(q)$ y el largo de la cadena r_0 también por lo tanto el costo total de la construcción del comodín $(E = E_0, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0})$ también lo será.

3. La parte de reducibilidad

Debemos implementar ahora la función de reducibilidad $Red : \mathcal{B} \times \mathcal{K} \to \mathcal{B}$ donde en este caso $\mathcal{B} = \{PLD_E : E \in \mathcal{A}(q, N, \mathcal{O})\}$ (y el conjunto de comodines $\mathcal{K}$ definidos como en la sección previa). Recordemos que la función f a computar es $f = PLD$ por lo tanto la propiedad que debe cumplir la función Red es $Red(PLD_{E'}, k_E) = PLD_E$ donde $(E', k_E) = Ran(E)$.

La primera entrada del algoritmo es una función, para calcular el costo de la función Red. No tendremos en cuenta el costo que implica la implementación de $PLD_{E'}$ (que de hecho no sabemos), suponemos que teniendo $PLD_{E'}$ podemos calcular $PLD_{E'}(P', Q')$ para cualquier instancia (P', Q') con costo unitario (o sea, pensaremos $PLD_{E'}$ como un oráculo tal que cada llamada tiene costo de una unidad de computo). Esto implica que si tenemos $Ran(E) = (E', k_E)$ y contamos con un algoritmo eficiente para calcular $PLD_{E'}$ (polinomial en $\log(q)$) y Red solo realiza una cantidad de llamadas a $PLD_{E'}$ también polinomial en $\log(q)$ (en nuestro caso realizará solo una llamada) entonces tendremos un algoritmo eficiente para resolver PLD_E en cualquiera de sus instancias.

Sea $E \in \mathcal{A}$ una instancia para f y sea $(E', k_E) = Ran(E)$, veamos como definir $Ran(F, k)$ tal que si $k = k_E$ y $F = PLD_{E'}$ entonces $Ran(F, k) = PLD_E$. Tomemos entonces una pareja (P, Q) con $P, Q \in E(\mathbb{F}_q)$ tales que $Q = nP$, como una primera posibilidad podemos aprovechar las isogenias de k para obtener una instancia del logaritmo discreto en E' definiendo $(P_0, Q_0) = (P, Q)$ y $(P_i, Q_i) = \varphi_i(P_{i-1}, Q_{i-1})$ para $i = 1, 2, \ldots, r_0$. La pareja (P_{r_0}, Q_{r_0}) es una instancia particular del problema del logaritmo discreto en E_{r_0}, de esa forma usando $F = PLD_{E_{r_0}}$ podemos obtener $n' \in \mathbb{Z}^+$ tal que $Q_{r_0} = n'P_{r_0}$.

Hay un caso de instancia (P, Q) en donde la reducción se trivializa.

Definición 3.10. Una pareja (P, Q) con $P, Q \in E(\mathbb{F}_q)$ decimos que es fiel respecto la cadena $k = (E = E_0, \varphi_1, \varphi_2, \ldots, \varphi_{r_0}, E_{r_0} = E')$ (donde las $\varphi_i : E_{i-1} \to E_i$ son isogenias

[6]Podríamos considerar aquellos ℓ tales que $\ell | d_K$ pero entonces tendríamos que modificar el método de la elección del j-invariante ya que estos ℓ nos aportan una único j-invariante.

definidas sobre $\mathbb{F}_q$) si $o(P_{i-1}) = o(P_i)$ para $1 \leq i \leq r_0$, donde $P_0 = P$ y $P_i = \varphi_i(P_{i-1})$ para $1 \leq i \leq r_0$ (es decir, si cada isogenia preserva el orden cuando vamos iterando el punto P).

Observación 3.11. Usando el Primer Teorema de Isomorfismo en $\varphi_i : \langle P_{i-1}\rangle \to \langle P_i\rangle$ resulta que $\frac{\langle P_{i-1}\rangle}{\langle P_{i-1}\rangle \cap \ker(\varphi_i)} \simeq \langle P_i\rangle$. Si $\deg(\varphi_i) = \#\ker(\varphi_i) = \ell$ primo entonces por Lagrange las únicas opciones son $o(P_{i-1}) = o(P_i)$ u $o(P_{i-1}) = o(P_i)\ell$.

En el caso que partamos de una instancia (P, Q) fiel a la cadena k, si $Q_{r_0} = n'P_{r_0}$ entonces yendo hacia atrás iterativamente tenemos que $Q_i = n'P_i$ para $0 \leq i \leq r_0$ en particular con $i = 0$ resulta que $Q = n'P$ y habremos conseguido resolver el problema del logaritmo discreto en $E_0 = E$ para esa instancia particular.

Cuando nos topamos con una isogenia $\varphi_i : E_{i-1} \to E_i$ que no preserva el orden de P_{i-1}, por la observación previa tenemos que $o(P_{i-1}) = \ell \cdot o(P_i)$. Conociendo n_i tal que $Q_i = n_iP_i$, si queremos determinar n_{i-1} tal que $Q_{i-1} = n_{i-1}P_{i-1}$ entonces sabemos que necesariamente $n_{i-1} \equiv n_i \pmod{o(P_i)}$ (pues $Q_{i-1} = n_{i-1}P_{i-1} \Rightarrow Q_i = n_{i-1}P_i$ aplicando φ_i a ambas partes) y por lo tanto $n_{i-1} = n_i + to(P_i)$ que sustituyendo nos queda $Q_{i-1} = n_{i-1}P_{i-1} = n_iP_{i-1} + to(P_i)P_{i-1}$. Llamando $Q' = Q_{i-1} - n_iP_{i-1}$ y $P' = o(P_i)P_{i-1}$ el problema se resume a hallar t tal que $Q' = tP'$ donde t queda determinado módulo $o(P') = o(P_{i-1})/o(P_i) = \ell$. Como para nuestro algoritmo los grados de las isogenias son primos $\ell < B = p(\log(q))$ pequeños podemos aplicar algún algoritmo genérico (por ejemplo Baby Step - Giant Step) obteniendo t (y por lo tanto n_{i-1}) en $\widetilde{O}(\ell)$ pasos[7], de esa forma podríamos ir para atrás partiendo de $P_{r-1} = n'Q_{r_1}$, realizando el proceso anterior en una cantidad $r_0 = g(\log(q))$ de pasos obtener n_0 tal que $P = n_0Q$.

El método anterior requiere por ejemplo computación en cada una de las curvas E_i donde se requiera hacer la reducción, vamos a utilizar en su lugar una estrategia alternativa. Observemos que si partimos de una pareja (P, Q) (con $P, Q \in E(\mathbb{F}_q)$, $Q = nP$) tal que el orden de P es B-smooth (es decir, $o(P)$ descompone como producto de factores primos menores que B), al ser B polinomial en $\log(q)$ entonces podemos resolver directamente el problema del logaritmo discreto para dicha instancia (P, Q) sin utilizar la reducción (que llamaremos a tales instancias triviales).

Por lo tanto dada una instancia cualquiera (P, Q) para el problema del logaritmo discreto en E vamos a partir el problema en dos instancias (de PLD_E), una instancia (P_0, Q_0) que este formada por una pareja fiel (para la cual el proceso de reducción sea trivial) y una instancia (P', Q') trivial (donde el PLD_E se resuelve efectivamente con métodos genéricos para dicha instancia) y luego con el Teorema del Resto Chino reunir ambas informaciones para obtener $PLD_E(P, Q)$ como resultado.

3.1. Descomposición de una instancia para PLD_E en una pareja fiel y otra trivial.

Supongamos que tenemos precomputada una factorización de N en un producto $N = N_0 \cdot p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}$ donde $p_i \leq B$ para $1 \leq i \leq t$ y $mcd(N_0, B!) = 1$ (es decir tal que

[7]Se recuerda que $f(t) = \widetilde{O}(g(t)) \Leftrightarrow f(t) = O(g(t)\log(g(t))^m)$ para algún $m \in \mathbb{N}$.

N_0 no acepte en su descomposición factorial factores primos menores o iguales que B)[8], llamemos $N' = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ a la parte B-smooth de N.

Consideremos una instancia particular (P, Q) del logaritmo discreto en E y consideremos a partir de ella dos instancias $(P_0, Q_0) = (N'P, N'Q)$ y $(P', Q') = (N_0 P, N_0 Q)$. Observemos que $o(P_0) = o(P)/mcd(o(P), N')$ y como $o(P)|N$ entonces $o(P_0)|\frac{N}{N'} = N_0$ y por lo tanto $o(P_0)$ no posee factores primos menores o iguales que B, esto implica que la pareja (P_0, Q_0) resulte fiel con la cadena k (obtenida a partir del algoritmo Ran) ya que las isogenias que aparecen todas tienen grado primo $\ell < B$. En efecto, si alguna isogenia $\varphi_i : E_{i-1} \to E_i$ no preservara el orden de P_{i-1} por lo visto en la observación 3.11 esto implicaria que $\ell | o(E_{i-1})$ y por iteración hacia atrás estaría implicando que $\ell | o(E)$ lo cual es absurdo puesto que $\ell < B$. De la misma forma llegamos a que $o(P')|N'$ que como N' es B-smooth (donde $B = p(\log(q))$ polinomial en $\log(q)$) podemos computar $PLD_E(P', Q')$ eficientemente usando algoritmos genéricos.

Ahora supongamos que tenemos computado PLD_E para las instancias (P_0, Q_0) y (P', Q'), supongamos que $Q_0 = n_0 P_0$ y $Q' = n' P'$, si queremos hallar $n \in \mathbb{Z}^+$ tal que $Q = nP$, claramente n verificará también $Q_0 = nP_0$ y $Q' = nP'$ y por lo tanto el sistema de congruencias:

$$\begin{cases} n \equiv n_0 \pmod{N_0} \\ n \equiv n' \pmod{N'} \end{cases} \tag{11}$$

resolviendo obtenemos una solución módulo N (pues $mcd(N_0, N') = 1$ y $N = N_0 N'$) y reduciendo módulo $o(P)$ obtenemos $n = PLD_E(P, Q)$ como queríamos.

3.2. Algoritmos genéricos para la parte trivial. Aquí expondremos un repaso de resultados sobre el PLD_G cuando el orden del grupo G es smooth[9]. Si bien todos los resultados que expondremos son clásicos y muy conocidos, vamos a colocarlos aquí por conveniencia.

En nuestro caso, el grupo a considerar es $E(\mathbb{F}_q)$ donde $E \in \mathcal{A}(q, N, \mathcal{O})$, si bien el orden $|E(\mathbb{F}_q)| = N$ no tiene porque ser smooth, cuando realizamos la descomposición de una instancia (P, Q) obtenemos una nueva instancia (P', Q') donde el orden de P' es B-smooth. Como dijimos antes esta instancia puede ser resuelta usando algoritmos genéricos, vamos a dar un pantallazo de cuales serían esos posibles algoritmos:

3.2.1. Baby step - Giant step. Queremos resolver el PLD_G en un grupo G en una instancia (g, h) donde $h = g^t$ con $t \leq n$ y n es una cota conocida (por ejemplo $n = |G|$ o $n = o(G)$). Consideramos $m = \lceil n \rceil$, tomando división entera por m sabemos que nuestro t será de la forma $t = im + j$ con $0 \leq i < m$ y $0 \leq j < m$ sustituyendo resulta que $h = g^t \Leftrightarrow g^j = h(g^{-m})^i$ así que tenemos el siguiente algoritmo para el cálculo de t:

1. Computamos $g_0 = g^{-m} = (g^{-1})^m$
2. (Baby step) Para $j = 0, 1, 2, \dots, m-1$ calculamos g^j y almacenamos todos los valores (j, g^j) en una tabla.

[8]Observemos que si bien el problema de factorizar N es difícil para N grande (aquí N es del orden de q que es exponencial en $\log(q)$), realizar dicha descomposición puede hacerse en forma efectiva ya que los primos p_i están acotados por B que es polinomial en $\log(q)$.

[9]Es decir, cuando descompone en producto de primos pequeños.

3. (Giant step) Para $i = 0, 1, 2, \ldots, m-1$ calculamos vamos calculando hg_0^i (usando que $hg_0^i = hg_0^{i-1} \cdot g_0$) hasta encontrar una colisión con alguna segunda componente g^j de las parejas almacenadas en el paso anterior (resultando una ecuación de la forma $hg_0^i = g^j$ que implica $h = g^{mi+j}$).
4. Retornar $im + j$.

Sin contar el paso de verificar la colisión (que puede hacerse en forma eficiente utilizando un Hash), el costo de este algoritmo resulta del orden $O(\sqrt{t})$.

3.2.2. Levantamiento p-ádico. Cuando queremos resolver una instancia (g, h) del PLD_G en un grupo G y el orden de g factoriza en forma no trivial entonces podemos reducir el costo de calcular $PLD_G(g, h) = t$. El caso más sencillo es cuando $o(g) = p^\alpha$ con p primo y $\alpha \in \mathbb{Z}^+$, $\alpha > 1$ (suponemos conocida dicha factorización o precomputada de antemano).

En primer lugar podemos considerar la instancia $(g_1, h_1) = \left(g^{p^{\alpha-1}}, h^{p^{\alpha-1}}\right)$ que como el orden $o(g_1) = o(g)/p^{\alpha-1} = p$ tenemos una cota para $t_1 = PLD(g_1, h_1)$ que es p así que podemos aplicar por ejemplo Baby step - Giant step para obtener t_1 con un costo $O(\sqrt{p})$. Claramente $t = PLD_G(g, h)$ también verificará $h_1 = g_1^t$ así que tenemos la relación $t \equiv t_0 \pmod{p}$.

Veamos ahora el paso del levantamiento, supongamos que conocemos t_i tal que $t \equiv t_i \pmod{p^i}$ con $i < \alpha$ (recordar que $t \pmod{p^\alpha}$ es lo que queremos hallar) queremos t_{i+1} tal que $t \equiv t_{i+1} \pmod{p^{i+1}}$. Definamos $(g_i, h_i) = \left(g^{p^{\alpha-i}}, h^{p^{\alpha-i}}\right)$ para $0 \leq i \leq \alpha$ y observemos que $h = g^t \Rightarrow h_{i+1} = g_{i+1}^t$ y sustituyendo t por $t = t_i + ap^i$ (donde a queda a determinar) obtenemos $h_{i+1} = g_{i+1}^{t_i} \cdot g_1^a$ (pues $g_{i+1}^{p^i} = g_1$) donde el problema se reduce a hallar a tal que $g_1^a = h_{i+1} g_{i+1}^{-t_i}$ con $a < p$ (pues $o(g_1) = p$) y por lo tanto podemos aplicar nuevamente Baby step - Giant step para hallar a en $O(\sqrt{p})$ pasos y de esa forma obtener $t_{i+1} = t_i + ap^i$ repitiendo este proceso podemos obtener t en α luego de α pasos. Escribamos el algoritmo en pseudo código:

1. Calculamos en forma iterativa $g_i = g^{p^{\alpha-i}}$ y $h_i = h^{p^{\alpha-i}}$ (usando $(g_\alpha, h_\alpha) = (g, h)$ y $(g_{i-1}, h_{i-1}) = (g_i^p, h_i^p)$) para $i = \alpha, \alpha-1, \ldots, 1$.
2. Hallamos t_1 solución de $h_1 = g_1^{t_1}$ usando Baby step - Giant step.
3. Para $i = 1, 2, 3, \ldots, \alpha - 1$ calculamos $c_i = h_{i+1} g_{i+1}^{-t_i}$ hallamos a solución de $c_i = g_1^a$ usando Baby step - Giant step y definimos $t_{i+1} = t_i + ap$ (de esa forma iterativamente para obteniendo $t_2, t_3, \ldots, t_\alpha$).
4. Retornar t_α.

Observemos que tenemos que resolver en total α logaritmos discretos con base g_1 que tiene orden p, podemos aprovechar el almacenamiento de los Baby step ya que es común a todas las instancias.

Respecto al costo, la primer parte del algoritmo tiene costo $O(\alpha \log(p))$ (de hacer 2α elevaciones a la p), la segunda parte $O(\sqrt{p})$, la tercer parte para cada i tenemos $O(\log(p))$ para el cálculo de c_i y $O(\sqrt{p})$ para resolver el logaritmo discreto (en total $O(\log(p) + \sqrt{p}) = O(\sqrt{p})$) y como hay α iteraciones resulta un costo de $O(\alpha\sqrt{p})$. Como $\log(p)$ resulta despreciable respecto $\sqrt{p}$ el costo del algoritmo se estima en $O(\alpha\sqrt{p})$ (que es más eficiente que $O(p^{\frac{\alpha}{2}})$ si $\alpha > 1$ que es el costo de aplicar directamente un método

genérico).

3.2.3. Reducción usando Teorema del Resto Chino. El caso anterior es un caso particular en donde se quiere resolver PLD_G es una instancia (g, h) donde se tiene una factorización no trivial de $o(g)$, para ver el caso general supongamos que tenemos una factorización conocida de $o(g) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ con p_i primos distintos y $\alpha_i \in \mathbb{Z}^+$ y el problema a resolver es hallar n tal que $h = g^n$. Definimos $a_i = o(g)/p_i^{\alpha_i}$ para $i = 1, 2, \dots, m$, como $o(g^{a_i}) = o(g)/a_i = p_i^{\alpha_i}$ podemos para cada i resolver el PLD_G para la instancia (g^{a_i}, h^{a_i}) con costo $O(\alpha_i \sqrt{p_i})$ usando levantamiento p_i-ádico (obteniendo como salida un n_i tal que $h^{a_i} = (g^{a_i})^{n_i}$).

Como $h = g^n \Rightarrow h^{a_i} = (g^{a_i})^n$ entonces $n \equiv n_i \pmod{p_i^{\alpha_i}}$ por lo tanto podemos hallar n como solución del sistema de congruencias

$$\begin{cases} n \equiv n_1 \pmod{p_1^{\alpha_1}} \\ n \equiv n_2 \pmod{p_2^{\alpha_2}} \\ \qquad \vdots \\ n \equiv n_m \pmod{p_m^{\alpha_m}} \end{cases}$$

Por el Teorema del Resto Chino este sistema tiene solución única módulo $o(g) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$.

Respecto a costos, denotemos por $N = o(P) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$. En primer lugar utilizamos $m = O(\log(N))$ veces el método del levantamiento para obtener los n_i que tiene un costo total de $O(\alpha_1 \sqrt{p_1} + \dots + \alpha_m \sqrt{p_m}) = O(m\alpha p) = O(\log(N)^2 p)$ donde $\alpha = \text{máx}\{\alpha_1, \alpha_2, \dots, \alpha_m\} = O(\log(N))$ y $p = \text{máx}\{p_1, p_2, \dots, p_m\}$, luego tenemos que resolver el sistema de congruencias. Para ello debemos resolver $m = O(\log(N))$ algoritmos de Euclides extendidos con entradas $(N, N/p_i^{\alpha_i})$ para $i = 1, 2, \dots, m$ cuyo costo es $O(\log(N)^2)$ para cada i (Cap.10 de [**10**]) así que en total tenemos un costo para la segunda parte de $O(\log(N)^3)$ (pues $m = O(\log(N))$). Reuniendo ambas partes el costo total es de $O\left(\log(N)^2 (\log(N) + p)\right)$ donde p es el mayor primo divisor de N.

3.3. Costo de la implementación de *Red* y comentarios. El algoritmo *Red* toma como entrada (F, k) donde $F = PLD_{E'}$ y $k = (E, \varphi_1, \varphi_2, \dots, \varphi_{r_0}, E'')$, si $E'' \neq E'$ devolvemos $\perp$ en caso contrario procedemos como a continuación.

Recordemos la convención de tomar como costo unitario la evaluación de $F = PLD_{E'}$ en cualquiera de sus instancias, el primer paso entonces consiste en dada una instancia (P, Q) de PLD_E descomponerla en dos parejas (P_0, Q_0) y (P', Q') la primera fiel respecto de la cadena k y la segunda trivial. Suponemos precomputada la factorización de $N = N_0 N'$ con $mcd(N_0, B!) = 1$ y N' B-smooth, obtener $P_0 = N'P, Q_0 = N'Q, P' = N_0 P$ y $Q' = N_0 Q$ requiere $O(4\log(N)) = O(\log(q))$ duplicaciones de puntos en E, cada duplicación requiere $O(1)$ operaciones en $\mathbb{F}_q$ y cada operación sobre $\mathbb{F}_q$ tiene costo $O(\log(q)^2)$ así que el costo total es de $O(\log(q)^3)$.

Resolver el PLD_E para la instancia (P', Q') utilizando métodos genéricos vimos que requeria $O\left(\log(N)^2 (\log(N) + p_0)\right)$ donde $N = \#E(\mathbb{F}_q) = O(\log(q))$ y p_0 el mayor primo divisor de $o(P')$ (el orden de P' en $E(\mathbb{F}_q)$) que es menor que $B = O(p(\log(q)))$ por construcción (p es el polinomio del Teorema de Jao-Miller-Venkatesan) así que este paso tiene costo $O(\log(q)^2 p(\log(q)))$ y por lo tanto polinomial en $\log(q)$.

La siguiente instancia consta de las sucesivas evaluaciones $\varphi_i(P_{i-1}, Q_{i-1}) = (P_i, Q_i)$ para $i = 1, 2, \ldots, r_0$ donde cada isogenia tiene grado ℓ acotado por $B = O(p(\log(q)))$. El costo de evaluar una ℓ-isogenia es del orden $O(\ell^2 \log(q)^2) = O(\log(q)^2 p(\log(q))^2)$ y la cantidad de evaluaciones es $r_0 = g(\log(q))$ (donde g es el polinomio del Teorema de Jao-Miller-Venkatesan) así que el costo total es $O(\log(q)^2 p(\log(q))^2 g(\log(q)))$ que también es polinomial en $\log(q)$.

La obtención de $n_0 = PLD_{E'}(P_{r_0}, Q_{r_0})$ convenimos que tiene costo unitario. Una vez obtenido $n' = PLD_E(P', Q')$ y $n_0 = PLD_E(P_0, Q_0)$ (recordemos que $PLD_E(P_0, Q_0) = PLD_{E'}(P_{r_0}, Q_{r_0})$ puesto que (P_0, Q_0) era fiel respecto la cadena k) resolver el Teorema del Resto Chino (11) consiste en resolver el Algoritmo de Euclides Extendido para hallar (x, y) tales que $xN_0 + yN' = 1$ que tiene costo $O(\log(q)^2)$ (pues N_0 y N' son de orden $O(N) = O(\log(q))$) y luego obtenemos $n = n'xN_0 + n_0yN'$ (mód N) que tiene orden $O(\log(q)^2)$.

La etapa más costosa es la segunda que tiene un costo preponderante de $O(\log(q)^2 p(\log(q))^2 g(\log(q)))$ por lo tanto es la que domina el costo total del algoritmo.

Un comentario importante es que en la práctica se suele elegir un N de forma que tenga un gran factor primo preponderante f y para $E \in \mathcal{A}(q, N, \mathcal{O})$ solo interesan instancias de la forma (P, Q) con $o(P) = f$ en este caso (si $f > B$) la instancia (P, Q) ya es de por si fiel respecto de k y por lo tanto se evita así la primer parte y la última del algoritmo, de todas formas esto no baja la complejidad asintótica del algoritmo.

4. Implementación en Sage de (Ran, Red)

En esta sección describiremos una implementación realizada en Sage de un algoritmo de autoreducibilidad aleatoria (Ran, Red) para el problema de determinar si dos curvas definidas sobre el mismo cuerpo finito, con la misma cantidad de puntos y el mismo tipo de anillo de endomorfismo tienen la misma dificultad respecto del problema del logaritmo discreto. Para resumir solo describiremos a grandes rasgos los principales pasos del algoritmo. Más detalle sobre la implementación (así como los códigos completos de los algoritmos implementados en Sage) pueden verse en mi página personal `http://www.fing.edu.uy/~cqureshi/`.

4.1. Parámetros a fijar y precomputaciones previas al algoritmo. Vamos a discutir en primer lugar los parámetros a fijar previos al algoritmo. Supongamos que estamos interesados en resolver el PLD para cierta curva elíptica $E'/\mathbb{F}_q$ y conocemos algoritmos para resolver el PLD para cierta familia S de curvas elípticas, todas ellas definidas sobre $\mathbb{F}_q$, con cardinal $N = \#E'(\mathbb{F}_q)$ y anillo de endomorfismo $\mathcal{O} = \mathrm{End}(E')$. Lo primero a determinar será entonces los parámetros q y N (esas variables que se definen al inicio no deben ser modificadas en el resto del algoritmo).

Determinación de B y r_0 del Teorema 2.47. Recordemos que según la construcción $B = p(\log(q))$ y $r_0 = g(\log(q))$ para ciertos polinomios p y g, donde p lo elegiamos de la forma $p(x) = x^{2+\delta} + C_1$ con $\delta > 0$ y la tesis del Teorema 2.47 se verificaba (asumiendo GRH) para cierto polinomio g de la forma $g(x) = 2x + C_2$ donde las constantes[10] C_1 y C_2 no son explícitas. Como por el momento no tenemos forma de estimar dichas constantes,

[10]En el sentido que no dependen de q, de N ni de $D = discr(\mathcal{O})$, solo depende del $\delta > 0$ escogido

vamos a dejarlas como parámetros fuera del algoritmo, sería interesante como línea de trabajo futura encontrar buenas estimativas para B y r_0, dependiente o independiente de GRH.

En resumen, antes de comenzar a correr el algoritmo debemos fijar los parámetros (N, q, B, r_0).

4.2. Los polinomios modulares $\phi_\ell(x, y)$. El siguiente paso previo al algoritmo es la determinación de una lista de polinomios ℓ-modulares módulo p, donde p es la característica de $\mathbb{F}_q$ (en realidad nosotros nos enfocaremos en el caso en que q sea primo y por lo tanto $p = q$). Como dijimos antes, la propiedad de los polinomios ϕ_ℓ que nos interesa es que para curvas elípticas E y E' definidas sobre $\mathbb{F}_q$, existe una ℓ-isogenia $\phi : E \to E'$ definida sobre $\mathbb{F}_q$ si y solo si $\phi_\ell\left(j(E), j(E')\right) = 0$.

En esta subsección describiremos la teoría que envuelve dichos polinomios modulares y su propiedad de caracterizar relación de isogenías entre curvas elípticas, así también como algoritmos para su computación.

4.2.1. Definición de polinomios modulares y vínculo con Teoría de Formas modulares. En primer lugar cabe destacar que los polinomios modulares surgen naturalmente de la Teoría de formas modulares, vamos a repasar los principales puntos siguiendo el libro de Cox [**11**] (Capítulo 11, secciones B,C y D). Algunos resultados sobre funciones modulares que fueron estudiados en mi monografía de grado [**32**] (Capítulo 2) serán asumidos.

Un papel clave en la teoría de formas modulares lo juega la función j, así que vamos a comenzar repasando sus propiedades. En el Capítulo 1 Sección 1.2.1 se definió el j-invariante de una curva elíptica, en el Capítulo 2 de mi monografía de grado probamos que curvas elípticas corresponden con toros complejos ($\mathbb{C}/\Lambda$ donde Λ es un látice) vía la función $\wp$ de Wierstrass (Teoremas 2.19 y 2.20 de [**32**]), de ese modo se podia definir la función j de un látice como $j(\Lambda) = j(E_\Lambda)$ donde E_Λ es la curva elíptica compleja que corresponde con el toro $\mathbb{C}/\Lambda$. Del hecho que curvas elípticas isomorfas corresponden con látices homotéticos resultaba que j era invariante por rotohomotecias (vista como función de látices). Recordemos además que todo látice puede llevarse vía una rotohomotecia a un látice de la forma $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ con $Im(\tau) > 0$, por lo tanto basta conocer j en los látices Λ_τ, de modo que resulta natural considerar j como función del semiplano superior $\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$ a valores complejos dada por $j(\tau) = j(\Lambda_\tau)$.

Esa función $j : \mathcal{H} \to \mathbb{C}$ resulta ser una función modular, es decir, meromorfa en $\mathcal{H}$, Γ-invariante[11](donde $\Gamma = Sl_2(\mathbb{Z})$ es el grupo modular), y meromorfa en el infinito[12]. De hecho fue probado que j es una función modular holomorfa en $\mathcal{H}$ con un polo simple en ∞ (Teorema 2.26 y Proposición 2.30 de [**32**]). Ahora probaremos el importante hecho de que toda función modular holomorfa en $\mathcal{H}$ puede expresarse como un polinomio en $j(\tau)$.

[11]Recordar que $\Gamma = Sl_2(\mathbb{Z})$ es el grupo de matrices 2×2 a coeficientes enteros y determinante 1, que actuan en el semiplano superior vía transformaciones de Mobius.

[12]La condición de Γ-invariancia implica periodicidad con período 1 por tanto posee q-expansión de la forma $f(\tau) = \sum_{n=-\infty}^{+\infty} a_n q^n$ donde $q = e^{2\pi i \tau}$. El hecho de que sea meromorfa en ∞ quiere decir que existe un n_0 tal que $a_n = 0$ para todo $n < n_0$.

Lema 3.12. *Toda función modular holomorfa en $\mathcal{H}$ y sin polos en ∞ debe ser constante.*

Demostración: Recordemos que asociado con el grupo modular Γ tenemos un subconjunto asociado

$$\mathcal{R}_\Gamma = \{\tau \in \mathcal{H} : \frac{-1}{2} \leq Re(\tau) \leq \frac{1}{2}, ||z|| \geq 1\} \cup \{\infty\}$$

llamado región fundamental de Γ que cumple la propiedad que cada punto de $\mathcal{H}$ es Γ-equivalente a algún punto de $\mathcal{R}_\Gamma$. Sea f una función modular holomorfa en $\mathcal{H}$, para probar que f es constante basta probar que $K = f(\mathcal{H} \cup \{\infty\})$ es compacto (por el Principio del módulo máximo), por la Γ-invariancia $K = f(\mathcal{R}_\Gamma)$. Denotemos por $\mathcal{R}_\Gamma(N) = \{\tau \in \mathcal{R}_\Gamma : Im(\tau) \leq N\}$ y consideremos $(f(\tau_n))_{n\geq 1}$ una sucesión en K, con $\tau_n \in \mathcal{R}_\Gamma$ para todo $n \geq 1$.

Si la sucesión $(\tau_n)_{n\geq 1}$ está contenida en $\mathcal{R}_\Gamma(N)$ para algún N, como $\mathcal{R}_\Gamma(N)$ es compacto entonces existe una subsucesión convergente en $\mathcal{R}_\Gamma$, $(\tau_{n_k})_{k\geq 1}$ y por lo tanto $(f(\tau_{n_k}))_{k\geq 1}$ será una subsucesión convergente de $(f(\tau_n))_{n\geq 1}$. En caso contrario existe una subsucesión $(\tau_{n_k})_{k\geq 1}$ convergente a ∞ y por lo tanto $f(\tau_{n_k}) \to f(\infty)$ (recordar que por hipótesis f no posee polo en ∞, por lo tanto $f(\infty) \in \mathbb{C}$ está definido) y nuevamente encontramos una subsucesión convergente de $(f(\tau_n))_{n\geq 1}$, por lo tanto $f(\mathcal{R}_\Gamma)$ es compacto y por lo tanto f es constante.

□

Proposición 3.13. *Toda función modular holomorfa en $\mathcal{H}$ puede expresarse como un polinomio en $j(\tau)$.*

Demostración: Si f es una función modular holomorfa con q-expansión de la forma $f(\tau) = p(q^{-1}) + \sum_{n=0}^{\infty} a_n q^n$, como $j(\tau)$ tiene un polo simple en ∞ (por lo tanto $j(\tau) = \frac{r}{q} + \sum_{i=0}^{\infty} a_n q^n$) entonces es posible conseguir un polinomio $A(X)$ tal que $A(j(\tau)) = -p(q^{-1}) + \sum_{n=0}^{\infty} a'_n q^n$. Por lo tanto $f - A(j(\tau))$ es una función modular holomorfa en $\mathcal{H}$, sin polos en ∞ y por lo tanto constante por el lema previo.

□

El grupo modular Γ posee ciertos subgrupos importantes que definiremos a continuación.

Definición 3.14 (Subgrupos de congruencia)**.** Un subgrupo de congruencias para el subgrupo modular Γ es un subgrupo de la forma

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod{m} \right\}$$

donde $m \in \mathbb{Z}^+$ (se observa que $\Gamma = \Gamma_0(1)$).

Asociado al subgrupo de congruencia $\Gamma_0(m)$ tenemos un conjunto de matrices $C(m)$ que nos ayuda a tener una descripción más explícita del conjunto cociente $\Gamma/\Gamma_0(m) = \{\Gamma_0(m)\gamma : \gamma \in \Gamma\}$.

Definición 3.15. Definimos el subgrupo de matrices $C(m)$ asociado al subgrupo de congruencia $\Gamma_0(m)$ como

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{Z}) : ad = m, a > 0, 0 \leq b < d, mcd(a, b, d) = 1 \right\}$$

Observemos que $C(m)$ posee el elemento $\theta_0 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}$ que actua como multiplicación por m, es decir, $\theta_0(\tau) = m\tau$ para todo $\tau \in \mathcal{H}$. La descripción de las clases laterales de Γ por el subgrupo de congruencias viene dada por la siguiente proposición.

Proposición 3.16. *Existe una correspondencia biunívoca entre $C(m)$ y el conjunto de clases laterales derecha $\Gamma/\Gamma_0(m) = \{\Gamma_0(m)\gamma : \gamma \in \Gamma\}$ dado por $\theta \mapsto \left(\theta_0^{-1}\Gamma\theta\right) \cap \Gamma$.*

Demostración: Es un ejercicio básico de Teoría de grupos, el enunciado es el Lema 11.11 del libro de Cox [**11**] y su demostración está como ejercicio guiado en el mismo libro (Ejercicio 11.8).

El siguiente hecho es clave para la definición de los polinomios modulares:

Lema 3.17. *Sean $\gamma_1, \gamma_2, \ldots, \gamma_t \in \Gamma$ un conjunto de representantes*[13] *de las clases laterales por $\Gamma_0(m)$ y sea $s \in \mathbb{C}[X_1, \ldots, X_t]$ un polinomio simétrico en las variables $X_1, \ldots, X_t$. Entonces la función $f : \mathcal{H} \to \mathbb{C}$ dada por:*

$$f(\tau) = s\left(j\left(m\gamma_1\tau, m\gamma_2\tau, \ldots, m\gamma_t\tau\right)\right)$$

es una función modular holomorfa en $\mathcal{H}$ (y por lo tanto un polinomio en $j(\tau)$).

Demostración: En primer lugar observemos que si $\Gamma\gamma_i = \Gamma\gamma_i' \Rightarrow j(m\gamma_i\tau) = j(m\gamma_i'\tau)$. En efecto, si $\Gamma\gamma_i = \Gamma\gamma_i'$ por la Proposición 3.16 tenemos que $\gamma, \gamma' \in \sigma_0^{-1}\Gamma\sigma$ para el mismo $\sigma \in C(m)$ por lo tanto $m\gamma_i = \mu_i\sigma$ y $m\gamma_i' = \mu'\sigma$ con $\mu, \mu' \in \Gamma$ de forma que

$$j(m\gamma_i\tau) = j(\mu_i\theta\tau) = j(\sigma\tau) = j(\mu_i'\theta\tau) = j(m\gamma'\tau).$$

Ahora observemos que, para cualquier $\gamma \in \Gamma$ las coclases $\Gamma\gamma_1, \ldots, \Gamma\gamma_t$ son una permutación de $\Gamma\gamma_1\gamma, \ldots, \Gamma\gamma_t\gamma$ de donde resulta que $j(m\gamma_1\tau), \ldots, j(m\gamma_t\tau)$ son uns permutación de $j(m\gamma_1\gamma\tau), \ldots, j(m\gamma_t\gamma\tau)$ y al ser s una función simétrica de sus variables resulta que $f(\tau) = f(\gamma\tau)$ para todo $\gamma \in \Gamma$; o sea, f es Γ-invariante.

Claramente f es holomorfa en $\mathcal{H}$ (al serlo j, γ_i para $1 \leq i \leq t$ y σ_0), así que solo resta probar que f es meromorfa en ∞.

Por la primer parte, resulta que para cada i tenemos que $j(m\gamma_i\tau) = j(\theta\tau)$ para algún $\theta \in C(m)$. Supongamos que $\theta = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ entonces $q(\theta\tau) = q\left(\frac{a\tau+b}{c}\right) = q\left(\frac{a^2\tau+ab}{m}\right) = c_\theta \cdot q_m^{a^2}$ donde $q_m = q^{\frac{1}{m}} = e^{\frac{2\pi i\tau}{m}}$ y $c_\theta = e^{\frac{2\pi iab}{m}}$ es una constante.

[13] En el sentido que $\Gamma = \Gamma_0(m)\gamma_1 \uplus \Gamma_0(m)\gamma_2 \uplus \ldots \uplus \Gamma_0(m)\gamma_t$.

Como j tiene un polo de orden 1 en infinito, entonces $j(m\gamma_i\tau)$ tendrá una q-expansión[14] de la forma

$$j(m\gamma_i\tau) = \frac{c}{q_m^{a^2}} + \sum_{n=0}^{\infty} c_n c_\theta^n q_m^{a^2 n}$$

Luego $f(\tau)$ tendrá una q-expansión de la forma:

$$f(\tau) = \sum_{n=1}^{N} b_n q_m^{-n} + \sum_{n=0}^{\infty} a_n q_m^n$$

de modo que para $m > N/m$ se tiene que $\lim_{Im(\tau)\to\infty} q^m f(\tau) = 0$ y por lo tanto f tiene un polo en ∞.

□

Ahora estamos listos para probar la existencia de los polinomios modulares.

Teorema 3.18. *Existe un polinomio $\phi_m(X,Y) \in \mathbb{C}[X,Y]$ tal que*

$$\phi_m\left(X, j(\tau)\right) = \prod_{\theta\in C(m)} \left(X - j(\theta\tau)\right) \tag{12}$$

Demostración: Consideremos $\gamma_1, \ldots, \gamma_t \in \Gamma$ un conjunto de representantes de las clases laterales por $\Gamma_0(m)$, la Proposición 3.16 establece una biyección $\alpha : C(m) \to \{\gamma_1, \ldots, \gamma_t\}$ definida para $\theta \in C(m)$ por la propiedad $\left(\theta_0^{-1}\Gamma\theta\right) \cap \Gamma = \Gamma_0(\gamma_i) \Leftrightarrow \alpha(\theta) = \gamma_i$. Pero $\alpha(\theta) = \gamma_i \Rightarrow \gamma_i = \theta_0^{-1}\widehat{\gamma}_i\theta$ con $\widehat{\gamma}_i \in \Gamma \Rightarrow \theta_0\gamma_i = \widehat{\gamma}_i\theta \Rightarrow j(\theta\tau) = j(\widehat{\gamma}_i\theta\tau) = j(\theta_0\gamma_i\tau) = j(m\gamma_i\tau)$, luego:

$$\prod_{\theta\in C(m)} \left(X - j(\theta\tau)\right) = \prod_{i=1}^{t} \left(X - j(m\gamma_i\tau)\right) = \sum_{i=0}^{t} (-1)^{t-i} s_{t-i}\left(j(m\gamma_1\tau), \ldots, j(m\gamma_t\tau)\right) X^i \tag{13}$$

donde $s_i \in \mathbb{C}[X_1, \ldots, X_t]$ es la i-ésima función simétrica elemental. Por el Lema 3.17, resulta que cada $s_i\left(j(m\gamma_1\tau), \ldots, j(m\gamma_t\tau)\right) = P_i(j(\tau))$ para algún polinomio $P_i \in \mathbb{C}[Y]$, sustituyendo en (13) se tiene que:

$$\prod_{\theta\in C(m)} \left(X - j(\theta\tau)\right) = \sum_{i=0}^{t} (-1)^{t-i} P_{t-i}\left(\tau(j)\right) X^i = \phi_m(X, \tau(j)) \tag{14}$$

para algún polinomio $\phi_m \in C[X,Y]$ como queríamos probar.

□

Definición 3.19 (Polinomio modular)**.** Al polinomio ϕ_m del Teorema anterior lo llamamos el m-ésimo polinomio modular o polinomio m-modular.

Usando un poco de Teoría de Galois es posible probar de hecho que $\phi_m \in \mathbb{Z}[X,Y]$ (Teorema 11.18 del libro de Cox [**11**]) y que $\phi_m(X,Y) = \phi_m(Y,X)$ (Teorema 3, Capítulo 5.2 del libro de Lang [**27**]).

[14] Aquí estamos haciendo un abuso de notación (la misma que el libro de Cox [**11**]) ya que en general el término q-expansión se usa para denotar un desarrollo en potencias de q pero en este caso el desarrollo es en potencias de $q_m = q^{\frac{1}{m}}$.

Observación 3.20. Para el caso en que $m = \ell$ primo, el grado del polinomio modular $\phi_\ell(X, Y)$ es $\#C(\ell) = \ell + 1$.

Antes de probar que el polinomio modular $\phi_\ell(X, Y)$ parametriza pares de curvas ℓ-isógenas, vamos a prestar atención al conjunto $C(\ell)$. Observemos primero que

$$\begin{pmatrix} 1 & \ell \\ 0 & \ell \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

por lo tanto, a todos los efectos la matriz $\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in C(\ell)$ puede ser sustituida por $\begin{pmatrix} 1 & \ell \\ 0 & \ell \end{pmatrix}$ en el conjunto $C(\ell)$. Con ese cambio nuestro conjunto $C(\ell)$ nos queda:

$$C(\ell) = \left\{ \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix} : 1 \leq k \leq \ell \right\}$$

Denotaremos de ahora en más $\sigma_0 = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ (como lo veniamos haciendo antes) y $\sigma_k = \begin{pmatrix} 1 & k \\ 0 & \ell \end{pmatrix}$ para $1 \leq k \leq \ell$.

Teorema 3.21. *Sea ℓ primo. Si dos curvas elípticas complejas E y E' verifican que $\phi_\ell(j(E'), j(E)) = 0$ entonces existe una ℓ-isogenia $\phi_\ell : E \to E'$.*

Demostración: Sea $E = \mathbb{C}/\Lambda$, sabemos que todo látice Λ es rotohomotético a un látice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$ con $\tau \in \mathcal{H}$, luego existe un isomorfismo $\eta : E \to \mathbb{C}/E_\tau$ donde $E_\tau = \mathbb{C}/\Lambda_\tau$ y tenemos que $j(E) = j(E_\tau) = j(\tau)$. En la demostración del Teorema de Kohel (Teorema 2.38) se probó que salvo isomorfismo hay $\ell + 1$ curvas ℓ-isógenas a E y son de la forma $E_i = \mathbb{C}/\Lambda_i$ donde $\Lambda_0 = \langle \frac{1}{\ell}, \tau \rangle$ y $\Lambda_i = \langle 1, \frac{\tau + k}{\ell} \rangle$ para $1 \leq i \leq \ell$.

Observamos ahora que

$$j(E_0) = j\left(\left\langle \frac{1}{\ell}, \tau \right\rangle \right) = j\left(\frac{\tau}{1/\ell} \right) = j(\ell\tau) = j\left(\sigma_0(\tau)\right)$$

Mientras que para $k = 1, 2, \ldots, \ell$ se tiene que

$$j(E_k) = j\left(\left\langle 1, \frac{\tau + k}{\ell} \right\rangle \right) = j\left(\frac{\tau + k}{\ell} \right) = j\left(\sigma_k(\tau)\right)$$

Pero por definición del polinomio modular, las raices del polinomio $\phi_\ell\left(X, j(E)\right) = \phi_\ell\left(X, j(\tau)\right)$ son $j\left(\sigma_k(\tau)\right)$ para $k = 0, 1, \ldots, \ell$; que por lo visto anteriormente coincide con $j(E_k)$ para $k = 0, 1, \ldots, \ell$.

Luego si $E'/\mathbb{C}$ es tal que $\phi_\ell\left(j(E'), j(E)\right)$ entonces $j(E') = j(E_i)$ para algún i y por lo tanto existe un isomorfismo $\nu : E_i \to E'$, si llamamos $\varphi_i : E_\tau \to E_i$ la ℓ-isogenia que conecta E_τ con E_i entonces tenemos la ℓ-isogenia $\nu \circ \varphi_i \circ \eta : E \to E'$ entre E y E', por lo tanto E y E' son ℓ-isógenias como queríamos probar.

□

De esta forma queda claro que el polinomio modular $\phi_\ell(X, Y)$ parametriza curvas ℓ-isógenas, al menos para curvas elípticas complejas. Puede probarse que todo reduce bien módulo $p \neq \ell$ obteniendo el resultado para curvas sobre cuerpos finitos, esto está hecho

en el libro de Lang [**27**], pero la prueba escapa del alcance de este trabajo.

4.2.2. Computación de polinomios modulares. Existe mucha literatura sobre la implementación de los polinomios modulares ya que ellos son usados en muchos algoritmos de Teoría de números computacional relacionada con curvas elípticas, como por ejemplo la versión mejorada de Elkies para el algoritmo de Schoof [**13**], [**34**]; para algoritmo de G. Bisson y A. Sutherland para computar el anillo de endomorfismo de una curva elíptica ordinaria [**3**] y por supuesto, para nuestro algoritmo de autoreducibilidad aleatoria.

Los primeros algoritmos para el cálculo de los polinomios modulares fueron basados en la ecuación $\phi_m\left(j(\tau), j(m\tau)\right) = 0$ (que se obtiene directamente de la ecuación (12) evaluando en $X = j(m\tau)$ observando que $\sigma_0 \in C(m)$), comparando la q-expansión de $j(\tau)$ y $j(m\tau)$, algunos artículos basados en este método son [**4**], [**13**], [**21**].

Otro enfoque para calcular los polinomios modulares consiste en calcular $\phi_\ell(X, Y)$ (mód p) para varios primos p y luego utilizar el Teorema del Resto Chino para obtener $\phi_\ell(X, Y)$ (mód p). La idea es escoger (inteligentemente) curvas elípticas $E/\mathbb{F}_p$ y con las fórmulas de Vélu obtener curvas elípticas E' definidas en alguna extensión de $\mathbb{F}_p$ que sean ℓ-isogenias a E, cada par (E, E') de curvas ℓ-isogenas son brinda una ecuación $\phi_\ell\left(j(E), j(E')\right) = 0$ (cuyas incógnitas son los coeficientes del polinomio modular ϕ_ℓ). D. Charles y K. Lauter utilizan este enfoque utilizando isogenias entre curvas supersingulares en [**8**]; A. Sutherland, R. Broker, K. Lauter implementan versiones mejoradas basándose en el grafo de isogenias para curvas ordinarias (eligiendo habilmente los primos p) en [**5**] y [**43**]. Nuestra computación de polinomios modulares la haremos siguiendo este último enfoque.

Ingredientes del Algoritmo **polymod2** implementado en Sage para la computación del polinomio modular:

- Algoritmo jvecinostodos2 $\longrightarrow$ Algoritmo casipolymod2 $\longrightarrow$ Algoritmo polymod2

El algoritmo **jvecinostodos2** toma como entrada una curva elíptica $E/\mathbb{F}_q$ y un primo $\ell > 3$ tal que $p > \frac{\ell^2-1}{2}$ (donde p es la característica de $\mathbb{F}_q$) y devuelve una lista de j-invariantes $\left[j\left(\frac{E}{\langle P\rangle}\right) : P \in E[\ell]\right]$ (donde $E[\ell] = \{P \in E(\overline{F}_q) : \ell P = \mathcal{O}\}$) y el cuerpo finito donde viven esos j-invariantes. Los principales pasos de este algoritmo son:

i) Calcular el polinomio de ℓ-división ψ_ℓ para E.
ii) Factorizar ψ_ℓ en $\mathbb{F}_q[x]$ y calcular $t = 2mcm\{gr(p) : p$ es un factor irreducible de $\psi_\ell\}$ (esto t garantiza que las coordenadas de los puntos de $E[\ell]$ se encuentran en la extensión $\mathbb{F}_{q^t}$).
iii) Crear una lista Lroots formada por todas las raices de ψ_ℓ en $\mathbb{F}_{q^t}[x]$ (esta lista contiene todas las coordenadas-x de los puntos de $E[\ell]$).
iv) Tomar un x_0 en la lista Lroots y hallar $y_0 \in \mathbb{F}_{q^t}$ tal que $P = (x_0, y_0) \in E$ (se tiene en realidad que $P \in E[\ell]$).
v) Calcular una lista Pmult cuyos elementos son los múltiplos de P (Pmult= $[nP : 0 \leq n < \ell]$).
vi) Hallar x_1 en Lroots, tal que x_1 no sea una coordenada-x de ningún punto de la lista Pmult y calcular $y_1 \in \mathbb{F}_{q^t}$ tal que $Q = (x_1, y_1) \in E$ (se tiene que $Q \in E[\ell]$ pero $Q \notin \langle P\rangle$).

vii) Del hecho que $E[\ell] = \frac{\mathbb{Z}}{\ell\mathbb{Z}}P \oplus \frac{\mathbb{Z}}{\ell\mathbb{Z}}Q$ obtener los $\ell+1$ subgrupos de orden ℓ de $E[\ell]$ (aquí se usa que $E[\ell] \simeq \frac{\mathbb{Z}}{\ell\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}}$ para $\ell \neq p$).

viii) Para cada subgrupo $G = \{(x_1, y_1), \ldots, (x_s, y_s), (x_1, -y_1), \ldots, (x_s, -y_s), \mathcal{O}\}$ de orden ℓ (donde $s = \frac{\ell-1}{2}$) calcular el polinomio $f_G(x) = (x - x_1)(x - x_2)\ldots(x - x_s)$ que será el polinomio definidor del kernel de una ℓ-isogenia $\phi_G : E \to E/\langle T\rangle$ y crear una lista J con cada j-invariante $j(E/\langle T\rangle)$.

ix) Devolver la pareja J, $\mathbb{F}_{q^t}$.

Como ejemplo, tomemos la curva $E : y^2 = x^3 + 299x + 59$ definida sobre $\mathbb{F}_{331}$ que tiene j-invariante igual a 3 y tomemos el primo $\ell = 5$:

> `E=EllipticCurve(GF(331),[299,59])`
> `E.j_invariant(): 3`
> `(J,F) = jvecinostodos2(E,5)`
> `J:`
> $[166, 129a^3 + 250a^2 + 230a + 300, 59a^3 + 140a^2 + 195a + 37, 9,$
> $202a^3 + 81a^2 + 101a + 36, 272a^3 + 191a^2 + 136a + 101]$
> `F: Finite Field in a of size` 331^4`.`
> `F.an_element().charpoly():` $x^4 + 3x^2 + 290x + 3$

Esto quiere decir que los j-invariantes de curvas 5-isógenas con $E/\mathbb{F}_{331}$ (definidos en $\overline{\mathbb{F}}_{331}$) vienen dados por los elementos de la lista J, donde $a = X \pmod{f(X)}$ es un elemento del cuerpo finito $\mathbb{F}_{331^4} = \mathbb{F}_{331}[X]/\langle f(X)\rangle$ donde $f(X) = X^4 + 3X^2 + 290X + 3$ (se observa que $f \in \mathbb{F}_{331}[X]$ es un polinomio irreducible).

El algoritmo **casipolymod2** toma como entrada lo mismo que el algoritmo anterior y devuelve el polinomio $p(X) = \phi_\ell(X, j(E))$. Este algoritmo es simple de describir, utilizamos el algoritmo anterior para crear una lista J con todos los j-invariantes que se relacionan con $j(E)$ por una ℓ-isogenia. Por propiedad del polinomio modular estas son las raices de $p(X)$ y por lo tanto podemos reconstruir $p(X) = \prod_{j\in J}(X - j)$. Se observa que aunque los elementos de J no estén en $\mathbb{F}_p$, el polinomio resultante $p(X)$ tiene coeficientes en $\mathbb{F}_p$.

Aplicando este algoritmo para el ejemplo anterior (para $E : y^2 = x^3 + 299x + 59/\mathbb{F}_{331}$ y $\ell = 5$) obtenemos:

> `casipolymod2(E,5):` $x^6 + 13x^5 + 159x^4 + 217x^3 + 13x^3 + 329x + 193$

Y por último, el algoritmo **polymod2**. A grandes razgos el algoritmo consiste en usar el algoritmo casipolymod2 para distintos valores de j, por cada valor de j obtenemos los coeficientes del polinomio $p(X) = \phi_\ell(X, j)$, que nos brinda una relación entre los coeficientes del polinomio modular $\phi_\ell(X, Y)$, con suficientes ecuaciones conseguimos determinar los coeficientes del polinomio modular.

El algoritmo consiste en dos partes, la primer parte consiste en capturar una lista de j-invariantes para aplicarle el algoritmo casipolymod2. La clave aquí está en la forma de elegir esos j-invariantes. Recordemos que el algoritmo casipolymod2 usa el algoritmo jvecinostodos2, el cual necesita extender el cuerpo de definición de las curvas E de forma de contener las coordenadas de todos los puntos de ℓ-torsión y cuanto mayor esa extensión,

mucho menos eficiente se vuelve el algoritmo[15]. Así que necesitamos escoger cuidadosamente esa lista de j-invariantes.

La segunda parte toma la lista de j-invariantes $L = [j_0, j_1, \ldots, j_\ell]$ y les aplica el algoritmo casipolymod2, cada uno de esos j-invariantes j_i nos brinda una ecuación de la forma:

$$\phi_\ell\,(X, j_i) = X^{\ell+1} + b_{i\ell}X^\ell + \ldots + b_{i1}X + b_{i0} \tag{15}$$

Si escribimos al polinomio modular $\phi_\ell(X, Y)$ como polinomio en $\mathbb{Z}[Y][X]$ nos queda una expresión de la forma

$$\phi_\ell(X, Y) = X^{\ell+1} + p_\ell(Y)X^\ell + \ldots + p_1(Y)X + p_0(Y) + Y^{\ell+1} \tag{16}$$

donde cada p_k es un polinomio de grado menor o igual que ℓ, o sea de la forma $p_k(Y) = a_{k\ell}Y^\ell + a_{k\ \ell-1}Y^{\ell-1} + \ldots + a_{k1}Y + a_{k0}$, determinar el polinomio modular $\phi_\ell(X, Y)$ (módulo p), equivale a determinar cada uno de los coeficientes a_{ki} para $0 \leq k, i \leq \ell$.

Para cada $i = 0, 1, \ldots, \ell$, colocando $Y = j_i$ en la ecuación (16) y comparando con (15), obtenemos que $p_k(j_i) = b_{ik}$ si $k \neq 0$ y $p_0(j_i) + j_i^{\ell+1} = b_{i0}$, es decir, para $i = 0, 1, \ldots, \ell$ se tiene:

$$\begin{cases} a_{0\ell}j_i^\ell + a_{0\ \ell-1}j_i^{\ell-1} + \ldots + a_{01}j_i + a_{00} = b_{i0} - j_i^{\ell+1} & \text{para } k = 0 \\ a_{k\ell}j_i^\ell + a_{k\ \ell-1}j_i^{\ell-1} + \ldots + a_{k1}j_i + a_{k0} = b_{ik} & \text{para } k \neq 0 \end{cases}$$

Matricialmente obtenemos una ecuación de la forma $AJ = B$ donde

$$A = \begin{pmatrix} a_{00} & a_{01} & \ldots & a_{0\ell} \\ a_{10} & a_{11} & \ldots & a_{1\ell} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\ell 0} & a_{\ell 1} & \ldots & a_{\ell\ell} \end{pmatrix}, J = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ j_0 & j_1 & \ldots & j_\ell \\ \vdots & \vdots & \ddots & \vdots \\ j_0^\ell & j_1^\ell & \ldots & j_\ell^\ell \end{pmatrix}$$

y $$B = \begin{pmatrix} b_{00} - j_0^{\ell+1} & b_{10} - j_1^{\ell+1} & \ldots & b_{\ell 0} - j_\ell^{\ell+1} \\ b_{01} & b_{11} & \ldots & b_{\ell 1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{0\ell} & b_{1\ell} & \ldots & b_{\ell\ell} \end{pmatrix}$$

Como J resulta ser una matriz de Vandermonde y los j_i son distintos dos a dos, entonces resulta ser una matriz invertible y podemos calcular la matriz A como $A = BJ^{-1}$.

Por ejemplo, implementando esta rutina en Sage podemos obtener los primeros polinomios modulares para $q = 331$:

> `polymod2(3,331,6)`
$-x^2y^2 + x^3 + 164x^2y + 164xy^2 + y^3 - 141x^2 + 133xy - 141y^2 + 7x + 7y + 111$

> `polymod2(3,331,6)`
$-x^3y^3 - 85x^3y^2 - 85x^2y^3 + x^4 - 164x^3y - 118x^2y^2 - 164xy^3 + y^4 - 132x^3 + 54x^2y + 54xy^2 - 132y^3 - 150x^2 - 19xy - 150y^2 - 117x - 117y$

> `polymod2(5,331,4)`
$-x^5y^5 + 79x^5y^4 + 79x^4y^5 - 21x^5y^3 - 79x^4y^4 - 21x^3y^5 + 157x^5y^2 + 148x^4y^3 + 148x^3y^4 + 157x^2y^5 + x^6 + 143x^5y - 134x^4y^2 - 16x^3y^3 - 134x^2y^4 + 143xy^5 + y^6 - 136x^5 - 128x^4y - 138x^3y^2 - 138x^2y^3 - 128xy^4 - 136y^5 - 150x^4 - 84x^3y - 35x^2y^2 - 84xy^3 - 150y^4 - 108x^3 + 162x^2y + 162xy^2 - 108y^3 + 103x^2 - 10xy + 103y^2 - 42x - 42y + 106$

[15]Cuidado: extensiones de grado mayor que 24 casi siempre hacen caer el servidor de Sage del Cmat!

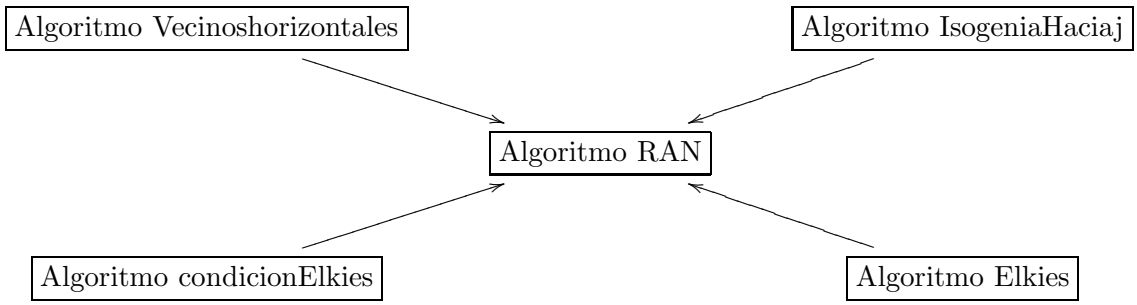
El último parámetro corresponde al máximo grado de la extensión permitida para los j-invariantes que son usados para obtener el polinomio modular, el cual puede ser estimado observando el orden de magnitud del mínimo común múltiplo de los factores irreducibles del polinomio de ℓ-división para varias curvas $E/\mathbb{F}_p$.

Detalles sobre la implementación en Sage pueden ser encontrados en mi página personal `http://www.fing.edu.uy/~cqureshi/`, en la worksheet llamada computando polymods.sws.

4.3. Implementación de la parte aleatoria: Algoritmo Ran. En esta parte describiremos más en detalle la parte aleatoria del Algoritmo de Autoreducibilidad aleatoria (RAN,RED) para el problema de determinar si curvas elípticas definidas sobre el mismo cuerpo $\mathbb{F}_q$, con la misma cantidad de puntos y el mismo tipo de endomorfismo tienen la misma dificultad respecto al problema del logaritmo discreto.

Recordemos que suponemos predeterminados los parámetros (B, r_0, q, N) del algoritmo, así como que tenemos precomputado una diccionario Phi de polinomios modulares de la forma Phi= {2:phi2, 3:phi3, 5:phi5, 7phi7, ..., ℓ_0:phiℓ_0} donde ℓ_0 es el mayor primo menor o igual a B (en realidad nuestro algoritmo funciona aunque el diccionario Phi no esté completo).

Por claridad antes de definir el algoritmo **Ran**, vamos a definir y describir algunas subrutinas (algoritmos previos) por separados que son **Vecinoshorizontales, Isogenia-Haciaj, condicionElkies** y **Elkies**.



Comenzemos primero con el algoritmo **Vecinoshorizontales**, este algoritmo toma un vértice j del grafo $\mathcal{G}_{q,N,\ell}$ y el polinomio modular ϕ_ℓ (mód p) y nos devuelve una lista con todos los vecinos horizontales de j en el grafo $\mathcal{G}_{q,N,\ell}$.

Conociendo ϕ_ℓ podemos calcular facilmente la cantidad de vecinos de un j-invariante j como $vec(j) = \{j' \in \mathbb{F}_q : \phi_\ell(j', j) = 0\}$ (multiconjunto, cada j' se cuenta tantas veces como su multiplicidad como cero de $\phi_\ell(X, j)$) y su grado $gr(j) = \#vec(j)$.

- Paso 1: Calcular $vec(j)$ y $gr(j)$.

Aquí pueden presentarse varias posibilidades, si $gr(j) = 0$ entonces j no posee vecinos horizontales (por no poseer vecinos) y el algoritmo devuelve la lista vacia [ ].

Si $gr(j) = 1$ entonces hay dos posibilidades, así que calculamos $vec(j')$ donde j' es el (único) vecino de j. Si $vec(j') = [j]$ entonces necesariamente estamos en el caso degenerado

(y por lo tanto la arista (j, j') es horizontal) y devolvemos $[j']$. Caso contrario (o sea, si $gr(j') > 1$) entonces estamos en el caso no degenerado y j está en el piso, por lo tanto no posee vecinos horizontales y el algoritmo devuelve la lista vacia $[\,]$.

Si $gr(j) = 2$, esto solo puede darse en el caso degenerado (y $\left(\frac{d_{\mathbb{K}}}{\ell}\right) = 1$) y por lo tanto ambos vecinos de j son horizontales y el algoritmo retorna $vec(j)$.

Si $gr(j) > 2$ entonces estamos necesariamente en el caso no degenerado y j es un vértice que no está en el piso del grafo $\mathcal{G}_{q,N,\ell}$, en este caso definimos la lista $A = [[v, j, v] : v \in vec(j)]$ y vamos al paso 2.

- Paso 2: Sustituir cada tripleta $[v, j_1, j_2] \in A$ por todas las tripletas de la forma $[v, j_2, j_3]$ donde $j_3 \in vec(j_2)$, $j_3 \neq j_1$. Si luego de realizar todas las sustituciones, tenemos alguna tripleta $[v, j_2, j_3]$ con $gr(j_3) = 1$ (o sea j_3 en el piso) vamos al paso 3, en caso contrario volvemos a repetir el paso 2.

Observar que las primeras tripletas en llegar al piso, son de la forma $[v, j_2, j_3]$ donde v es un vecino descendente de j, así que si eliminamos esas tripletas de la lista A, nos quedaremos con tripletas $[v, j_2, j_3]$ donde v es un vecino horizontal o ascendente de j.

- Paso 3: Eliminar todas las tripletas de la forma $[v, j_2, j_3]$ con $gr(j_3) = 1$ de A y definir una nueva lista $Jhor = [\,]$.
- Paso 4: Tomar una tripleta $[v, j_1, j_2] \in A$ y calcular $vec(j_2)$.
  - Si para algún $j_3 \in vec(j_2)$ se tiene que $gr(j_3) = 1$ (j_3 está el piso, lo cual implica que v era un vecino horizontal de j), agregar v a la lista $Jhor$ y quitar de la lista A a todas las tripletas que comienzen en v.
    - Si $A = \varnothing \Rightarrow$ retornar $Jhor$.
    - Si $A \neq \phi \Rightarrow$ volver al paso 4.
  - Si $vec(j_2)$ no tiene vértices del piso, entonces quitar $[v, j_1, j_2]$ de la lista A (o bien v está es un vecino ascendente de j o bien es un vecino horizontal y la tripleta $[v, j_2, j_3]$ no se obtuvo de un camino estrictamente descendente).
    - Si $A = \varnothing \Rightarrow$ retornar $Jhor$.
    - Si $A \neq \phi \Rightarrow$ volver al paso 4.

En el final obtenemos una lista $Jhor$ formado por los vecinos horizontales de j.

Ahora describiremos el algoritmo **IsogeniaHaciaj**, este algoritmo toma como entrada una curva elíptica $E/\mathbb{F}_q$, un primo ℓ y un j-invariante $j_2 \in \mathbb{F}_q$ tal que $\phi_\ell(j(E), j_2) = 0$. y devuelve una ℓ-isogenia $\phi : E \to E_2$ definida sobre $\mathbb{F}_q$ con $j(E_2) = j_2$.

A grandes razgos, sin detalles de implementación, el algoritmo consiste en considerar todos los subgrupos G de orden ℓ de $E[\ell]$ y construir para cada uno, una isogenia $f_G : E \to E/G$, cuando encuentre un G tal que $j(E/G) = j_2$ entonces devuelve f_G.

Antes de ir a la implementación, una proposición que nos servirá para mejorar la eficiencia del algoritmo.

Proposición 3.22. *Sea $E/\mathbb{F}_q$ una curva elíptica y $P \in E$ un punto de ℓ-torsión (no necesariamente definido sobre $\mathbb{F}_q$). Entonces una condición necesaria para que $j(E/\langle P\rangle) \in \mathbb{F}_q$ es que $\#orb(P) < \ell$, donde $orb(P) = \{\sigma_q^k(P) : k \geq 0\}$ es la órbita por la acción del*

grupo de Galois $\mathrm{Gal}(\overline{F}_q/\mathbb{F}_q)$ *(y* σ_q *es el q-frobenius).*

Demostración: Observemos que $j(E/\langle P\rangle) \in \mathbb{F}_q$ es equivalente a que el subgrupo $\langle P\rangle$ esté definido sobre $\mathbb{F}_q$ y esto es a su vez, equivale a que $\sigma_q(P) \in \langle P\rangle$ puesto que si $\sigma_q(P) = mP \Rightarrow \sigma_q(kP) = \pm k\sigma_q(P) \in \langle P\rangle$ (como $E/\mathbb{F}_q$ entonces las coordenadas de $x(kP)$ son una función racional con coeficientes en $\mathbb{F}_q$ de $x(P)$ y por lo tanto $\sigma_q(x(kP)) = x(k\sigma_q(P))$). Pero a su vez $\sigma_q(P) \in \langle P\rangle$ implica que $orb(P) \subseteq \langle P\rangle$ (pues σ_q preserva el orden de los puntos de E, dado que E está definida sobre $\mathbb{F}_q$). Por otra parte $\mathcal{O} \notin orb(P)$, así que $orb(P) \subset \langle P\rangle\backslash\{\mathcal{O}\}$, luego, tomando cardinales resulta que se debe tener que $\#orb(P) < \ell$.

□

Corolario 3.23. *Sean* ℓ *primo impar diferente de p,* ψ_ℓ *el polinomio de* ℓ*-división de E (con* ℓ *impar,* $\ell \neq p$*), y* $f \in \mathbb{F}_q[x]$ *un factor irreducible de* ψ_ℓ *de grado mayor que* $\ell - 1$*. Si* $x_0 \in \overline{F}_q$ *verifica* $f(x_0) = 0$ *y* $P_0 = (x_0, y_0) \in E[\ell]$ *entonces* $\langle P\rangle$ *no está definido sobre* $\mathbb{F}_q$ *(y por lo tanto* $j(E/\langle P\rangle) \notin \mathbb{F}_q$*)*

Demostración: Las raices de f en $\overline{F}_q$ está dada por la $\mathrm{Gal}(\overline{F}_q/\mathbb{F}_q)$-órbita de x_0, que a su vez son las coordenadas-x de los puntos de $orb(P_0)$ por lo tanto $\#orb(P_0) \geq \#orb(x_0) = gr(f) \geq \ell$. Por absurdo, si $\langle P\rangle$ estuviese definido sobre $\mathbb{F}_q$ entonces por la Proposición anterior tenemos que $\#ord(P_0) < \ell$ contradiciendo $\#orb(P_0) \geq \ell$. Luego $\langle P\rangle$ no está definido sobre $\mathbb{F}_q$.

□

Comentario 3.24. En realidad es posible probar que el corolario vale para $gr(f) > \frac{\ell-1}{2}$ (que es menos restrictivo que pedir que $gr(f) > \ell - 1$), esto aparece mencionado en el libro de Galbraith [**19**], Capítulo 25.2.

Ahora comentamos la sobre la implementación del algoritmo, vamos a ver primero el caso en que $\ell = 2s + 1$ sea impar.

- Paso 1: Computar una lista L formada por los factores irreducibles del polinomio de ℓ-división de E, que tengan grado menor que ℓ.

En Sage tenemos los comandos E.division_polynomial(ℓ) (donde E es la curva elíptica en cuestión) para obtener el ℓ-ésimo polinomio modular de E y factor(ψ_ℓ) para factorizar el polinomio de ℓ-división ψ_ℓ en producto de polinomios irreducibles.

- Paso 2: Tomar $f \in L$, calcular $x \in \overline{\mathbb{F}}_q$ tal que $f(x) = 0$ e $y \in \overline{\mathbb{F}}_q$ tal que $(x, y) \in E[\ell]$ y calcular $\sigma_q(P)$.

Para calcular una raíz de f en una clausura algebraica en Sage es necesario conocer alguna extensión finita donde viva esa raíz, si llamamos $r = gr(f)$, es claro que cada raíz x de f genera una extensión de grado r sobre $\mathbb{F}_q$, por lo tanto podemos encontrar las raices de f en Sage a través del comando f.roots($\mathbb{F}_{q^r}$). En realidad, como luego vamos a resolver la ecuación (en y) $y^2 = x^3 + ax + b$ (donde $E : Y^2 = X^3 + aX + b$), conviene trabajar en el cuerpo $\mathbb{F}_{q^{2r}}$ en lugar de $\mathbb{F}_{q^r}$. Un detalle adicional de implementación es que para poder trabajar con el punto $P = (x, y) \in E[\ell]$ entonces debemos extender el cuerpo de definición de la curva E, eso se logra con el comando $E.base\_extend(\mathbb{F}_{q^{2r}})$.

- Paso 3a: Si $\sigma_q(P) \notin \langle P\rangle$ entonces quitamos f de la lista L y volvemos al paso 2.

- Paso 3b: Si $\sigma_q(P) \in \langle P \rangle$, tenemos que $\langle P \rangle = \{\mathcal{O}\} \cup \{(x_1, y_1), \ldots, (x_s, y_s)\} \cup \{(x_1, -y_1), \ldots, (x_s, -y_s)\}$ donde $iP = (x_i, y_i)$ para $1 \leq i \leq s$. Computamos el polinomio $f(X) = (X - x_1) \ldots (X - x_s)$ (polinomio definidor del kernel).
- Paso 4: A partir del polinomio f definidor del kernel calculamos la isogenia $\phi : E \to \frac{E}{\langle P \rangle}$ (es Sage se usa el comando EllipticCurveIsogeny(E,f)) y calculamos $j' = j(\frac{E}{\langle P \rangle})$ (en sage usamos el comando $\phi.codomain().j\_invariant()$).
- Paso 5: Si $j' = j_2$ entonces devolvemos la isogenia ϕ calculada en el paso 4. Caso contrario quitamos f de la lista L y volvemos al paso 2.

En el caso que $\ell = 2$ es mucho más sencillo (y eficiente), si $E : Y^2 = f(X)$ entonces hallamos las raices de f en $\mathbb{F}_q$ (pues para orden 2 vale $\langle P \rangle$ está definido sobre $\mathbb{F}_q$ si y solo si P lo está). Si x_0 es una de esas raices entonces calculamos la isogenia que tiene como polinomio definidor del kernel al polinomio $X - x_0$, al igual que en el caso ℓ impar, comparamos el j-invariante del codominio con el j_2 que queremos. Repetimos esto con cada raíz hasta obtener la isogenia con codominio de j-invariante j_2.

Con respecto a los algoritmos **condicionElkies** y **Elkies**, el primero es simplemente para verificar que estemos en las hipótesis de algoritmo de Elkies, el segundo es el algoritmo de Elkies, cuyo pseudocódigo fue escrito en la sección 2.2.2 en este capítulo. Recordamos que este algoritmo tomaba como entrada una curva elíptica $E/\mathbb{F}_q$, un primo $\ell > 2$, el polinomio modular $\phi_\ell(X, Y)$ (mód p) y un j-invariante $j_2 \in \mathbb{F}_q$ tal que $\phi_\ell(j(E), j_2) = 0$. En caso de cumplirse las condición:

$$j_1 \cdot j_2 \cdot \frac{\partial \phi_\ell}{\partial x}(j_1, j_2) \cdot \frac{\partial \phi_\ell}{\partial y}(j_1, j_2) \neq 0$$

donde $j_1 = j(E)$ (esto es chequeado justamente con el algoritmo **condicionElkies**), el algoritmo **Elkies** devuelve el polinomio definidor del kernel de una ℓ-isogenia definida sobre $\mathbb{F}_q$ $\phi : E \to E_2$ donde $j(E_2) = j_2$. Algunos detalles sobre este algoritmo pueden encontrarse en el libro de Galbraith [**19**], Capítulo 25.2.1.

Ahora finalmente describiremos el algoritmo **Ran**, este algoritmo toma una curva elíptica $E/\mathbb{F}_q$ cuyo j-invariante $j(E) = j$ representa un vértice del grafo de isogenias $S_{N,q,B}$ (donde $N = \#E(\mathbb{F}_q)$) y devuelve una pareja (k, E'). Escencialmente este algoritmo consiste de tres partes, la elaboración de una lista de primos con distribución adecuada (a continuación aclararemos que quiere decir esto), el sorteo de un primo ℓ de esa lista y la elaboración de una ℓ-isogenia que hará parte de nuestro comodín (aquí hay que distinguir dos tipos de primos) y la construcción de la función de transición. Pasaremos a discutir ahora el código Sage del algoritmo **Ran** (ver página 113).

El algoritmo comienza construyendo una lista de primos $\ell \leq B$ con la distribución adecuada, eso es realizado en las líneas 2-12.

Llamemos $\mathcal{O} = \mathrm{End}(E)$, recordemos que nuestro comodín estará compuesto por isogenias horizontales, por lo tanto es necesario que $\mathcal{O}$ esté en la superficie con respecto del ℓ considerado (esto siempre se cumple para el caso degenerado) y en ese caso la cantidad de aristas que salen de un vértice dado será $1 + \left(\frac{\ell}{d_K}\right)$. Los primos ℓ tales que $\left(\frac{\ell}{d_K}\right) = -1$ no aportarán aristas horizontales y por lo tanto pueden ser omitidos de la lista ℓ. Aquellos primos tales que $\left(\frac{\ell}{d_K}\right) = 0$ aportarán una arista horizontal (si $\mathcal{O}$ es maximal respecto de ℓ) y les otorgaremos peso 1 mientras que los primos tales que $\left(\frac{\ell}{d_K}\right) = 1$ aportarán dos

aristas horizontales (si $\mathcal{O}$ es maximal respecto de ℓ) y les otorgaremos peso 2.

Hay dos tipos de primos a considerar, recordemos que $\mathcal{O}$ es maximal con respecto de ℓ (lo que equivale a decir que $\mathcal{O}$ corresponde a un nivel maximal en el grafo $\mathcal{G}_{q,N,\ell}$) si y solo si $\ell \nmid [\mathcal{O}_{\mathbb{K}} : \mathcal{O}]$, por lo tanto los primos que dividen al conductor de $\mathcal{O}$ deben ser descartados.

Pero calcular el conductor de $\mathcal{O}$ es muy caro, así que en su lugar, consideraremos los primos ℓ que dividen al conductor del frobenius (recordar que $\mathbb{Z}[\phi_q] \subset \mathcal{O}$ por lo tanto el conductor de $\mathcal{O}$ divide al conductor del frobenius) y los llamaremos de primos problematicos[16]. Los primos no problematicos corresponden siempre al caso degenerado y en ese caso, cualquier arista que tomemos va a ser horizontal, pero en el caso problematico debemos asegurarnos de que nuestro orden $\mathcal{O}$ sea maximal respecto de ℓ y de que la arista sorteada sea horizontal.

El segundo paso es la construcción del comodín (líneas 13-39), nuestro comodín comienza con nuestra curva elíptica E y luego le sigue una cadena de ℓ-isogenias horizontales (con $\ell \in L$) de largo r_0 y culmina con la curva imagen de la última isogenia considerada (que coincide con la función de transición tr aplicada a (E, k) donde k es el comodín construido). Para construir dicha cadena de isogenias sorteamos en cada paso un primo $\ell \in L$ (con la distribución dada anteriormente) y separamos en dos casos seguún el primo sorteado sea problemático o no.

En el caso que el primo ℓ sea problemático (líneas 16-30), calculamos una lista V formada por sus vecinos horizontales usando el algoritmo **Vecinoshorizontales**. En caso de que esta lista sea vacia, esto indica que $\mathcal{O}$ no es un nivel maximal respecto de ℓ (recordar que ya habiamos descartados los primos ℓ tal que $\left(\frac{\ell}{d_K}\right) = -1$) y por lo tanto borramos a ℓ de nuestra lista. Caso contrario sorteamos algún $j' \in V$ y calculamos una ℓ-isogenia hacia una curva $E'/\mathbb{F}_q$ con j-invariante igual a j usando **Elkies** si condicionElkies=True o **IsogeniaHaciaj** en caso contrario.

En el caso que el primo ℓ no sea problemático (líneas 31-39), no tenemos el problema de poder salirnos del nivel, en ese caso calculamos una lista V formada por sus vecinos (que van a ser necesariamente horizontales), sortemos $j' \in V$ y construimos una isogenia hacia una curva $E'/\mathbb{F}_q$ con $j(E') = j'$ usando **Elkies** si condicionElkies=True o **IsogeniaHaciaj** en caso contrario.

Repetimos ese procedimiento hasta obtener una lista de isogenias de largo r_0 y agregamos al comodín k la curva E', curva imagen de la última isogenia obtenida (líneas 40-41), esta curva $E' = tr(E, k)$ por lo tanto retornamos el par $[E', k]$.

Todos los algoritmo en Sage utilizados (incluyendo los algoritmos previos a **Ran**) pueden encontrarse en mi página personal `http://www.fing.edu.uy/~cqureshi/`.

[16]Problemático en el sentido que hay que tener especial cuidado de asegurarnos que $\mathcal{O}$ sea maximal con respecto de ℓ, ya que sin ese cuidado podríamos estar sorteando una isogenia que se escape del nivel $\mathcal{O}$ de nuestro grafo.

Algoritmo Ran. Usa como subrutina los algoritmos Vecinoshorizontales, IsogeniaHaciaj, condicionElkies, Elkies. Requiere precomputación previa de un diccionario Phi de polinomios modulares y establecer los parámetros B y r_0.

Entrada: Una curva elíptica $E/\mathbb{F}_q$.
Salida: Una pareja (E', k) donde k es el comodín y $E' = tr(E, k)$.

```
1. def Ran(E):
.....................................................................................
2.    F= E.base_field()                (# Construcción de primos con distribución adecuada.)
3.    dK=NumberField(E.frobenius_polynomial(),'a').discriminant()
4.    dpi = E.frobenius_order().discriminant(); cpi = ZZ(sqrt(dpi/dK))
5.    P1=[ ] ; P2=[ ]
6.    for l in prime_range(B):
7.       k = kronecker(dK,l)
8.       if k==0:
9.          P1.append(l)
10.      if k==1:
11.         P2.append(l)
12.   P=P1+P2 ; R=len(P1)*[1]+len(P2)*[2]; Ds=GeneralDiscreteDistribution(R)
.....................................................................................
13.   Comodin=[E]; isog=E.identity_morphism()    (# Comenzando a construir el comodín)
14.   while len(Comodin)<r0+1:
15.      E = isog.codomain(); j= E.j_invariant(); l=P[Ds.get_random_element()]
.....................................................................................
16.      if l%cpi ==0:                          (# Primos problematicos por separado.)
17.         V=Vecinoshorizontales(j,Phi[l])
18.         if len(V)==0:
19.            P.remove(l)
20.            if dK%l==0:
21.               R.remove(1)
22.            else:
23.               R.remove(2)
24.            Ds=GeneralDiscreteDistribution(R)
25.         else:
26.            j2=choice(V)
27.            if condicionElkies(E,l,j2,Phi[l]):
28.               f=Elkies(E,l,j2,Phi[l]); isog = EllipticCurveIsogeny(E,f)
29.               Comodin+=[isog]
30.            else:
31.               isog=IsogeniaHaciaj(E,l,j2); Comodin+=[isog]
.....................................................................................
32.      else:                                          (# Primos no problematicos.)
33.         if l in Phi:
34.            T.⟨x⟩=F[ ]; g=T(Phi[l].subs(y=j))
35.            j2= choice([x[0] for x in g.roots()])
36.            if condicionElkies(E,l,j2,Phi[l]):
37.               f=Elkies(E,l,j2,Phi[l]); isog = EllipticCurveIsogeny(E,f)
38.               Comodin+=[isog]
39.            else:
40.               isog=IsogeniaHaciaj(E,l,j2); Comodin+=[isog]
41.         else:
42.            f = isogenia2(E,l); isog = EllipticCurveIsogeny(E,f)
43.            Comodin+=[isog]
.....................................................................................
44.   E2=isog.codomain()                    (#Calculando la función de transición.)
45.   wildcard = Comodin+[E2]
46.   trans = wildcard[len(wildcard)-1]
47.   return [trans,wildcard]
```

Código Sage del Algoritmo Ran.

Como ejemplo corremos este algoritmo en Sage comenzando con la curva $E : Y^2 = X^3 + 299X + 59/\mathbb{F}_{331}$ tomando como parámetros $(B, r_0) = (20, 10)$.

```
>  E= EllipticCurve(GF(331),[299,59]); N= E.cardinality()
>  q=331 ; (B,r0)=(20,10)
> [E2,k]= Ran(E)
>  E2 :
Elliptic Curve defined by y^2 = x^3 + 288*x + 126 over Finite Field of size 331
>  for i=[1..r0]:
       print k[i]
```

- Isogeny of degree 13 from Elliptic Curve defined by $y^2 = x^3 + 299x + 59$ over Finite Field of size 331 to Elliptic Curve defined by $y^2 = x^3+31x+197$ over Finite Field of size 331
- Isogeny of degree 5 from Elliptic Curve defined by $y^2 = x^3 + 31x + 197$ over Finite Field of size 331 to Elliptic Curve defined by $y^2 = x^3+252x+231$ over Finite Field of size 331

  ⋮
- Isogeny of degree 13 from Elliptic Curve defined by $y^2 = x^3 + 252x + 231$ over Finite Field of size 331 to Elliptic Curve defined by $y^2 = x^3+149x+326$ over Finite Field of size 331

Podemos ver los mapas racionales que definien las isogenias usando el comando $\phi.rational\_maps()$ (donde ϕ es la isogenia a la que le queremos determinar sus mapas racionales), por ejemplo aplicándolo a nuestra primer isogenia $\phi_1 = k[1]$ resulta que $\phi_1 = (f, g)$ donde f e g son mapas racionales dados por:

$$f = \frac{x^{13}+193x^{12}+14x^{11}+173x^{10}+29x^9+89x^8+212x^7+207x^6+180x^5+322x^4+210x^3+58x^2+97x+110}{x^{12}+193x^{11}+159x^{10}+90x^9+322x^8+213x^7+63x^6+100x^5+203x^4+273x^3+149x^2+221x+121}$$

$$g = \frac{x^{18}y+124x^{17}y+243x^{16}y+216x^{15}y+35x^{14}y+35x^{13}y+285x^{12}y+211x^{11}y+11x^{10}y+262x^9y+\ldots}{x^{18}+124x^{17}+98x^{16}+307x^{15}+158x^{14}+117x^{13}+42x^{12}+315x^{11}+232x^{10}+273x^9+\ldots}$$

4.4. Implementación de la autoreducibilidad: Algoritmo Red. En esta parte veremos como implementar el algoritmo Red en Sage. La descripción a grandes razgos de esta etapa ya fue vista en la Sección 3, ahora daremos el código en Sage (en la siguiente carilla) y luego describiremos los principales aspectos de la implementación.

Este algoritmo escencialmente consiste en definir una función F que compute el PLD en E a partir de una función G que compute el PLD en $E' = tr(E, k)$, la eficiencia del algoritmo para computar F dependerá exclusivamente de que tan eficiente sea G para calcular el PLD en la curva E'. Como observamos, hay cuatro etapas bien distinguidas del algoritmo.

La primer etapa consiste en la descomposición de la pareja (P, Q) a la cual queremos calcularle el PLD a través de la función F (líneas 3-8). Comenzamos descomponiendo $N = N_0N_1$ con N_1 B-smooth, aquí una pequeña diferencia respecto a lo comentado en la sección 3 para mejorar aún más la eficiencia del algoritmo, observemos que en la descomposición de (P, Q) en $(P_0, Q_0) = (N_1P, N_1Q)$ y $(P_1, Q_1) = (N_0P, N_0Q)$, para probar que (P_0, Q_0) era fiel, solo usamos que $ord(P_0) = N_0$ no divide al grado de ninguna isogenia que aparece en k, por lo tanto no tenemos problema en dejar que N_0 tenga primos pequeños siempre que estos no dividan al grado de ninguna de las isogenias que aparecen en k, por lo

tanto tomaremos N_1 como la parte de N que contiene a los primos que aparecen en alguna isogenia de k (en lugar de contener a todos los primos menores que B) y N_0 coprimo con N_1 tal que $mcd(N_0, N_1) = 1$.

Algoritmo Red. Supone determinado el parámetro N.
Entrada: Una función $G = PLD_{E'}$ y un comodín k.
Salida: Si $(E', k) = Ran(E)$ devuelve $F = PLD_E$.

```
1. def Red(G,k):
.....................................................................................
2.    def F(P,Q):                          (#Definiendo F = PLD_E a partir de G = PLD_E')
.....................................................................................
3.       N0=N ; N1=1                                   (#Descomponiendo N = N0 · N1)
4.       for f in k[1:len(k)-1]:
5.          l=f.degree(); v=N0.valuation(l); t=l^v
6.          N0=ZZ(N0/t); N1= N1*t
.....................................................................................
7.       [P0,Q0]=[N1*P,N1*Q]          (#Descomponiendo (P,Q) en una parte fiel (P0,Q0)
8        [P1,Q1]=[N0*P,N0*Q]                    y una trivial (P1,Q1))
.....................................................................................
9.       for i in [1..len(k)-2]:              (#Translado por isogenias de (P0,Q0))
10.         phi=k[i]
11.         P0=phi(P0); Q0=phi(Q0)
12.      n0=G(P0,Q0)
.....................................................................................
13.      n1=discrete_log(Q1,P1,operation='+')  (#Resolviendo F(P1,Q1) con métodos
                                                              genéricos)
.....................................................................................
14.      (d,a,b)=xgcd(N0,N1)                  (#Recuperando el n a través del Teorema
15.      n=(n1*a*N0+n0*b*N1) %N                        del Resto Chino)
16.      return n
17.   return F
```

Código Sage del Algoritmo Red.

La segunda etapa (líneas 9-12) consiste en transladar la parte fiel (P_0, Q_0) a través de las isogenias que aparecen en el comodín k obteniendo al final un punto $(P', Q') \in E'$ (donde $E' = tr(E, k)$), aquí resolvemos $PLD_{E'}(P', Q')$ usando nuestra función G, obteniendo $n_0 = G(P', Q')$ y como (P_0, Q_0) es fiel resultará que $n_0 = PLD_E(P_0, Q_0)$.

La tercera etapa consiste en resolver $PLD_E(P_1, Q_1)$ usando métodos genéricos, en Sage tenemos la función bf discrete_log que utiliza Pohlig-Hellman y Baby-Step Giant-Step para calcular el logaritmo discreto en un grupo genérico. Observar que aquí es fundamental que $o(P_1) = N_1$ sea B-smooth, para que pueda resolverse el PLD con métodos genéricos en forma eficiente.

La cuarta y última etapa consiste en utilizar los datos $n_i = PLD_E(P_i, Q_i)$ para $i = 0, 1$ de las etapas anteriores y obtener $F(P, Q) = PLD_E(P, Q)$ utilizando el Teorema del Resto Chino.

Como ejemplo consideremos la curva elíptica $E : Y^2 = X^3 + 299X + 59$ sobre el cuerpo finito $\mathbb{F}_{331}$ (la misma que en el ejemplo para el algoritmo Ran), utilizamos los valores de $(E_2, k) = Ran(E)$, o sea, nuestra curva de llegada era $E_2 : Y^2 = X^3 + 288X + 126$ obtenidos al correr el algoritmo Ran en el ejemplo anterior. Vamos a tomar como función $G = PLD_{E_2}$ la que nos da Sage para resolver el logaritmo discreto con métodos genérico.

```
> def G(P,Q):
      return discrete_log(Q,P,operation='+')
```

Consideremos ahora los puntos $P = (223, 96)$ y $Q = (270, 21)$ en la curva E y vamos a resolver el $PLD_E(P, Q)$ usando la función G como función que resulve el PLD en la curva E_2.

```
> P=E(223,96); Q=E(270,21); PLD=Red(G,k)
> PLD(P,Q): 97
> Q==97*P: True
```

Lo mismo tomando $P = (59, 216)$ y $Q = (218, 112)$.

```
> P=E(59,216); Q=E(218,112); PLD(P,Q): 123
> Q==123*P: True
```

Claro, este algoritmo para resolver el PLD en E es ineficiente puesto que la función G utilizada para resolver el PLD en E_2 lo es. Esto fue solo a modo de ejemplo para verificar que la reducción funciona bien.

En la práctica, sería interesante si sabemos resolver el logaritmo en un subconjunto significativo S del grafo de isogenias $S_{N,q,B}(\mathcal{O})$, por ejemplo para un conjunto de cardinal $\frac{h_{\mathcal{O}}}{c}$, donde $h_{\mathcal{O}}$ es el cardinal de $S_{N,q,B}(\mathcal{O})$ y $c \in \mathbb{Z}^+$ cierta constante fija independiente de q y queremos un algoritmo para resolver el PLD en una cierta curva $E \notin S$ pero cuyo invariante pertenezca al mismo grafo $S_{N,q,B}(\mathcal{O})$. Entonces podríamos aplicar el algoritmo Ran a E reiteradas veces para obtener un comodín k que termine en alguna curva $E' \in S$ (se necesitarán en promedio unas $2c$ tiradas para tener probabilidad cercana a $\frac{1}{2}$ de que eso ocurra). Luego aplicando el algoritmo Red con el comodín k obtenido en la parte anterior, tendríamos un algoritmo eficiente para resolver el PLD en E (desde que el algoritmo para resolver el PLD en $E' \in S$ sea eficiente).

4.5. Discución de la elección de B y r_0 para nuestro ejemplo. Recordemos que del Teorema de Jao Miller Venkatesan (Teorema 2.47) deducimos que bajo la GRH[17], tomando $B = p(\log(x))$ y $r_0 = g(\log(x))$ donde $p(x) = (\log x)^{2+\delta} + C_1$ con $\delta > 0$ y $g(x) = 2x + C_2$ donde C_1 y C_2 son constantes (solo dependiente de $\delta > 0$), pero dichas constantes no eran computadas ni estimadas en forma explícita.

Para justificar que nuestra elección de parámetros $B = 20$ y $r_0 = 10$ tomados en nuestro ejemplo son buenas elecciones se debe tener al menos que paseando al azar con caminatas de largo $r_0 = 20$ en $S_{N,q,B}(\mathcal{O})$ (para nuestros parámetros $N = 312, q = 331, B = 20$ y $\mathcal{O} = \mathrm{End}(E)$ donde $E : Y^2 = X^3 + 299X + 59/\mathbb{F}_{331}$), partiendo de un vértice dado tendremos probabilidad de caer en otro vértice cualquiera dado de al menos $1/2h$ donde h

[17]Hipótesis de Riemann Generalizada.

es el número de vértices del grafo $S_{N,q,B}(\mathcal{O})$ (que por la correspondencia con el grafo de Cayley del grupo de clases de $\mathcal{O}$-ideales, resulta ser igual al número de clases del orden $\mathcal{O}$). Claramente esta condición implica conectividad del grafo $S_{N,q,B}(\mathcal{O})$.

Observemos que para este caso tenemos traza de Frobenius igual a $t = q + 1 - N = 20$ y por lo tanto:

$$d_\pi = t^2 - 4q = -924 = 4 \cdot (-231), \quad c_\pi = 2 \quad \text{y} \quad d_{\mathbb{K}} = -231$$

donde d_π y c_π son el discriminante y conductor del Frobenius respectivamente y $d_{\mathbb{K}}$ el discriminante del orden maximal $\mathcal{O}_{\mathbb{K}}$ que contiene $\mathcal{O}$. Con Sage podemos calcular el número de clases del orden maximal $\mathcal{O}_{\mathbb{K}}$,

```
> K=NumberField(E.frobenius_polynomial(),'a')
> K.class_number(): 12
```

Como $1 + \left(\frac{2}{-231}\right) = 2$ entonces podemos concluir que cada uno de esos 12 vértices que se encuentran en el orden maximal, tiene dos vecinos horizontales y como su grado es tres, cada uno de ellos tendrá exactamente un vecino horizontal (que corresponden al suborden de conductor 2, el generado por el frobenius). Recíprocamente, cada vértice del orden correspondiente al frobenius tiene un vecino ascendente que corresponde a un vértice del orden maximal, de esa forma tenemos una correspondencia biunívoca entre los vértices del orden maximal y el generado por el frobenius de modo que podemos concluir que el número de clases correspondiente al orden generado por el frobenius también tendrá cardinal $h = 12$.

Aplicando el algoritmo del Capítulo 2 Sección 2 para construir la componente conexa del grafo de 2-isogenia que contiene a $j(E) = 3$ obtenemos 6 curvas en el nivel correspondiente al orden maximal y 6 en el nivel correspondiente al suborden de conductor 2 (observar que el único caso no degenerado se obtiene con $\ell = 2$, pues es el único primo que divide al conductor del Frobenius).

Como $1 + \left(\frac{-231}{3}\right) = 1$ y $3 \nmid c_\pi$ entonces el grafo de 3-isogenia es unión de aristas disjuntas (alguna posiblemente degenerando en un lazo); utilizando el polinomio modular para $\ell = 3$ resulta que cada vértice encontrado al computar la componente conexa de $j = 3$ para el grafo de 2-isogenias, está conectado con un nuevo vértice que no se encuentra en dicha componente. De esa forma encontramos los otros 12 vértices del grafo $S_{N,q,B}$ que nos faltaban, por la biyección entre niveles, 6 corresponderán al nivel maximal y 6 al generado por el frobenius.

Los vértices de abajo corresponden al orden generado por el frobenius, mientras que los de arriba corresponden al nivel asociado al orden maximal. Como nuestro j-invariante $j = 3$ corresponde al orden $\mathcal{O}$ generado por el frobenius, estamos interesados en el grafo $S_{N,q,B}(\mathcal{O})$ cuyos vértices consiste de los j-invariantes $V = \{3, 6, 83, 165, 170, 237, 42, 210, 166, 192, 9, 201\}$.

Para facilitar notación vamos a enumerar los vértices V con elemento de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times 6\mathbb{Z}$, donde la primer coordenada indica en que componente conexa se encuentran (asignamos 0 a la componente conexa de $j = 3$ y 1 a la otra) y numeramos en cada componente los vértices en sentido horario comenzando con $j = 3$ y $j = 42$. De ese modo (denotando por

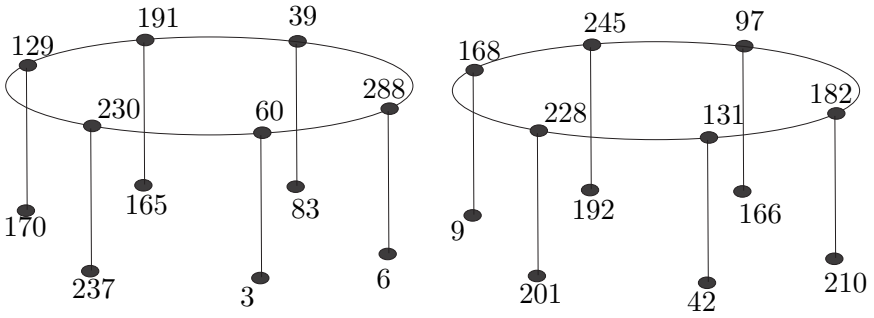


FIGURA 1. El grafo de 2-isogenias $\mathcal{G}_{312,331,2}$.

ab al par $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times 6\mathbb{Z}$) nos queda:

j-invariante:	3	6	83	165	170	237	42	210	166	192	9	201
valor asignado:	00	01	02	03	04	05	10	11	12	13	14	15

donde en la primera línea aparecen los elementos de V y en la segunda el correspondiente elemento de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times 6\mathbb{Z}$. Los grafos de ℓ-isogenia (para el orden $\mathcal{O}$) para $\ell = 3, 5, 7, 11, 13$ y 19 (como $1 + \left(\frac{17}{-231}\right) = 0$ entonces el grafo de 17-isogenias resulta un conjunto de vértices aislados) se muestran a la figura 4.5.

Observemos que la 7-isogenia entre los vértices representados por 00 y 13, conecta las dos componentes del grafo de 5-isogenias por lo que para $B \geq 7$ el grafo $S_{N=312,q=331,B}(\mathcal{O})$ ya resulta conexo, para $B = 20$ obtenemos el dibujo de la figura 4.5

Además en la figura 4.5 se ve claramente los grafos de ℓ-isogenia como grafos de Cayley, observemos que el caso de aristas disjuntos se da cuando $1+\left(\frac{-231}{\ell}\right) = 1$, o sea para $\ell = 3, 7$ y 11. Por otra parte, para que un grafo de Cayley tenga esa forma, el conjunto generador de aristas debe estar formado por un elemento no nulo g tal $2g = 0$ (usando notación aditiva), en $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ esto ocurre para $g = 03, 10$ y 13 que corresponde justamente para los casos $\ell = 11, 3$ y 7 respectivamente.

Valores de ℓ:	3	5	7	11	13	19
Generador del grafo de ℓ-isogenias como grafo de Cayley:	10	12	13	03	11	11

Volviendo a nuestro asunto de interés, que es discutir sobre nuestra elección de $(B, r_0) = (20, 10)$ para nuestro ejemplo, en principio pasa el test de conectividad (es decir, el grafo resulta conexo dado que $B > 6$), pero eso no alcanza. Debemos asegurarnos de que si seleccionamos dos vértices j y j', la probabilidad de que realizando una caminata al azar en el grafo $S_{312,331,20}(\mathcal{O})$ que comienze en j de largo $r_0 = 10$ termine en j' sea de al menos $\frac{1}{2h} = \frac{1}{24}$.

Con la ayuda de ser grafos de Cayley, es sencillo computar en Sage las matrices de adyacencia de los grafos $\mathcal{G}_{312,331,\ell}$ para $\ell = 3, 5, 7, 11, 13$ y 19; luego la suma de dichas matrices nos dá la matriz M generadora del grafo $S_{312,331,20}(\mathcal{O})$.

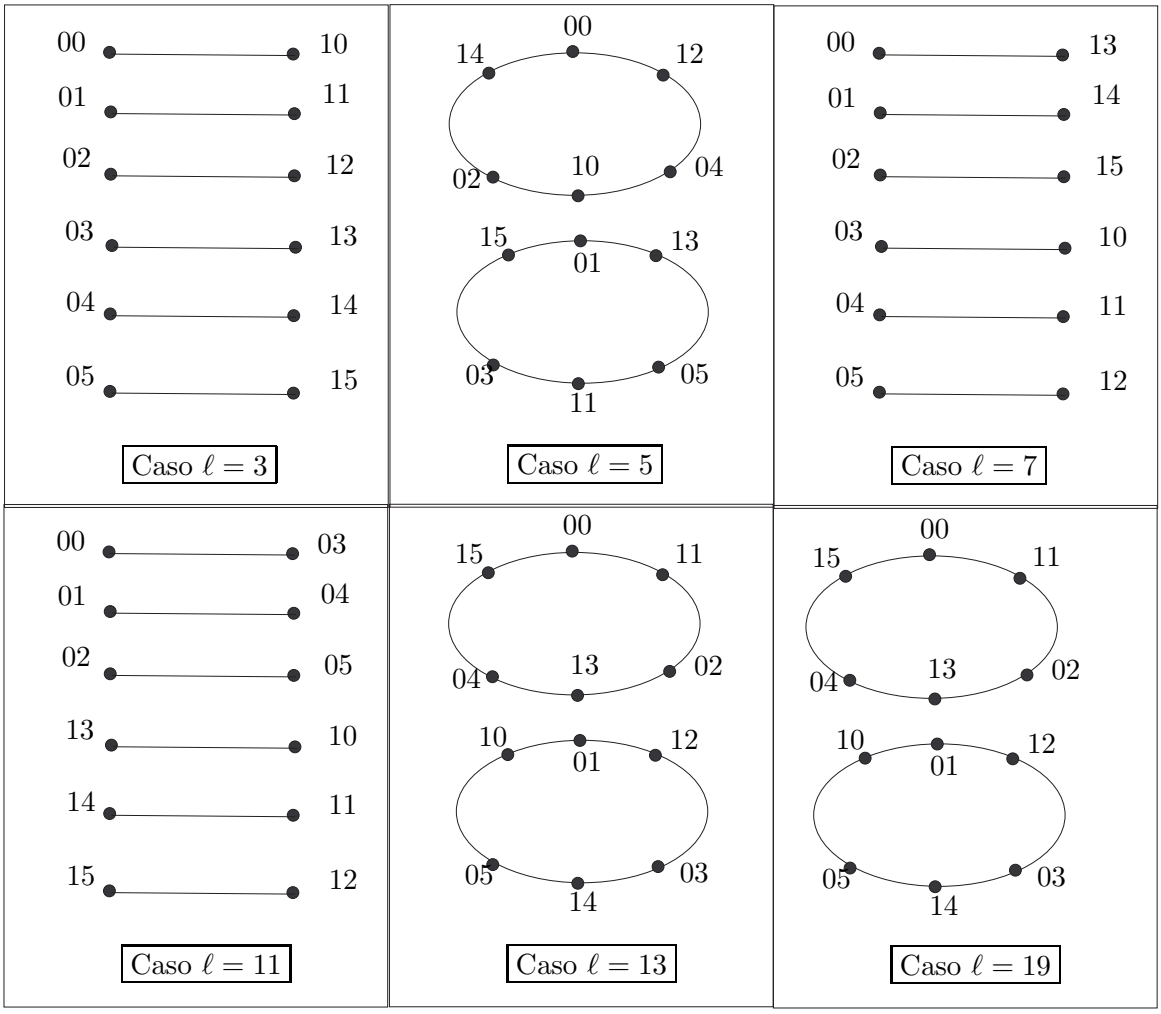


FIGURA 2. El grafo de ℓ-isogenias $\mathcal{G}_{312,331,\ell}(\mathcal{O})$ para $\ell = 3, 5, 7, 11, 13$ y 19.

Fijando j y j', recordar que la cantidad de caminos de largo $r_0 = 10$ que parten de j y llegan a j' viene dado por $M^{10}(j, j')$, como la cantidad de largo $r_0 = 10$ que hay partiendo de j es 9^{10} (pues el grado del grafo regular $S_{312,331,20}(\mathcal{O})$ viene dado por $\sum_\ell \left(\frac{-231}{\ell}\right) = 9$ donde ℓ varia en todos los primos con $3 \leq \ell < 20$). Por lo tanto la probabiliad de saliendo de j llegar a j' con un camino al azar de largo $r_0 = 10$ viene dado por

$$P(j, j') = \frac{M^{10}(j, j')}{9^{10}}.$$

Calculando ese valor en Sage tomando $j = 3$ (que corresponde al valor 00), para los distintos valores de j' obtenemos:

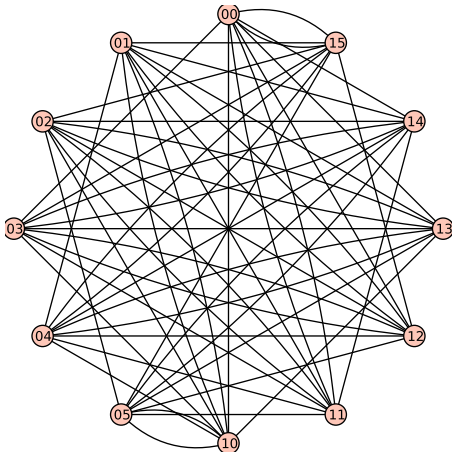


FIGURA 3. El grafo de isogenias $S_{312,331,20}(\mathcal{O})$.

Valor de j'	Probabilidad de llegar a j' partiendo de $j = 00$
00	0.0900859350265288
01	0.0900830145706505
02	0.0900857881863628
03	0.0900830145706505
04	0.0900857881863628
05	0.0900830145706505
10	0.0765835541547727
11	0.0765808295813814
12	0.0765837009949386
13	0.0765808295813814
14	0.0765837009949386
15	0.0765808295813814

Todas esas probabilidades superan ampliamente el valor mínimo aceptado que es $\frac{1}{24} = 0{,}041666\ldots$ (además están muy próximos al valor de distribución uniforme que sería cuando cada probabilidad es igual a $\frac{1}{12} = 0{,}08333\ldots$). En el gráfico de probabilidades de la figura 4.5 la línea de abajo representa el valor mínimo aceptado $\frac{1}{24}$ y la segunda línea el valor $\frac{1}{12}$ correspondiente a una distribución uniforme.

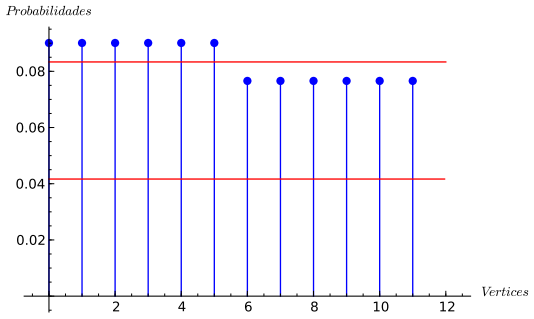


FIGURA 4. Probabilidades de caer en cada curva.

Podemos repetir esto con cada vértice j o verificar si el grafo $S_{312,331,20}(\mathcal{O})$ es vértice transitivo[18], esto se puede hacer en Sage con el comando G.is_vertex_transitive(), donde G es el grafo considerado.

```
> G= Graph(M)
> G.is_vertex_transitive(): True
```

Por lo tanto considerando diferentes vértices j, al realizar una tabla de probabilidades, los valores obtenidos resultarán ser una permutación de los obtenidos para $j = 3$, de modo que también tendremos probabildades mayor que $\frac{1}{24}$ de caer en ellos.

Por las consideraciones hecha anteriormente, podríamos concluir que $(B, r_0) = (20, 10)$ son valores aceptables para correr nuestro algoritmo para nuestro ejemplo concreto. Cabe recalcar que este análisis fue hecho con propósito puramente ilustrativo, puesto que resulta completamente inviable realizar un análisis similar para valores grandes de q, la determinación de buenos valores para B y r_0 es todavía un punto a resolver para una implementación eficiente de nuestro algoritmo para valores grandes de q.

5. Conclusión y Perspectivas.

En el artículo de Jao, Miller y Venkatesan, "Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?" [**24**], se prueba el primer resultado de autoreducibiilidad aleatoria para el problema de determinar si la complejidad del Problema del logaritmo discreto entre curvas elípticas del mismo cardinal, definidas sobre el mismo cuerpo finito son equivalentes. Este resultado puede ser interpretado de dos maneras, digamos optimista o pesimista[19]. Visto de la manera optimista sería que, si tenemos seguridad de que el logaritmo discreto es difícil de resolver para cierta curva $E/\mathbb{F}_q$, entonces podemos estar seguros que también lo será para cualquier otra curva elíptica $E'/\mathbb{F}_q$ con $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ y $\mathrm{End}(E) \simeq \mathrm{End}(E')$. Adoptando este punto de vista, este hecho puede ser aprovechado computacionalmente para intentar obtener muchas curvas elípticas buenas desde el punto de vista criptográfico a partir de alguna curva que consideremos fuerte, eso es por ejemplo lo que hacen los autores del artículo [**30**], que obtienen un método para la computación masiva de curvas buenas (a partir de ciertos parámetros q y N que se consideren seguros) analizando las componentes conexas de los grafos de ℓ-isogenia (que son llamadas de cordilleras).

La perspectiva pesimista sería sin embargo, si se lograse quebrar el problema del logaritmo discreto para un cierto conjunto de curvas elípticas definidas sobre el mismo cuerpo finito $\mathbb{F}_q$, con igual cardinal N y tipo de anillo de endomorfismo $\mathcal{O}$ (que represente una proporción significativa de dichas curvas), entonces podríamos quebrar el problema del logaritmo discreto para cualquier curva elíptica que comparta los mismos parámetros $(N, q, \mathcal{O})$. ¿Pero en este caso que podríamos hacer desde el punto de vista computacional? En este caso podría resultar conveniente crear un algoritmo que sea capaz de resolver el PLD en cualquier curva con parámetros $(N, q, \mathcal{O})$ a partir de que sabemos resolverlo en algún conjunto de curvas S con los mismos parámetros. El algoritmo Ran-Red que describimos en este capítulo nos proporciona una forma sistemática de hacerlo que sirve

[18] O sea, para cada par de vértices del grafo j_1 y j_2, existe un automorfismo del grafo que lleva j_1 a j_2.

[19] Desde el punto de vista del criptógrafo, no de la persona que desee quebrar el critosistema.

para cualquier problema de autoreducibilidad aleatoria, en el caso de curvas elípticas, el resultado de Jao Miller y Venkatesan nos asegura que (asumiendo GRH) este algoritmo funciona en forma eficiente para q es suficientemente grande.

En el desarrollo de esta tesis además se detalla, en el capítulo 1, los resultados generales sobre curvas elípticas (especialmente para las definidas sobre cuerpos finitos) que están vinculados con el algoritmo y en el capítulo 2 se brinda un resumen, mucho más específico, de herramientas y teoría viculadas con el grafo de isogenias. Se trata además el tema de la computación de polinomios modulares que son usados para nuestro algoritmo junto con referencias de los principales trabajos relacionados a la implementación de dichos polinomios (que continua siendo un área activa), con código Sage para poder computarlos.

Cuando no es demasiado extenso se brinda el código para implementar nuestros algoritmos en Sage y en otros casos se los describe y se da referencia a mi pagina personal `http://www.fing.edu.uy/~cqureshi/` para quien estuviese interesado en implementarlos.

Directamente vinculado con este trabajo quedan varias cosas para hacer, por ejemplo una estimación de los parámetros B y r_0, generalizar el resultado para curvas entre diferentes niveles o mejoras en la implementación del algoritmo. Respecto de generalizar el resultado para curvas entre diferentes niveles, los propios autores de [**24**] ya notaron que el resultado de la autoreducibilidad aleatoria se puede prescindir de la condición de estar en el mismo nivel siempre que el conductor del orden asociado al endomorfismo de frobenius no sea divisible entre un primo muy grande y experimentalmente comprobaron que eso es lo que suele suceder en la práctica, al menos con las curvas estándares más utilizadas. También puede generalizarse al caso de curvas con niveles comparables[20] o que no haya ningún primo muy grande dividiendo a alguno de los conductores, como es observado por Galbraith en [**18**].

Respecto a mejoras en la implementación podemos destacar el artículo de Galbraith [**18**] en donde propone un par de estrategias que mejoran la eficiencia del algoritmo para el cálculo de isogenias vía caminatas al azar (que se aplica directamente a nuestro algoritmo de autoreducibilidad aleatoria Ran-Red). Una de las estrategias consiste en favorecer isogenias de grado pequeño, esto implica en un aumento en el largo de la caminata (por hacer menos "aleatoria" la caminata) pero este costo extra es compensado (ampliamente) con el abaratamento en el costo de cómputo de las isogenias que forman parte del camino; esta estrategia también puede ser aplicada en la parte de la construcción del comodín, mejorando la eficiencia del algoritmo Ran-Red. La otra idea propuesta por Galbraith es utilizar una estrategia de colisión paralela, que consiste en primero utilizar un conjunto de curvas distinguidas X tal que sea fácil verificar si $E \in X$, luego utilizar $2t$ servidores (con $t \geq 1$) cada uno computando una caminata al azar hasta alcanzar una curva en X (t de los servidores comienzan en E_0 y los otros t en E_1, donde E_0 y E_1 son las curvas que deseamos hallar una isogenia), cuando uno de los servidores llega a una curva de X esa información es guardada por el servidor para encontrar una colisión (que luego es usado para construir el camino de isogenias) y el servidor reinicia nuevamente realizando una nueva caminata al azar. Esta estrategia no puede ser aplicada directamente para mejorar una parte concreta de nuestro algoritmo de autoreducibilidad Ran-Red, más bien sugiere

[20]Decimos que los niveles $\mathcal{O}$ y $\mathcal{O}'$ (órdenes en un mismo cuerpo cuadrático imaginario) son comparables si para todo primo grande ℓ tenemos que el exponente de ℓ en ambos conductores es el mismo.

una nueva implementación en donde tenga en cuenta el conjunto de curvas S (en las cuales sabemos como resolver el logaritmo discreto) y utilizando t de los servidores para realizar caminatas aleatorias partiendo de E (la curva a la cual le queremos aplicar el algoritmo Ran) y t servidores para realizar caminatas aleatorias partiendo de una curva al azar de S, seguramente esto implique una mejora significativa en el tiempo de ejecución de nuestro algoritmo (en lugar de aplicar varias veces el algoritmo $Ran(E)$ hasta caer en una curva de S).

Es importante recalcar que aunque el problema de computar una isogenia entre dos curvas elípticas y el problema de la autoreducibilidad aleatoria para el caso de curvas elípticas (en el sentido de Jao Miller y Venkatesan) son problemas intimamente relacionados (una mejora para el primero implica una mejora para el segundo), no son lo mismo. La existencia de un algoritmo de autoreducibilidad aleatoria de tiempo polinomial no implica que dadas dos curvas elípticas podamos computar una isogenia entre ellas en tiempo polinomial[21]. De hecho aún no se conoce ningún algoritmo de tiempo polinomial o subexponencial (incondicional o condicional a HRG), para resolver el problema de computar una isogenia entre dos curvas elípticas. Basados en este hecho algunos autores han propuesto criptosistemas basados en la dificultad de computar una isogenia entre dos curvas elípticas, como en [**33**] y [**38**].

Aunque son desconocidos algoritmos clásicos polinomial o subexponencial para calcular una isogenia entre dos curvas elípticas dadas, A. Childs, D. Jao y V. Soukharev han encontrado un algoritmo cuántico de tiempo subexponencial para resolver dicho problema. Desde la perpectiva cuántica sería interesante también ver si es posible obtener un algoritmo polinomial cuántico incondicional a HRG, que resuelva el problema de la autoreducibilidad aleatoria.

Vinculado con el grafo de isogenias de curvas elípticas ordinarias (también llamado grafo volcán de isogenias), ha habido mucha investigación y teoría desarrollada que ha servido para resolver varios problemas computacionales, en su mayoria relacionados con criptografía basada en curvas elípticas. Un buen artículo expositorio que resume gran parte de la teoría y recientes desarrollos es el artículo de Sutherland [**42**].

Entre esas investigaciones recientes relacionadas con el grafo volcán de isogenias, se encuentra un artículo de S. Ionica y A. Joux [**20**], en donde utilizan pairing de curvas elípticas para mejorar la computación de isogenias horizontales o ascendentes sin necesidad de calcular todas y luego verificar cuales son horizontales o ascendentes (que era lo que básicamente hacia nuestro algoritmo Vecinoshorizontales), por lo cual es muy posible que utilizando pairing podamos mejorar la eficiencia del algoritmo Ran-Red. Otro resultado es la implementación de Sutherland [**41**] de un algoritmo que determina el tipo de curva elíptica (si es ordinaria o supersingular) en tiempo $O(n^3 \log^2 n)$ que mejora el tiempo del algoritmo más eficiente conocido hasta el momento para resolver dicho problema, este algoritmo está las diferencias estructurales entre el grafo volcán de isogenias y el grafo de curvas supersingulares.

En resumen quedan aún varios problemas abiertos en torno al problema de autoreducibilidad aleatoria para curvas elípticas y en general para algoritmos basados en la

[21]Polinomial en $\log(q)$ donde $\mathbb{F}_q$ es el cuerpo finito donde ambas curvas están definidas.

estructura del grafo de isogenias que tienen directa relación con criptografia. Además existe mucha teoría desarrollada en torno a esa área y es un tema de investigación actual, lo cual lo hace un área interesante para investigación.

Apéndice A

Tipos de Extensiones y Teoría de Galois.

Cuando estudiamos curvas sobre cuerpos finitos $\mathbb{F}_q$ con $q = p^k$ (p primo), aparecen naturalmente las extensiones finitas de cuerpos infinitos de característica p (que corresponden a los cuerpos de funciones de dichas curvas) y por lo tanto es necesario comprender mejor dichas extensiones. Lo que se expone en esta sección suele verse en un curso inicial de Álgebra de licenciatura y puede encontrarse en casi cualquier libro introductorio de Teoría de Cuerpos, pero damos como referencia [**29**], Capítulo 4, de donde baso este resumen.

Todas las extensiones de cuerpos que aparecen en esta sección se asumirán finitas, salvo que se diga lo contrario.

Se observa que cuando la característica es cero, toda extensión finita es separable, lo cual es consecuencia de que si f es irreducible entonces es coprimo con f' (en característica p falla pues f' podría ser nula), asi que de aqui en mas nuestros cuerpos tienen característica positiva p.

Al comienzo del Capítulo 1 se recuerdan las definiciones de extensiones finitas separables y extensiones normales, cuando una extensión no es separable se dice que es inseparable. Hay un caso extremo de extensión inseparable, que son las extensiones puramente inseparables.

1. Extensiones puramente inseparables.

Definición A.1. Una extensión $\mathbb{K} \subset \mathbb{L}$ se dice puramente inseparable si para todo $s \in \mathbb{L}$ su polinomio irreducible sobre $\mathbb{K}$ tiene exactamente una raiz en $\overline{\mathbb{K}}$ ($\overline{\mathbb{K}}$ es una clausura algebraica de $\mathbb{K}$ que contiene a $\mathbb{L}$).

Observación A.2. Si $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$, como para todo $s \in \mathbb{L}$ se tiene que $Irr_{\mathbb{F}}(s) | Irr_{\mathbb{K}}(s)$ se tiene que si $\mathbb{K} \subset \mathbb{L}$ es puramente inseparable entonces $\mathbb{K} \subset \mathbb{F}$ y $\mathbb{F} \subset \mathbb{L}$ también lo serán.

El grado una extensión puramente inseparable debe ser necesariamente una potencia de la característica p sobre el cuerpo base, esto es consecuencia del siguiente resultado sobre polinomios irreducibles.

Proposición A.3. *Todo polinomio irreducible $f \in \mathbb{K}[x]$ se escribe como $f = q(x^{p^k})$ con $k \in \mathbb{N}$ y $q \in \mathbb{K}[x]$ un polinomio irreducible separable.*

Demostración: Tomar k máximo con esa propiedad, si $q' \equiv 0$ entonces $q(x) = r(x^k)$ con $r \in \mathbb{K}[x]$ contradiciendo la maximalidad de k, asi que q' no es el polinomio nulo asi que es coprimo con q lo cual implica la separabilidad de q.

□

Corolario A.4. *Si $\mathbb{K} \subset \mathbb{L}$ es puramente inseparable y $s \in \mathbb{L}$ entonces $Irr_{\mathbb{K}}(s) = x^{p^k} - s_0$ con $s_0 = s^{p^k} \in \mathbb{K}$ (es decir, el grado de todo elemento en una extensión puramente inseparable es potencia de la característica p).*

Demostración: Si escribimos $Irr_{\mathbb{K}}(s) = q(x^{p^k})$, como la extensión es puramente inseparable entonces $gr(q) = 1$ y por lo tanto $q = x - s_0$ con $s_0 \in \mathbb{K}$.

Corolario A.5. *Si $\mathbb{K} \subset \mathbb{L}$ es puramente inseparable entonces $[\mathbb{L} : \mathbb{K}] = q$ con $q = p^k$ para algún entero k.*

Demostración: Sea $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \ldots \subset \mathbb{K}_t = \mathbb{L}$ con $\mathbb{K}_i \subset \mathbb{K}_{i+1}$ monógena y puramente inseparable (pues $\mathbb{K} \subset \mathbb{L}$ lo es) y por lo tanto $[\mathbb{K}_{i+1} : \mathbb{K}_i] = p^{k_i}$ por corolario anterior, asi que $[\mathbb{L} : \mathbb{K}] = \Pi[\mathbb{K}_{i+1} : \mathbb{K}_i]$ también será potencia de p.

Las siguientes propiedades sobre extensiones puramente inseparables nos será de utilidad cuando estudiemos el Frobenius. Un caso especial de extensiones puramente inseparables viene dado por las extensiones $\mathbb{L}^q \subset \mathbb{L}$ donde $\mathbb{L}^q = \{s^q : s \in \mathbb{L}\}$.

Proposición A.6. *La extensión de cuerpos $\mathbb{L}^q \subset \mathbb{L}$ es puramente inseparable. En el caso de ser monógena, su grado es un divisor de q.*

Demostración: Si $s \in \mathbb{L}$ entonces es raiz del polinomio $f(x) = x^q - s^q \in \mathbb{L}^q[x]$, luego $Irr_{\mathbb{L}/\mathbb{L}^q}(s) | f(x) = (x - s)^q$ y por lo tanto el polinomio irreducible de s sobre $\mathbb{L}^q$ posee una única raiz en la clausura algebraica. Por lo visto anteriormente, el grado de todo elemento no puede superar a q y por el Corolario 2.5 debe dividir a q.

□

Observar que en general la extensión $\mathbb{L}^q \subset \mathbb{L}$ no será monógena y por lo tanto no puede concluirse a priori nada sobre el grado de dicha extensión. La siguiente proposición prueba que toda extensión (finita) puramente inseparable es una subextensión de una extensión ese tipo.

Proposición A.7. *Si $\mathbb{K} \subset \mathbb{L}$ es una extensión separable de grado q entonces $\mathbb{L}^q \subset \mathbb{K}$.*

Demostración: Si $s \in \mathbb{L}$, por lo anteriormente visto su polinomio irreducible es de la forma $x^{p^i} - s_0$ con $s_0 \in \mathbb{K}$ y $p^i = gr_{\mathbb{K}}(s) | q$, y por lo tanto $s^{p^i} = s_0 \in \mathbb{K}$ lo cual implica $s^q = s_0^{q/p^i} \in \mathbb{K}$.

□

2. Extensiones separables y clausura separable.

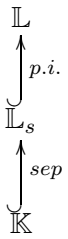
Recordemos que una extensión $\mathbb{K} \subset \mathbb{L}$ es separable si todo $s \in \mathbb{L}$ es separable sobre $\mathbb{K}$ (lo cual quiere decir que su polinomio irreducible sobre $\mathbb{K}$ no tiene raices múltiples en $\overline{\mathbb{K}}$). Las extensiones separables se comportan bien con respecto a las subextensiones en el sentido de que si tenemos una cadena de extensiones $\mathbb{K} \subset \mathbb{F} \subset \mathbb{L}$ se cumple que $\mathbb{K} \subset \mathbb{L}$ es separable si y solo si $\mathbb{K} \subset \mathbb{F}$ y $\mathbb{F} \subset \mathbb{L}$ lo son. Puede probarse además que una extensión

es separable si y solo si está generada por elementos separables (ambos resultados están probados en [**29**],Cáp.4). A partir de lo anterior se define clausura separable.

Definición A.8. Sea $\mathbb{K} \subset \mathbb{L}$ una extensión de cuerpos (algebraica y finita), definimos $\mathbb{L}_s = \mathbb{K}(\{x \in \mathbb{L} : \ x \text{ es separable sobre } \mathbb{K}\})$ como la clausura separable de $\mathbb{K}$ en $\mathbb{L}$ (a veces denotada también como $\mathbb{K}^{sep}$ en lugar de $\mathbb{L}_s$).

Observación A.9. La extensión $\mathbb{K} \subset \mathbb{K}^{sep}$ resulta separable y maximal entre las extensiones separables de $\mathbb{K}$ contenidas en $\mathbb{L}$.

Usando la propiedad de maximalidad de la clausura separable puede probarse que $\mathbb{K}^{sep} \subset \mathbb{L}$ resulta puramente inseparable de donde toda extensión finita $\mathbb{K} \subset \mathbb{L}$ puede descomponerse de la forma:



Esta descomposición jugará un papel fundamental cuando estudiemos isogenias entre curvas elípticas a traves de extensiones entre los cuerpos de funciones que estas inducen.

3. Equivalencias con el Teorema de correspondencia de Galois.

Una de las principales herramentas para estudiar extensiones separables es la Teoría de Galois. Al principio del primer capítulo se recuerda el Teorema de correspondencia de Galois para el caso finito y el caso infinito, que bajo la hipótesis de que la extensión $\mathbb{K} \subset \mathbb{L}$ sea Galois (es decir, algebraica, separable y normal) establece una biyección que invierte inclusión y preserva grados entre los cuerpos intermedios y ciertos subgrupos del grupo de Galois de la extensión.

Será útil recordar las distintas versiones equivalentes de la correspondencia, que generalmente se conoce como el Teorema principal de la Teoría de Galois.

Teorema A.10. *(Teorema principal de T.de Galois finita).* Sea $\mathbb{K} \subset \mathbb{L}$ extensión de cuerpos. Las siguientes afirmaciones son equivalentes.

1. La extensión $\mathbb{K} \subset \mathbb{L}$ es finita (y por lo tanto algebraica), separable y normal.
2. La extensión $\mathbb{K} \subset \mathbb{L}$ es finita y se cumple el Teorema de correspondencia entre los cuerpos intermedios y subgrupos de $Aut(\mathbb{L}/\mathbb{K})$.
3. $\mathbb{K} = \mathbb{L}^G$ para algún subgrupo finito G de $Aut(\mathbb{L})$.
4. La extensión $\mathbb{K} \subset \mathbb{L}$ es finita y $\#Aut(\mathbb{L}/\mathbb{K}) = [\mathbb{L} : \mathbb{K}]$.
5. $\mathbb{L}$ es el cuerpo de descomposición de un polinomio mónico separable f con coeficientes en $\mathbb{K}$.

Para el caso infinito (sobretodo nos interesa el grupo de Galois absoluto) tenemos la siguiente versión.

Teorema A.11. *(Teorema principal de T.de Galois infinita).* Sea $\mathbb{K} \subset \mathbb{L}$ extensión de cuerpos. Las siguientes afirmaciones son equivalentes.

1. La extensión $\mathbb{K} \subset \mathbb{L}$ es algebraica, separable y normal.
2. La extensión $\mathbb{K} \subset \mathbb{L}$ es algebraica y se cumple el Teorema de correspondencia entre los cuerpos intermedios y subgrupos cerrados de $Aut(\mathbb{L}/\mathbb{K})$.
3. $\mathbb{K} = \mathbb{L}^G$ para algún subgrupo compacto G de $Aut(\mathbb{L})$.
4. $\mathbb{L}$ es la unión de todos sus subcuerpos $\mathbb{E}$ que son Galois finitos sobre $\mathbb{K}$.
5. $\mathbb{L}$ es el cuerpo de descomposición de una familia de polinomios mónicos separables con coeficientes en $\mathbb{K}$.

Se recuerda que la topología en $Aut(\mathbb{L})$ es la inducida por la topología producto en $\Pi_{x \in \overline{K}} \overline{K}$, cada factor con la topología discreta.

Apéndice B

Enteros $\ell-$ádicos.

Recordar que los enteros ℓ-adicos están definido como el límite inverso de los $\mathbb{Z}/\ell\mathbb{Z}$:

$$\mathbb{Z}_\ell = \varprojlim \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$$

Por lo tanto un elemento $\lambda \in \mathbb{Z}_\ell$ puede verse como una sucesión $\lambda = (\lambda_1, \lambda_2, \ldots)$ donde $\lambda_i \in \mathbb{Z}/\ell^i\mathbb{Z}$ y $\lambda_{i+1} \equiv \lambda_i \pmod{\ell^i}$. Con la suma y producto miembro a miembro $\mathbb{Z}_\ell$ tiene estructura de anillo con neutro multiplicativo $\mathbf{1} = (1, 1, 1, \ldots)$.

Los enteros pueden verse dentro de $\mathbb{Z}_\ell$ en forma fiel bajo la correspondencia:

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_\ell \qquad \text{dada por} \qquad n \mapsto n \cdot \mathbf{1} = (n, n, n, \ldots)$$

Esta correspondencia preserva la estructura de anillo.

La valuación $\ell-$adica de los enteros puede extenderse a los enteros $\ell-$adicos de la forma obvia:

$$\nu_\ell(\lambda) = k - 1 \qquad \text{donde } k \text{ es el índice de la menor coordenada no nula de } \lambda$$

Para $\lambda = 0$ definimos $\nu_\ell(\lambda) = +\infty$ como en los enteros. Es claro que para valores enteros coincide con la valuación $\ell-$ádica usual.

Observación B.1. Todo entero $\ell-$ádico $\lambda \neq 0$ se escribe de forma única como $\lambda = \ell^n\lambda'$ con $\nu_\ell(\lambda') = 0$, $n = \nu_\ell(\lambda)$.

Demostración: Sea $\nu_\ell(\lambda) = n$ asi que $\lambda_n \equiv 0 \pmod{\ell^n}$ luego para todo $i \geq 1$ tenemos que $\lambda_{n+i} \equiv \lambda_n \equiv 0 \pmod{\ell^n}$ asi que $\lambda_{n+i} \equiv \lambda_i'\ell^n \pmod{\ell^{n+i}}$ (observemos que λ_i' está determinado unívocamente módulo ℓ^i). Veamos que ese $\lambda' = (\lambda_1', \lambda_2', \ldots)$ funciona, en efecto, para $1 \leq i \leq n$ se cumple que $\ell^n\lambda_i' \equiv 0 \pmod{\ell^i}$ y como $\lambda_i \equiv 0 \pmod{\ell^i}$ para $1 \leq i \leq n = \nu_\ell(\lambda)$ se cumple que $\lambda_i \equiv \ell^n\lambda_i'$. Para $i > n$ tenemos que $\ell^n\lambda_i' \equiv \lambda_{n+i} \pmod{\ell^{n+i}} \Rightarrow \ell^n\lambda_i' \equiv \lambda_{n+i} \pmod{\ell^i}$ y $\lambda_{n+i} \equiv \lambda_i \pmod{\ell^i}$ asi que $\ell^n\lambda_i' \equiv \lambda_i \pmod{\ell^i}$. Juntando ambas cosas tenemos que $\lambda = \ell^n\lambda'$ además como $\lambda_1'\ell^n \equiv \lambda_{n+1} \not\equiv 0 \pmod{\ell^{n+1}}$ se tiene que $\lambda_1' \not\equiv 0 \pmod{\ell}$ y por lo tanto $\nu_\ell(\lambda') = 0$.

□

Proposición B.2. *Si $\lambda, \mu \in \mathbb{Z}_\ell$ entonces $\nu_\ell(\lambda\mu) = \nu_\ell(\lambda)\nu_\ell(\mu)$.*

Demostración: Para el caso en que ambos tengan valuación $\ell-$ádica nula es directo, pues $\lambda_1 \not\equiv 0 \pmod{\ell}$ y $\mu_1 \not\equiv 0 \pmod{\ell}$ implica $\lambda_1\mu_1 \not\equiv 0 \pmod{\ell}$ pues ℓ es primo, asi que $\lambda\mu$ también tendrá valuación $\ell-$ádica nula. Supongamos que $\nu_\ell(\lambda) = n$ y $\nu_\ell(\mu) = m$ entonces por la observaciń previa podemos escribir $\lambda = \ell^n\lambda'$ y $\mu = \ell^m\mu'$ con $\nu_\ell(\lambda') = \nu_\ell(\mu') = 0$. Luego $\lambda\mu = \ell^{n+m}\lambda'\mu'$ con $\nu_\ell(\lambda'\mu') = 0$ (pues $\nu_\ell(\lambda') = \nu_\ell(\mu') = 0$), claramente esto implica $\nu_\ell(\lambda\mu) \geq n + m$, veamos que da igual, en efecto, $\lambda_{n+m+1} \equiv \lambda_n \equiv 0 \pmod{\ell^n}$

y $\lambda_{n+m+1} \equiv \lambda_{n+1} \not\equiv 0 \pmod{\ell^{n+1}}$ entonces $\lambda_{n+m+1} \equiv a\ell^n \pmod{\ell^{n+m+1}}$ con $a \neq \dot{\ell}$ y de forma similar $\mu_{n+m+1} \equiv b\ell^m \pmod{\lambda^{n+m+1}}$ asi que $\lambda_{n+m+1}\mu_{n+m+1} \equiv ab\ell^{n+m} \not\equiv 0 \pmod{\ell^{n+m+1}}$ puesto que $\ell \not| ab$ como queríamos probar.

□

Teorema B.3. *$\mathbb{Z}_\ell$ es un $\mathbb{Z}-$módulo libre de rango infinito.*

Demostración: Sea $\lambda \in \mathbb{Z}_\ell$ y $n \in \mathbb{Z}^+$ ninguno de ellos nulos entonces $\nu_\ell(\lambda) < \infty$ y $\nu_\ell(n) < \infty$ por lo tanto $\nu_\ell(n\lambda) = \nu_\ell(n) + \nu_\ell(\lambda) < \infty$ y por lo tanto $n\lambda \neq 0$.

Si fuese de rango finito n entonces $\mathbb{Z}_\ell \cong \mathbb{Z}^n$ como $\mathbb{Z}-$módulo, en particular la existencia de esa biyección implica

$$\aleph_0 = \#\mathbb{Z} = \#\mathbb{Z}^n = \#\mathbb{Z}_\ell = \#\mathbb{R} = \aleph_1$$

lo cual es absurdo (para la penúltima igualdad se usa que las sucesiones infinitas formadas por $1, \ldots, \ell$ están en biyección con los reales).

□

Teorema B.4. *Los elementos invertibles de $\mathbb{Z}_\ell$ son los de valuación $\ell-$ádica nula (en particular un entero es invertible si y solo si no es múltiplo de ℓ).*

Demostración: Como $\nu_\ell(\mathbf{1}) = 0$ y $\nu_\ell(x) \in \mathbb{N} \cup \{\infty\}$ $\forall x \in \mathbb{Z}_\ell$, para que $\lambda\mu = \mathbf{1}$ es necesario que ambos $\nu_\ell(\lambda) = \nu_\ell(\mu) = 0$ (pues $\nu_\ell(\lambda) + \nu_\ell(\mu) = \nu_\ell(\mathbf{1}) = 0$). Recíprocamente, si λ tiene valuación $\ell-$ádica nula entonces λ_1 no es múltplo de ℓ asi que para todo $n \geq 1$ tampoco λ_n puede ser múltiplo de ℓ pues $\lambda_n \equiv \lambda_1 \pmod{\ell}$. Para cada $n \geq 1$ sea $\mu_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ tal que $\mu_n\ell_n \equiv 1 \pmod{\ell^n}$, como $\mu_n\lambda_n \equiv 1 \equiv \mu_{n+1}\lambda_{n+1} \equiv \mu_{n+1}\lambda_n \pmod{\ell^n}$ entonces $\mu_{n+1} \equiv \mu_n \pmod{\ell^n}$ asi que $\mu \in \mathbb{Z}_\ell$ y claramente $\lambda\mu = \mathbf{1}$.

□

Apéndice C

Producto tensorial.

Sean R y S dos A-módulos, los elementos de $R \otimes_A S$ son sumas finitas de la forma $\sum_i r_i \otimes s_i$ donde los $r_i \in R, s_i \in S$. La igualdad $r \otimes s = r' \otimes s'$ no implica que $r = r'$ y $s = s'$, está construido para que se cumpla $(r_1 + r_2) \otimes s = r_1 \otimes s + r_2 \otimes s$, $r \otimes (s_1 + s_2) = r \otimes s_1 + r \otimes s_2$ y $ar \otimes s = r \otimes as$. Esta última propiedad permite definir en $R \otimes S$ una estructura de $A-$módulo, por supuesto la acción viene dada por $a \cdot (r \otimes s) = (ar) \otimes s = r \otimes (as)$. El producto tensorial está caracterizado por la siguiente propiedad:

Propiedad universal del producto tensorial. Toda forma bilineal $f : R \times S \to L$ (donde $L \in A-$mód) balanceada (o sea que $f(r, as) = f(ra, s)\ \forall a \in A$) se extiende a un morfismo de $A-$módulos:

$$\widehat{f} : R \otimes S \to L \quad / \quad \widehat{f}\left(\sum_i r_i \otimes s_i\right) = \sum_i f(r_i, s_i)$$

En el caso que S sea además un anillo (es decir, que S sea una $A-$álgebra), el $A-$módulo $R \otimes S$ gana estructura de $S-$módulo definiendo la acción por $s' \cdot \sum_i r_i \otimes s_i = \sum_i r_i \otimes s_i s'$. Esta acción está bien definida, para verlo basta considerar la función $f : R \times S \to R \otimes S$, $(r, s) \to r \otimes ss'$ la cual es fácil chequear que es bilineal equilibrada y por lo tanto define una función en $R \otimes S$ dada por $\widehat{f}(\sum_i r_i \otimes s_i) = \sum_i r_i \otimes s_i s'$.

Como veremos a continuación, bajo ciertas condiciones, R puede identificarse como un A-submódulo de $R \otimes S$ bajo la correspondencia $r \mapsto r \otimes 1$.

Proposición C.1 (Inmersión en el producto tensorial)**.** *Sean R y S $A-$módulos con R finitamente generado y libre de torsión sobre A (i.e. $a \neq 0$ y $ax = 0$ entonces $x = 0$ para $x \in R$), con A dip entonces $R \to R \otimes S$ dada por $r \mapsto r \otimes 1$ es un morfismo inyectivo de $A-$módulos.*

Demostración: Por teorema de estructura de módulos sobre dips, si R es un $A-$módulo finitamente generado y libre de torsión entonces $R \cong A^n$ como $A-$módulo. Es decir, existen $r_1, r_2, \ldots, r_n \in R$ tales que $R = Ar_1 \oplus Ar_2 \oplus \ldots \oplus Ar_n$ y consideremos π_i la proyección $i-$ésima (es decir $\pi_i : R \to A$ es tal que $\pi_i(\sum_j a_j r_j) = a_i$ para $i = 1, 2, \ldots, n$).

Claramente $r \mapsto r \otimes 1$ define un morfismo de $A-$módulos, para probar que es inyectiva alcanza ver que tiene kernel trivial. Sea $x \in R$ tal que $x \otimes 1 = 0$, queremos probar que $x = 0$ o equivalentemente que $\pi_i(x) = 0$ para $i = 1, 2, \ldots, n$.

Sea i fijo, $1 \leq i \leq n$ y consideremos el mapa $R \times S \to S$ dado por $(r, s) \mapsto \pi_i(r)s$ que es claramente bilineal y balanceada y por tanto define un morfismo de $A-$módulos

$f_i : R \otimes S \to S$ definido por $f_i(r \otimes s) = \pi_i(r)s$. Pero entonces $\pi_i(x) = f_i(x \otimes 1) = f_i(0) = 0$ para todo $i = 1, 2 \ldots, n$ y por lo tanto $x = 0$.

□

Hay un caso particular de producto tensorial donde las cosas se vuelven mas fáciles que es cuando A es un dip y S su cuerpo de fracciones (por ejemplo $A = \mathbb{Z}$ y $S = \mathbb{Q}$):

Proposición C.2. *Si R es un $A-$módulo con A dominio de integridad y S el cuerpo de fracciones de A entonces todo elemento de $R \otimes S$ es de la forma $r \otimes s$ con $r \in R$ y $s \in S$.*

Demostración: Sea $x = \sum_i^n r_i \otimes s_i$ y consideremos $a \in A, a \neq 0$ tal que $b_i = as_i \in A$ para todo $i = 1, 2, \ldots, n$ (por ejemplo tomando a el producto de los denominadores de los s_i), se tiene que:

$$x = \sum_i^n (r_i \otimes s_i) = \sum_i^n \left(r_i \otimes \frac{b_i}{a} \right) = \sum_i^n \left(b_i r_i \otimes \frac{1}{a} \right) = \left(\sum_i^n b_i r_i \right) \otimes \frac{1}{a}$$

Tomando $r = \sum_i^n b_i r_i$ y $q = 1/a$ se cumple que $x = r \otimes q$.

□

Los siguientes resultados son sobre la conservación de generadores y conjuntos l.i. cuando se toma tensores.

Proposición C.3 (Conservación de generadores.)**.** *Sea S una $A-$álgebra y M es un $A-$módulo, supongamos que $\{m_1, m_2, \ldots, m_n\} \subset M$ sea un generador de M (como $\mathbb{Z}-$módulo) entonces $\{m_1 \otimes 1, m_2 \otimes 1, \ldots, m_n \otimes 1\} \subset M \otimes S$ será un generador de $M \otimes S$ como $S-$módulo.*

Demostración: Sea $x = \sum_{i=1}^t x_i \otimes s_i \in M \otimes S$ con $x_i \in M$ y $s_i \in S$ para $i = 1, 2, \ldots, t$. Como $x_i \in M$ entonces $x_i = \sum_{j=1}^n a_{ij} m_j$ con $a_{ij} \in A$, y por lo tanto:

$$x = \sum_{i=1}^t x_i \otimes s_i = \sum_{i=1}^t \sum_{j=1}^n a_{ij} m_j \otimes s_i = \sum_{j=1}^n (\sum_{i=1}^t a_{ij} s_i)(m_j \otimes 1)$$

como queríamos probar.

Proposición C.4 (Conservación de independencia.)**.** *Sea S una $A-$álgebra y M un $A-$módulo y $m_1, m_2, \ldots, m_t$ un conjunto l.i sobre A (es decir que si $\sum_{i=1}^t a_i m_i = 0$ con $a_i \in A$, $\forall i$ entonces $a_i = 0$ $\forall i$) entonces $m_1 \otimes 1, m_2 \otimes 1, \ldots, m_t \otimes 1 \in M \otimes S$ es un conjunto l.i sobre S.*

Demostración: Consideremos $M' = m_1 A + m_2 A + \ldots + m_t A$ por la independencia $\{m_1, m_2, \ldots, m_t\}$ es una $A-$base de M' y por lo tanto tenemos definidas las proyecciones $\pi_i : M' \to A$ para $1 \leq i \leq t$ dadas por $\pi_i(\sum_j a_j m_j) = a_i$ donde los $a_j \in A$.

Supongamos que $\sum_{j=1}^t \lambda_i (m_i \otimes 1) = \sum_{j=1}^t (m_i \otimes \lambda_i) = 0$ con $\lambda_1, \lambda_2, \ldots, \lambda_t \in S$ queremos probar que $\lambda_j = 0$ para todo j. Para cada i las funciones $f_i : M' \times S \to S$ dada por $x \otimes \lambda \mapsto \pi_i(x)\lambda$ son claramente bilineales balanceadas y por lo tanto definen en el producto

tensorial morfismos de $A-$módulos $f_i : M' \otimes S \to S$ tales que $f_i(m \otimes \lambda) = \pi_i(m)\lambda$ en particular tenemos que:

$$0 = f\left(\sum_{j=1}^{t}(m_i \otimes \lambda_i)\right) = \sum_{j=1}^{t} f(m_j \otimes \lambda_j) = \sum_{j=1}^{t}\pi_i(m_j)\lambda_j = \lambda_i \quad \text{para } i = 1, 2, \ldots, t$$

como queriamos probar.

□

Corolario C.5. *En particular esto prueba que $rango_A(M) \leq rango_S(M \otimes S)$ (donde el rango se define como el máximo cardinal de un conjunto l.i. sobre los escalares considerados).*

Corolario C.6. *Si $M = m_1A \oplus m_2A \oplus \ldots \oplus m_tA$ entonces $M \otimes S = m_1'S \oplus m_2'S \oplus \ldots \oplus m_t'S$ donde $m_i' = m_i \otimes 1$.*

Observación C.7. Hay que tener cuidados especiales a veces cuando se identifica M con el conjunto $\{m \otimes 1 : m \in M\} \subset M \otimes S$. Por ejemplo consideremos $M \in \mathbb{Z}-$Mod, dado por $M = \sqrt{2}\mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$ y tomemos $S = \mathbb{R}$ tenemos que $M \otimes \mathbb{R} = (\sqrt{2} \otimes 1)\mathbb{R} \oplus (\sqrt{3} \otimes 1)\mathbb{R}$, bajo la identificación descrita arriba tenemos que $\sqrt{3}\sqrt{2} - \sqrt{2}\sqrt{3} \neq 0$ (la cual debe entenderse como $\sqrt{3}(\sqrt{2} \otimes 1) - \sqrt{2}(\sqrt{3} \otimes 1) \neq 0$) dado que $\sqrt{2} \otimes 1$ y $\sqrt{3} \otimes 1$ son l.i sobre $\mathbb{R}$. Por eso algunas veces cuando pueda causar confunsión, no usaremos dicha identificación.

Para terminar, veremos que en ciertos casos alcanza la invertibilidad de los enteros no nulos para conseguir el cuerpo de fracciones.

Proposición C.8. *Sea R un dominio conmutativo, con una involución $\alpha \mapsto \widehat{\alpha}$ que verifica $\alpha\widehat{\alpha} \in \mathbb{Z}^+$ $\forall \alpha \in R, \alpha \neq 0$ entonces $R \otimes \mathbb{Q} \cong R_f$, el cuerpo de fracciones de R (el producto en $R \otimes \mathbb{Q}$ queda definido por $(r_1 \otimes q_1)(r_2 \otimes q_2) = r_1r_2 \otimes q_1q_2$.*

Demostración: Observemos que en $R_f \otimes \mathbb{Q}$ se cumple que:

$$\frac{r_1}{r_2} \otimes 1 = \frac{r_1}{r_2} \otimes \frac{r_2\widehat{r_2}}{r_2\widehat{r_2}} = r_1\widehat{r_2} \otimes \frac{1}{r_2\widehat{r_2}}$$

para todo $r_1, r_2 \in R$ con $r_2 \neq 0$. En función de lo anterior parece natural definir el mapa φ de la siguiente manera:

$$\varphi : R_f \to R \otimes \mathbb{Q} \quad / \quad \frac{r_1}{r_2} \mapsto r_1\widehat{r_2} \otimes \frac{1}{r_2\widehat{r_2}}$$

Veamos que está bien definida, si $r_1, r_2, r \in R$ con $r_2 \neq 0, r \neq 0$ entonces:

$$\varphi\left(\frac{rr_1}{rr_2}\right) = rr_1\widehat{rr_2} \otimes \frac{1}{rr_2\widehat{rr_2}} = r\widehat{r}r_1\widehat{r_2} \otimes \frac{1}{r_2\widehat{r_2}r\widehat{r}} = r_1\widehat{r_2} \otimes \frac{1}{r_2\widehat{r_2}} = \varphi\left(\frac{r_1}{r_2}\right)$$

Veamos que respeta la suma:

$$\varphi\left(\frac{r_1}{r_2} + \frac{s_1}{s_2}\right) = \varphi\left(\frac{r_1s_2 + r_2s_1}{r_2s_2}\right) = (r_1s_2 + s_1r_2)\widehat{r_2s_2} \otimes \frac{1}{r_2s_2\widehat{r_2s_2}} = r_1\widehat{r_2}s_2\widehat{s_2} \otimes \frac{1}{r_2\widehat{r_2}s_2\widehat{s_2}} + s_1\widehat{s_2}r_2\widehat{r_2} \otimes \frac{1}{r_2\widehat{r_2}s_2\widehat{s_2}}$$

$$= \varphi\left(\frac{r_1}{r_2}\right) + \varphi\left(\frac{s_1}{s_2}\right)$$

Con respecto al producto se tiene:

$$\varphi\left(\frac{r_1}{r_2}\cdot\frac{s_1}{s_2}\right)=r_1s_1\widehat{r_2}\widehat{s_2}\otimes\frac{1}{r_2s_2\widehat{r_2}\widehat{s_2}}=\left(r_1\widehat{r_2}\otimes\frac{1}{r_2\widehat{r_2}}\right)\cdot\left(s_1\widehat{s_2}\otimes\frac{1}{s_2\widehat{s_2}}\right)=\varphi\left(\frac{r_1}{r_2}\right)\varphi\left(\frac{s_1}{s_2}\right)$$

Por lo tanto φ resulta un morfismo de anillos entre R_f y $R\otimes\mathbb{Q}$, para probar que es un isomorfismo basta construir su función inversa, consideremos la siguiente función:

$$\psi : R\otimes\mathbb{Q}\to R_f \quad / \quad r\otimes q\mapsto qr$$

Está bien definida dado que el mapa $(r,q)\mapsto qr$ es claramente bilineal y equilibrada, falta chequear que es la inversa de φ. Sea $x\in R\otimes\mathbb{Q}$ pongamos $x=\sum_i r_i\otimes q_i$ donde $q_i=m_i/n_i$ con $m_i,n_i\in\mathbb{Z}$, $n_i\neq 0$, se tiene que:

$$\begin{aligned}\varphi\circ\psi(x)&=\varphi\left(\sum_i r_iq_i\right)=\sum_i\varphi\left(\frac{r_im_i}{n_i}\right)=\sum_i r_im_i\widehat{n_i}\otimes\frac{1}{n_i\widehat{n_i}}\\&=\sum_i r_i\otimes\frac{m_in_i}{n_in_i}=\sum_i r_i\otimes\frac{m_i}{n_i}=\sum_i r_i\otimes q_i=x\end{aligned}$$

donde se usó que $\widehat{n}=n$ si $n\in\mathbb{Z}$ (pues $\alpha\mapsto\widehat{\alpha}$ es una involución).

Recíprocamente, si $y\in R_f$ entonces $y=r_1/r_2$ con $r_1,r_2\in R$ y $r_2\neq 0$, se tiene:

$$\psi\circ\varphi(y)=\psi\left(r_1\widehat{r_2}\otimes\frac{1}{r_2\widehat{r_2}}\right)=r_1\widehat{r_2}\cdot\frac{1}{r_2\widehat{r_2}}=y$$

por lo tanto $\varphi : R_f\to R\otimes\mathbb{Q}$ establece un isomorfismo de cuerpos.

□

Apéndice D

Módulos cuadráticos.

Definición D.1. Sea A un subanillo de $\mathbb{R}$ y M un $A-$módulo, una forma cuadrática en M es una función $q : M \to A$ que verifica las siguientes dos propiedades:

i) $q(x) = q(-x)$ para todo $x \in M$.
ii) La función $\langle x, y\rangle = q(x + y) - q(x) - q(y)$ es una forma bilineal.

Si además verifica la condición de positividad:

iii) $q(x) \geq 0$ con igualdad si y solo si $x = 0$.

Entonces decimos que la forma cuadrática q es definida positiva.

Es para nosotros de particular interés el caso en que M sea un grupo (i.e. un $\mathbb{Z}-$módulo).

Definición D.2. Un A-módulo cuadrático es una pareja (M, q) donde M es un $A-$módulo y q una forma cuadrática en M (para el caso $A = \mathbb{Z}$ lo llamaremos grupo cuadrático).

Comenzemos viendo que propiedades de las formas cuadráticas se siguen conservando para formas cuadráticas sobre módulos.

Proposición D.3. *Si q es una forma cuadrática en M entonces $q(0) = 0$.*

Demostración: Por ii) tenemos que $0 = \langle 0, 0\rangle = q(0) - 2q(0) = -q(0) \Rightarrow q(0) = 0$.

□

Proposición D.4. *Si q es una forma cuadrática en M entonces $q(\lambda x) = \lambda^2 q(x)$ para todo $\lambda \in A, x \in M$.*

Demostración: Observemos primero que se cumple para $a = 2$, en efecto, por un lado $\langle x, -x\rangle = q(0)-q(x)-q(-x) = -2q(x)$ y por otro lado $\langle x, -x\rangle = -\langle x, x\rangle = -q(2x)+2q(x)$ asi que igualando tenemos que $-2q(x) = -q(2x) + 2q(x) \Rightarrow q(2x) = 4q(x)$.

Observemos ahora que $\langle x, x\rangle = q(2x) - 2q(x) = 2q(x)$ asi que $2q(\lambda x) = \langle \lambda x, \lambda x\rangle = \lambda^2\langle x, x\rangle = \lambda^2 \cdot 2q(x)$, cancelando los 2 de ambos lados tenemos lo que queríamos.

□

Teorema D.5. *[Desigualdad de Cauchy-Schwarz] Si q es una forma cuadrática en M definida positiva entonces para todo $\alpha, \beta \in M$ se tiene que:*

$$|\langle \alpha, \beta\rangle| \leq 2\sqrt{q(\alpha)}\sqrt{q(\beta)}$$

dándose la igualdad si y solo si α y β son colineales (i.e. $\exists a, b \in A$ no ambos nulos tales que $a\alpha + b\beta = 0$).

Demostración: Es simplemente adaptar la prueba clásica de Cauchy-Schwarz, observemos que $\mathbb{Z} \subset A$ por ser A un anillo contenido en $\mathbb{R}$. Observemos que si $\alpha = 0$ se da el igual, asi que podemos suponer que $\alpha, \beta \in M$ con $\alpha \neq 0$. Sea $r = n/m \in \mathbb{Q}$ con $n \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$, por la positividad:

$$0 \leq q(n\alpha + m\beta) = \langle n\alpha, m\beta\rangle + q(n\alpha) + q(m\beta) = nm\langle\alpha, \beta\rangle + n^2 q(\alpha) + m^2 q(\beta)$$

dividiendo de ambos lados de la desigualdad por m^2 nos queda que:

$$0 \leq r\langle\alpha, \beta\rangle + r^2 q(\alpha) + q(\beta)$$

por lo tanto el polinomio (con coeficientes reales) $f(x) = q(\alpha)x^2 + \langle\alpha, \beta\rangle x + q(\beta)$ que cumple $f(x) \geq 0\ \forall x \in \mathbb{Q}$ cumplirá también $f(x) \geq 0\ \forall x \in \mathbb{R}$ (por continuidad) asi que su discriminante $\Delta = \langle\alpha, \beta\rangle^2 - 4q(\alpha)q(\beta) \leq 0 \Rightarrow \langle\alpha, \beta\rangle^2 \leq 4q(\alpha)q(\beta) \Rightarrow |\langle\alpha, \beta\rangle| \leq 2\sqrt{q(\alpha)}\sqrt{q(\beta)}$ que es la primer parte del teorema.

Para terminar observemos que la igualdad se da si y solo si $\Delta = 0 \Leftrightarrow \exists x \in \mathbb{R}/f(x) = 0$ observemos que los coeficientes de f están en A asi que si tiene raiz doble x esta debe estar en el cuerpo de fracciones de A (de hecho $x = -\frac{\langle\alpha,\beta\rangle}{q(\alpha)}$) asi que lo anterior es equivalente a que existan $n, m \in A$ tales que $f(n/m) = 0 \Leftrightarrow q(\alpha n + \beta m) = 0 \Leftrightarrow \alpha n + \beta m = 0$ culminando la prueba.

□

Observemos que para el caso q definida positiva, podemos definir como es usual $||x|| = \sqrt{\langle x, x\rangle} = \sqrt{2q(x)}$ y con esta notación la desigualdad de Cauchy-Schwarz quedaría $|\langle\alpha, \beta\rangle| \leq ||\alpha|| \cdot ||\beta||$, similar a la versión clásica para espacios vectoriales (o sea cuando el anillo A es un cuerpo).

A continuación veremos un teorema de extensión de formas cuadráticas al ampliar los escalares.

Al igual que antes tenemos un $A-$módulo cuadrático (M, q) donde A es un subanillo de $\mathbb{R}$, supongamos además que M es libre de torsión sobre A (es decir, si $am = 0$ con $a \neq 0$ entonces $m = 0$) entonces tenemos la inclusión $M \hookrightarrow M \otimes_A \mathbb{R}$ dada por supuesto por $m \mapsto m \otimes 1$. Queremos extender el A-módulo cuadrático (M, q) a un $\mathbb{R}-$módulo cuadrático $(M \otimes_A \mathbb{R}, \widehat{q})$ de forma que $\widehat{q}(x) = q(x)$ para todo $x \in M$, veremos además que si q es definida positiva entonces también lo será $\widehat{q}$.

Teorema D.6 (Extensión de módulos cuadráticos)**.** *Sea $A \subset \mathbb{R}$ un subanillo y $M \in A-$mód.*

i) *Si (M, q) es un $A-$módulo cuadrático entonces existe un $\mathbb{R}$-módulo cuadrático $(M \otimes_A \mathbb{R}, \widehat{q})$ tal que $\widehat{q}|_M = q$.*
ii) *Si q es definida positiva y M es libre y finitamente generado (como A-módulo), con A dip, entonces $\widehat{q}$ es semidefinida positiva. Si la matriz asociada a q en cualquier $A-$base de M tiene determinante no nulo entonces $\widehat{q}$ es definida positiva.*

Demostración: i) La clave es extender primero la forma bilineal inducida por q dada por $\langle x, y\rangle = q(x+y) - q(x) - q(y)$. Para cada y fijo consideremos $\varphi_y(x) = \langle x, y\rangle$ es A-lineal

y claramente la función $M \times \mathbb{R} \to \mathbb{R}$ dada por $(x, \lambda) \mapsto \varphi_y(x)\lambda$ es $A-$bilineal y balanceada por lo tanto define una función A-lineal en $M \otimes_A \mathbb{R}$ dada por:

$$T_y : M \otimes_A \mathbb{R} \to \mathbb{R}$$

$$x \otimes \lambda \mapsto \varphi_y(x)\lambda$$

Consideremos ahora un $\omega = \sum_i m_i \otimes \lambda_i \in M \otimes_A \mathbb{R}$ fijo y consideremos la función $M \times \mathbb{R} \to \mathbb{R}$ dada por $(y, \lambda) \mapsto T_y(\omega)\lambda = \sum_i \varphi_y(m_i)\lambda_i\lambda = \sum_i \langle m_i, y\rangle \lambda_i \lambda$ es claramente $A-$lineal con respecto a la segunda variable pero también con respecto a la primer variable (usar la linealidad respecto de la segunda variable de la forma bilineal inducida por q) y balanceada (tambien por lo mismo). De esa forma tenemos inducida una función $A-lineal$ en $M \otimes_A \mathbb{R}$ dada por:

$$S_\omega : M \otimes_A \mathbb{R} \to \mathbb{R}$$

$$y \otimes \lambda \mapsto T_y(\omega)\lambda = \sum_i \langle m_i, y\rangle \lambda_i \lambda$$

Finalmente definimos la forma bilineal en $M \otimes \mathbb{R}$:

$$\langle \omega, \omega' \rangle_2 = S_\omega(\omega')$$

Es decir, si $\omega = \sum_i m_i \otimes \lambda_i$ y $\omega' = \sum_j m'_j \otimes \lambda'_j$ entonces:

$$\langle \omega, \omega' \rangle_2 = \sum_i \sum_j \langle m_i, m'_j \rangle \lambda_i \lambda'_j$$

que es claramente una extensión a $M \otimes \mathbb{R}$ de la forma bilineal asociada a q. Definimos la función $\widehat{q} : M \otimes \mathbb{R} \to \mathbb{R}$ como $\widehat{q}(\omega) = \frac{1}{2}\langle \omega, \omega \rangle_2$, con un chequeo directo se vé que $\widehat{q}(\omega + \omega') - \widehat{q}(\omega) - \widehat{q}(\omega') = \langle \omega, \omega' \rangle_2$. Además si $\omega = \sum_i m_i \otimes \lambda_i$ se cumple que:

$$\widehat{q}(-\omega) = \frac{1}{2} \sum_i \sum_j \langle -m_i, -m_j \rangle \lambda_i \lambda_j = \frac{1}{2} \sum_i \sum_j \langle -m_i, -m_j \rangle \lambda_i \lambda_j = \widehat{q}(\omega)$$

lo cual prueba que $\widehat{q}$ es efectivamente una forma cuadrática, que extiende a q es inmediato.

ii) Por el teorema de estructura para módulos f.g. sobre dips, como M es libre de torsión resulta que $M \cong A^n$ como $A-$módulo para algún $n \in \mathbb{Z}^+$. Sea $\{m_1, m_2, \ldots, m_n\}$ una base de M como $A-$módulo, tenemos que $M = m_1 A \oplus m_2 A \oplus \ldots \oplus m_n A$ por la propiedad de extensión de bases del producto tensorial tenemos también que $\mathbb{R} = m_1\mathbb{R} \oplus m_2\mathbb{R} \oplus \ldots \oplus m_n\mathbb{R} \cong \mathbb{R}^n$ y $\widehat{q}$ resulta ser un polinomio homogeneo de grado 2 en las coordenadas en la base $\{m_1, m_2, \ldots, m_n\}$.
Sean $c_1, c_2, \ldots, c_n$ elementos en el cuerpo de fracciones de A, supongamos que $c_i = a_i/b_i$ con $a_i \in A, b_i \in A^*$ y definimos $\lambda = b_1 b_2 \ldots b_n \in A^*$. Tenemos que:

$$\lambda^2 \widehat{q}(c_1 m_1 + c_2 m_2 + \ldots + c_n m_n) = q(\lambda c_1 m_1 + \lambda c_2 m_2 + \ldots + \lambda c_n m_n) \geq 0$$

pues q es definida positiva y al ser $\lambda \neq 0$ resulta que $\widehat{q}(x) \geq 0$ para todo $x \in m_1 A_f + m_2 A_f + \ldots + m_n A_f$ donde A_f denota el cuerpo de fracciones de A. Al ser A un subanillo de $\mathbb{R}$, tenemos que $\mathbb{Q} \subset A_f$ y por lo tanto:

$$\widehat{q}(x) \geq 0 \qquad \text{para todo } x \in M' = m_1\mathbb{Q} + m_2\mathbb{Q} + \ldots + m_n\mathbb{Q}$$

Como M' es denso en $M \otimes \mathbb{R}$ y $\widehat{q}$ continua en $M \otimes R \cong \mathbb{R}^n$ se deduce que $\widehat{q}$ debe ser semidefinida positiva. Para probar la segunda parte basta considerar $\{m_1, m_2, \ldots, m_n\}$ la base para la cual la matriz Q asociada a q en esa base es no singular, por la parte anterior $\widehat{q}$ es semidefinida y la matriz Q continua siendo una matriz asociada a $\widehat{q}$ (pues los m_i forman una $\mathbb{R}-$base de $M \otimes \mathbb{R}$) por lo tanto sus valores propios son no negativos y ninguno puede

ser nulo (pues $det(Q) \neq 0$) asi que todos sus valores propios son positivos y $\widehat{q}$ resulta ser definida positiva.

□

Para terminar una última observación sobre formas cuadráticas definidas sobre $\mathbb{R}$.

Proposición D.7. *Si $\widehat{M}$ es un $\mathbb{R}-$espacio vectorial de dimensión finita (por ejemplo cuando $\widehat{M} = M \oplus_A \mathbb{R}$ con M un $A-$módulo finitamente generado) y $\widehat{q}$ una forma cuadrática en $\widehat{M}$ entonces $\widehat{q}$ es un polinomio homogeneo de segundo grado (en particular continua, considerando $\widehat{M}$ con la topología producto de $\mathbb{R}$).*

Demostración: Consideremos $\{e_1, e_2, \ldots, e_n\}$ una $\mathbb{R}-$base de $\widehat{M}$ y sea $x = \sum_i^n x_i e_i$. Si $\langle , \rangle$ denota la forma bilineal inducida por $\widehat{q}$ entonces:

$$\widehat{q}(x) = \frac{1}{2}\langle x, x\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\langle e_i, e_j\rangle x_i x_j$$

que es un polinomio homogeneo de segundo grado en las variables $(x_1, x_2, \ldots, x_n)$.

□

Bibliografía

[1] Tom M. Apostol, *Modular Function and Dirichlet Series in Number Theory*, Springer. 1990.

[2] Juliana Belding, Reinier Bröker, Andreas Enge and Kristin Lauter, *Computing Hilbert Class Polynomials*, Algorithmic number theory, Lecture Notes in Comput.Sci. 5011, 282-295. Springer. 2008.

[3] Gaetan Bisson and Andrew V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, Journal of Number Theory 113, 815-831. 2011.

[4] Ian F. Blake, János A. Csirik, Michael Rubinstein and Gadiel Seroussi, *On the computation of modular polynomials for elliptic curves*, Tech. report, Hewlett-Packard Laboratories, `http://www.math.uwaterloo.ca/~mrubinst/publications/publications.html`. 1999.

[5] Reinier Bröker, Kristin Lauter and Andrew V. Sutherland, *Modular Polynomial via Isogeny Volcanoes*, Mathematics of Computation 81, 1201-1231. 2012.

[6] Andries E. Brouwer and Willem H. Haemers, *Spectra of Graphs*, Springer. 2011.

[7] Denis Charles, *The Characteristic Polynomial of Frobenius and the Isogeny Class of an Elliptic Curve*, `http://pages.cs.wisc.edu/~cdx/MathJournal/October/CharPoly04.pdf`. 2004.

[8] Denis Charles and Kristin Lauter, *Computing modular polynomials*, LMS Journal of Computation and Mathematics 8, 195-204. 2005.

[9] Andrew M. Childs, David Jao and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, preprint `http://arxiv.org/abs/1012.4019v2`. 2001.

[10] Henri Cohen and Gerhard Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC. 2005.

[11] David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication. 1997.

[12] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Springer. 2005.

[13] Noam D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational Perspective on Number Theory (D.A.Buell and J.T.Teitelbaum, eds.), Studies in Advanced Mathematics 7, 21-76. 1998.

[14] Mireille Fouquet and François Morain, *Isogenies Volcanoes and the SEA algorithm*, Algorithmic Number Theory - Lecture Notes in Comput.Sci. 2369, 276-291. Springer. 2002.

[15] William Fulton, *Curvas Algebraicas*. Editorial Reverté, `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`. 1971.

[16] Steven D. Galbraith, *Constructing Isogenies between Elliptic Curves over Finite Fields*, LMS J. Comput. Math. 2, 118-138 (electronic), `http://www.math.auckland.ac.nz/~sgal018/pubs.html`. 1999.

[17] Steven D. Galbraith, *Supersingular Curves in Cryptography*. ASIACRYPT2001. Lecture notes in Computer Science 2248, 495-513, Springer. 2001.

[18] Steven D. Galbraith and Anton Stolbunov, *Improved algorithm for the isogeny problem for ordinary elliptic curves*, preprint `http://arxiv.org/abs/1105.6331`. 2011.

[19] Steven D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press. 2012.

[20] Sorina Ionica and Antoine Joux, *Pairing the volcano*, preprint `http://arxiv.org/abs/1110.3602v1`. 2001.

[21] Hideji Ito, *Computation of the modular equation*, Proc.Japan Acad. Ser. A 71, 48-50. 1995.

[22] Carlos Ivorra Castillos, *Curvas elípticas*, `http://www.uv.es/~ivorra/Libros/Libros.htm`.

[23] Henryk Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics 17 - American Mathematical Society, Providence, RI. 1997.

[24] David Jao, Stephen Miller and Ramarathnam Venkatesan, *Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?*, ASIACRYPT2005. LNCS 3788, 21-40. Springer. 2005.

[25] David Kohel, *Endomorphism Ring on Elliptic Curves over Finites Fields*, PhD. Thesis, University of California at Berkeley, `\http://echidna.maths.usyd.edu.au/kohel/pub/thesis.pdf`. 1996.

[26] Noemi M. Lalin, *Introducción a las Curvas Elípticas*, Tesis de Grado - UBA, `http://dms.umontreal.ca/~mlalin`. 1999.

[27] Serge Lang, *Elliptic Functions 2nd edition*, Springer. 1987.

[28] Rudolf Lidl and Harald Niederreiter, *Introduction to Finite Fields and their applications*, Cambridge University Press. 1994.

[29] Héctor A. Mercklen, *Estructuras Algebraicas V (Teoría de Cuerpos)*, Secretaría General de la Organización de los Estados Americanos - Programa Regional de Desarrollo Científico y Tecnológico. 1979.

[30] Josep Miret, Daniel Sadornil, Juan Tena, Rosana Tomas and Magda Valls, *Isogeny cordillera algorithm to obtain cryptographically good elliptic curves*, Conferences in Research and Practice in Information Technology (CRPIT) 68, 127-131. 2007.

[31] Nozomu Nishihara, Ryuichi Harasawa, Yutaka Sueyoshi and Aichi Kudo *A remark on the computation of cube roots in finite fields*, IACR Cryptology, ePrint Archive `http://eprint.iacr.org/2009/457.pdf`. 2009.

[32] Claudio Qureshi, *Introducción a las Curvas Elípticas*, Monografía de Licenciatura - Udelar, `http://www.cmat.edu.uy/cmat/biblioteca/documentos/copy_of_monografias/Qur2007`. 2007.

[33] Alexander Rostovtsev and Anton Stolbunov, *Public-key cryptosystem based on isogenies*, IACR Cryptology ePrint Archive 2006 145 `http://eprint.iacr.org/2006/145`. 2006.

[34] René Schoof, *Counting Points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux 7, 219-254. 1995.

[35] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer. 2009.

[36] Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer. 1992.

[37] William Stein, *Sage: Open Source Mathematical Software (Version 4.8)*, The Sage group. 2011.

[38] Anton Stolbunov, *Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves*, Adv. Math. Commun. 4, no. 2, 215-235. 2010.

[39] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. 80, no. 273, 501-538. 2011.

[40] Andrew V. Sutherland, *Accelerating the CM method*, LMS Journal of Computation and Mathematics, preprint `http://arxiv.org/abs/1009.1082`. 2012.

[41] Andrew V. Sutherland, *Identifying Supersingular Elliptic Curves*, preprint `http://arxiv.org/abs/1107.1140`. 2012.

[42] Andrew V. Sutherland, *Isogeny Volcanoes*, preprint `http://arxiv.org/abs/1208.5370`. 2012.

[43] Andrew V. Sutherland, *On the evaluation of Modular Polynomials*, preprint `http://arxiv.org/abs/0712.4046`. 2012.