Un algoritmo para construir ciclos en $\mathcal{G}_\ell(p^2, (p+1)^2)$

Gora Adj [1] Josep M. Miret [1] Jordi Pujolàs [1] Juan G. Tena [2] Javier Valera [1]

[1] Universidad de Lleida

{ gadj , miret , jpujolas , jvalera }@matematica.udl.cat

[2] Universidad de Valladolid

tena@agt.uva.es

***Resumen*—Fijado un grafo de isogenias supersingulares $\mathcal{G}_\ell(p^2, (p+1)^2)$ y dado un vértice $j \notin \mathbb{F}_p$, en este artículo se presenta un algoritmo para construir un ciclo sin retroceso con inicio en j.**

***Index Terms*—Cycle · Supersingular · Isogeny · Graph.**

I. Introducción

Este trabajo surge de nuestro interés en algunos problemas matemáticos destinados al diseño de protocolos criptográficos resistentes tanto a algoritmos tradicionales como cuánticos. Uno de ellos consiste en encontrar un cierto camino en un grafo de isogenias (de curvas elípticas) supersingulares. En la última década han aparecido diversos protocolos basados en dicho problema, siendo los más conocidos el SIDH [8] y el CSIDH [5]. El primero de ellos (renombrado como SIKE debido a variaciones con respecto a su implementación inicial) fue presentado en 2017 al concurso organizado por el NIST para escoger nuevos estándares en encapsulación de claves. Actualmente ya ha superado dos rondas y ha sido seleccionado como "candidato alternativo" (véase [3]). No obstante, de poder calcular el anillo de endomorfismos de cualquier curva elíptica supersingular, tanto el SIDH como el CSIDH serían vulnerables. Tal y como se explica en [6], una forma de calcularlo consiste en hallar ciclos en diversos grafos de isogenias supersingulares.

Dado un vértice de un grafo de isogenias supersingulares, en este artículo se presenta un algoritmo para construir un cierto tipo de ciclo en dicho grafo. El algoritmo se basa en una propiedad de tales grafos, a saber, la simetría de reflexión [11].

II. Grafos de isogenias supersingulares

Sea $\mathbb{F}_q$ un cuerpo finito de orden q y característica p, sea $\overline{\mathbb{F}}_q$ la clausura algebraica de $\mathbb{F}_q$ y sea $\ell \neq p$ un número primo. Dada una curva elíptica E definida sobre $\mathbb{F}_q$ y dado un subgrupo G de $(E(\overline{\mathbb{F}}_q), +)$ de orden ℓ, denótese con E/G a la curva elíptica ℓ-isógena de E que se obtendría a partir de las fórmulas de Vélu [12]. Considérense todas las clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas definidas sobre $\mathbb{F}_q$ con un determinado cardinal m y supóngase que cada una de ellas es un vértice de un grafo dirigido $\mathcal{G}_\ell(q, m)$. Sea v un vértice de $\mathcal{G}_\ell(q, m)$ y sea E una curva elíptica perteneciente a v. El grado de salida r de v es igual al número de subgrupos $\mathbb{F}_q$-racionales de $(E(\overline{\mathbb{F}}_q), +)$ de orden ℓ. Supóngase que $r \neq 0$ y sean $G_1, \ldots, G_r$ los subgrupos $\mathbb{F}_q$-racionales de $(E(\overline{\mathbb{F}}_q), +)$ de orden ℓ. Sea v' un vértice de $\mathcal{G}_\ell(q, m)$ y sea E' una curva elíptica perteneciente a v'. El número de arcos que van desde v a v' es igual al número de curvas elípticas E/G_i que son isomorfas sobre $\mathbb{F}_q$ a E'. Cuando los vértices de $\mathcal{G}_\ell(q, m)$ son clases de isomorfía de curvas elípticas supersingulares, entonces se dice que $\mathcal{G}_\ell(q, m)$ es un grafo de isogenias supersingulares.

Supóngase a partir de ahora que $p \geq 5$ y $\ell \geq 3$. En este artículo se trabaja en el grafo de isogenias supersingulares $\mathcal{G}_\ell(p^2, (p+1)^2)$. Este grafo es conexo y el grado de salida de cada uno de sus vértices es $\ell+1$. Además, un representante de cada vértice es el j-invariante de sus curvas elípticas. Véase [1] y [9] para más información.

III. Ciclos sin retroceso

La información referente a esta sección ha sido extraída o deducida a partir de [1] y [4].

Sean v_1 y v_2 dos vértices de $\mathcal{G}_\ell(p^2, (p+1)^2)$ y sean E_1 y E_2 dos curvas elípticas pertenecientes a v_1 y v_2, respectivamente. Sean $a_{1,2}, b_{1,2} = (v_1, v_2)$ dos arcos de $\mathcal{G}_\ell(p^2, (p+1)^2)$ y sean $\phi_{1,2}, \psi_{1,2} : E_1 \to E_2$ dos ℓ-isogenias representantes de $a_{1,2}$ y $b_{1,2}$, respectivamente. Se dice que $\phi_{1,2}$ y $\psi_{1,2}$ son equivalentes si existe un automorfismo ρ de E_2 tal que $\psi_{1,2} = \rho \circ \phi_{1,2}$. Se tiene que $a_{1,2} = b_{1,2}$ si y sólo si $\phi_{1,2}$ y $\psi_{1,2}$ son equivalentes.

Sea $a_{2,1} = (v_2, v_1)$ un arco de $\mathcal{G}_\ell(p^2, (p+1)^2)$ y sea $\phi_{2,1} : E_2 \to E_1$ una ℓ-isogenia representante de $a_{2,1}$. Se dice que $a_{2,1}$ es dual de $a_{1,2}$ si $\phi_{2,1}$ y $\hat{\phi}_{1,2}$ son equivalentes. Se dice que un ciclo $[a_1, \ldots, a_s]$ de $\mathcal{G}_\ell(p^2, (p+1)^2)$ no presenta retroceso si $s = 1$ o para todo $i \in \{1, \ldots, s-1\}$ se tiene que a_{i+1} no es dual de a_i. Si $v_1 \neq v_2$, $j(E_1) \notin \{0, 1728\}$, $a_{1,2} \neq b_{1,2}$ y $a_{2,1}$ es dual de $a_{1,2}$, entonces $[b_{1,2}, a_{2,1}]$ es un ciclo sin retroceso.

A partir de ahora se supone que se dispone de un algoritmo $\mathrm{Dual}(a)$ el cual devuelve el arco dual de uno dado a.

IV. Niveles y tipos de arcos

Considérese el siguiente trozo de pseudocódigo:

```
01:  /* Φ_ℓ(X,Y) = polinomio modular de nivel ℓ */
02:  S_0 := { j-invariantes de curvas elípticas
03:           definidas sobre F_p con cardinal p+1 } ;
04:  continuar := falso ;
```

```
05:  para  j ∈ S_0  hacer
06:  .  para  j' ∈ F_{p^2}  tal que  Φ_ℓ(j,j') = 0  hacer
07:  .  .  si  j' ∉ S_0  entonces
08:  .  .  .  si  ¬continuar  entonces
09:  .  .  .  .  S_{-1} := { } ;
10:  .  .  .  .  continuar := cierto ;
11:  .  .  .  fin si
12:  .  .  .  Incluir j' en S_{-1} ;
13:  .  .  fin si
14:  .  fin para
15:  fin para
16:  N := 1 ;
17:  mientras  continuar  hacer
18:  .  N := N + 1 ;
19:  .  continuar := falso ;
20:  .  para  j ∈ S_{-N+1}  hacer
21:  para  j' ∈ F_{p^2}  tal que  Φ_ℓ(j,j') = 0  hacer
22:  .  .  .  si  j' ∉ (S_{-N+1} ∪ S_{-N+2})  entonces
23:  .  .  .  .  si  ¬continuar  entonces
24:  .  .  .  .  .  S_{-N} := { } ;
25:  .  .  .  .  .  continuar := cierto ;
26:  .  .  .  .  fin si
27:  .  .  .  .  Incluir j' en S_{-N} ;
28:  .  .  .  fin si
29:  fin para
30:  .  fin para
31:  fin mientras
```

Este trozo de pseudocódigo distribuye los vértices de $\mathcal{G}_\ell(p^2,(p+1)^2)$ en N conjuntos disjuntos $S_0,\ldots,S_{-N+1}$. Los vértices del conjunto S_{-k} con $k\in\{0,\ldots,N-1\}$ forman el nivel $-k$.

Un arco de un vértice j a un vértice j' es de uno de los siguientes tres tipos:

- Ascendente:
  $\mathrm{Nivel}(j')=\mathrm{Nivel}(j)+1$
  ($\mathrm{Nivel}(j)\in[-N+1,0)$ con $N\geq 2$);
- Horizontal:
  $\mathrm{Nivel}(j')=\mathrm{Nivel}(j)$
  ($\mathrm{Nivel}(j)\in[-N+1,0]$);
- Descendente:
  $\mathrm{Nivel}(j')=\mathrm{Nivel}(j)-1$
  ($\mathrm{Nivel}(j)\in(-N+1,0]$ con $N\geq 2$).

Véase la figura 1 para un ejemplo.

V. Algoritmo

En esta sección se da un algoritmo para construir un ciclo sin retroceso en $\mathcal{G}_\ell(p^2,(p+1)^2)$ con inicio en un cierto vértice.

Sea E una curva elíptica perteneciente a un vértice de $\mathcal{G}_\ell(p^2,(p+1)^2)$ de ecuación

$$y^2=x^3+ax+b.$$

Sea $\bar{E}$ la curva elíptica de ecuación

$$\bar{y}^2=\bar{x}^3+a^p\bar{x}+b^p.$$

Existe una isogenia

$$\phi_{p,E}:E\to\bar{E}$$

tal que

$$P=(x,y)\quad\mapsto\quad\bar{P}=(\bar{x},\bar{y})=(x^p,y^p).$$

Tal isogenia se denomina la isogenia de Frobenius de E a la p-ésima potencia. Nótese que $\phi_{p,E}$ está definida sobre $\mathbb{F}_{p^2}$. No obstante, si E está definida sobre $\mathbb{F}_p$, entonces $\phi_{p,E}$ también lo está. En dicho caso, $\phi_{p,E}$ es un endomorfismo de E. Nótese que

$$\#E(\mathbb{F}_{p^2})=\#\bar{E}(\mathbb{F}_{p^2})$$

y

$$j(\bar{E})=j(E)^p.$$

Un camino de longitud mayor que 0 en $\mathcal{G}_\ell(p^2,(p+1)^2)$ es ascendente, horizontal o descendente si está formado únicamente por arcos ascendentes, horizontales o descendentes, respectivamente. Un camino de longitud 0 es a la vez ascendente, horizontal y descendente.

Supóngase que $N\geq 2$. Considérese un vértice j tal que $\mathrm{Nivel}(j)\neq 0$.

- Desde j siempre sale como mínimo un arco ascendente. Tomando sucesivos arcos ascendentes cualesquiera a partir de j siempre se llega a un vértice del nivel 0. Si k es el número de arcos tomados, entonces $\mathrm{Nivel}(j)=-k$.
- Si desde j salen ℓ arcos descendentes, entonces tomando sucesivos arcos descendentes cualesquiera a partir de j siempre se llega a un vértice del cual no salen ℓ arcos descendentes.

Los pasos que sigue el algoritmo para construir un ciclo sin retroceso con inicio en j son los siguientes:

- **Paso 1.** Calcular un camino ascendente desde j hasta un vértice del nivel 0:

$$\underbrace{j=j_{[\blacktriangle](0)}\xrightarrow{a_{[\blacktriangle](1)}}\cdots\xrightarrow{a_{[\blacktriangle](k)}}j_{[\blacktriangle](k)}}_{\text{camino ascendente de longitud } k\geq 1}\ .$$

- **Paso 2.** Tomar sucesivos arcos descendentes cualesquiera a partir de j hasta detectar un vértice del cual salgan dos arcos ascendentes (opción A) o uno horizontal (opción B):
  - Opción A:

$$\underbrace{j=j_{[\blacktriangledown](0)}\xrightarrow{a_{[\blacktriangledown](1)}}\cdots\xrightarrow{a_{[\blacktriangledown](n)}}\overbrace{j_{[\blacktriangledown](n)}\xrightarrow{a_{[\bullet]}}j_{[\bullet]}}^{\text{camino ascendente de longitud 1}}}_{\text{camino descendente de longitud } n\geq 0}\ .$$

    Si $n=0$, entonces se conocía el arco ascendente $a_{[\blacktriangle](1)}$ y se detectó el arco ascendente $a_{[\bullet]}\neq a_{[\blacktriangle](1)}$. Si $n\geq 1$, entonces se conocía el arco ascendente $\mathrm{Dual}(a_{[\blacktriangledown](n)})$ y se detectó el arco ascendente $a_{[\bullet]}\neq\mathrm{Dual}(a_{[\blacktriangledown](n)})$.
  - Opción B:

$$\underbrace{j=j_{[\blacktriangledown](0)}\xrightarrow{a_{[\blacktriangledown](1)}}\cdots\xrightarrow{a_{[\blacktriangledown](n)}}\overbrace{j_{[\blacktriangledown](n)}\xrightarrow{a_{[\bullet]}}j_{[\bullet]}}^{\text{camino horizontal de longitud 1}}}_{\text{camino descendente de longitud } n\geq 0}\ .$$

    Casos que deben ser tratados y que permiten finalizar el algoritmo:
  - Opción A:
    - $n=0$ y $j_{[\bullet]}=j_{[\blacktriangle](1)}$: Devolver $[a_{[\bullet]},\mathrm{Dual}(a_{[\blacktriangle](1)})]$.

- $n=1$ y $j_{[\bullet]}=j$: Devolver
$$[a_{[\blacktriangledown](1)},a_{[\bullet]}]\ .$$
- $n\geq 2$ y $j_{[\bullet]}=j_{[\blacktriangledown](n-1)}$: Devolver
$$[a_{[\blacktriangledown](1)},\dots,a_{[\blacktriangledown](n)},a_{[\bullet]},$$
$$\mathrm{Dual}(a_{[\blacktriangledown](n-1)}),\dots,\mathrm{Dual}(a_{[\blacktriangledown](1)})]\ .$$

- Opción B:
  - $j_{[\bullet]}=j_{[\blacktriangledown](n)}$:
    - $n=0$: Devolver
    $$[a_{[\bullet]}]\ .$$
    - $n\geq 1$: Devolver
    $$[a_{[\blacktriangledown](1)},\dots,a_{[\blacktriangledown](n)},a_{[\bullet]},$$
    $$\mathrm{Dual}(a_{[\blacktriangledown](n)}),\dots,\mathrm{Dual}(a_{[\blacktriangledown](1)})]\ .$$
  - $j_{[\bullet]}=j^p_{[\blacktriangledown](n)}$: Por lo explicado en [11] (véase, también, el apartado 2.1 de [2]) se sabe que existen los siguientes caminos:
  $$j^p=j^p_{[\blacktriangle](0)}\xrightarrow{a^{(p)}_{[\blacktriangle](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangle](k)}}j^p_{[\blacktriangle](k)}=j_{[\blacktriangle](k)}\ ,$$
  $$j^p=j^p_{[\blacktriangledown](0)}\xrightarrow{a^{(p)}_{[\blacktriangledown](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangledown](n)}}j^p_{[\blacktriangledown](n)}=j_{[\bullet]}\ .$$
  Por lo tanto:
    - $n=0$: Devolver
    $$[a_{[\blacktriangle](1)},\dots,a_{[\blacktriangle](k)},$$
    $$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\dots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),\mathrm{Dual}(a_{[\bullet]})]\ .$$
    - $n\geq 1$: Devolver
    $$[a_{[\blacktriangle](1)},\dots,a_{[\blacktriangle](k)},$$
    $$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\dots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),$$
    $$a^{(p)}_{[\blacktriangledown](1)},\dots,a^{(p)}_{[\blacktriangledown](n)},$$
    $$\mathrm{Dual}(a_{[\bullet]}),\mathrm{Dual}(a_{[\blacktriangledown](n)}),\dots,\mathrm{Dual}(a_{[\blacktriangledown](1)})]\ .$$

- **Paso 3.** Calcular un camino ascendente desde $j_{[\bullet]}$ hasta un vértice del nivel 0:
  - Opción A:
  $$\underbrace{j_{[\bullet]}=j_{[\triangle](0)}\xrightarrow{a_{[\triangle](1)}}\cdots\xrightarrow{a_{[\triangle](k+n-1)}}j_{[\triangle](k+n-1)}}_{\text{camino ascendente de longitud } k+n-1\geq 0}\ .$$
  - Opción B:
  $$\underbrace{j_{[\bullet]}=j_{[\triangle](0)}\xrightarrow{a_{[\triangle](1)}}\cdots\xrightarrow{a_{[\triangle](k+n)}}j_{[\triangle](k+n)}}_{\text{camino ascendente de longitud } k+n\geq 1}\ .$$

  Si durante el cálculo del camino se detecta una colisión, entonces construir un ciclo sin retroceso con inicio en j y devolverlo.
- **Paso 4.** Por lo explicado en [11] (véase, también, el apartado 2.1 de [2]) se sabe que existen los siguientes caminos:
  - Opción A:
  $$j^p=j^p_{[\blacktriangle](0)}\xrightarrow{a^{(p)}_{[\blacktriangle](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangle](k)}}j^p_{[\blacktriangle](k)}=j_{[\blacktriangle](k)}\ ,$$
  $$j^p=j^p_{[\blacktriangledown](0)}\xrightarrow{a^{(p)}_{[\blacktriangledown](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangledown](n)}}j^p_{[\blacktriangledown](n)}\xrightarrow{a^{(p)}_{[\bullet]}}j^p_{[\bullet]}\ ,$$
  $$j^p_{[\bullet]}=j^p_{[\triangle](0)}\xrightarrow{a^{(p)}_{[\triangle](1)}}\cdots$$
  $$\cdots\xrightarrow{a^{(p)}_{[\triangle](k+n-1)}}j^p_{[\triangle](k+n-1)}=j_{[\triangle](k+n-1)}\ .$$
  - Opción B:
  $$j^p=j^p_{[\blacktriangle](0)}\xrightarrow{a^{(p)}_{[\blacktriangle](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangle](k)}}j^p_{[\blacktriangle](k)}=j_{[\blacktriangle](k)}\ ,$$
  $$j^p=j^p_{[\blacktriangledown](0)}\xrightarrow{a^{(p)}_{[\blacktriangledown](1)}}\cdots\xrightarrow{a^{(p)}_{[\blacktriangledown](n)}}j^p_{[\blacktriangledown](n)}\xrightarrow{a^{(p)}_{[\bullet]}}j^p_{[\bullet]}\ ,$$
  $$j^p_{[\bullet]}=j^p_{[\triangle](0)}\xrightarrow{a^{(p)}_{[\triangle](1)}}\cdots$$
  $$\cdots\xrightarrow{a^{(p)}_{[\triangle](k+n)}}j^p_{[\triangle](k+n)}=j_{[\triangle](k+n)}\ .$$

Por lo tanto:
- Opción A:
  - $n=0$:
    - $k=1$: Devolver
    $$[a_{[\blacktriangle](1)},\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),a^{(p)}_{[\bullet]},\mathrm{Dual}(a_{[\bullet]})]\ .$$
    - $k\geq 2$: Devolver
    $$[a_{[\blacktriangle](1)},\dots,a_{[\blacktriangle](k)},$$
    $$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\dots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),$$
    $$a^{(p)}_{[\bullet]},a^{(p)}_{[\triangle](1)},\dots,a^{(p)}_{[\triangle](k-1)},$$
    $$\mathrm{Dual}(a_{[\triangle](k-1)}),\dots,\mathrm{Dual}(a_{[\triangle](1)}),\mathrm{Dual}(a_{[\bullet]})]\ .$$
  - $n\geq 1$: Devolver
  $$[a_{[\blacktriangle](1)},\dots,a_{[\blacktriangle](k)},$$
  $$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\dots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),$$
  $$a^{(p)}_{[\blacktriangledown](1)},\dots,a^{(p)}_{[\blacktriangledown](n)},$$
  $$a^{(p)}_{[\bullet]},a^{(p)}_{[\triangle](1)},\dots,a^{(p)}_{[\triangle](k+n-1)},$$
  $$\mathrm{Dual}(a_{[\triangle](k+n-1)}),\dots,\mathrm{Dual}(a_{[\triangle](1)}),\mathrm{Dual}(a_{[\bullet]}),$$
  $$\mathrm{Dual}(a_{[\blacktriangledown](n)}),\dots,\mathrm{Dual}(a_{[\blacktriangledown](1)})]\ .$$
- Opción B:
  - $n=0$: Devolver
  $$[a_{[\blacktriangle](1)},\dots,a_{[\blacktriangle](k)},$$
  $$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\dots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),a^{(p)}_{[\bullet]},$$
  $$a^{(p)}_{[\triangle](1)},\dots,a^{(p)}_{[\triangle](k)},$$
  $$\mathrm{Dual}(a_{[\triangle](k)}),\dots,\mathrm{Dual}(a_{[\triangle](1)}),\mathrm{Dual}(a_{[\bullet]})]\ .$$

- $n \geq 1$: Devolver

$$[a_{[\blacktriangle](1)},\ldots,a_{[\blacktriangle](k)},$$
$$\mathrm{Dual}(a^{(p)}_{[\blacktriangle](k)}),\ldots,\mathrm{Dual}(a^{(p)}_{[\blacktriangle](1)}),$$
$$a^{(p)}_{[\blacktriangledown](1)},\ldots,a^{(p)}_{[\blacktriangledown](n)},a^{(p)}_{[\bullet]},$$
$$a^{(p)}_{[\triangle](1)},\ldots,a^{(p)}_{[\triangle](k+n)},$$
$$\mathrm{Dual}(a_{[\triangle](k+n)}),\ldots,\mathrm{Dual}(a_{[\triangle](1)}),\mathrm{Dual}(a_{[\bullet]}),$$
$$\mathrm{Dual}(a_{[\blacktriangledown](n)}),\ldots,\mathrm{Dual}(a_{[\blacktriangledown](1)})]\ .$$

En la figura 2 se muestra un ciclo obtenido con el algoritmo anterior cuando se alcanza el paso 4 con la opción B y $n \geq 1$.

VI. Pruebas y resultados

Primera batería de pruebas:

- $p = 2^a \cdot 3^b - 1, \qquad 2 \leq a \leq 12, \qquad 1 \leq b \leq 7;$
- $\ell \leq 17.$

Resultado 1.

$$N = \lfloor \log_\ell(\sqrt{p}) \rfloor + \epsilon, \qquad \epsilon \in \{0,1,2,3\}.$$

Segunda batería de pruebas:

- $p = 2^a \cdot 3^b - 1, \qquad 2 \leq a \leq 12, \qquad 1 \leq b \leq 7;$
- $\ell \leq 17;$
- $N \geq 4.$

Resultado 2.

P_{-k} = probabilidad de que de un vértice del nivel $-k$ con $k \in \{1,\ldots,N-2\}$ salgan ℓ arcos descendentes.

$$P_{-i} \geq P_{-i-1}, \qquad \forall i \in \{1,\ldots,N-3\}.$$

VII. Interrogantes

Las preguntas a las que se intentará responder en un futuro próximo son las siguientes:

(a) ¿Existe un algoritmo $\mathrm{Nivel}(j)$ que permita calcular de manera eficiente el nivel donde se encuentra situado un vértice j?
(b) ¿Existe un invariante para los niveles?
(c) ¿$N = \lfloor \log_\ell(\sqrt{p}) \rfloor + \epsilon$ con $\epsilon = 0$ o $\epsilon > 0$ un entero muy pequeño?
(d) ¿El segundo resultado de la sección anterior siempre es cierto?

Nótese que de ser ciertas las preguntas (a) y (c), entonces la implementación del algoritmo dado en la sección V utilizando el algoritmo Nivel será eficiente siempre y cuando ℓ sea pequeño y el coste de calcular una ℓ-isogenia sea bajo.

Retomando la notación introducida en la sección II, cuando los vértices de $\mathcal{G}_\ell(q,m)$ son clases de isomorfía de curvas elípticas ordinarias, cada componente conexa de $\mathcal{G}_\ell(q,m)$ es un volcán de ℓ-isogenias [7]. En el caso de un volcán de ℓ-isogenias, cada nivel representa un orden, el cual es isomorfo a los anillos de endomorfismos de las curvas elípticas situadas en dicho nivel. Al ascender un nivel se pasa de un orden de conductor f a uno de conductor f/ℓ. Hasta un cierto nivel, una forma sencilla de saber en qué nivel se halla una curva elíptica es calcular su subgrupo de ℓ-Sylow (véase [10]). En el caso de curvas elípticas supersingulares, a día de hoy, la pregunta (b) es un misterio.

Agradecimientos

Este estudio ha sido financiado por el Fondo Europeo de Desarrollo Regional de la Unión Europea en el marco del "Programa Operatiu FEDER de Catalunya 2014-2020" (proyecto COMRDI16-1-0060), por el Ministerio de Ciencia, Innovación y Universidades (proyecto MTM2017-83271-R) y por la Generalitat de Catalunya (grupo consolidado 2017 SGR 1158).

Referencias

[1] Gora Adj, Omran Ahmadi y Alfred Menezes. On isogeny graphs of supersingular elliptic curves over finite fields. Finite Fields and Their Applications, vol. 55, pp. 268-283, 2019.
[2] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl y Jana Sotáková. Adventures in Supersingularland. ArXiv, 2019.
[3] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev y David Urbanik. Supersingular Isogeny Key Encapsulation. Second Round Candidate of the NIST's post-quantum cryptography standardization process. 2017.
[4] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison y Jennifer Park. Cycles in the Supersingular ℓ-Isogeny Graph and Corresponding Endomorphisms. Research Directions in Number Theory, Association for Women in Mathematics Series, vol. 19, pp. 41-66, 2019.
[5] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny y Joost Renes. CSIDH: An Efficient Post-Quantum Commutative Group Action. ASIACRYPT 2018, Lecture Notes in Computer Science, vol. 11274, pp. 395-427, 2018.
[6] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison y Christophe Petit. Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions. EUROCRYPT 2018, Lecture Notes in Computer Science, vol. 10822, pp. 329-368, 2018.
[7] Mireille Fouquet y François Morain. Isogeny Volcanoes and the SEA Algorithm. ANTS 2002, Lecture Notes in Computer Science, vol. 2369, pp. 276-291, 2002.
[8] David Jao y Luca De Feo. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. PQCrypto 2011, Lecture Notes in Computer Science, vol. 7071, pp. 19-34, 2011.
[9] Kristin E. Lauter y Christophe Petit. Supersingular isogeny graphs in cryptography. Surveys in Combinatorics 2019, London Mathematical Society Lecture Note Series, vol. 456, pp. 143-165, 2019.
[10] Josep M. Miret, Ramiro Moreno, Daniel Sadornil, Juan Tena y Magda Valls. Computing the height of volcanoes of ℓ-isogenies of elliptic curves over finite fields. Applied Mathematics and Computation, vol. 196, núm. 1, pp. 67-76, 2008.
[11] Josep M. Miret, Jordi Pujolàs y Javier Valera. Simetría de reflexión en los grafos de isogenias de curvas elípticas supersingulares. ResearchGate, 2019.
[12] Jacques Vélu. Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris Sér. A-B, vol. 273, pp. A238-A241, 1971.

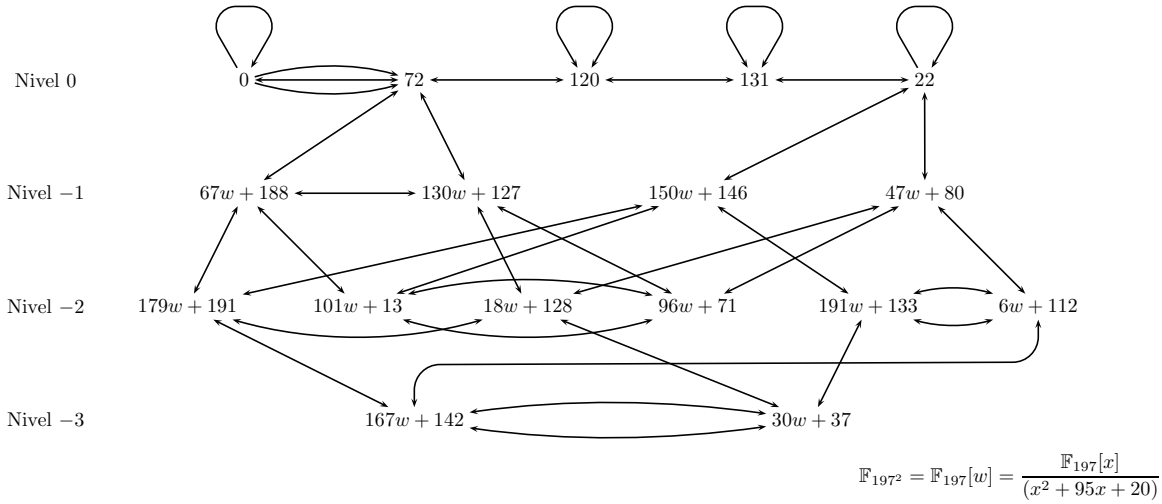

Figura 1. $\mathcal{G}_3(197^2, 198^2)$

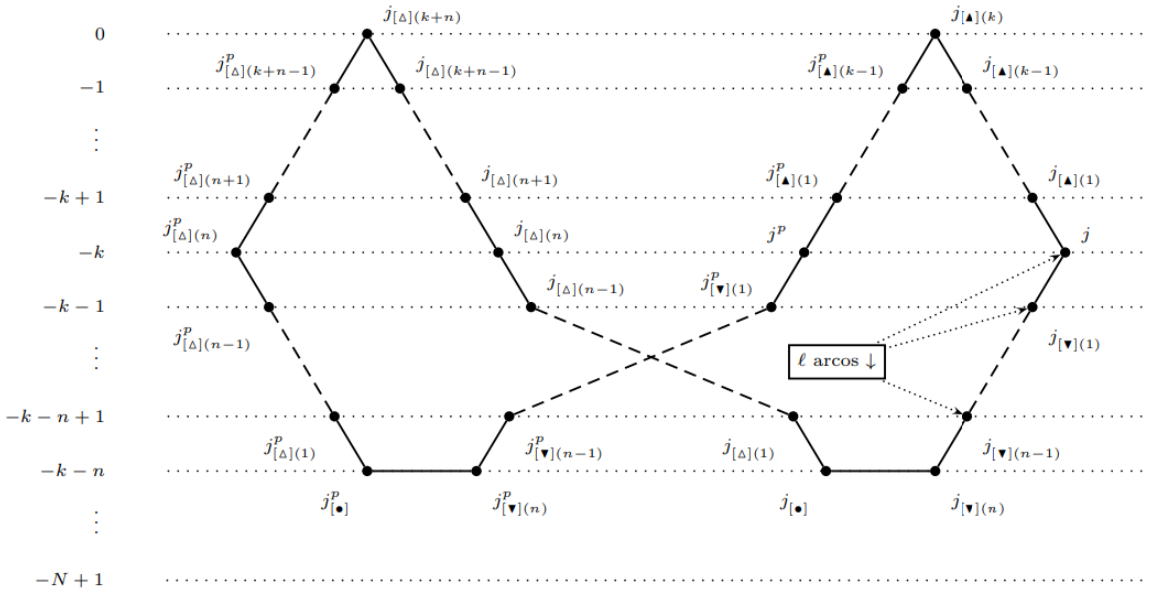

Figura 2. Ejemplo de ciclo