Volcanes de ℓ–isogenias de curvas elípticas

Autor: Javier Valera Martín
Director: Josep M. Miret Biosca

Universitat de Lleida
Escola Politècnica Superior
Ingeniería en Informática

Sistemas Informáticos
(Trabajo de Final de Carrera)

Septiembre de 2011

Índice general

Índice de figuras

Índice de cuadros

Índice de algoritmos

Introducción

La seguridad de los sistemas actuales de clave pública radica en la resolución de algún problema matemático que es casi imposible de resolver en la práctica. Actualmente los tres problemas matemáticos más utilizados son el problema de la factorización de enteros (IFP – Integer Factorization Problem), el problema del logaritmo discreto sobre el grupo multiplicativo de un cuerpo finito (DLP – Discrete Logarithm Problem) y el problema del logaritmo discreto sobre el grupo de puntos de una curva elíptica definida sobre un cuerpo finito (ECDLP – Elliptic Curve Discrete Logarithm Problem). De todos ellos, para el único que no se conoce un algoritmo subexponencial para resolverlo es para el ECDLP (para el IFP se tiene la Number Field Sieve [BLP93] y para el DLP se tiene el Index–Calculus [How98]). Esta circunstancia nos permite obtener con los sistemas basados en el ECDLP niveles de seguridad similares a los que obtendríamos con los basados en el IFP y en el DLP pero con parámetros iniciales (claves, etc.) mucho más pequeños [Bel00]. Entonces, como es lógico, al utilizar parámetros más pequeños, los elementos con los que operar también lo son, por lo que dichos sistemas son recomendables en dispositivos donde los recursos (memoria, poder de cómputo, etc.) son limitados: tarjetas inteligentes, teléfonos móviles, etc.

El único inconveniente que presentan los sistemas basados en el ECDLP es que no todas las curvas elípticas existentes ofrecen los mismos niveles de seguridad. Por lo que se sabe hasta ahora, la validez para el ECDLP de una curva elíptica E definida sobre un cuerpo finito $\mathbb{F}_q$ solamente depende de su

cardinal sobre $\mathbb{F}_q$ [Bel00]. Aunque en un primer momento podríamos pensar que para saber si E es válida lo único que tenemos que hacer es calcular su cardinal, esta opción, a priori, no siempre es viable ya que calcular el cardinal de una curva elíptica es un problema computacionalmente muy costoso. Entonces parece razonable pensar que si E es válida, podamos obtener a partir de ella otras curvas elípticas que también lo sean, es decir, que también tengan su mismo cardinal sobre $\mathbb{F}_q$. Dos curvas elípticas tienen el mismo cardinal sobre $\mathbb{F}_q$ si y sólo si entre ambas existe una isogenia $\mathbb{F}_q$–racional. Una isogenia $\mathbb{F}_q$–racional entre dos curvas elípticas es un morfismo $\mathbb{F}_q$–racional entre ambas que preserva el punto del infinito. A las isogenias de grado d se las denomina d–isogenias. Vemos, entonces, que para obtener una curva elíptica con el mismo cardinal sobre $\mathbb{F}_q$ que el de E lo único que tenemos que hacer es calcular a partir de E una isogenia $\mathbb{F}_q$–racional.

Supongamos que E es ordinaria y sea ℓ un número primo tal que ℓ no divide a q. Entonces, si a partir de E calculamos sucesivas ℓ–isogenias $\mathbb{F}_q$–racionales, lo que obtenemos es un digrafo llamado volcán de ℓ–isogenias cuyos vértices representan clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas ordinarias y cuyos arcos representan ℓ–isogenias $\mathbb{F}_q$–racionales [Fou01]. Los volcanes de ℓ–isogenias son importantes porque permiten mejorar el algoritmo SEA [IKNY98], siendo el SEA el mejor algoritmo conocido actualmente para calcular el cardinal de una curva elíptica.

Organización de la memoria

Esta memoria está estructurada en tres capítulos. En el primer capítulo explicamos qué son las ℓ–isogenias de curvas elípticas y damos un algoritmo para calcularlas. En el segundo capítulo explicamos qué son los volcanes de ℓ–isogenias y damos algoritmos para calcular cierta información sobre ellos (altura, tamaño de cráter, ...). Finalmente, en el tercer capítulo, damos los resultados que hemos obtenido a partir de la implementación de los algoritmos de los dos capítulos anteriores así como las conclusiones a las

que hemos llegado después de realizar este trabajo.

Notaciones

En esta memoria hemos utilizado principalmente las notaciones usadas en [Mor05]. Esto se debe a que no hemos incluido un capítulo de preliminares matemáticos y otro de curvas elípticas. Las notaciones, definiciones y consideraciones más importantes son las siguientes:

- $\mathbb{K}$: un cuerpo cualquiera (p. e. $\mathbb{Q}$).
- $\overline{\mathbb{K}}$: clausura algebraica de $\mathbb{K}$.
- $\mathbb{K}[X_1, X_2, \ldots, X_n]$: anillo de polinomios en X_1, X_2, ..., X_n con coeficientes en $\mathbb{K}$.
- $(f(x))$: ideal generado por el polinomio $f(x)$.
- $\mathbb{F}_q$: cuerpo finito de q elementos.
- ℓ : número primo que no divide a q.
- $a \mid b$ ($a \nmid b$) : a divide a b (a no divide a b).
- $a \simeq b$ ($a \not\simeq b$) : a es isomorfo a b (a no es isomorfo a b).
- Todas las curvas elípticas tienen una ecuación general de Weierstrass como modelo de ecuación.
  Ecuación general de Weierstrass en coordenadas proyectivas:

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

- $\mathcal{O} = (0 : 1 : 0)$: punto del infinito común a todas las curvas elípticas.
- $x(P)$: abscisa de un punto $P \neq \mathcal{O}$ ($x(P) = u$ si $P = (u, v)$).
- $y(P)$: ordenada de un punto $P \neq \mathcal{O}$ ($y(P) = v$ si $P = (u, v)$).

- Un punto P de una curva elíptica E definida sobre $\mathbb{F}_q$ es $\mathbb{F}_q$–racional si y sólo si $x(P)$ e $y(P)$ son elementos de $\mathbb{F}_q$ o $P = \mathcal{O}$.
- $E(\mathbb{F}_q)$: conjunto de puntos $\mathbb{F}_q$–racionales de una curva elíptica E definida sobre $\mathbb{F}_q$.
- $\#E(\mathbb{F}_q)$: cardinal de $E(\mathbb{F}_q)$.
- $(E(\mathbb{F}_q), +)$: grupo de puntos $\mathbb{F}_q$–racionales de una curva elíptica E definida sobre $\mathbb{F}_q$.
- $nP = \begin{cases} P + \overset{(n)}{\cdots} + P & \text{si } n > 0, \\ \mathcal{O} & \text{si } n = 0, \\ (-P) + \overset{(n)}{\cdots} + (-P) & \text{si } n < 0. \end{cases}$
- El orden de un punto $P \in E(\mathbb{F}_q)$ es el entero positivo más pequeño n tal que $nP = \mathcal{O}$.
- Un punto $P \in E(\mathbb{F}_q)$ es de n–torsión, $n > 0$, si y sólo si $nP = \mathcal{O}$.
- $E(\mathbb{F}_q)[n]$: grupo de puntos $\mathbb{F}_q$–racionales de n–torsión de una curva elíptica E definida sobre $\mathbb{F}_q$.
- $j(E)$: j–invariante de una curva elíptica E.
- $< P >$: grupo generado por el punto P.

Agradecimientos

En estos años tan difíciles para mí, quiero agradecerle a mi novia, a mis padres, a mi abuela y a mi director el que no hayan pasado de mí y que a su manera hayan intentado ayudarme. A todos ellos, muchísimas gracias.

Capítulo 1

Isogenias de curvas elípticas

En este capítulo explicamos qué son las ℓ–isogenias de curvas elípticas y damos un algoritmo para calcularlas.

1.1. Definición y propiedades

Sean E y E' dos curvas elípticas definidas sobre $\mathbb{K}$. Una isogenia entre E y E' es una aplicación regular

$$\varphi\colon E \to E'$$

tal que $\varphi(\mathcal{O}) = \mathcal{O}$. El núcleo de la isogenia φ es

$$\ker \varphi = \{P \in E(\overline{\mathbb{K}}) \mid \varphi(P) = \mathcal{O}\}.$$

La isogenia φ es $\mathbb{K}$–racional (φ está definida sobre $\mathbb{K}$) si y sólo si $\varphi(E(\mathbb{K})) \subseteq E'(\mathbb{K})$. La isogenia φ es constante si y sólo si $\varphi(E(\overline{\mathbb{K}})) = \{\mathcal{O}\}$. Las curvas elípticas E y E' son isógenas sobre $\mathbb{K}$ si y sólo si entre ambas existe una isogenia no constante $\mathbb{K}$–racional.

Teorema 1. *Sea $\varphi\colon E \to E'$ una isogenia $\mathbb{K}$–racional. Entonces para todo*

par de puntos P y Q de $E(\overline{\mathbb{K}})$ se tiene que

$$\varphi(P+Q) = \varphi(P) + \varphi(Q),$$

es decir, φ es un homomorfismo de grupos.

Teorema 2. *Sean E y E' dos curvas elípticas definidas sobre $\mathbb{F}_q$. Entonces E y E' son isógenas sobre $\mathbb{F}_q$ si y sólo si $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

El grado de las isogenias constantes, por convenio, es 0. Las isogenias no constantes se clasifican en separables, inseparables y puramente inseparables. El grado de una isogenia separable es igual al cardinal de su núcleo (para saber cómo se definen los grados de las isogenias inseparables y puramente inseparables, como para saber en qué se diferencian éstas de las isogenias separables, véase [Mor05]). Si $\varphi\colon E \to E'$ es una isogenia de grado m, entonces φ es una m–isogenia de E. Si φ es no constante, entonces E' es una curva elíptica m–isógena de E.

Teorema 3. *Sea E una curva elíptica definida sobre $\mathbb{K}$ y sea $G \subset E(\overline{\mathbb{K}})$ un grupo finito. Entonces existe una única (salvo isomorfismo) curva elíptica E/G y una isogenia separable $\varphi_G\colon E \to E/G$ tal que $\ker \varphi_G = G$.*

La aplicación multiplicación por $m \in \mathbb{Z} \setminus \{0\}$ en una curva elíptica E definida sobre $\mathbb{K}$,

$$\begin{array}{rccc} [m] & : & E(\overline{\mathbb{K}}) & \to & E(\overline{\mathbb{K}}) \\ & & P & \mapsto & mP \end{array},$$

es una isogenia de E en sí misma. La isogenia nula entre E y una curva elíptica E' se define como $[0](P) = \mathcal{O}$ para todo $P \in E(\overline{\mathbb{K}})$. La isogenia $[0]\colon E \to E'$ es la única isogenia constante entre E y E'.

Teorema 4. *Sea $\varphi\colon E \to E'$ una isogenia no constante de grado m. Entonces existe una única isogenia $\hat{\varphi}\colon E' \to E$ tal que $\hat{\varphi} \circ \varphi = [m]$ en E y $\varphi \circ \hat{\varphi} = [m]$ en E'. Tal isogenia $\hat{\varphi}$ se denomina la isogenia dual de φ y su grado es m.*

Nota 1. La dual de la isogenia $[0]\colon E \to E'$ es la isogenia $[0]\colon E' \to E$.

Nota 2. La isogenia φ_G es $\mathbb{F}_q$–racional si y sólo si $\hat{\varphi}_G$ también lo es.

A partir de ahora, en lo que queda de documento, y salvo que no digamos lo contrario, supondremos que

- todas las isogenias son separables;
- una curva elíptica E definida sobre $\mathbb{K}$ tendrá tantas m–isogenias como subgrupos de orden m haya en $(E(\overline{\mathbb{K}}), +)$.

Para obtener más información sobre lo explicado en esta sección véase [BSS00, Sil86].

1.2. Fórmulas de Vélu

Dada una curva elíptica

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

definida sobre $\mathbb{K}$ y dado un subgrupo finito G no trivial de $(E(\overline{\mathbb{K}}), +)$, las fórmulas de Vélu, véase [Vé71], nos permiten calcular los coeficientes de la curva elíptica

$$E/G\colon Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

y las ecuaciones de la isogenia φ_G. Tales fórmulas son las siguientes:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \end{aligned}$$

$$R \text{ tal que } \begin{cases} G \setminus E(\overline{\mathbb{K}})[2] = R \cup (-R) \\ R \cap (-R) = \emptyset \end{cases}$$

$$S = R \cup (G \cap E(\overline{\mathbb{K}})[2] \setminus \{\mathcal{O}\})$$

$T \in S$

$$
\begin{aligned}
f^x(T) &= 3x(T)^2 + 2a_2x(T) + a_4 - a_1y(T) \\
f^y(T) &= -2y(T) - a_1x(T) - a_3 \\
t(T) &= \begin{cases} f^x(T) & \text{si } T \notin R \\ 2f^x(T) - a_1f^y(T) = 6x(T)^2 + b_2x(T) + b_4 & \text{si } T \in R \end{cases} \\
u(T) &= 4x(T)^3 + b_2x(T)^2 + 2b_4x(T) + b_6
\end{aligned}
$$

$$
\begin{aligned}
t &= \sum_{T \in S} t(T) \\
w &= \sum_{T \in S} (u(T) + x(T)t(T))
\end{aligned}
$$

$$
\begin{aligned}
A_1 &= a_1 \\
A_2 &= a_2 \\
A_3 &= a_3 \\
A_4 &= a_4 - 5t \\
A_6 &= a_6 - b_2t - 7w
\end{aligned}
$$

$P = (x, y) \in E(\overline{\mathbb{K}})$

$$
\varphi_G(P) = \begin{cases} \mathcal{O} & \text{si } P \in G \\ (X, Y) & \text{si } P \notin G \end{cases}
$$

$$
\begin{aligned}
X &= x + \sum_{T \in S} \left(\frac{t(T)}{x - x(T)} + \frac{u(T)}{(x - x(T))^2} \right) \\
Y &= y - \sum_{T \in S} \left(u(T) \frac{2y + a_1x + a_3}{(x - x(T))^3} + \right. \\
&\quad \left. + t(T) \frac{a_1(x - x(T)) + y - y(T)}{(x - x(T))^2} + \frac{a_1u(T) - f^x(T)f^y(T)}{(x - x(T))^2} \right)
\end{aligned}
$$

1.3. Órdenes de cuerpos cuadráticos

Un cuerpo cuadrático es una extensión de grado 2 de $\mathbb{Q}$. Si K es un cuerpo cuadrático, entonces existe un entero N libre de cuadrados tal que

$$K = \mathbb{Q}(\sqrt{N}) = \{\alpha + \beta\sqrt{N} \mid \alpha, \beta \in \mathbb{Q}\}.$$

Nótese que para cualquier entero positivo k,

$$\mathbb{Q}(\sqrt{k^2 N}) = \mathbb{Q}(\sqrt{N}).$$

Dependiendo de si N es positivo o negativo se dice que K es real o imaginario. El discriminante del cuerpo cuadrático K es

$$d_K = \begin{cases} N & \text{si } N \equiv 1 \pmod 4, \\ 4N & \text{si } N \not\equiv 1 \pmod 4. \end{cases}$$

El anillo de enteros de K, siendo

$$\omega_K = \frac{d_K + \sqrt{d_K}}{2},$$

es $O_K = \mathbb{Z}[\omega_K]$.

Un orden de K es un subconjunto de K que además de ser un subanillo unitario de K es también un $\mathbb{Z}$–módulo libre de rango 2. El orden maximal de K, es decir, el orden de K que contiene a todos los demás, es

$$O_K = \mathbb{Z} \oplus \omega_K \mathbb{Z}.$$

Un orden O de K es de la forma

$$\mathbb{Z} + fO_K = \mathbb{Z} \oplus f\omega_K \mathbb{Z}.$$

Al entero positivo

$$f = [O_K : O],$$

índice de O en O_K, se le denomina el conductor de O. El discriminante del orden O es

$$D = f^2 d_K.$$

Si O' es un orden de K de discriminante D', $O \subseteq O'$ si y sólo si $D = k^2 D'$ para algún entero positivo k ($O = O' \iff D = D'$).

Para más información véase [Cox89].

1.4. Número de ℓ–isogenias $\mathbb{F}_q$–racionales

Sea E una curva elíptica definida sobre $\mathbb{F}_q$. El conjunto de todas las isogenias de E en sí misma tiene estructura de anillo con la suma y el producto (composición) de isogenias, es decir, es un anillo con

$$(\varphi_1 + \varphi_2)(P) = \varphi_1(P) + \varphi_2(P)$$

y con

$$(\varphi_1 \varphi_2)(P) = \varphi_1(\varphi_2(P)).$$

A este anillo se le denomina el anillo de endomorfismos de E y se le denota con $\mathrm{End}(E)$.

El endomorfismo de Frobenius de orden q de E se define como

$$\begin{array}{rccc} \pi & : & E(\overline{\mathbb{F}_q}) & \to & E(\overline{\mathbb{F}_q}) \\ & & (x, y) & \mapsto & (x^q, y^q) \end{array} .$$

Este endomorfismo es puramente inseparable y su grado es q.

Supongamos que E es ordinaria y que

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

Entonces el anillo de endomorfismos de E es isomorfo a un orden del cuerpo cuadrático imaginario

$$K = \mathbb{Q}(\sqrt{t^2 - 4q}).$$

Un orden de este cuerpo cuadrático es el orden $\mathbb{Z}[\pi]$. El discriminante de $\mathbb{Z}[\pi]$ es $d_\pi = g^2 d_K = t^2 - 4q$. Si O es el orden de K isomorfo a $\mathrm{End}(E)$, entonces $\mathbb{Z}[\pi] \subseteq O$. Si $D = f^2 d_K$ es el discriminante de O, entonces

- $D = -3 \iff j(E) = 0$;
- $D = -4 \iff j(E) = 1728$.

Cuando D es igual a -3 o es igual a -4, $D = d_K$, es decir, $O = O_K$. El número de clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas ordinarias con cardinal m y anillos de endomorfismos isomorfos a O_K cuando d_K es igual a -3 o es igual a -4 es igual a 1. Dicha clase de isomorfía o bien es la clase de j–invariante 0 o bien es la clase de j–invariante 1728.

El anillo de endomorfismos de una curva elíptica E' isógena a E también es isomorfo a un orden de K. Si E' es isógena a E sobre $\mathbb{F}_q$ y O' es el orden de K isomorfo a $\mathrm{End}(E')$, entonces $\mathbb{Z}[\pi] \subseteq O'$.

Sea $\varphi\colon E \to E'$ una isogenia de grado ℓ. Entonces se nos presenta uno de los siguientes tres casos:

- $O \subset O'$ y $[O' : O] = \ell$,
- $O = O'$ y $[O' : O] = 1$,
- $O' \subset O$ y $[O : O'] = \ell$.

Dependiendo de cada caso se dice que φ es ascendente ($\uparrow$), horizontal ($\rightarrow$) o descendente ($\downarrow$). Notemos que

- φ es ascendente si y sólo si $\hat{\varphi}$ es descendente;
- φ es horizontal si y sólo si $\hat{\varphi}$ también lo es.

Dependiendo de la posición respecto a ℓ de O en relación con $\mathbb{Z}[\pi]$ y O_K podemos saber cuántas ℓ–isogenias $\mathbb{F}_q$–racionales tiene E de cada tipo. Dicha información es la que damos a continuación.

$$\left(\frac{D}{\ell}\right) \;=\; \text{Símbolo de Kronecker}$$

- $\ell \nmid [O_K : O] \quad (\ell \nmid f)$
  - $\ell \nmid [O : \mathbb{Z}[\pi]] \quad (\ell \nmid (g/f))$

    $$\boxed{1 + \left(\frac{D}{\ell}\right) \ \rightarrow}$$

  - $\ell \mid [O : \mathbb{Z}[\pi]] \quad (\ell \mid (g/f))$

    $$\boxed{1 + \left(\frac{D}{\ell}\right) \ \rightarrow} \qquad \boxed{\ell - \left(\frac{D}{\ell}\right) \ \downarrow}$$

- $\ell \mid [O_K : O] \quad (\ell \mid f)$
  - $\ell \nmid [O : \mathbb{Z}[\pi]] \quad (\ell \nmid (g/f))$

    $$\boxed{1 \ \uparrow}$$

  - $\ell \mid [O : \mathbb{Z}[\pi]] \quad (\ell \mid (g/f))$

    $$\boxed{1 \ \uparrow} \qquad \boxed{\ell \ \downarrow}$$

La información referente a esta sección la hemos extraído de [Cox89, Koh96].

1.5. Cálculo de las ℓ–isogenias $\mathbb{F}_q$–racionales de una curva elíptica

Sea

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

una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ y sea G un subgrupo de $(E(\overline{\mathbb{F}_q}), +)$ de orden ℓ. Entonces, como ℓ es un número primo, G es cíclico y todos los puntos de G, a excepción de $\mathcal{O}$, son puntos de orden ℓ y generadores de G, es decir, si P es un punto de G distinto de $\mathcal{O}$, entonces

$$G =< P >= \{P, 2P, \ldots, \ell P = \mathcal{O}\}.$$

Los inversos de los puntos P, $2P$, ..., nP, siendo

$$n = \begin{cases} 1 & \text{si } \ell = 2, \\ (\ell - 1)/2 & \text{si } \ell \neq 2, \end{cases}$$

son, respectivamente, los puntos $(\ell - 1)P$, $(\ell - 2)P$, ..., $(\ell - n)P$, ya que como sabemos, el inverso de un punto Q es el punto R tal que $Q + R = \mathcal{O}$, y por lo tanto, $kP + (\ell - k)P = \ell P = \mathcal{O}$ para todo $k \in \{1, 2, \ldots, n\}$. Entonces, teniendo en cuenta que un punto y su inverso tienen la misma abscisa, vemos que podemos construir un polinomio mónico de grado n cuyas raíces sean las abscisas de los puntos de $G \setminus \{\mathcal{O}\}$, a saber,

$$g(x) = \prod_{k=1}^{n} (x - x(kP)).$$

Démonos cuenta que este polinomio representa inequívocamente a G ya que si al punto del infinito le añadimos los puntos cuyas abscisas son sus raíces lo que obtenemos es G. Entonces decimos que G es $\mathbb{F}_q$–racional si y sólo si $g(x) \in \mathbb{F}_q[x]$. La isogenia φ_G es $\mathbb{F}_q$–racional si y sólo si G también lo es.

Tal y como podemos ver en [Ler97], en $(E(\overline{\mathbb{F}_q}), +)$ hay un total de $\ell + 1$ subgrupos de orden ℓ. Cada uno de estos subgrupos es el núcleo de una ℓ–isogenia de E. Por lo que acabamos de explicar, una ℓ–isogenia de E es $\mathbb{F}_q$–racional si y sólo si su núcleo también lo es. Por lo que hemos explicado en la sección anterior, o bien E no tiene ℓ–isogenias $\mathbb{F}_q$–racionales o bien E tiene 1, 2 o $\ell + 1$. Entonces, teniendo en cuenta todo esto, vemos que en $(E(\overline{\mathbb{F}_q}), +)$ o bien no hay subgrupos $\mathbb{F}_q$–racionales de orden ℓ o bien hay 1, 2 o $\ell + 1$.

El polinomio de ℓ–división asociado a E en una indeterminada, véase [Mor05], es

$$\tau_\ell(x) = \begin{cases} f_\ell(x) & \text{si } \ell \neq 2, \\ 4x^3 + b_2x^2 + 2b_4x + b_6 & \text{si } \ell = 2, \end{cases}$$

siendo

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = a_1a_3 + 2a_4,$$
$$b_6 = a_3^2 + 4a_6.$$

La principal característica de este polinomio es que sus raíces son las abscisas de los puntos de $E(\overline{\mathbb{F}_q})$ de orden ℓ. Entonces, como las raíces de $g(x)$ son abscisas de puntos de orden ℓ, vemos que $g(x) \mid \tau_\ell(x)$, es decir, $g(x)$ es un factor (de grado n) de $\tau_\ell(x)$.

Si $\ell \neq 2$, entonces es posible modificar las fórmulas de Vélu para obtener E/G y φ_G a partir únicamente de los coeficientes de $g(x)$, es decir, sin necesidad de conocer los puntos de G. Tales fórmulas para el cálculo de E/G son las que siguen (para las del cálculo de φ_G véase [Ler97]).

$$g(x) = x^n + g_1x^{n-1} + \cdots + g_{n-1}x + g_n$$

$$g_i = (-1)^i \sum_{1 \leq k_1 < k_2 < \cdots < k_i \leq n} (x(k_1P)x(k_2P)\cdots x(k_iP)) \qquad (1 \leq i \leq n)$$

$$S = \{P, 2P, \ldots, nP\}$$

$$U_1 = \sum_{T \in S} x(T) = -g_1$$

$$U_2 = \sum_{T \in S} x(T)^2 = \begin{cases} g_1^2 & \text{si } \ell = 3 \ (n = 1) \\ g_1^2 - 2g_2 & \text{si } \ell \geq 5 \ (n \geq 2) \end{cases}$$

$$U_3 = \sum_{T \in S} x(T)^3 = \begin{cases} -g_1^3 & \text{si } \ell = 3 \ (n = 1) \\ -g_1^3 + 3g_1g_2 & \text{si } \ell = 5 \ (n = 2) \\ -g_1^3 + 3g_1g_2 - 3g_3 & \text{si } \ell \geq 7 \ (n \geq 3) \end{cases}$$

$$
\begin{aligned}
t &= \sum_{T \in S} t(T) = \\
&= \sum_{T \in S} (6x(T)^2 + b_2 x(T) + b_4) = \\
&= 6 \sum_{T \in S} x(T)^2 + b_2 \sum_{T \in S} x(T) + n b_4 = \\
&= 6U_2 + b_2 U_1 + n b_4
\end{aligned}
$$

$$
\begin{aligned}
w &= \sum_{T \in S} (u(T) + x(T)t(T)) = \\
&= \sum_{T \in S} (10x(T)^3 + 2b_2 x(T)^2 + 3b_4 x(T) + b_6) = \\
&= 10 \sum_{T \in S} x(T)^3 + 2b_2 \sum_{T \in S} x(T)^2 + 3b_4 \sum_{T \in S} x(T) + n b_6 = \\
&= 10U_3 + 2b_2 U_2 + 3b_4 U_1 + n b_6
\end{aligned}
$$

Entonces, teniendo en cuenta estas fórmulas, a partir de ahora supondremos que disponemos de un algoritmo IsÓGENA tal que al pasarle E y $g(x)$ nos devuelve E/G.

Finalmente, un algoritmo para calcular todas las curvas elípticas ℓ–isógenas de E sobre $\mathbb{F}_q$ es el que a continuación damos.

algoritmo IsÓGENAS(E, ℓ) **devuelve** S

Entrada: Una curva elíptica ordinaria

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

definida sobre $\mathbb{F}_q$ y un número primo ℓ tal que $\ell \nmid q$.

Salida: Una secuencia S que contiene todas las curvas elípticas ℓ–isógenas de E sobre $\mathbb{F}_q$.

$S \leftarrow []$

Calcular el polinomio de ℓ–división $\tau_\ell(x) \in \mathbb{F}_q[x]$ asociado a E

si $\ell = 2$ **entonces**

$\rho(x) \leftarrow \tau_\ell(x)$

mientras $\exists \xi \in \mathbb{F}_q$ tal que $\rho(\xi) = 0$ **hacer**

Calcular el punto P tal que $x(P) = \xi$

Calcular E/G utilizando las fórmulas de Vélu ($G = \{P, \mathcal{O}\}$)

Guardar E/G en S

$\rho(x) \leftarrow \rho(x)/(x - \xi)$

fin mientras

sino si $\ell = 3$ **entonces**

$\rho(x) \leftarrow \tau_\ell(x)$

mientras $\exists \xi \in \mathbb{F}_q$ tal que $\rho(\xi) = 0$ **hacer**

$g(x) \leftarrow x - \xi$

$E/G \leftarrow$ IsógenA$(E, g(x))$

Guardar E/G en S

$\rho(x) \leftarrow \rho(x)/g(x)$

fin mientras

sino

$n \leftarrow (\ell - 1)/2$

Factorizar $\tau_\ell(x)$ en $\mathbb{F}_q[x]$ y guardar los factores irreducibles en una secuencia U

$final \leftarrow$ **falso**

repetir

si $\#S < 2$ **entonces**

si grado$(U[1]) > n$ **entonces**

Eliminar de U el factor $U[1]$

sino

Calcular una raíz ξ de $U[1]$ en $\mathbb{F}_{q^{\text{grado}(U[1])}}[x]$

/* Un polinomio irreducible de grado d en $\mathbb{F}_q[x]$ tiene todas sus raíces en $\mathbb{F}_{q^d}[x]$ */

Calcular un punto P tal que $x(P) = \xi$

/* $P \in E(\mathbb{F}_{q^{\text{grado}(U[1])}})$ o $P \in E(\mathbb{F}_{q^{2\text{grado}(U[1])}}) \setminus E(\mathbb{F}_{q^{\text{grado}(U[1])}})$ */

$g(x) \leftarrow \prod_{k=1}^{n} (x - x(kP))$

/* Las abscisas de los puntos kP son elementos de $\mathbb{F}_{q^{\text{grado}(U[1])}}$ y éstas podrían calcularse únicamente a partir de ξ, es decir, no

haría falta conocer el punto P */

si $g(x) \notin \mathbb{F}_q[x]$ **entonces**

Eliminar de U los factores que tengan como mínimo una raíz en común con $g(x)$

sino

$E/G \leftarrow$ IsógenA$(E, g(x))$

Guardar E/G en S

Eliminar de U los factores que dividan a $g(x)$

fin si

fin si

$k \leftarrow 0$

para $i \leftarrow 1$ **hasta** $\#U$ **hacer**

$k \leftarrow k + \text{grado}(U[i])$

fin para

si $(\#S < 2 \wedge k < n) \vee (\#S = 2 \wedge k \neq n(\ell - 1))$ **entonces**

$final \leftarrow$ **cierto**

fin si

sino si $\#S = 2$ **entonces**

si $\text{grado}(U[1]) > n$ **entonces**

$final \leftarrow$ **cierto**

sino

Calcular una raíz ξ de $U[1]$ en $\mathbb{F}_{q^{\text{grado}(U[1])}}[x]$

Calcular un punto P tal que $x(P) = \xi$

$g(x) \leftarrow \prod_{k=1}^{n} (x - x(kP))$

si $g(x) \notin \mathbb{F}_q[x]$ **entonces**

$final \leftarrow$ **cierto**

sino

$E/G \leftarrow$ IsógenA$(E, g(x))$

Guardar E/G en S

Eliminar de U los factores que dividan a $g(x)$

fin si

fin si

sino si $\#S \neq \ell$ **entonces**

si $\text{grado}(U[1]) = n$ **entonces**

$g(x) \leftarrow U[1]$

sino

Calcular una raíz ξ de $U[1]$ en $\mathbb{F}_{q^{\text{grado}\,(U[1])}}[x]$

Calcular un punto P tal que $x(P) = \xi$

$g(x) \leftarrow \prod_{k=1}^{n} (x - x(kP))$

fin si

$E/G \leftarrow \text{IsógenA}(E, g(x))$

Guardar E/G en S

Eliminar de U los factores que dividan a $g(x)$

sino

$g(x) \leftarrow \prod_{i=1}^{\#U} U[i]$

$E/G \leftarrow \text{IsógenA}(E, g(x))$

Guardar E/G en S

$final \leftarrow$ **cierto**

fin si

hasta $final$

fin si

devolver S

fin algoritmo

Capítulo 2

Volcanes de ℓ–isogenias

En este capítulo explicamos qué son los volcanes de ℓ–isogenias y damos algoritmos para calcular cierta información sobre ellos (altura, tamaño de cráter, ...).

2.1. Definición y características

Consideremos todas las clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas ordinarias con un determinado cardinal sobre $\mathbb{F}_q$ y supongamos que cada una de ellas representa un vértice de un digrafo G. Sean v_1 y v_2 dos vértices de G y sean E_1 una curva elíptica de v_1 y E_2 una curva elíptica de v_2. Entonces existe un arco de v_1 a v_2 si y sólo si entre E_1 y E_2 existe una ℓ–isogenia $\mathbb{F}_q$–racional (el número exacto de arcos que salen de v_1 a v_2 es igual al número de curvas elípticas ℓ–isógenas de E_1 isomorfas sobre $\mathbb{F}_q$ a E_2). Notemos que si existe un arco de v_1 a v_2, entonces también existe un arco de v_2 a v_1 ya que si existe una ℓ–isogenia $\mathbb{F}_q$–racional φ_1 entre E_1 y E_2, entonces también existe una ℓ–isogenia $\mathbb{F}_q$–racional φ_2 entre E_2 y E_1, a saber, $\varphi_2 = \hat{\varphi}_1$. Notemos, también, que $v_1 = v_2$ si y sólo si $j(E_1) = j(E_2)$. Esto es así por lo que a continuación explicamos. Dos curvas elípticas ordinarias E y E' son isomorfas sobre $\mathbb{F}_q$ si y sólo si $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ y $j(E) = j(E')$. Los vértices v_1 y v_2 son el mismo si y sólo si E_1 y E_2 son isomorfas sobre $\mathbb{F}_q$.

Como todas las curvas elípticas de G tienen el mismo cardinal sobre $\mathbb{F}_q$, E_1 y E_2 son isomorfas sobre $\mathbb{F}_q$ si y sólo si $j(E_1) = j(E_2)$. Entonces, teniendo en cuenta esto, vemos que un buen representante para cada vértice de G es el j–invariante de sus curvas elípticas. Cada componente conexa de G es un volcán de ℓ–isogenias o ℓ–volcán sobre $\mathbb{F}_q$.

Sea V un ℓ–volcán sobre $\mathbb{F}_q$. Entonces, como todas las curvas elípticas de V son isógenas entre sí, por lo explicado en la sección 1.4, vemos que todos sus anillos de endomorfismos son isomorfos a órdenes de un mismo cuerpo cuadrático imaginario K. Como además son isógenas sobre $\mathbb{F}_q$, dichos órdenes están comprendidos entre los órdenes $\mathbb{Z}[\pi]$ y O_K (véase la sección 1.4). Otra característica importante de estos órdenes es que sus conductores difieren los unos de los otros únicamente en la potencia de ℓ ya que si $\varphi\colon E \to E'$ es una ℓ–isogenia y $O \simeq \mathrm{End}(E)$ es igual a $\mathbb{Z} + \ell^k w O_K$ con ℓ no dividiendo a w, entonces, dependiendo de si φ es ascendente, horizontal o descendente, $O' \simeq \mathrm{End}(E')$ es igual a $\mathbb{Z} + \ell^{k-1} w O_K$, $\mathbb{Z} + \ell^k w O_K$ o $\mathbb{Z} + \ell^{k+1} w O_K$. Entonces, teniendo en cuenta esto, vemos que podemos situar los diferentes vértices de V en distintos niveles, siendo cada nivel, como es obvio, un orden de K, es decir, cada orden representa un nivel. Aunque en un primer momento podríamos pensar que el orden de conductor $\ell^k w$ representa el nivel k, esto no es así. Si esto fuera así, entonces, al considerar una ℓ–isogenia ascendente, lo que haríamos sería descender un nivel, y parece más razonable pensar, ya que la ℓ–isogenia es ascendente, que lo que tendría que suceder es que ascendiéramos, es decir, en lugar de pasar del nivel k al nivel $k-1$ deberíamos pasar del nivel k al nivel $k+1$. Por lo tanto, para que esto sea así, el orden de conductor $\ell^k w$ representará el nivel $h-k$, siendo h la valoración ℓ–ádica del conductor de $\mathbb{Z}[\pi]$. Al valor h se le denomina la altura de V. Notemos que dicho valor es igual al número total de niveles que hay en V menos 1. Los vértices situados en el nivel h forman el cráter de V. Al número total de vértices que hay en este nivel lo denotamos con c. Los vértices situados en el nivel 0, siempre y cuando h sea mayor que 0, forman el suelo de V. Los vértices que no pertenecen ni

al cráter ni al suelo, siempre y cuando h sea mayor que 1, forman la ladera de V. Un resumen de lo que acabamos de explicar es el siguiente:

- $h = 0$

$$O_0 = \mathbb{Z} + \ell^0 w O_K \quad \text{NIVEL } 0 \quad \begin{pmatrix} \ell \nmid [O_K : O_0] \\ \ell \nmid [O_0 : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{CRÁTER}$$

- $h = 1$

$$O_0 = \mathbb{Z} + \ell^0 w O_K \quad \text{NIVEL } 1 \quad \begin{pmatrix} \ell \nmid [O_K : O_0] \\ \ell \mid [O_0 : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{CRÁTER}$$

$$\vert$$

$$O_1 = \mathbb{Z} + \ell^1 w O_K \quad \text{NIVEL } 0 \quad \begin{pmatrix} \ell \mid [O_K : O_1] \\ \ell \nmid [O_1 : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{SUELO}$$

- $h \geq 2$

$$O_0 = \mathbb{Z} + \ell^0 w O_K \quad \text{NIVEL } h \quad \begin{pmatrix} \ell \nmid [O_K : O_0] \\ \ell \mid [O_0 : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{CRÁTER}$$

$$\vdots$$

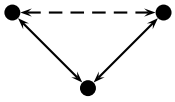
$$O_k = \mathbb{Z} + \ell^k w O_K \quad \text{NIVEL } h-k \quad \begin{pmatrix} \ell \mid [O_K : O_k] \\ \ell \mid [O_k : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{LADERA}$$

$$\vdots$$

$$O_h = \mathbb{Z} + \ell^h w O_K \quad \text{NIVEL } 0 \quad \begin{pmatrix} \ell \mid [O_K : O_h] \\ \ell \nmid [O_h : \mathbb{Z}[\pi]] \end{pmatrix} \quad \text{SUELO}$$

De cada uno de los vértices del cráter de V salen $r = 0, 1, 2$ arcos horizontales. Los posibles cráteres de V en función de dicho valor y del tamaño c de su cráter son los que mostramos en el cuadro 2.1. Si $h > 0$, entonces de cada uno de los vértices del cráter de V también salen $s = \ell + 1 - r$ arcos descendentes. Estos s arcos descendentes, a excepción de dos casos, siempre van a parar a s vértices distintos. Los dos casos en los que esto no es así son los casos en los que en V o bien aparece el j–invariante 0 o bien aparece el j–invariante 1728. En estos dos casos, $c = 1$ y dicho vértice o bien es el 0 o bien es el 1728. En el primer caso, los s arcos descendentes van a parar a $s/3$ vértices distintos, mientras que en el segundo, van a parar

a $s/2$. A priori, el número de arcos descendentes que van a parar a cada uno de estos vértices es el mismo. De cada uno de los vértices del suelo de V solamente sale 1 arco ascendente. Si $h > 1$, entonces de cada uno de los vértices de la ladera de V salen ℓ arcos descendentes y 1 ascendente. Estos ℓ arcos descendentes siempre van a parar a ℓ vértices distintos. Finalmente, lo último que debemos saber es que dos arcos descendentes que salen cada uno de dos vértices distintos situados en un mismo nivel es imposible que vayan a parar a un mismo vértice.

$r = 0$	$r = 1$	
$c = 1$	$c = 1$	$c = 2$
		
$r = 2$		
$c = 1$	$c = 2$	$c \geq 3$
		

Cuadro 2.1: Posibles cráteres de un ℓ–volcán en función de r y c.

A partir de ahora, en lo que queda de capítulo, supondremos que todas las estructuras, aplicaciones, etc. están definidas sobre $\mathbb{F}_q$.

Para obtener más información sobre lo explicado en esta sección véase [Koh96, Fou01].

2.2. Cálculo de la ubicación de una curva elíptica en un ℓ–volcán

Sea V un ℓ–volcán y sea E una curva elíptica de V. Un camino descendente a partir de E en V es una secuencia de curvas elípticas (ℓ–isogenias)

$$E = E_0 \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_k} E_k$$

tal que E_k se halla en el nivel 0 de V y cada ℓ–isogenia φ_i es descendente. Entonces es fácil darse cuenta que la longitud k de este camino es precisamente el nivel de V donde se halla E.

Cuando E no tiene ℓ–isogenias descendentes, $k = 0$. Cuando E sí tiene ℓ–isogenias descendentes, $k > 0$. La curva elíptica E tiene ℓ–isogenias descendentes si y sólo si E tiene $\ell + 1$ isogenias de grado ℓ. Un procedimiento para calcular k en el caso en el que E sí que tiene ℓ–isogenias descendentes es el que a continuación explicamos.

Supongamos, inicialmente, que $k = 1$ y que $\varphi : E \to E'$ es una ℓ–isogenia descendente. Entonces o bien E' se halla en el suelo de V o bien E' se halla en su ladera. Si E' se halla en el suelo de V, entonces el valor de k es el correcto y hemos terminado. Si E' se halla en su ladera, entonces lo primero que tenemos que hacer es aumentar en una unidad k y lo segundo que tenemos que hacer es descender al nivel inferior donde se halla E'. Para descender al nivel inferior donde se halla E' lo que tenemos que hacer es escoger una curva elíptica E'' ℓ–isógena de E' tal que E'' no sea isomorfa a E, es decir, debemos de evitar la única ℓ–isogenia de E' que no es descendente. Entonces, una vez la tenemos, suponemos que E es E' y que E' es E'' y volvemos a comprobar si E' se halla o no en el suelo de V. Como es lógico, este proceso debemos repetirlo hasta que E' se halle en el suelo de V.

En pseudocódigo, el procedimiento que acabamos de explicar quedaría de la siguiente manera:

$k \leftarrow 1$

$\varphi : E \to E'$ ℓ–isogenia $\downarrow$
$S' \leftarrow$ IsógenAs(E', ℓ)
mientras $\#S' \neq 1$ **hacer**
$k \leftarrow k + 1$
si $S'[1] \not\simeq E$ **entonces**
$E \leftarrow E'$
$E' \leftarrow S'[1]$
sino
$E \leftarrow E'$
$E' \leftarrow S'[2]$
fin si
$S' \leftarrow$ IsógenAs(E', ℓ)
fin mientras

El único inconveniente que presenta este procedimiento es que hemos supuesto que E' se halla en el nivel inferior donde se halla E, y esto, a priori, sin tener ninguna otra información, es imposible saberlo. Entonces lo que tenemos que hacer para calcular k es aplicar el procedimiento anterior con 3 curvas elípticas ℓ–isógenas de E, ya que entonces, como mínimo, una de ellas se hallará en el nivel inferior donde se halla E, y por lo tanto, con ella, sí seremos capaces de calcular la longitud de un camino descendente a partir de E. Escogemos 3 porque en el peor de los casos E podría tener 2 isogenias de grado ℓ no descendentes. Entonces, teniendo en cuenta esto, un algoritmo para calcular el nivel de V donde se halla E es el siguiente:

algoritmo Nivel(E, ℓ, S) **devuelve** k

Entrada: Una curva elíptica ordinaria E definida sobre $\mathbb{F}_q$, un número primo ℓ tal que $\ell \nmid q$ y una secuencia S que contiene todas las curvas elípticas ℓ–isógenas de E sobre $\mathbb{F}_q$.

Salida: El nivel k de V donde se halla E, siendo V el volcán de ℓ–isogenias sobre $\mathbb{F}_q$ al que pertenece E.

$k \leftarrow 0$

si $\#S = \ell + 1$ **entonces**
$k \leftarrow k + 1$
$i \leftarrow 0$
repetir
$i \leftarrow i + 1$
$E_i \leftarrow E$
$E'_i \leftarrow S[i]$
$S'_i \leftarrow \text{IsógenAs}(E'_i, \ell)$
$suelo \leftarrow \#S'_i = 1$
hasta $i = 3 \vee suelo$
mientras $\neg suelo$ **hacer**
$k \leftarrow k + 1$
$i \leftarrow 0$
repetir
$i \leftarrow i + 1$
si $S'_i[1] \not\cong E_i$ **entonces**
$E_i \leftarrow E'_i$
$E'_i \leftarrow S'_i[1]$
sino
$E_i \leftarrow E'_i$
$E'_i \leftarrow S'_i[2]$
fin si
$S'_i \leftarrow \text{IsógenAs}(E'_i, \ell)$
$suelo \leftarrow \#S'_i = 1$
hasta $i = 3 \vee suelo$
fin mientras
fin si
devolver k
fin algoritmo

Supongamos, finalmente, que E' es una curva elíptica ℓ–isógena de E y que $k > 0$. Entonces un algoritmo para saber si E' se halla en el nivel $k - 1$

es el que a continuación damos.

algoritmo NIVELINFERIOR(E, ℓ, k, E', S') **devuelve** t

Entrada:

- Una curva elíptica ordinaria E definida sobre $\mathbb{F}_q$.
- Un número primo ℓ tal que $\ell \nmid q$.

$$V = \ell\text{–volcán sobre } \mathbb{F}_q \text{ al que pertenece } E$$

- El nivel $k > 0$ de V donde se halla E.
- Una curva elíptica E' ℓ–isógena a E sobre $\mathbb{F}_q$.
- Una secuencia S' que contiene todas las curvas elípticas ℓ–isógenas de E' sobre $\mathbb{F}_q$.

Salida:

- $t = \begin{cases} \textbf{cierto} & \text{si } E' \text{ se halla en el nivel } k-1 \text{ de } V, \\ \textbf{falso} & \text{en caso contrario.} \end{cases}$

mientras $k \neq 1$ **hacer**
  $k \leftarrow k - 1$
  si $S'[1] \not\simeq E$ **entonces**
    $E \leftarrow E'$
    $E' \leftarrow S'[1]$
  sino
    $E \leftarrow E'$
    $E' \leftarrow S'[2]$
  fin si
  $S' \leftarrow$ ISÓGENAS(E', ℓ)
fin mientras
$t \leftarrow \#S' = 1$
devolver t

fin algoritmo

2.3. Cálculo de las características principales de un ℓ–volcán

Sea V un ℓ–volcán y sea E una curva elíptica de V. Un procedimiento para calcular la altura h de V a partir de E es el que a continuación explicamos. Supongamos, inicialmente, que h es igual al nivel de V donde se halla E. Entonces debemos buscar una curva elíptica E' ℓ–isógena de E o que bien se halle en el nivel h o que bien se halle en el nivel $h+1$. Si no la encontramos, entonces E se halla en el cráter de V, por lo que el valor de h es el correcto y hemos terminado (en este caso sabemos que E se halla en el cráter de V porque o bien E no tiene ℓ–isogenias o porque o bien todas ellas son descendentes). Si la encontramos y E' se halla en el nivel h, entonces E y E' se hallan en el cráter de V, por lo que al igual que en el caso anterior, h es el valor que estábamos buscando y hemos terminado (en este caso sabemos que E y E' se hallan en el cráter de V porque la ℓ–isogenia que existe entre ambas es horizontal). Finalmente, si E' se halla en el nivel $h+1$, entonces lo primero que tenemos que hacer es aumentar en una unidad h y suponer que E es E', es decir, debemos ascender un nivel, y lo segundo que tenemos que hacer es volver a buscar una curva elíptica E' ℓ–isógena de E tal que E' o bien se halle en el nivel h o bien se halle en el nivel $h+1$, es decir, debemos volver a comprobar si hemos terminado o si por el contrario debemos volver a ascender. Como es lógico, este proceso debemos repetirlo hasta que E se halle en el cráter de V. En pseudocódigo, el procedimiento que acabamos de explicar quedaría de la siguiente manera:

$S \leftarrow$ Isógenas(E, ℓ)
$h \leftarrow$ Nivel(E, ℓ, S)
$final \leftarrow$ **falso**
repetir
  $i \leftarrow 0$
  $encontrada \leftarrow$ **falso**

mientras $i < \#S \wedge \neg encontrada$ **hacer**

$i \leftarrow i + 1$

$E' \leftarrow S[i]$

$U \leftarrow$ IsógenAs(E', ℓ)

$t \leftarrow$ Nivel(E', ℓ, U)

$encontrada \leftarrow t \geq h$

fin mientras

si $\neg encontrada$ **entonces**

$final \leftarrow$ **cierto**

sino si $t = h$ **entonces**

$final \leftarrow$ **cierto**

sino

$E \leftarrow E'$

$S \leftarrow U$

$h \leftarrow h + 1$ /* $h \leftarrow t$ */

fin si

hasta $final$

Sean, ahora, c el número de vértices que hay en el cráter de V y r el número de arcos horizontales que salen de cada uno de ellos. Lo primero que tenemos que hacer para calcular c y r es mirar en qué caso del procedimiento anterior hemos detectado el cráter de V. Si lo hemos hecho en el caso en el que E' no existe, entonces $c = 1$ y $r = 0$. Si lo hemos hecho, en cambio, en el caso en el que E' sí existe, entonces $c \geq 1$ y r es igual a 1 o es igual a 2. Para saber si r es igual a 1 o es igual a 2 lo que tenemos que hacer es ver si existe otra curva elíptica E^* ℓ–isógena de E situada en su mismo nivel. Si no existe, entonces $r = 1$. Si existe, entonces $r = 2$. Dependiendo de cada caso, los posibles valores de c son los siguientes:

- $r = 1$
  - $c = 1 \iff E' \simeq E$
  - $c = 2 \iff E' \not\simeq E$

- $r = 2$
  - $c = 1 \iff E^* \simeq E' \simeq E$
  - $c = 2 \iff E^* \simeq E' \not\simeq E$
  - $c \geq 3 \iff E^* \not\simeq E' \not\simeq E \not\simeq E^*$

Vemos, entonces, que para el único caso para el cual no tenemos el valor de c es para el caso en el que $r = 2$ y E, E' y E^* no son isomorfas entre sí. Para calcular c en este caso lo primero que tenemos que hacer es suponer que $c = 3$, ya que 3, inicialmente, son los vértices que ya conocemos, a saber, E, E' y E^*. Entonces, lo siguiente y último que tenemos que hacer es recorrer uno a uno, y sin repetir, el resto de vértices del cráter de V e ir aumentando el valor de c a medida que los vayamos recorriendo. Dicho recorrido, en pseudocódigo, quedaría de la siguiente manera:

```
c ← 3
/* U es la secuencia que contiene todas las curvas elípticas ℓ–isógenas de
E' */
mientras ∄E'' ∈ U tal que E'' ≃ E* hacer
    c ← c + 1
    i ← 0
    encontrada ← falso
    repetir
        i ← i + 1
        E'' ← U[i]
        si E'' ≄ E entonces
            S ← IsógenasDeGrado(E'', ℓ)
            si h = 0 entonces
                encontrada ← cierto
            sino si ¬NivelInferior(E', ℓ, h, E'', S) entonces
                encontrada ← cierto
            fin si
```

fin si

hasta *encontrada*

$E \leftarrow E'$

$E' \leftarrow E''$

$U \leftarrow S$

fin mientras

Sean e_1 y e_2 dos elementos de $\mathbb{F}_q$ y sea ElementoAEntero el siguiente algoritmo:

algoritmo ElementoAEntero(e) **devuelve** i

Entrada: Un elemento e de $\mathbb{F}_q$.

$$\mathbb{F}_q = \mathbb{F}_{p^n} = \frac{\mathbb{F}_p[w]}{(f(w))}$$

(p primo y $f(w) \in \mathbb{F}_p[w]$ irreducible de grado n)

$$e = e_{n-1}w^{n-1} + e_{n-2}w^{n-2} + \cdots + e_1 w + e_0$$

Salida: Un entero $i \in [0, q-1]$ que representa a e.

para $k \leftarrow 0$ **hasta** $n-1$ **hacer**

Obtener el entero $i_k \in [0, p-1]$ que representa a e_k

fin para

$i \leftarrow i_{n-1}p^{n-1} + i_{n-2}p^{n-2} + \cdots + i_1 p + i_0$

devolver i

fin algoritmo

Entonces $e_1 < e_2$ si y sólo si

$$\text{ElementoAEntero}(e_1) < \text{ElementoAEntero}(e_2).$$

Sean V_1 y V_2 dos ℓ–volcanes y sean u_1 y u_2 los vértices de los cráteres, respectivamente, de V_1 y V_2 con los j–invariantes más pequeños. Entonces si $\mathcal{E}_1$ es una curva elíptica de u_1 y $\mathcal{E}_2$ es una curva elíptica de u_2, $V_1 = V_2$ si y sólo si $\mathcal{E}_1 \simeq \mathcal{E}_2$.

Un algoritmo que recoge todo lo que hemos explicado en esta sección es el siguiente:

algoritmo $\textsc{Info}(E, \ell)$ **devuelve** $h, r, c, \mathcal{E}$

Entrada: Una curva elíptica ordinaria E definida sobre $\mathbb{F}_q$ y un número primo ℓ tal que $\ell \nmid q$.

Salida:

$$V = \ell\text{–volcán sobre } \mathbb{F}_q \text{ al que pertenece } E$$

- La altura h de V.
- El número de arcos horizontales r que salen de cada uno de los vértices del cráter de V.
- El número de vértices c que hay en el cráter de V.
- Una curva elíptica $\mathcal{E}$ del vértice del cráter de V con el j–invariante más pequeño.

```
/* EAE = ElementoAEntero */
S ← Isógenas(E, ℓ)
h ← Nivel(E, ℓ, S)
final ← falso
repetir
  i ← 0
  encontrada ← falso
  mientras i < #S ∧ ¬encontrada hacer
    i ← i + 1
    E' ← S[i]
    U ← Isógenas(E', ℓ)
    t ← Nivel(E', ℓ, U)
    encontrada ← t ≥ h
  fin mientras
  si ¬encontrada entonces
```

$r \leftarrow 0$

$c \leftarrow 1$

$\mathcal{E} \leftarrow E$

$final \leftarrow$ **cierto**

sino si $t = h$ **entonces**

$encontrada \leftarrow$ **falso**

mientras $i < \#S \wedge \neg encontrada$ **hacer**

$i \leftarrow i + 1$

$E^* \leftarrow S[i]$

si $h = 0$ **entonces**

$encontrada \leftarrow$ **cierto**

sino si $\neg$NivelInferior$(E, \ell, h, E^*,$ Isógenas$(E^*, \ell))$ **entonces**

$encontrada \leftarrow$ **cierto**

fin si

fin mientras

si $\neg encontrada$ **entonces**

$r \leftarrow 1$

si $E' \simeq E$ **entonces**

$c \leftarrow 1$

$\mathcal{E} \leftarrow E$

sino

$c \leftarrow 2$

si $\mathrm{EAE}(j(E)) < \mathrm{EAE}(j(E'))$ **entonces**

$\mathcal{E} \leftarrow E$

sino

$\mathcal{E} \leftarrow E'$

fin si

fin si

sino

$r \leftarrow 2$

si $E^* \simeq E'$ **entonces**

si $E' \simeq E$ **entonces**
$c \leftarrow 1$
$\mathcal{E} \leftarrow E$
sino
$c \leftarrow 2$
si $\mathrm{EAE}(j(E)) < \mathrm{EAE}(j(E'))$ **entonces**
$\mathcal{E} \leftarrow E$
sino
$\mathcal{E} \leftarrow E'$
fin si
fin si
sino
$c \leftarrow 3$
si $\mathrm{EAE}(j(E)) < \mathrm{EAE}(j(E'))$ **entonces**
$\mathcal{E} \leftarrow E$
sino
$\mathcal{E} \leftarrow E'$
fin si
si $\mathrm{EAE}(j(E^*)) < \mathrm{EAE}(j(\mathcal{E}))$ **entonces**
$\mathcal{E} \leftarrow E^*$
fin si
mientras $\nexists E'' \in U$ tal que $E'' \simeq E^*$ **hacer**
$c \leftarrow c + 1$
$i \leftarrow 0$
$encontrada \leftarrow$ **falso**
repetir
$i \leftarrow i + 1$
$E'' \leftarrow U[i]$
si $E'' \not\simeq E$ **entonces**
$S \leftarrow \textsc{Isógenas}(E'', \ell)$
si $h = 0$ **entonces**

$encontrada \leftarrow$ **cierto**

sino si $\neg$NIVELINFERIOR(E', ℓ, h, E'', S) **entonces**

$encontrada \leftarrow$ **cierto**

fin si

fin si

hasta $encontrada$

si $\mathrm{EAE}(j(E'')) < \mathrm{EAE}(j(\mathcal{E}))$ **entonces**

$\mathcal{E} \leftarrow E''$

fin si

$E \leftarrow E'$

$E' \leftarrow E''$

$U \leftarrow S$

fin mientras

fin si

fin si

$final \leftarrow$ **cierto**

sino

$E \leftarrow E'$

$S \leftarrow U$

$h \leftarrow h + 1$

fin si

hasta $final$

devolver $h, r, c, \mathcal{E}$

fin algoritmo

Capítulo 3

Resultados y conclusiones

En este capítulo damos los resultados que hemos obtenido a partir de la implementación de los algoritmos de los dos capítulos anteriores así como las conclusiones a las que hemos llegado después de realizar este trabajo. La implementación de los algoritmos la hemos realizado con el paquete matemático MAGMA [BCP97]. No damos la implementación porque nuestro pseudocódigo y el código de MAGMA son casi idénticos.

3.1. Resultados

En esta sección, si V es un ℓ–volcán, denotamos con h a su altura, con r al número de arcos horizontales que salen de cada uno de los vértices de su cráter y con c al tamaño de su cráter.

Una vez comentado esto, lo primero que vamos a ver en esta sección son algunos ejemplos de ℓ–volcanes. En dichos ejemplos, los vértices de cada ℓ–volcán están numerados del 1 al n, siendo n el número de vértices de cada ℓ–volcán. Para cada vértice damos una curva elíptica

$$E : y^2 = x^3 + ax + b$$

y $j(E)$. A la curva elíptica E la denotamos por $[a, b]$. Una vez comentado esto, los ejemplos son los que siguen.

Ejemplo 1 (figura 3.1)

- $\mathbb{F}_{523}$
- $\ell = 11$
- $(h, r, c) = (0, 0, 1)$

Ejemplo 2 (figura 3.2)

- $\mathbb{F}_{101}$
- $\ell = 5$
- $(h, r, c) = (0, 1, 1)$

Ejemplo 3 (figura 3.3)

- $\mathbb{F}_{103}$
- $\ell = 3$
- $(h, r, c) = (0, 1, 2)$

Ejemplo 4 (figura 3.4)

- $\mathbb{F}_{101}$
- $\ell = 5$
- $(h, r, c) = (0, 2, 1)$

Ejemplo 5 (figura 3.5)

- $\mathbb{F}_{109}$
- $\ell = 7$
- $(h, r, c) = (0, 2, 2)$

Ejemplo 6 (figura 3.6)

- $\mathbb{F}_{691}$
- $\ell = 5$
- $(h, r, c) = (0, 2, 4)$

Ejemplo 7 (figura 3.7)

- $\mathbb{F}_{10657}$
- $\ell = 2$
- $(h, r, c) = (3, 0, 1)$

Ejemplo 8 (figura 3.8)

- $\mathbb{F}_{20021}$
- $\ell = 11$
- $(h, r, c) = (1, 0, 1)$

Ejemplo 9 (figura 3.9)

- $\mathbb{F}_{12007}$
- $\ell = 3$
- $(h, r, c) = (2, 1, 1)$

Ejemplo 10 (figura 3.10)

- $\mathbb{F}_{1009}$
- $\ell = 3$
- $(h, r, c) = (3, 1, 1)$

Ejemplo 11 (figura 3.11)

- $\mathbb{F}_{6067}$

- $\ell = 3$
- $(h, r, c) = (2, 1, 2)$

Ejemplo 12 (figura 3.12)

- $\mathbb{F}_{541}$
- $\ell = 2$
- $(h, r, c) = (2, 2, 1)$

Ejemplo 13 (figura 3.13)

- $\mathbb{F}_{20021}$
- $\ell = 5$
- $(h, r, c) = (1, 2, 1)$

Ejemplo 14 (figura 3.14)

- $\mathbb{F}_{5233}$
- $\ell = 7$
- $(h, r, c) = (1, 2, 1)$

Ejemplo 15 (figura 3.15)

- $\mathbb{F}_{659}$
- $\ell = 5$
- $(h, r, c) = (1, 2, 2)$

Ejemplo 16 (figura 3.16)

- $\mathbb{F}_{10657}$
- $\ell = 3$

- $(h, r, c) = (1, 2, 5)$

Sea A el conjunto de clases de isomorfía sobre $\mathbb{F}_q = \mathbb{F}_{691}$ de curvas elípticas ordinarias con cardinal

$$m = q + 1 - t = 700.$$

Entonces, como

$$t = q + 1 - m = 691 + 1 - 700 = -8,$$

$$t^2 - 4q = (-8)^2 - 4 \cdot 691 = (2 \cdot 3 \cdot 5)^2(-3)$$

y $-3 \equiv 1 \pmod 4$, los anillos de endomorfismos de las curvas elípticas de A son isomorfos a órdenes del cuerpo cuadrático imaginario K de discriminante $d_K = -3$. Dichos órdenes, tal y como sabemos, están comprendidos entre los órdenes $\mathbb{Z}[\pi]$ y O_K. Como el discriminante de $\mathbb{Z}[\pi]$ es

$$d_\pi = t^2 - 4q = g^2 d_K = (2 \cdot 3 \cdot 5)^2(-3),$$

vemos que en total hay 8 órdenes:

$$\begin{array}{ccc} & O_K & \\ \mathbb{Z} + 2O_K & \mathbb{Z} + 3O_K & \mathbb{Z} + 5O_K \\ \mathbb{Z} + (2 \cdot 3)O_K & \mathbb{Z} + (2 \cdot 5)O_K & \mathbb{Z} + (3 \cdot 5)O_K \\ & \mathbb{Z}[\pi] = \mathbb{Z} + (2 \cdot 3 \cdot 5)O_K & \end{array}$$

Si clasificamos las 38 clases de isomorfía que hay en A en función de estos 8 órdenes lo que obtenemos es el cuadro 3.1 (en dicho cuadro, para cada clase de isomorfía damos una curva elíptica $[a, b]$ y su j–invariante). Como $g = 2 \cdot 3 \cdot 5$, vemos que la altura de los ℓ–volcanes sobre $\mathbb{F}_{691}$ a los que pertenecen las curvas elípticas de A o bien es 1 o bien es 0, siendo 1 si $\ell \leq 5$ o 0 si $\ell > 5$. Los ℓ–volcanes para $\ell = 2$, 3, 5 y 7 son los que damos, respectivamente, en las figuras 3.17, 3.18, 3.19 y 3.20. Notemos que para

cada ℓ, el número de arcos horizontales que salen de cada uno de los vértices de los cráteres de los ℓ–volcanes es el mismo. Esto es así porque si O es un orden de K de discriminante $D = f^2 d_K$ tal que $\ell \nmid f$, O se identifica con el cráter de un ℓ–volcán V y

$$\left(\frac{D}{\ell}\right) = \left(\frac{f^2}{\ell}\right)\left(\frac{d_K}{\ell}\right) = \left(\frac{d_K}{\ell}\right),$$

por lo que el número de arcos horizontales que salen de cada uno de los vértices del cráter de V es igual a

$$\left(\frac{D}{\ell}\right) + 1 = \left(\frac{d_K}{\ell}\right) + 1,$$

es decir, dicho valor solamente depende de

$$\left(\frac{d_K}{\ell}\right),$$

valor el cuál es idéntico para todos los ℓ–volcanes cuyos niveles se identifican con órdenes de K.

En los cuadros 3.2, 3.3, 3.4, 3.5 y 3.6 damos para $\ell = 2$, 3, 5, 7 y 11 el número de ℓ–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c. Lo primero que podemos observar en estos cuadros es que el número de ℓ–volcanes en función de h, h y r y h, r y c siempre es un número par. Esto es así por lo que a continuación explicamos. Sea E una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ tal que $\#E(\mathbb{F}_q) = q + 1 - t$. Entonces existe una única (salvo isomorfismo) curva elíptica ordinaria E' definida sobre $\mathbb{F}_q$ tal que $\#E'(\mathbb{F}_q) = q + 1 + t$ y $j(E') = j(E)$. Tal curva elíptica E' es isomorfa a E sobre $\mathbb{F}_{q^2}$ (E y E' no son isomorfas sobre $\mathbb{F}_q$ porque $\#E(\mathbb{F}_q) \neq \#E'(\mathbb{F}_q)$). Si V y V' son, respectivamente, los ℓ–volcanes sobre $\mathbb{F}_q$ a los que pertenecen E y E', entonces la única diferencia entre V y V' es que las curvas elípticas de V tienen cardinal $q + 1 - t$ y las de V' tienen cardinal $q + 1 + t$ (si para cada vértice de V y V' sólo diéramos su j–invariante, entonces veríamos que $V = V'$; sobre $\mathbb{F}_{q^2}$, $V = V'$). Entonces, teniendo en cuenta esto, vemos que

para cada ℓ–volcán sobre $\mathbb{F}_q$ con cardinal $q+1-t$ existe otro con cardinal $q+1+t$ con los mismos valores h, r y c. Este es el motivo por el cual el número de ℓ–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c siempre es un número par.

Lo siguiente que podemos observar es que cuanto mayor es h, menos ℓ–volcanes hay. También podemos observar que para una determinada ℓ no todos los tipos de cráteres se dan, siendo los que siempre se dan el $(r=0, c=1)$ y el $(r=2, c>2)$. El tipo de cráter que más se da es el $(r=0, c=1)$. El segundo tipo que más se da, si es que se da, es el $(r=1, c=2)$. El tercer tipo que más se da es el $(r=2, c>2)$. Los tipos $(r=1, c=1)$, $(r=2, c=1)$ y $(r=2, c=2)$ casi no se dan.

Observemos, finalmente, que para $\ell=3$ y $\ell=7$ todos los ℓ–volcanes tienen altura 0 y $r \neq 1$, lo cual es equivalente a decir que no existe ninguna curva elíptica con cardinal $7019+1-t$ tal que $t^2-4\cdot 7019$ sea divisible por 3 o por 7.

Si V es un volcán de ℓ–isogenias sobre $\mathbb{F}_q$ de altura mayor que 0, entonces al considerarlo sobre $\mathbb{F}_{q^\ell}$ su altura aumenta en una unidad (para una demostración véase [Fou01]). Un ejemplo de esta característica es el que damos en las figuras 3.21 y 3.22. Notemos que la estructura del 3–volcán sobre $\mathbb{F}_{67}$ de la figura 3.21 se mantiene intacta sobre $\mathbb{F}_{67^3}$ (figura 3.22).

3.2. Conclusiones

Antes de realizar este trabajo ya se habían realizado otros sobre volcanes de ℓ–isogenias. Concretamente se habían realizado implementaciones para $\ell=2$, 3, 5 y 7. En dichos trabajos, los núcleos de las ℓ–isogenias únicamente estaban formados por puntos $\mathbb{F}_q$–racionales. Éste, pues, iba a ser el primer trabajo en el que los núcleos de las ℓ–isogenias no iban a estar exclusivamente formados por puntos $\mathbb{F}_q$–racionales. Aunque en un primer momento sólo se iba a tratar el caso $\ell=5$, al final, viendo que los algoritmos eran prácticamente los mismos, se decidió que fuera para cualquier ℓ. También

se decidió, al igual que en los trabajos precedentes, que las ℓ–isogenias se calculasen a partir de los polinomios de ℓ–división. Entonces, teniendo en cuenta esto y viendo lo que hemos hecho, creemos que los objetivos se han cumplido satisfactoriamente.

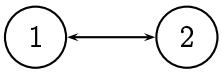
Aunque los algoritmos de este documento son correctos, éstos presentan dos problemas. El primero de ellos lo encontramos en el algoritmo ISÓGENAS ya que en él, en determinadas ocasiones, para calcular raíces del polinomio de ℓ–división, debemos de subir a extensiones de $\mathbb{F}_q$, por lo que su tiempo de ejecución aumenta considerablemente. Lo ideal, en este caso, sería poder trabajar siempre en $\mathbb{F}_q$. El segundo problema lo tenemos en que siempre calculamos todas las curvas elípticas ℓ–isógenas de una curva elíptica dada cuando a lo mejor solamente necesitamos unas pocas. En este caso, lo ideal sería poder ir calculándolas una a una a medida que las fuéramos necesitando. Entonces, una solución a estos problemas sería utilizar los polinomios modulares [BSS00] ya que si E es una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ de j–invariante $j \neq 0, 1728$ y $\phi_\ell(X, Y)$ es el polinomio ℓ–modular sobre $\mathbb{F}_q[X, Y]$, entonces las raíces de $\phi_\ell(X, j)$ son los j–invariantes de las curvas elípticas ℓ–isógenas de E sobre $\mathbb{F}_q$. Los coeficientes de estos polinomios primero se calculan sobre $\mathbb{Z}$ y después se consideran sobre $\mathbb{F}_q$. Y he aquí el principal problema de estos polinomios, que cuanto mayor es ℓ más grandes son sus coeficientes sobre $\mathbb{Z}$. Por lo tanto, como futuro trabajo, estaría bien implementar nuestros algoritmos con estos polinomios y ver que implementación es mejor.

1	$[385, 276]$	127

Figura 3.1: Volcán de ℓ–isogenias del ejemplo 1.

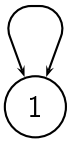
1	$[22, 57]$	7

Figura 3.2: Volcán de ℓ–isogenias del ejemplo 2.



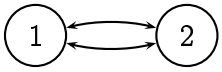
1	$[94, 18]$	63
2	$[63, 76]$	44

Figura 3.3: Volcán de ℓ–isogenias del ejemplo 3.



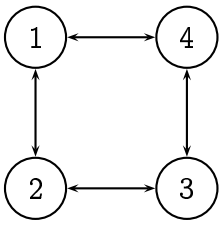
1	$[90, 22]$	24

Figura 3.4: Volcán de ℓ–isogenias del ejemplo 4.



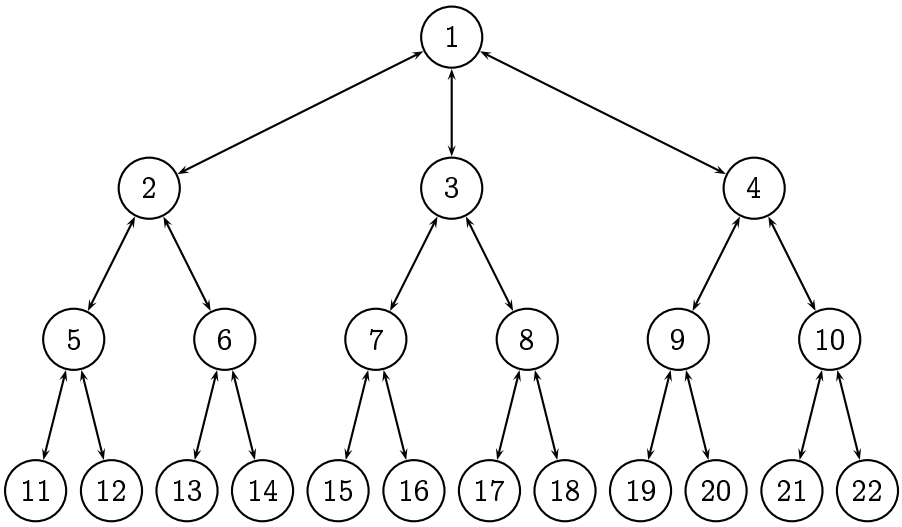
1	$[101, 16]$	1
2	$[12, 57]$	54

Figura 3.5: Volcán de ℓ–isogenias del ejemplo 5.



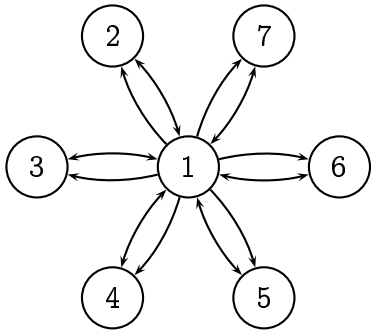
1	$[172, 347]$	306
2	$[466, 258]$	594
3	$[152, 513]$	631
4	$[117, 320]$	575

Figura 3.6: Volcán de ℓ–isogenias del ejemplo 6.



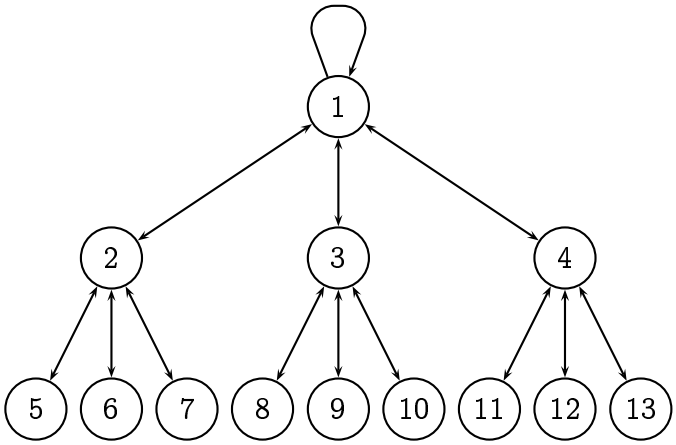
1	$[7894, 7616]$	9416	2	$[7934, 7308]$	8267	3	$[4936, 93]$	1318
4	$[1338, 5033]$	980	5	$[6322, 301]$	5999	6	$[10186, 5260]$	4874
7	$[2357, 6620]$	8380	8	$[2815, 2316]$	5400	9	$[333, 6972]$	155
10	$[4017, 8294]$	6270	11	$[2786, 768]$	5830	12	$[5380, 9637]$	2071
13	$[2786, 867]$	5925	14	$[333, 6465]$	4938	15	$[7817, 8953]$	8142
16	$[8918, 6392]$	8019	17	$[4433, 6045]$	2078	18	$[9889, 2318]$	1375
19	$[2162, 10310]$	6999	20	$[3738, 10503]$	691	21	$[10468, 6863]$	9262
22	$[8459, 5289]$	7559						

Figura 3.7: Volcán de ℓ–isogenias del ejemplo 7.



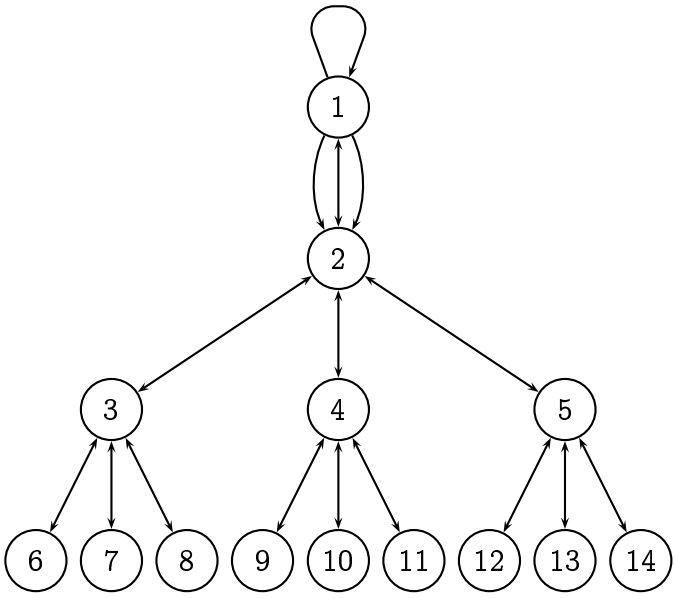
1	$[1, 0]$	1728	2	$[15629, 10182]$	17918
3	$[645, 16796]$	16593	4	$[4743, 2070]$	19300
5	$[2247, 4602]$	10921	6	$[5997, 5937]$	4551
7	$[18107, 17022]$	9195			

Figura 3.8: Volcán de ℓ–isogenias del ejemplo 8.



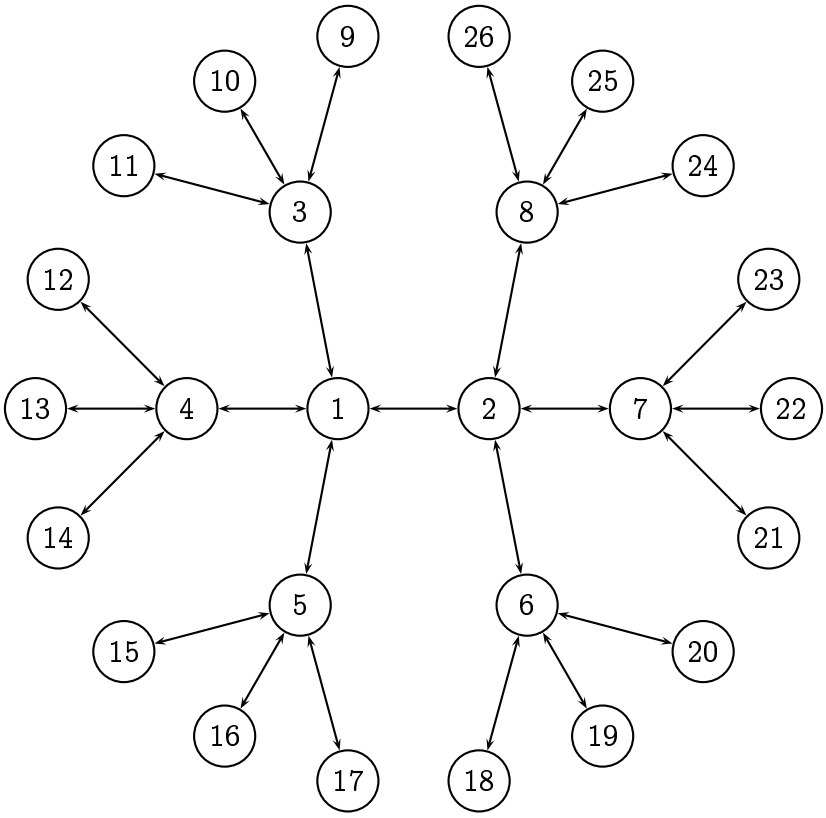
1	$[7216, 9582]$	5972	2	$[6935, 2610]$	5464
3	$[1844, 6750]$	3323	4	$[4113, 11150]$	7632
5	$[10912, 9789]$	1879	6	$[5542, 2495]$	9519
7	$[5604, 3926]$	5703	8	$[155, 9938]$	7220
9	$[1752, 2251]$	1009	10	$[745, 8737]$	11796
11	$[10111, 3525]$	11261	12	$[11345, 9417]$	10837
13	$[3694, 10908]$	6148			

Figura 3.9: Volcán de ℓ–isogenias del ejemplo 9.



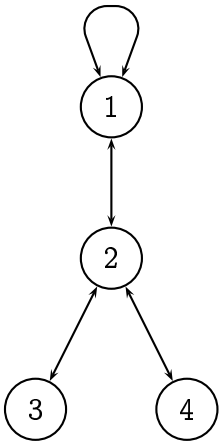
1	$[0, 565]$	0	2	$[588, 676]$	611
3	$[909, 413]$	433	4	$[846, 354]$	110
5	$[214, 451]$	652	6	$[92, 879]$	366
7	$[39, 547]$	153	8	$[345, 805]$	65
9	$[236, 487]$	705	10	$[747, 802]$	760
11	$[255, 132]$	944	12	$[680, 22]$	217
13	$[542, 66]$	410	14	$[405, 698]$	143

Figura 3.10: Volcán de ℓ–isogenias del ejemplo 10.



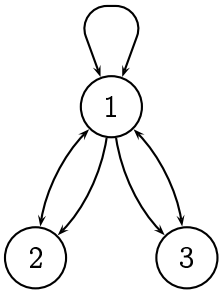
1	$[2102, 3176]$	1621	2	$[5418, 5615]$	3184	3	$[5484, 3234]$	3923
4	$[2881, 1263]$	2275	5	$[5043, 3193]$	253	6	$[272, 2399]$	4081
7	$[4125, 3425]$	5543	8	$[1371, 5354]$	5032	9	$[1954, 1250]$	4654
10	$[3324, 1129]$	1644	11	$[6034, 1069]$	2653	12	$[3960, 3961]$	973
13	$[1467, 5998]$	2586	14	$[5645, 730]$	4923	15	$[2329, 4309]$	4753
16	$[3842, 1226]$	879	17	$[4499, 4303]$	4517	18	$[1587, 3390]$	1911
19	$[5256, 1711]$	1139	20	$[1837, 5561]$	1979	21	$[146, 5526]$	3233
22	$[1702, 3332]$	1086	23	$[2866, 528]$	3703	24	$[5914, 4334]$	4237
25	$[5288, 964]$	6032	26	$[4856, 2505]$	5095			

Figura 3.11: Volcán de ℓ–isogenias del ejemplo 11.



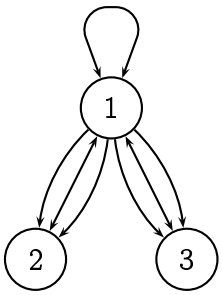
1	$[214, 113]$	412
2	$[392, 490]$	266
3	$[424, 58]$	194
4	$[503, 164]$	265

Figura 3.12: Volcán de ℓ–isogenias del ejemplo 12.



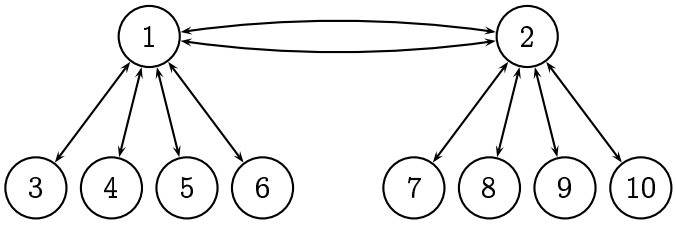
1	$[1, 0]$	1728
2	$[6243, 1437]$	3484
3	$[14100, 3832]$	2640

Figura 3.13: Volcán de ℓ–isogenias del ejemplo 13.



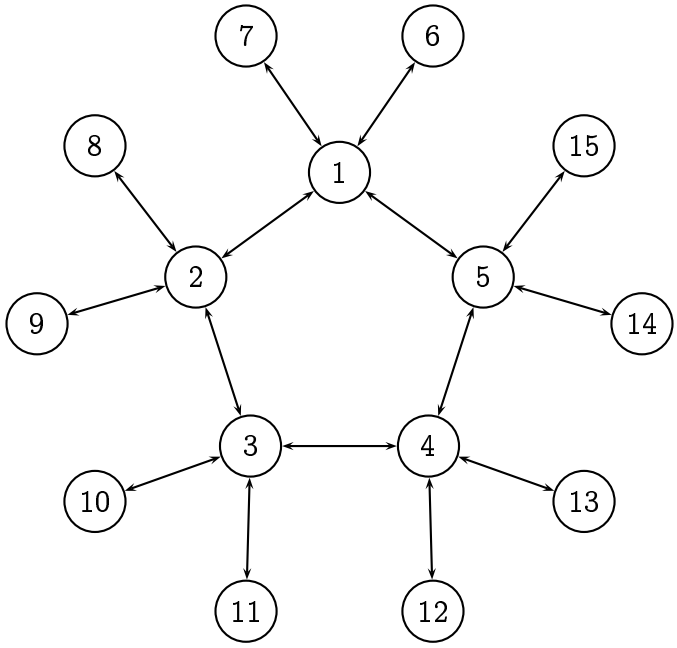
1	$[0, 1198]$	0
2	$[9, 4682]$	474
3	$[2993, 1723]$	4054

Figura 3.14: Volcán de ℓ–isogenias del ejemplo 14.



1	$[446, 426]$	427	2	$[335, 197]$	593
3	$[187, 354]$	370	4	$[188, 316]$	58
5	$[392, 555]$	153	6	$[430, 44]$	384
7	$[566, 558]$	273	8	$[357, 210]$	179
9	$[357, 276]$	471	10	$[556, 131]$	492

Figura 3.15: Volcán de ℓ–isogenias del ejemplo 15.



1	$[5195, 1686]$	2340	2	$[8425, 9201]$	3594	3	$[8815, 7355]$	6110
4	$[3783, 4252]$	4012	5	$[8948, 3694]$	4380	6	$[2179, 1210]$	871
7	$[1205, 5149]$	2990	8	$[5962, 5345]$	7639	9	$[5703, 4983]$	2234
10	$[8059, 4422]$	1620	11	$[3565, 10439]$	10540	12	$[4026, 881]$	4845
13	$[4567, 9036]$	1403	14	$[3241, 10226]$	5245	15	$[364, 9019]$	8376

Figura 3.16: Volcán de ℓ–isogenias del ejemplo 16.

- O_K
  - $[0, 525]$ (0)
- $\mathbb{Z} + 2O_K$
  - $[565, 394]$ (102)
- $\mathbb{Z} + 3O_K$
  - $[644, 94]$ (53)
- $\mathbb{Z} + 5O_K$
  - $[595, 406]$ (428) * $[37, 243]$ (651)
- $\mathbb{Z} + (2 \cdot 3)O_K$
  - $[414, 420]$ (52) * $[447, 488]$ (440) * $[513, 253]$ (460)
- $\mathbb{Z} + (2 \cdot 5)O_K$
  - $[400, 582]$ (83) * $[245, 487]$ (87) * $[135, 64]$ (181)
  - $[595, 179]$ (345) * $[6, 634]$ (540) * $[167, 192]$ (686)
- $\mathbb{Z} + (3 \cdot 5)O_K$
  - $[615, 152]$ (170) * $[569, 471]$ (497) * $[143, 248]$ (619)
  - $[465, 148]$ (635) * $[680, 17]$ (647) * $[379, 513]$ (674)
- $\mathbb{Z}[\pi] = \mathbb{Z} + (2 \cdot 3 \cdot 5)O_K$
  - $[603, 149]$ (61) * $[221, 249]$ (91) * $[294, 385]$ (98)
  - $[658, 568]$ (101) * $[459, 151]$ (118) * $[86, 311]$ (143)
  - $[139, 190]$ (161) * $[587, 319]$ (172) * $[589, 413]$ (192)
  - $[386, 132]$ (289) * $[369, 259]$ (316) * $[535, 471]$ (317)
  - $[245, 432]$ (406) * $[527, 329]$ (468) * $[133, 418]$ (573)
  - $[34, 573]$ (610) * $[245, 19]$ (654) * $[371, 60]$ (676)

Cuadro 3.1: Distribución de las clases de isomorfía sobre $\mathbb{F}_{691}$ con cardinal 700 en función de los órdenes.

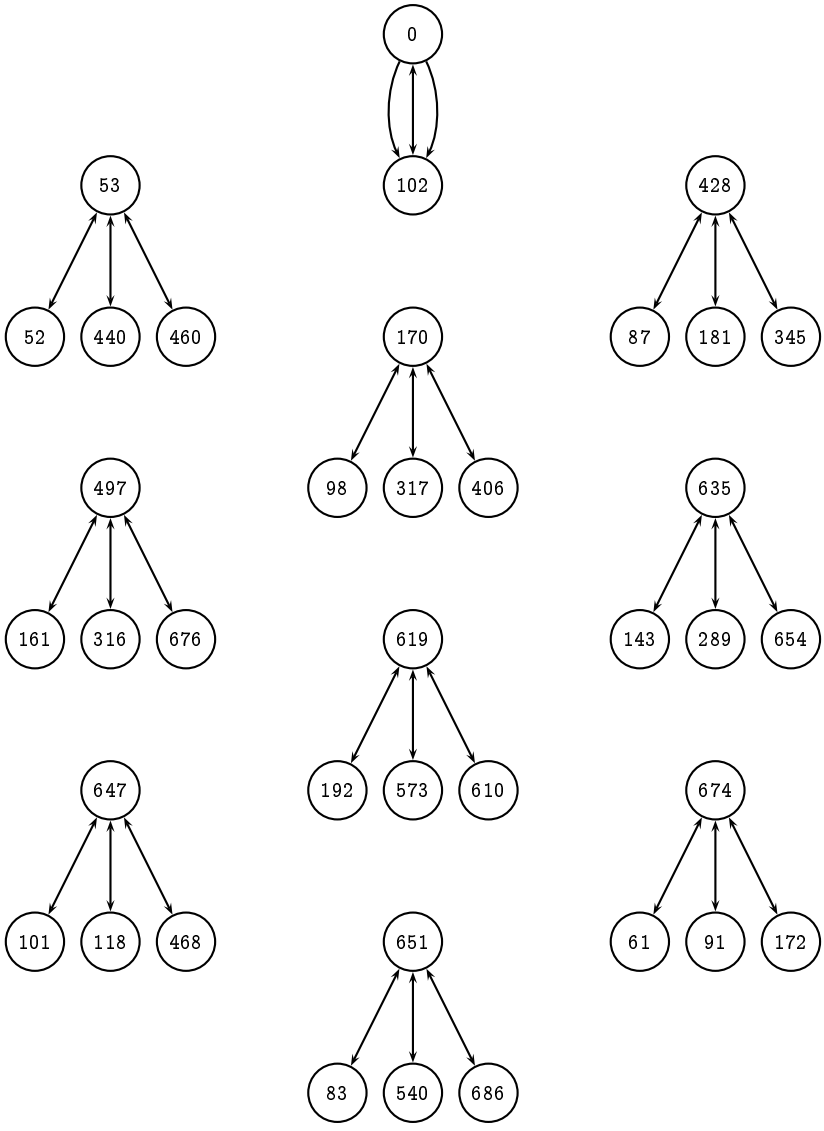


Figura 3.17: Volcanes de 2–isogenias sobre $\mathbb{F}_{691}$ con cardinal 700.

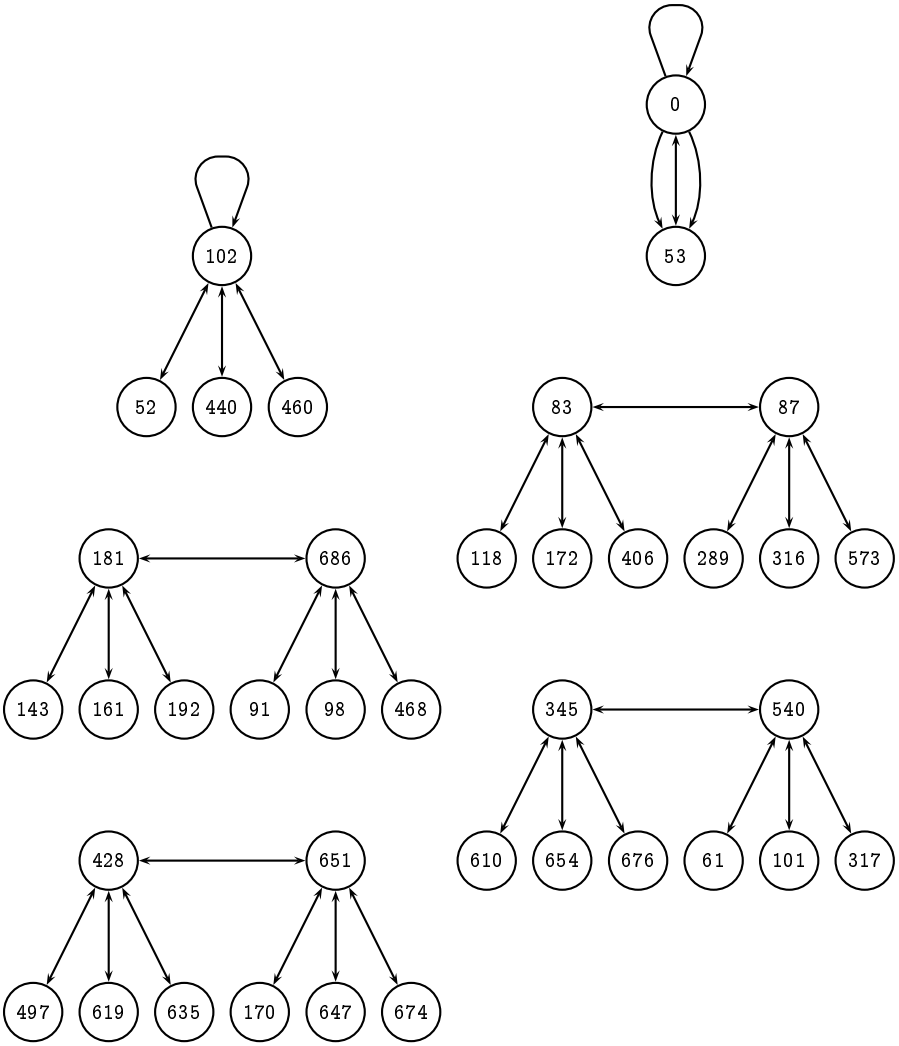


Figura 3.18: Volcanes de 3–isogenias sobre $\mathbb{F}_{691}$ con cardinal 700.

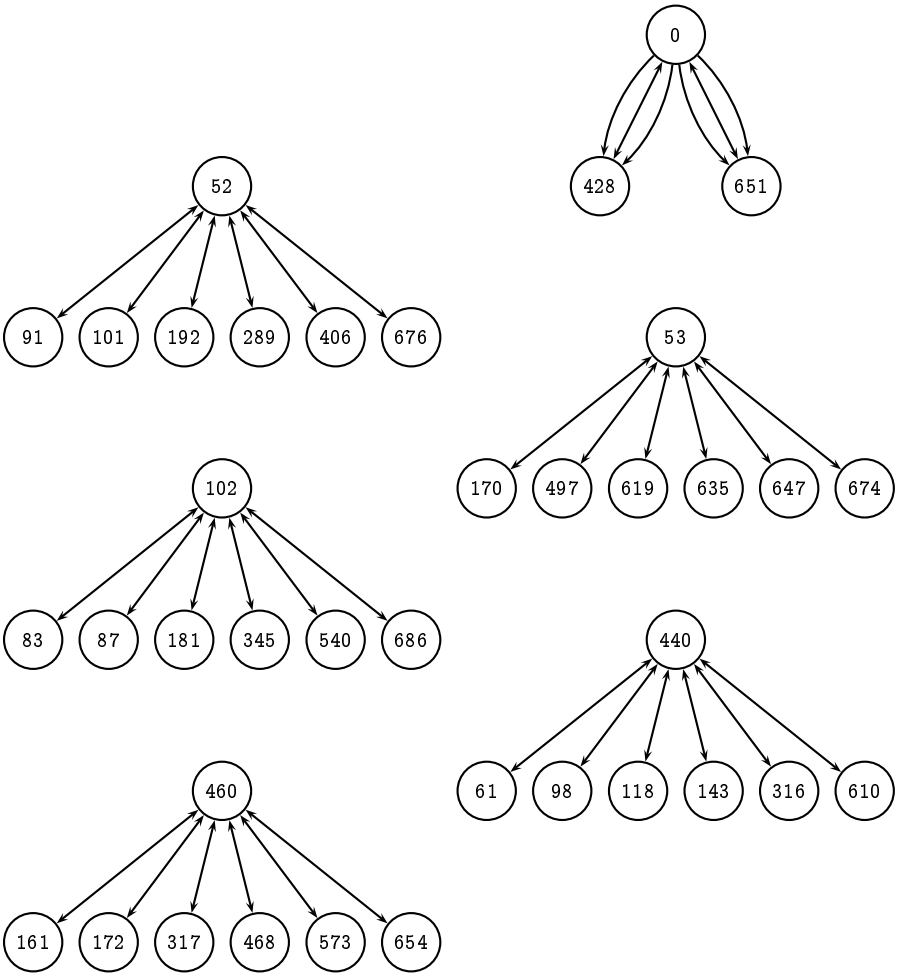


Figura 3.19: Volcanes de 5–isogenias sobre $\mathbb{F}_{691}$ con cardinal 700.

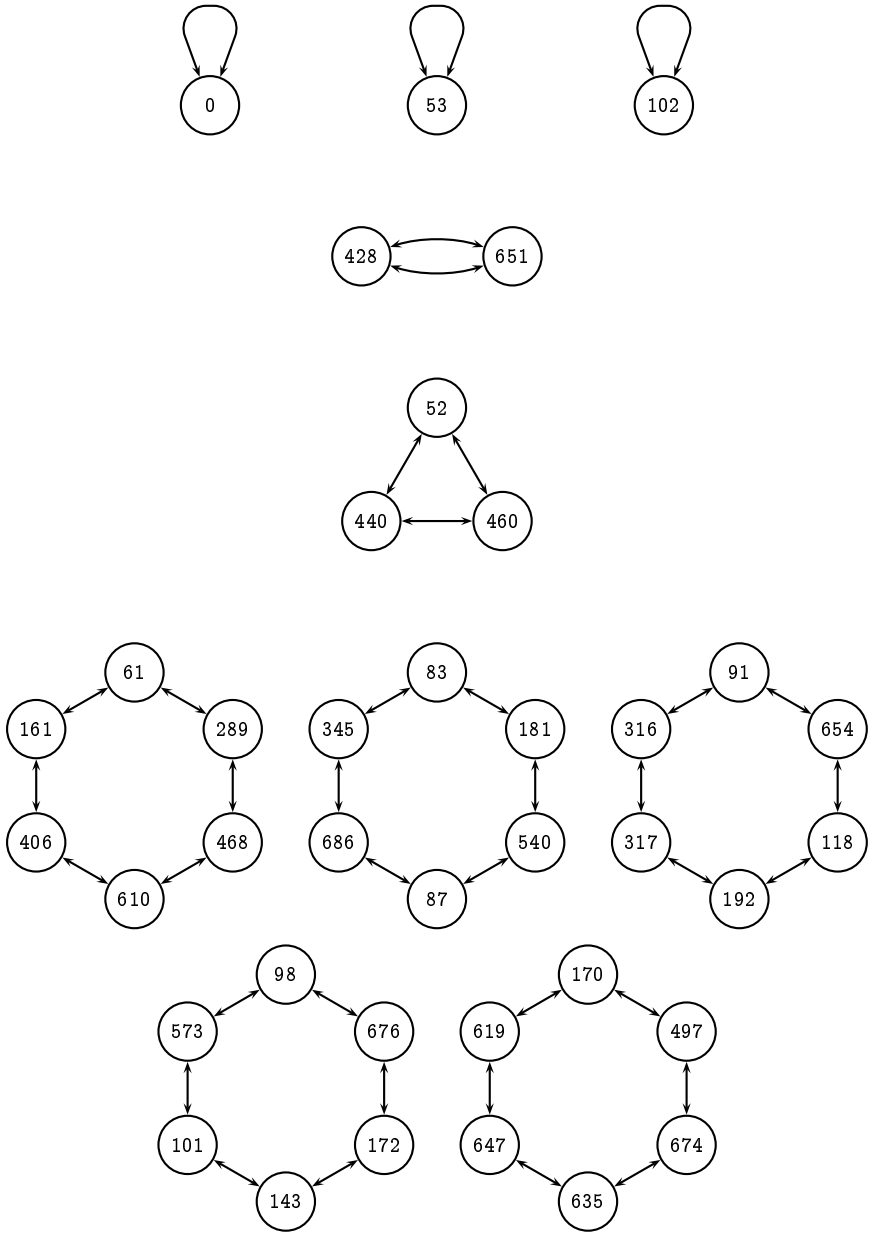


Figura 3.20: Volcanes de 7–isogenias sobre $\mathbb{F}_{691}$ con cardinal 700.

- $h = 0$ (6436)
  - $r = 0$ (4680)
    - $c = 1$ (4680)
  - $r = 1$ (1756)
    - $c = 1$ (2)
    - $c = 2$ (1754)
- $h = 1$ (608)
  - $r = 0$ (542)
    - $c = 1$ (542)
  - $r = 2$ (66)
    - $c = 5$ (2)
    - $c = 7$ (2)
    - $c = 8$ (2)
    - $c = 10$ (4)
    - $c = 11$ (12)
    - $c = 14$ (12)
    - $c = 19$ (2)
    - $c = 27$ (2)
    - $c = 29$ (2)
    - $c = 30$ (4)
    - $c = 34$ (6)
    - $c = 42$ (4)
    - $c = 43$ (2)
    - $c = 46$ (4)
    - $c = 57$ (2)
    - $c = 82$ (2)
    - $c = 92$ (2)

Cuadro 3.2: Número de 2–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c.

- $h = 0$ (7340)
  - $r = 0$ (7020)
    - $c = 1$ (7020)
  - $r = 2$ (320)
    - $c = 1$ (4)
    - $c = 3$ (6)
    - $c = 4$ (2)
    - $c = 5$ (8)
    - $c = 6$ (4)
    - $c = 7$ (12)
    - $c = 9$ (6)
    - $c = 10$ (10)
    - $c = 11$ (20)
    - $c = 12$ (64)
    - $c = 13$ (14)
    - $c = 14$ (12)
    - $c = 15$ (4)
    - $c = 16$ (4)
    - $c = 18$ (18)
    - $c = 19$ (12)
    - $c = 20$ (4)
    - $c = 21$ (20)
    - $c = 22$ (8)
    - $c = 24$ (8)
    - $c = 26$ (8)
    - $c = 29$ (4)
    - $c = 30$ (6)
    - $c = 31$ (4)
    - $c = 34$ (8)
    - $c = 36$ (4)
    - $c = 41$ (6)
    - $c = 42$ (4)
    - $c = 43$ (4)
    - $c = 45$ (2)
    - $c = 46$ (8)
    - $c = 48$ (2)
    - $c = 49$ (2)
    - $c = 52$ (2)
    - $c = 60$ (2)
    - $c = 62$ (2)
    - $c = 75$ (2)
    - $c = 78$ (2)
    - $c = 82$ (4)
    - $c = 92$ (4)

Cuadro 3.3: Número de 3–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c.

- $h = 0$ (7078)
  - $r = 0$ (4680)
    - $c = 1$ (4680)
  - $r = 1$ (2248)
    - $c = 2$ (2248)
  - $r = 2$ (150)
    - $c = 3$ (2)
    - $c = 5$ (12)
    - $c = 8$ (4)
    - $c = 9$ (6)
    - $c = 10$ (2)
    - $c = 11$ (2)
    - $c = 12$ (4)
    - $c = 13$ (10)
    - $c = 14$ (8)
    - $c = 15$ (4)
    - $c = 16$ (12)
    - $c = 18$ (4)
    - $c = 19$ (4)
    - $c = 22$ (4)
    - $c = 24$ (12)
    - $c = 25$ (6)
    - $c = 28$ (10)
    - $c = 29$ (4)
    - $c = 30$ (2)
    - $c = 31$ (2)
    - $c = 34$ (20)
    - $c = 39$ (2)
    - $c = 41$ (8)
    - $c = 45$ (2)
    - $c = 48$ (2)
    - $c = 68$ (2)
- $h = 1$ (102)
  - $r = 0$ (86)
    - $c = 1$ (86)
  - $r = 1$ (6)
    - $c = 2$ (6)
  - $r = 2$ (10)
    - $c = 3$ (2)
    - $c = 8$ (2)
    - $c = 12$ (4)
    - $c = 13$ (2)
- $h = 2$ (4)
  - $r = 2$ (4)
    - $c = 1$ (2)
    - $c = 3$ (2)

Cuadro 3.4: Número de 5–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c.

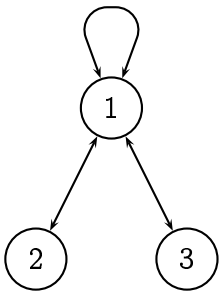
- $h = 0$ (7380)
  - $r = 0$ (7020)
    - $c = 1$ (7020)
  - $r = 2$ (360)
    - $c = 2$ (6)
    - $c = 3$ (2)
    - $c = 4$ (16)
    - $c = 5$ (28)
    - $c = 6$ (32)
    - $c = 7$ (4)
    - $c = 8$ (40)
    - $c = 10$ (30)
    - $c = 11$ (8)
    - $c = 12$ (22)
    - $c = 14$ (24)
    - $c = 16$ (4)
    - $c = 18$ (10)
    - $c = 19$ (8)
    - $c = 20$ (6)
    - $c = 22$ (18)
    - $c = 23$ (2)
    - $c = 24$ (8)
    - $c = 26$ (14)
    - $c = 27$ (6)
    - $c = 28$ (2)
    - $c = 30$ (6)
    - $c = 33$ (4)
    - $c = 34$ (12)
    - $c = 38$ (2)
    - $c = 40$ (2)
    - $c = 42$ (8)
    - $c = 43$ (4)
    - $c = 46$ (8)
    - $c = 48$ (6)
    - $c = 49$ (2)
    - $c = 62$ (4)
    - $c = 68$ (2)
    - $c = 75$ (2)
    - $c = 78$ (2)
    - $c = 84$ (2)
    - $c = 92$ (4)

Cuadro 3.5: Número de 7–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c.

- $h = 0$ (7394)
  - $r = 0$ (5744)
    - $c = 1$ (5744)
  - $r = 1$ (1220)
    - $c = 1$ (8)
    - $c = 2$ (1212)
  - $r = 2$ (430)
    - $c = 1$ (8)
    - $c = 3$ (14)
    - $c = 4$ (50)
    - $c = 5$ (38)
    - $c = 6$ (72)
    - $c = 7$ (28)
    - $c = 8$ (16)
    - $c = 9$ (14)
    - $c = 10$ (12)
    - $c = 12$ (36)
    - $c = 13$ (28)
    - $c = 14$ (16)
    - $c = 15$ (2)
    - $c = 16$ (8)
    - $c = 17$ (8)
    - $c = 18$ (6)
    - $c = 20$ (4)
    - $c = 22$ (2)
    - $c = 23$ (2)
    - $c = 25$ (6)
    - $c = 26$ (2)
    - $c = 27$ (8)
    - $c = 29$ (2)
    - $c = 31$ (4)
    - $c = 33$ (6)
    - $c = 34$ (8)
    - $c = 39$ (2)
    - $c = 41$ (4)
    - $c = 44$ (2)
    - $c = 46$ (16)
    - $c = 48$ (2)
    - $c = 49$ (2)
    - $c = 78$ (2)
- $h = 1$ (10)
  - $r = 0$ (8)
    - $c = 1$ (8)
  - $r = 2$ (2)
    - $c = 3$ (2)

Cuadro 3.6: Número de 11–volcanes sobre $\mathbb{F}_{7019}$ en función de h, h y r y h, r y c.

$$\mathbb{F}_q = \mathbb{F}_{67}$$
$$q + 1 - t = 55$$
$$t^2 - 4q = 3^2(-11)$$
$$K = \mathbb{Q}(\sqrt{-11})$$



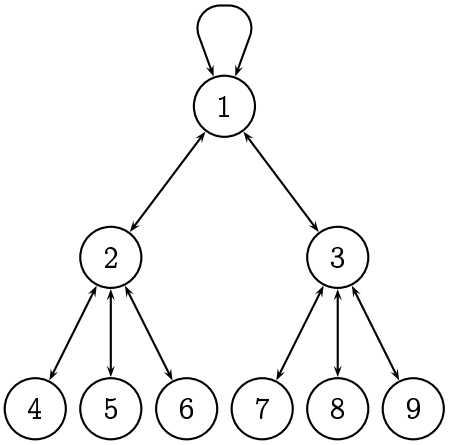
O_K

$\mathbb{Z} + 3O_K$

$$E_1 = [15, 37] \qquad j(E_1) = 62$$
$$E_2 = [22, 16] \qquad j(E_2) = 21$$
$$E_3 = [61, 32] \qquad j(E_3) = 48$$

Figura 3.21: Volcán de 3–isogenias sobre $\mathbb{F}_{67}$.

$$\mathbb{F}_{q^3} = \mathbb{F}_{67^3} = \frac{\mathbb{F}_{67}[u]}{(u^3 + 6u + 65)}$$
$$q^3 + 1 - t = 301180$$
$$t^2 - 4q^3 = (2 \cdot 3^2 \cdot 17)^2(-11)$$
$$K = \mathbb{Q}(\sqrt{-11})$$



O_K

$\mathbb{Z} + 3O_K$

$\mathbb{Z} + 9O_K$

$$E_1 = [15, 37] \qquad j(E_1) = 62$$
$$E_2 = [22, 16] \qquad j(E_2) = 21$$
$$E_3 = [61, 32] \qquad j(E_3) = 48$$
$$E_4 = [27u^2 + 37u + 51, 23u^2 + 66u + 30] \qquad j(E_4) = 8u^2 + 64u + 20$$
$$E_5 = [38u^2 + 52u + 28, 11u^2 + 66u + 49] \qquad j(E_5) = 22u^2 + 29u + 9$$
$$E_6 = [2u^2 + 45u + 18, 33u^2 + 2u + 3] \qquad j(E_6) = 37u^2 + 41u + 2$$
$$E_7 = [51u^2 + 15u + 33, 38u^2 + 17u + 41] \qquad j(E_7) = 65u^2 + 39u + 42$$
$$E_8 = [36u^2 + 2u + 40, 31u^2 + 23u + 13] \qquad j(E_8) = 6u^2 + 62u + 7$$
$$E_9 = [47u^2 + 50u + 17, 65u^2 + 27u + 15] \qquad j(E_9) = 63u^2 + 33u + 34$$

Figura 3.22: Volcán de 3–isogenias sobre $\mathbb{F}_{67^3}$.

Bibliografía

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[Bel00] G. Belingueres. Introducción a los criptosistemas de curva elíptica, 2000.

[BLP93] J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance. Factoring integers with the number field sieve. In *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*, pages 50–94. Springer, Berlin, 1993.

[BSS00] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000.

[Cox89] D. A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Fou01] M. Fouquet. *Anneau d'endomorphismes et cardinalité de courbes elliptiques : aspects algorithmiques*. PhD thesis, École polytechnique, 2001.

[How98] J. S. Howell. The index calculus algorithm for discrete logarithms. Master's thesis, Clemson University, 1998.

[IKNY98] T. Izu, J. Kogure, M. Noro, and K. Yokoyama. Efficient implementation of Schoof's algorithm. In *Advances in cryptology—ASIACRYPT'98 (Beijing)*, volume 1514 of *Lecture Notes in Computer Science*, pages 66–79. Springer, Berlin, 1998.

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.

[Ler97] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, École polytechnique, 1997.

[Mor05] R. Moreno. *Subgrupos de Sylow de las curvas elípticas definidas sobre cuerpos finitos*. PhD thesis, Universitat Politècnica de Catalunya, 2005.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Vé71] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.