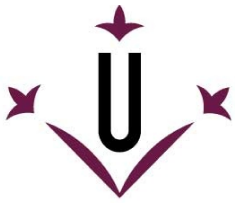
Universitat de Lleida

Contribuciones a la cardinalidad de curvas elípticas y a los volcanes de isogenias

Javier Valera Martín



Universitat de Lleida

TESI DOCTORAL

Contribuciones a la cardinalidad de curvas elípticas y a los volcanes de isogenias

Javier Valera Martín

Memòria presentada per optar al grau de
Doctor per la Universitat de Lleida

Programa de Doctorat en Enginyeria i Tecnologies de la Informació

Directors

Mireille Fouquet
Josep M. Miret

2017

Contribuciones a la cardinalidad de curvas elípticas y a los volcanes de isogenias

Javier Valera Martín

Directores

Mireille Fouquet y Josep M. Miret

Programa de Doctorado en Ingeniería
y Tecnologías de la Información

Universidad de Lleida

Septiembre de 2017

Índice general

Agradecimientos

Resumen

Aunque uno de los problemas matemáticos más utilizados hoy en día en el diseño de protocolos criptográficos es 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), no todas las curvas elípticas existentes son válidas para su uso en él. Por lo que se sabe hasta ahora, la validez para el ECDLP de una curva elíptica E definida sobre un cuerpo finito $\mathbb{F}_q$ depende de su cardinal sobre $\mathbb{F}_q$. Como calcular el cardinal de E es un problema computacionalmente costoso, 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 $\mathbb{F}_q$. Para ello lo único que tenemos que hacer es calcular curvas elípticas d–isógenas a E sobre $\mathbb{F}_q$, es decir, debemos calcular d–isogenias $\mathbb{F}_q$–racionales.

Sea ℓ un número primo tal que ℓ no divide a q. El conjunto de todas las clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas ordinarias con un determinado cardinal sobre $\mathbb{F}_q$ puede ser representado mediante un grafo dirigido cuyos vértices son las clases de isomorfía y cuyos arcos representan ℓ–isogenias $\mathbb{F}_q$–racionales entre curvas elípticas de los vértices. Cada componente conexa de este digrafo es un volcán de ℓ–isogenias o ℓ–volcán sobre $\mathbb{F}_q$. Los vértices de un ℓ–volcán se distribuyen por niveles. El número total de niveles menos uno es su altura. Calcular la altura de un ℓ–volcán puede mejorar la eficiencia del algoritmo SEA, siendo el SEA el mejor algoritmo conocido actualmente para calcular el cardinal de una curva elíptica. Otras

aplicaciones de los volcanes de ℓ–isogenias las encontramos en el cálculo de los polinomios de clases de Hilbert o los polinomios modulares. En todas ellas es preciso recorrer los vértices de ℓ–volcanes.

En esta tesis, por un lado, damos nuevos métodos para recorrer los vértices de los volcanes de ℓ–isogenias. Por otro lado, conocida la valoración ℓ–ádica del cardinal de E sobre $\mathbb{F}_q$, estudiamos la valoración ℓ–ádica del cardinal de E sobre una extensión de grado k de $\mathbb{F}_q$. Conocida la estructura del subgrupo de ℓ–Sylow de E sobre $\mathbb{F}_q$, también estudiamos la del subgrupo de ℓ–Sylow de E sobre $\mathbb{F}_{q^k}$.

Resum

Avui en dia, un dels problemes matemàtics més utilitzats a l'hora de dissenyar protocols criptogràfics és el problema del logaritme discret sobre el grup de punts d'una corba el.líptica definida sobre un cos finit (ECDLP – Elliptic Curve Discrete Logarithm Problem). No obstant, no totes les corbes el.líptiques existents són vàlides per a aquest problema. Pel que se sap fins ara, la validesa per al ECDLP d'una corba el.líptica E definida sobre un cos finit $\mathbb{F}_q$ depèn del seu cardinal sobre $\mathbb{F}_q$. Donat que el càlcul del cardinal de E és un problema computacionalment costós, sembla raonable pensar que si E és vàlida, puguem obtenir a partir d'ella altres corbes el.líptiques que també ho siguin, és a dir, que també tinguin el seu mateix cardinal sobre $\mathbb{F}_q$. Per dur a terme aquesta tasca només hem de calcular corbes el.líptiques d–isògenes a E sobre $\mathbb{F}_q$, és a dir, hem de calcular d–isogènies $\mathbb{F}_q$–racionals.

Sigui ℓ un nombre primer tal que ℓ no divideix a q. El conjunt de totes les classes d'isomorfia sobre $\mathbb{F}_q$ de corbes el.líptiques ordinàries amb un determinat cardinal sobre $\mathbb{F}_q$ pot ser representat mitjançant un graf dirigit on els vèrtexs són les classes d'isomorfia i on els arcs representen ℓ–isogènies $\mathbb{F}_q$–racionals entre corbes el.líptiques dels vèrtexs. Cada component connexa d'aquest digraf és un volcà de ℓ–isogènies o ℓ–volcà sobre $\mathbb{F}_q$. Els vèrtexs d'un ℓ–volcà es distribueixen per nivells. El nombre total de nivells menys un és la seva altura. Calcular l'altura d'un ℓ–volcà pot millorar l'eficiència de l'algoritme SEA, sent aquest algoritme el millor conegut fins ara per al càlcul del cardinal d'una corba el.líptica. Altres aplicacions dels volcans de ℓ–isogènies les trobem en el càlcul dels polinomis de classes de Hilbert o dels

polinomis modulars. En totes elles cal recórrer els vèrtexs de ℓ–volcans.

En aquesta tesi, per una banda, donem nous métodes per recórrer els vèrtexs dels volcans de ℓ–isogènies. Per l'altra, coneguda la valoració ℓ–àdica del cardinal de E sobre $\mathbb{F}_q$, estudiem la valoració ℓ–àdica del cardinal de E sobre una extensió de grau k de $\mathbb{F}_q$. Coneguda l'estructura del subgrup de ℓ–Sylow de E sobre $\mathbb{F}_q$, també estudiem la del subgrup de ℓ–Sylow de E sobre $\mathbb{F}_{q^k}$.

Abstract

One of the most used mathematical problems for the design of modern cryptographic protocols is the discrete logarithm problem over the group of points of an elliptic curve defined over a finite field (ECDLP). However, not all existing elliptic curves are valid for this problem. The validity for the ECDLP of an elliptic curve E defined over a finite field $\mathbb{F}_q$ depends on its cardinality over $\mathbb{F}_q$. The computation of the group order of E is an expensive task. Therefore, if E has a "good" cardinality, it seems reasonable to obtain from E other elliptic curves with the same cardinality. For this task, we can compute some $\mathbb{F}_q$–rational d–isogenies of E, where d is a positive integer.

Let ℓ be a prime number such that ℓ does not divide q. The set of all $\mathbb{F}_q$–isomorphism classes of ordinary elliptic curves with a given group order over $\mathbb{F}_q$ can be represented as a directed graph whose vertices are the $\mathbb{F}_q$–isomorphism classes and whose arcs represent $\mathbb{F}_q$–rational ℓ–isogenies. Each connex component of this graph is a volcano of ℓ–isogenies or ℓ–volcano over $\mathbb{F}_q$. The vertices of a volcano of ℓ–isogenies can be stratified into levels. The number of levels minus one is called the height of the ℓ–volcano. The computation of this value can improve the SEA algorithm (the known best algorithm to compute the cardinality of an elliptic curve). Volcanoes of ℓ–isogenies have also been used to compute the Hilbert class polynomials or to compute the modular polynomials. In all these applications, it is necessary to go through the vertices of ℓ–volcanoes.

In this thesis, on one hand, we give new methods to go through the vertices of the ℓ–volcanoes. On the other hand, assuming the knowledge of

the ℓ–adic valuation of the cardinality of E over $\mathbb{F}_q$, we study the ℓ–adic valuation of the cardinality of E over an extension of degree k over $\mathbb{F}_q$. Assuming the structure of the ℓ–Sylow subgroup of E over $\mathbb{F}_q$ is known, we also study the structure of the ℓ–Sylow subgroup of E over $\mathbb{F}_{q^k}$.

Capítulo 1

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, GHS10]. 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 $\mathbb{F}_q$ [BSS99]. 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 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. Si a partir de E calculamos sucesivas ℓ–isogenias $\mathbb{F}_q$–racionales, entonces lo que obtenemos es un digrafo llamado volcán de ℓ–isogenias o ℓ–volcán cuyos vértices representan clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas ordinarias y cuyos arcos representan ℓ–isogenias $\mathbb{F}_q$–racionales. Los vértices de un ℓ–volcán se distribuyen en niveles. El nivel más alto se denomina cráter. El número total de niveles menos uno es la altura. El nivel más bajo, siempre y cuando la altura sea mayor que cero, se denomina el suelo. Para más información véase [Fou01, Sut13].

Recorrer eficazmente los vértices de un ℓ–volcán no es una tarea sencilla. Los primeros autores que abordaron este problema fueron Fouquet y Morain [FM02]. Su objetivo en [FM02] era, en primer lugar, determinar en qué nivel de un ℓ–volcán se halla una curva elíptica E y, en segundo lugar, a partir de E, ascender hasta el cráter, todo ello con el fin de calcular la altura del ℓ–volcán (en algunos casos puede determinarse a partir de las valoraciones ℓ–ádicas de $q-1$ y del cardinal de E sobre $\mathbb{F}_q$ [MMS$^+$06, MMS$^+$08]). Para

la primera tarea, principalmente, lo que hacen es calcular paralelamente tres caminos a partir de E. Escogen tres porque de esta forma se aseguran de que al menos uno de ellos será descendente hasta el suelo y, entonces, su longitud será el nivel donde se halla E (dicho método se basa en las ideas de Kohel [Koh96]). Utilizando este método llevan a cabo la segunda tarea. Por ejemplo, el siguiente paso sería calcular los niveles donde se hallan las curvas elípticas ℓ–isógenas de E para determinar si hay que ascender o no.

En [MST$^+$07], Miret et al. relacionan la estructura de los subgrupos de ℓ–Sylow de las curvas elípticas de un ℓ–volcán con los niveles donde éstas se hallan. Gracias a su trabajo, hasta un cierto nivel, llamado nivel de estabilidad, es posible determinar el nivel donde se halla una curva elíptica solamente conociendo la estructura de su subgrupo de ℓ–Sylow. Este hecho mejora el método anterior ya que no hay que calcular tres caminos. En relación a su trabajo, también debemos comentar que ellos clasifican los volcanes de ℓ–isogenias en regulares y no regulares: un ℓ–volcán es regular si y sólo si su nivel de estabilidad coincide con el nivel de su cráter.

En [IJ13], Ionica y Joux definen un nuevo nivel de estabilidad, el cual es igual o mayor que el anterior. A este nuevo nivel lo denominan el segundo nivel de estabilidad. Para su definición utilizan un emparejamiento simétrico. Ionica y Joux, hasta el segundo nivel de estabilidad, son capaces de determinar de una tacada qué ℓ–isogenias de una curva elíptica son no descendentes, por lo que su trabajo mejora las ideas iniciales de Fouquet y Morain.

La importancia de los volcanes de ℓ–isogenias radica en que permiten mejorar el algoritmo SEA [FM02], siendo el SEA [Sch95, IKNY98] el mejor algoritmo conocido actualmente para calcular el cardinal de una curva elíptica. A día de hoy también se utilizan para calcular los polinomios de clases de Hilbert [Sut11], los polinomios modulares [BLS12] y el anillo de endomorfismos de una curva elíptica ordinaria [Koh96, BS11].

1.1. Contribuciones

Tal y como acabamos de ver, recorrer los vértices de un ℓ–volcán ha sido un tema de estudio por varios autores. Aunque se ha avanzado mucho en dicho tema, aún quedan cuestiones por resolver. Por ejemplo, una cuestión sería la siguiente: dada una curva elíptica E situada más allá del segundo nivel de estabilidad de un ℓ–volcán, ¿es posible encontrar un método como el de Ionica y Joux para determinar qué ℓ–isogenias de E son no descendentes? La respuesta es sí y la abordamos en el siguiente artículo:

Distorting the volcano
enviado para publicar
[FMV17]

Antes de que diéramos con una posible solución al problema anterior, probamos con diferentes ideas. Aunque ninguna de ellas resultó ser válida, una sí que fue fructífera, ya que, en un determinado caso, nos permite recorrer eficazmente los vértices del cráter de un ℓ–volcán regular. Tal idea está recogida en el siguiente artículo:

Isogeny volcanoes of elliptic curves and Sylow subgroups
presentado en el congreso internacional
Latincrypt 2014
y publicado en la colección
Lecture Notes in Computer Science
[FMV15]

Gracias a la relación existente entre los niveles de un ℓ–volcán y los subgrupos de ℓ–Sylow de sus curvas elípticas, entre otros resultados, propios y no propios, hemos podido demostrar qué les sucede a los subgrupos de ℓ–Sylow cuando éstos se consideran sobre extensiones del cuerpo base. Este trabajo se encuentra recogido en los siguientes dos artículos:

On the ℓ–adic valuation of the cardinality
of elliptic curves over finite extensions of $\mathbb{F}_q$
publicado en la revista
Archiv der Mathematik
[MPV15]

On the 2–adic valuation of the cardinality
of elliptic curves over finite extensions of $\mathbb{F}_q$
enviado para publicar
[MPV17]

A continuación explicamos brevemente en qué consisten los artículos anteriores. Dicha explicación la hemos dividido en dos apartados: un primero que trata sobre volcanes de ℓ–isogenias y un segundo que trata sobre la valoración ℓ–ádica de los cardinales de curvas elípticas.

1.1.1. Volcanes de ℓ–isogenias

Dada una curva elíptica ordinaria E definida sobre un cuerpo finito $\mathbb{F}_q$ de característica $p \geq 5$ y dado un número primo $\ell \neq p$, en [FMV15] explicamos el comportamiento de una determinada isogenia de grado una potencia de ℓ en el volcán de ℓ–isogenias sobre $\mathbb{F}_q$ al que pertenece E. Concretamente, si $h \geq 1$ es la altura del ℓ–volcán y $P \in E(\mathbb{F}_q)$ es de orden ℓ^n, siendo $n \geq 2$ la valoración ℓ–ádica de $\#E(\mathbb{F}_q)$, entonces explicamos el comportamiento de la isogenia de núcleo $\langle P \rangle$: primero es ascendente (h pasos), después puede ser horizontal ($n - 2h$ pasos) y finalmente es descendente (h pasos). Gracias a este comportamiento somos capaces de diseñar un algoritmo para recorrer los vértices del cráter del ℓ–volcán siempre y cuando éste sea regular, $n > 2h$ y $c \geq 3$, siendo c el tamaño del cráter. Si $n - 2h \geq 2$, entonces nuestro algoritmo es más eficiente que el que podríamos diseñar con las ideas de Ionica y Joux.

Supongamos, ahora, que $\ell \geq 5$ y que no hay restricciones para p, es decir, p puede ser 2 o 3. Al igual que Ionica y Joux, en [FMV17] damos

una condición para determinar qué ℓ–isogenias $\mathbb{F}_q$–racionales de E son no descendentes. Dicha condición se basa en un endomorfismo φ de E, el cual se define como uno de los dos ciclos de m–isogenias que hay en el cráter del m–volcán sobre $\mathbb{F}_q$ al que pertenece E, siendo $m \neq \ell$ y estando E situada en el cráter. Para que la condición funcione, φ tiene que ser una aplicación de distorsión para un subgrupo $\mathbb{F}_q$–racional de orden ℓ de E. Gracias a esta condición, con diferentes números primos m, somos capaces de alcanzar y detectar el cráter del ℓ–volcán sobre $\mathbb{F}_q$ al que pertenece E. Además, nuestro método puede aplicarse más allá del segundo nivel de estabilidad.

1.1.2. Valoración ℓ–ádica de los cardinales

Dada una curva elíptica E definida sobre un cuerpo finito $\mathbb{F}_q$ de característica $p \neq 2$ y dado un número primo $\ell \neq 2, p$ tal que $\ell \mid \#E(\mathbb{F}_q)$, en [MPV15] estudiamos la diferencia entre la valoración ℓ–ádica de $\#E(\mathbb{F}_{q^k})$ y la de $\#E(\mathbb{F}_q)$, siendo k un entero positivo. Dicha diferencia es mayor que 0 si y sólo si $\ell \mid k$ o $q \not\equiv 1 \pmod{\ell}$ y $d \mid k$, siendo d el orden multiplicativo de q en $\mathbb{F}_\ell^*$. Además, si τ es la valoración ℓ–ádica de k, entonces

$$v_\ell(\#E(\mathbb{F}_{q^k})) = \begin{cases} v_\ell(\#E(\mathbb{F}_{q^{\ell^\tau}})) & \text{si } \begin{cases} q \equiv 1 \pmod{\ell}, \\ q \not\equiv 1 \pmod{\ell} \text{ y } d \nmid k, \end{cases} \\ v_\ell(\#E(\mathbb{F}_{q^{d\ell^\tau}})) & \text{si } q \not\equiv 1 \pmod{\ell} \text{ y } d \mid k. \end{cases}$$

Por lo tanto, en [MPV15] llegamos a la conclusión de que solamente debemos de estudiar dos casos:

1. $k = \ell$,
2. $k = d$ cuando $q \not\equiv 1 \pmod{\ell}$.

Para $k = \ell \geq 5$ obtenemos el siguiente resultado:

$$v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q)) = \begin{cases} 1 & \text{si } q \not\equiv 1 \pmod{\ell}, \\ 2 & \text{si } q \equiv 1 \pmod{\ell}. \end{cases}$$

En [MPV15], conocida la estructura del subgrupo de ℓ–Sylow de E sobre $\mathbb{F}_q$, también estudiamos la de E sobre $\mathbb{F}_{q^k}$. Para $k = \ell \geq 5$ obtenemos lo siguiente:

- $q \not\equiv 1 \pmod{\ell}$:

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^n\mathbb{Z} \quad \Longrightarrow \quad E[\ell^\infty](\mathbb{F}_{q^k}) \simeq \mathbb{Z}/\ell^{n+1}\mathbb{Z}$$

- $q \equiv 1 \pmod{\ell}$:

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^r\mathbb{Z}\times\mathbb{Z}/\ell^s\mathbb{Z} \quad \Longrightarrow \quad E[\ell^\infty](\mathbb{F}_{q^k}) \simeq \mathbb{Z}/\ell^{r+1}\mathbb{Z}\times\mathbb{Z}/\ell^{s+1}\mathbb{Z}$$

En [MPV17] ampliamos el trabajo anterior para $\ell = 2$. En dicho artículo p puede ser 2 y ℓ no tiene porque dividir a $\#E(\mathbb{F}_q)$.

1.2. Estructura

En este primer capítulo hemos contextualizado la tesis y hemos presentado los resultados obtenidos. En el capítulo 2 damos aquellos conceptos básicos para poder seguir posteriormente el capítulo siguiente. En el capítulo 3 damos los cuatro artículos que forman esta tesis. Finalmente, el capítulo 4 está dedicado a las conclusiones.

Capítulo 2

Preliminares

En este capítulo explicamos la teoría necesaria para poder entender posteriormente los artículos del capítulo siguiente. En él hemos usado las siguientes notaciones:

- $\mathbb{K}$: un cuerpo cualquiera;
- $\overline{\mathbb{K}}$: clausura algebraica de $\mathbb{K}$;
- $\mathbb{F}_q$: cuerpo finito de q elementos y característica p;
- ℓ : número primo distinto de p.

2.1. 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].

2.2. Curvas elípticas

Una curva elíptica E definida sobre $\mathbb{K}$ es una curva sin puntos singulares que viene dada por una ecuación de Weierstrass de la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{K}. \tag{2.1}$$

La ecuación (2.1) define una curva sin puntos singulares si y sólo si $\Delta \neq 0$, siendo

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

con

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

El j–invariante de E es

$$j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta}.$$

El conjunto de puntos $\mathbb{K}$–racionales de E se define como

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid (x, y) \text{ satisface } (2.1)\} \cup \{\mathcal{O}\}$$

donde $\mathcal{O}$ es un punto especial llamado punto del infinito. Este conjunto tiene estructura de grupo abeliano con una operación de suma cuyo elemento neutro es $\mathcal{O}$ (véase [Sil86]). Mediante el uso de esta operación es posible multiplicar un entero m por un punto $P \in E(\mathbb{K})$:

$$mP = \begin{cases} \underbrace{P + \cdots + P}_{m \text{ veces}} & \text{si } m > 0, \\ \mathcal{O} & \text{si } m = 0, \\ \underbrace{(-P) + \cdots + (-P)}_{m \text{ veces}} & \text{si } m < 0. \end{cases}$$

Sea E una curva elíptica definida sobre $\mathbb{F}_q$. Si $\#E(\mathbb{F}_q)$ denota el cardinal de $E(\mathbb{F}_q)$, entonces

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

con $|t| \leq 2\sqrt{q}$. Si $t^2 = 0$, q, $2q$, $3q$ o $4q$, entonces E es supersingular. En caso contrario, E es ordinaria.

El orden de un punto $P \in E(\mathbb{F}_q)$, denotado por $\mathrm{ord}(P)$, es el menor entero positivo n tal que $nP = \mathcal{O}$. El subgrupo generado por P es

$$\langle P \rangle = \{P, 2P, \ldots, nP\}.$$

El orden de $\langle P \rangle$, como es obvio, es n. El punto P es de m–torsión, $m > 0$, si y sólo si $mP = \mathcal{O}$. El conjunto de todos los puntos de m–torsión de $E(\mathbb{F}_q)$, denotado por $E[m](\mathbb{F}_q)$, es un subgrupo de $(E(\mathbb{F}_q), +)$. Este subgrupo, si no es trivial, o bien es cíclico o bien es de rango 2. El subgrupo de ℓ–Sylow de E sobre $\mathbb{F}_q$ se define como

$$E[\ell^\infty](\mathbb{F}_q) = \{P \in E(\mathbb{F}_q) \mid \mathrm{ord}(P) = \ell^e\}.$$

Este subgrupo, al igual que el anterior, puede ser trivial, cíclico o de rango 2.

Sean E y E' dos curvas elípticas definidas sobre $\mathbb{F}_q$. Un isomorfismo sobre $\mathbb{F}_q$ entre E y E' es una aplicación regular biyectiva sobre $\mathbb{F}_q$ entre ambas que preserva el punto del infinito. Si existe un isomorfismo sobre $\mathbb{F}_q$ entre E y E', entonces E y E' son isomorfas sobre $\mathbb{F}_q$. Este hecho se denota por $E \simeq E'$. Si E y E' son ordinarias, entonces $E \simeq E'$ si y sólo si $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$ y $j(E) = j(E')$. Todas las curvas elípticas isomorfas a E sobre $\mathbb{F}_q$ forman una clase de isomorfía sobre $\mathbb{F}_q$.

Para más información véase [Sil86].

2.3. Isogenias de curvas elípticas

En esta sección explicamos qué son las isogenias de curvas elípticas.

2.3.1. 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. *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. *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. *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* $\ker \varphi_G = G$.

Nota. E/G y φ_G pueden calcularse utilizando las fórmulas de Vélu [Vé71].

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

Nota. 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 capítulo, y salvo que no digamos lo contrario, supondremos que todas las isogenias son separables.

Para obtener más información sobre lo explicado en este apartado véase [Sil86].

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

Sea E una curva elíptica definida sobre $\mathbb{F}_q$. El conjunto de todas las isogenias (separables y no separables) 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 este apartado la hemos extraído de [Cox89, Fou01, Koh96, Sil86].

2.4. Volcanes de ℓ–isogenias

En esta sección explicamos qué son los volcanes de ℓ–isogenias.

2.4.1. 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 el apartado 2.3.2, 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 el apartado 2.3.2). Otra característica importante de estos órdenes es que sus conductores difieren los unos de los otros únicamente en una 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:

- $h = 0$

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

- $h = 1$

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

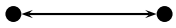
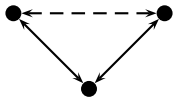
$$\Big| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$$

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

- $h \geq 2$

$$
\begin{array}{lll}
O_0 = \mathbb{Z} + \ell^0 w O_K & \text{NIVEL } h & \left(\begin{array}{c} \ell \nmid [O_K : O_0] \\ \ell \mid [O_0 : \mathbb{Z}[\pi]] \end{array} \right) \quad \text{CRÁTER} \\
\vdots & & \\
O_k = \mathbb{Z} + \ell^k w O_K & \text{NIVEL } h-k & \left(\begin{array}{c} \ell \mid [O_K : O_k] \\ \ell \mid [O_k : \mathbb{Z}[\pi]] \end{array} \right) \quad \text{LADERA} \\
\vdots & & \\
O_h = \mathbb{Z} + \ell^h w O_K & \text{NIVEL } 0 & \left(\begin{array}{c} \ell \mid [O_K : O_h] \\ \ell \nmid [O_h : \mathbb{Z}[\pi]] \end{array} \right) \quad \text{SUELO}
\end{array}
$$

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 $s/2$. 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.

En la figura 2.1 mostramos la estructura de un 3–volcán con $h = c = 3$.

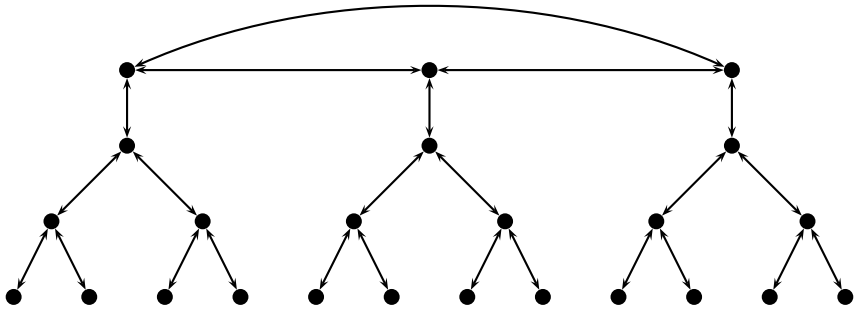


Figura 2.1: Volcán de 3–isogenias.

Para obtener más información sobre lo explicado en este apartado véase [Fou01, Koh96, Sut13].

2.4.2. Subgrupos de ℓ–Sylow y ℓ–volcanes

Sea E una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ y sea V el volcán de ℓ–isogenias sobre $\mathbb{F}_q$ al que pertenece E. Si $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z}$

con $r \geq s \geq 0$ y $r + s \geq 1$, entonces se tiene lo siguiente (véase [MST$^+$07]):

- Si $s < r$, entonces E se halla en el nivel s de V;
- Si $s = r$, entonces E se halla como mínimo en el nivel s de V.

El nivel de V a partir del cual, al ir descendiendo, la estructura del subgrupo de ℓ–Sylow es diferente en cada nivel se denomina el nivel de estabilidad. Se dice que V es regular si y sólo si el nivel de estabilidad coincide con su cráter.

Sea $n = r + s$ y sean E_0, E_1, ..., E_h curvas elípticas de V situadas, respectivamente, en el nivel 0, 1, ..., h, con h la altura de V. Entonces, por lo anterior, tenemos lo siguiente:

- Si V es regular ($n \geq 2h$),

$$\begin{aligned} E_0[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^n\mathbb{Z}, \\ E_1[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^{n-1}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}, \\ &\vdots \\ E_h[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^{n-h}\mathbb{Z} \times \mathbb{Z}/\ell^h\mathbb{Z}; \end{aligned}$$

- Si V no es regular (n par y $n < 2h$),

$$\begin{aligned} E_0[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^n\mathbb{Z}, \\ E_1[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^{n-1}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \\ &\vdots \\ E_{\frac{n}{2}}[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}, \\ &\vdots \\ E_h[\ell^\infty](\mathbb{F}_q) &\simeq \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z} \times \mathbb{Z}/\ell^{\frac{n}{2}}\mathbb{Z}. \end{aligned}$$

Capítulo 3

Artículos

El orden escogido para mostrar los artículos es el siguiente:

1. [FMV15] "Isogeny volcanoes of elliptic curves and Sylow subgroups";
2. [FMV17] "Distorting the volcano";
3. [MPV15] "On the ℓ–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$";
4. [MPV17] "On the 2–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$".

Por motivos de copyright solamente mostramos la primera página de cada artículo.

Isogeny Volcanoes of Elliptic Curves and Sylow Subgroups

Mireille Fouquet[1], Josep M. Miret[2], and Javier Valera[2(✉)]

[1] Institut de Mathématiques de Jussieu, Université Paris Diderot - Paris 7, Paris, France
fouquet@math.univ-paris-diderot.fr
[2] Dept. de Matemàtica, Universitat de Lleida, Lleida, Spain
{miret,jvalera}@matematica.udl.cat

Abstract. Given an ordinary elliptic curve over a finite field located in the floor of its volcano of ℓ-isogenies, we present an efficient procedure to take an ascending path from the floor to the level of stability and back to the floor. As an application for regular volcanoes, we give an algorithm to compute all the vertices of their craters. In order to do this, we make use of the structure and generators of the ℓ-Sylow subgroups of the elliptic curves in the volcanoes.

Keywords: Elliptic curves · Isogeny volcanoes · Sylow subgroups · Finite fields

1 Introduction

In the last decades, the usage of elliptic curves over finite fields in the design of secure cryptography protocols has grown significantly. Nevertheless, not all elliptic curves are useful in cryptography based on the discrete logarithm problem, since they must satisfy certain requirements related to their group orders or their embedding degrees. Concerning their group orders, they must be of the form $f \cdot q$ with q prime and f a small integer, otherwise the curves are vulnerable to the Pohlig-Hellman attack [17]. Regarding their embedding degrees, they must be ≥ 6 for curves of 160 bits, otherwise the curves are vulnerable to the MOV attack [12].

Isogenies between elliptic curves over finite fields, in particular, prime degree isogeny chains, have long been a subject of study with different approaches, since they play a central role in the SEA algorithm (see [3,18]) to compute the group order of an elliptic curve. The basic idea of this algorithm is the computation of the trace of the Frobenius endomorphism of a curve modulo different suitably chosen small primes ℓ.

Given two ordinary elliptic curves E and E' over a finite field $\mathbb{F}_q$ with endomorphism rings $\mathcal{O}$ and $\mathcal{O}'$, respectively, and an isogeny $\mathcal{I} : E \to E'$ of degree a prime ℓ such that $\ell \nmid q$, Fouquet and Morain [6] introduced, from the Kohel's Ph.D. thesis [9], the notion of direction of an ℓ-isogeny. It is *ascending, horizontal* or *descending* whether the index $[\mathcal{O}' : \mathcal{O}]$ is ℓ, 1 or $1/\ell$ respectively. With this

D.F. Aranha and A. Menezes (Eds.): LATINCRYPT 2014, LNCS 8895, pp. 162–175, 2015.
DOI: 10.1007/978-3-319-16295-9_9

Distorting the volcano

Mireille Fouquet[a], Josep M. Miret[b], Javier Valera[b,*]

[a] *Institut de Mathématiques de Jussieu - Paris Rive Gauche, Université Paris Diderot - Paris 7, France*
[b] *Departament de Matemàtica, Universitat de Lleida, Spain*

Abstract

Volcanoes of ℓ–isogenies of elliptic curves are a special case of graphs with a cycle called crater. In this paper, given an elliptic curve E of a volcano of ℓ–isogenies, we present a condition over an endomorphism φ of E in order to determine which ℓ–isogenies of E are non-descending. The endomorphism φ is defined as the crater cycle of an m–volcano where E is located, with $m \neq \ell$. The condition is feasible when φ is a distortion map for a subgroup of order ℓ of E. We also provide some relationships among the crater sizes of volcanoes of m–isogenies whose elliptic curves belong to a volcano of ℓ–isogenies.

Keywords: finite field, elliptic curve, isogeny, volcano, distortion map.
2010 MSC: 14H52, 14K02.

1. Introduction

Ordinary elliptic curves over a finite field $\mathbb{F}_q$ with the same cardinality together with ℓ–isogenies among them, where ℓ is a prime such that $\ell \nmid q$, can be represented in special graphs called volcanoes of ℓ–isogenies. These structures have interesting applications such as determining the endomorphism ring of an elliptic curve [15] or computing its group order in the SEA algorithm [21].

In a volcano of ℓ–isogenies the vertices are distributed in levels and the arcs represent ℓ–isogenies [11, 15]. The number of levels of a volcano minus one is its height. The vertices located in the highest level belong to a cycle called crater. An arc which goes out from a vertex of the level k can only go inwards to a vertex of the level $k+1$, k or $k-1$. Moreover, horizontal arcs can only occur at the crater. In each case it is said that the arc is, respectively, descending, horizontal or ascending.

Fouquet and Morain [11] gave an algorithm to compute the height of a volcano of ℓ–isogenies using an exhaustive search of several paths in the volcano. As

*Corresponding author
Email addresses: fouquet@math.univ-paris-diderot.fr (Mireille Fouquet), miret@matematica.udl.cat (Josep M. Miret), jvalera@matematica.udl.cat (Javier Valera)

Arch. Math. 105 (2015), 261–269

0003-889X/15/030261-9
published online August 20, 2015
DOI 10.1007/s00013-015-0798-6

Archiv der Mathematik

On the ℓ-adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$

Josep M. Miret, Jordi Pujolàs, and Javier Valera

Abstract. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of odd characteristic. Let $\ell \neq 2$ be a prime number different from the characteristic and dividing $\#E(\mathbb{F}_q)$. We describe how the ℓ-adic valuation of the number of points grows by taking finite extensions of the base field. We also investigate the group structure of the corresponding ℓ-Sylow subgroups.

Mathematics Subject Classification. 11G20.

Keywords. Elliptic curve, Finite field, Group order, ℓ-adic valuation.

1. Introduction. Let q be a power of a prime $p \neq 2$, and let E be an elliptic curve over a finite field $\mathbb{F}_q$. We compute the difference of valuations $v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q))$, where k is a natural number and $\ell \neq 2$, p is a prime number dividing $\#E(\mathbb{F}_q)$ (Theorems 1, 2). Our result agrees with the predictions of Iwasawa Theory.

Under the given assumptions, $v_\ell(\#E(\mathbb{F}_{q^k}))-v_\ell(\#E(\mathbb{F}_q)) > 0$ only if $v_\ell(k) > 0$ or if k is divisible by the multiplicative order d of q in $\mathbb{F}_\ell^*$ (see Proposition 2). Hence we can reduce the proofs to the cases $k = \ell$ or $k = d$. We also describe how the group structure of the ℓ-Sylow subgroup $E[\ell^\infty](\mathbb{F}_{q^k})$ changes with k. Namely, if

$$E[\ell^\infty](\mathbb{F}_q) \cong \mathbb{Z}/\ell^r\mathbb{Z} \times \mathbb{Z}/\ell^s\mathbb{Z} \quad \text{with} \quad 0 \leq r \leq s \quad \text{and} \quad r + s \geq 1,$$

we show how to determine integers r_k, s_k such that $E[\ell^\infty](\mathbb{F}_{q^k}) \cong \mathbb{Z}/\ell^{r_k}\mathbb{Z} \times \mathbb{Z}/\ell^{s_k}\mathbb{Z}$.

On this regard, a partial answer appeared in [3, Proposition 6.3] for $k = \ell$. The case of ordinary elliptic curves with $k = \ell$, $q \equiv 1 \pmod{\ell}$ and $t^2 - 4q \equiv 0 \pmod{\ell^2}$, for t the trace of the Frobenius endomorphism, was covered in [4, Proposition 4.2] using pairings. The case of supersingular elliptic curves for

On the 2-adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$

Josep M. Miret Jordi Pujolàs Javier Valera

Abstract. In this paper we study the difference between the 2-adic valuations of the cardinalities $\#E(\mathbb{F}_{q^k})$ and $\#E(\mathbb{F}_q)$ of elliptic curves E over $\mathbb{F}_q$. We also deduce information about the structure of the 2-Sylow subgroup $E[2^\infty](\mathbb{F}_{q^k})$ from the exponents of $E[2^\infty](\mathbb{F}_q)$.

1. Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p and let k be a positive integer. In this paper we are interested in the 2-adic valuation $v_2(\#E(\mathbb{F}_{q^k}))$ of the number of $\mathbb{F}_{q^k}$-valuated points of E compared to $v_2(\#E(\mathbb{F}_q))$. Moreover, if r and s are the exponents of the 2-primary subgroup

$$E[2^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2^s\mathbb{Z}, \qquad 0 \leq r \leq s,$$

we study the exponents of

$$E[2^\infty](\mathbb{F}_{q^k}) \simeq \mathbb{Z}/2^{r+\alpha}\mathbb{Z} \times \mathbb{Z}/2^{s+\beta}\mathbb{Z},$$

with, of course, $\alpha + \beta = v_2(\#E(\mathbb{F}_{q^k})) - v_2(\#E(\mathbb{F}_q))$.

In [8] we considered the analogous problem regarding ℓ-adic valuations of the cardinalities in the cases $\ell \neq 2$, under the assumptions q odd, $\ell \nmid q$ and $\ell \mid \#E(\mathbb{F}_q)$. Hence, in a sense the present paper complements [8]. As in [8], when E is ordinary and $2 \mid \#E(\mathbb{F}_q)$ our results agree with Iwasawa Theory [12, Theorem 13.13 and p. 130], which for large enough τ predicts $v_2(\#E(\mathbb{F}_{q^{2^\tau}})) = \lambda\tau + \nu$ for $0 \leq \lambda \leq 2$ and ν a constant (see Tables 1, 2, Propositions 1, 3 and Corollary 1).

In Section 2 we deal with even cardinality and in Section 3 with odd cardinality. Section 2 accounts for cases considered previously by other authors under various assumptions (see [3, 5]).

We let ϕ^k be the Frobenius endomorphism of E over $\mathbb{F}_{q^k}$ and we let t_k be the trace of ϕ^k (we write ϕ and t instead of ϕ^1 and t_1). In this paper we are using the well known formulas $t_2 = t^2 - 2q$ and $t_3 = t^3 - 3qt$.

Capítulo 4

Conclusiones

Las conclusiones a las que hemos llegado para cada artículo son las que a continuación damos.

Artículo 1

Isogeny volcanoes of elliptic curves and Sylow subgroups [FMV15]

Sea $\mathbb{F}_q$ un cuerpo finito de característica $p \geq 5$, sea $\ell \neq p$ un número primo, sea E una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ tal que $E[\ell^\infty](\mathbb{F}_q) = \langle P \rangle \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ con $n \geq 2$, sea V el volcán de ℓ–isogenias sobre $\mathbb{F}_q$ al que pertenece E y sean $h \geq 1$ y c la altura y el tamaño del cráter de V. En [FMV15] hemos probado que el comportamiento en V de la isogenia de núcleo $\langle P \rangle$ es el siguiente: primero es ascendente (h ℓ–isogenias), después puede ser horizontal ($n - 2h$ ℓ–isogenias) y finalmente es descendente (h ℓ–isogenias). Gracias a este comportamiento, cuando V es regular, $n > 2h$ y $c \geq 3$, hemos diseñado un algoritmo para recorrer todos los vértices del cráter de V. Cuando $n - 2h \geq 2$, nuestro algoritmo es más eficiente que el que podríamos diseñar con las ideas de Ionica y Joux.

Artículo 2

Distorting the volcano [FMV17]

Sea $\mathbb{F}_q$ un cuerpo finito, sea $\ell \geq 5$ un número primo tal que $\ell \nmid q$ y sea E una curva elíptica ordinaria definida sobre $\mathbb{F}_q$ tal que $j(E) \neq 0, 1728$ y

$E[\ell](\mathbb{F}_q) \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Mediante el uso de un determinado endomorfismo φ de E, en [FMV17] hemos diseñado un algoritmo (NonDescending) para determinar qué ℓ–isogenias de E son no descendentes. Tal endomorfismo φ se define como uno de los dos ciclos de m–isogenias que hay en el cráter del m–volcán sobre $\mathbb{F}_q$ al que pertenece E, siendo $m \neq \ell$ y estando E situada en el cráter. Para poder aplicar el algoritmo, φ tiene que ser una aplicación de distorsión para un subgrupo G de $(E(\mathbb{F}_q), +)$ de orden ℓ, es decir, $\varphi(G)$ tiene que ser distinto de G. Si esto es así, entonces los subgrupos de orden ℓ de $(E(\mathbb{F}_q), +)$ que son invariantes bajo la acción de φ son los núcleos de las ℓ–isogenias no descendentes de E. En [FMV17] hemos probado que siempre existen m_i–volcanes sobre $\mathbb{F}_q$ con tamaños de cráter $c_i = 1$ con los que poder construir aplicaciones de distorsión φ_i. Hemos dejado como trabajo futuro cómo encontrarlos. Finalmente debemos comentar que el algoritmo NonDescending puede aplicarse más allá del segundo nivel de estabilidad y que es eficiente para valores pequeños de m y c.

Artículos 3 y 4

On the ℓ–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$ [MPV15]

On the 2–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$ [MPV17]

Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ de característica p, sea ℓ un número primo y sea k un entero positivo. En [MPV15] y [MPV17] hemos estudiado cuánto crece la valoración ℓ–ádica del cardinal de E sobre $\mathbb{F}_q$ al considerarlo sobre $\mathbb{F}_{q^k}$. También hemos estudiado cómo cambia la estructura del subgrupo de ℓ–Sylow de E sobre $\mathbb{F}_q$ al considerarlo sobre $\mathbb{F}_{q^k}$. En ambos artículos hemos probado que

$$v = v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q))$$

es mayor que 0 solamente en un determinado número de casos. El caso más representativo de todos ellos se nos presenta cuando $p \neq 2$, $k = \ell \neq p$,

$\ell \mid \#E(\mathbb{F}_q)$ y E es ordinaria. Para $\ell \geq 5$ hemos obtenido el siguiente resultado:

- $q \not\equiv 1 \pmod{\ell}$: $\quad v = 1$

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^n\mathbb{Z} \quad \Longrightarrow \quad E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{n+1}\mathbb{Z}$$

- $q \equiv 1 \pmod{\ell}$: $\quad v = 2$

$$E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^r\mathbb{Z}\times\mathbb{Z}/\ell^s\mathbb{Z} \quad \Longrightarrow \quad E[\ell^\infty](\mathbb{F}_{q^\ell}) \simeq \mathbb{Z}/\ell^{r+1}\mathbb{Z}\times\mathbb{Z}/\ell^{s+1}\mathbb{Z}$$

Por lo tanto, para $\ell \geq 5$ hemos caracterizado v y $E[\ell^\infty](\mathbb{F}_{q^\ell})$ solamente a partir de la congruencia de q módulo ℓ. Para $\ell = 3$ hemos obtenido el mismo resultado que para $\ell \geq 5$ a excepción de cuando $q \equiv 1 \pmod{3}$ y $\#E(\mathbb{F}_q) \equiv 3 \pmod{9}$. En dicho caso, la caracterización la hemos realizado en función de ℓ, q y t, siendo t la traza del endomorfismo de Frobenius de orden q de E. El resultado para $\ell = 2$ de v es el siguiente:

- $v_2(\#E(\mathbb{F}_q)) > v_2(q+1) + 1$: $\quad v = v_2(q+1) + 1$;
- $v_2(\#E(\mathbb{F}_q)) = v_2(q+1) + 1$: $\quad v > v_2(\#E(\mathbb{F}_q))$;
- $v_2(\#E(\mathbb{F}_q)) < v_2(q+1) + 1$: $\quad v = v_2(\#E(\mathbb{F}_q))$.

Por lo tanto, para $\ell = 2$, a excepción de un caso, hemos caracterizado v a partir de las valoraciones 2–ádicas de $\#E(\mathbb{F}_q)$ y de $q+1$. Mediante el uso de los volcanes de 2–isogenias, hemos dado la estructura de $E[2^\infty](\mathbb{F}_{q^2})$. Como conclusión final hemos de decir que nuestros resultados concuerdan con las predicciones de la teoría de Iwasawa.

Bibliografía

[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, 1993.

[BLS12] R. Bröker, K. Lauter, and A. V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012.

[BS11] G. Bisson and A. V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 131(5):815–831, 2011.

[BSS99] 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, 1999.

[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., 1989.

[FM02] M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *ANTS–V*, volume 2369 of *Lecture Notes in Computer Science*, pages 276–291. Springer, 2002.

[FMV15] M. Fouquet, J. M. Miret, and J. Valera. Isogeny volcanoes of elliptic curves and Sylow subgroups. In *Latincrypt 2014*, volume 8895 of *Lecture Notes in Computer Science*, pages 162–175. Springer, 2015.

[FMV17] M. Fouquet, J. M. Miret, and J. Valera. Distorting the volcano, 2017. Submitted.

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

[GHS10] V. Gayoso, L. Hernández, and C. Sánchez. A survey of the Elliptic Curve Integrated Encryption Scheme. *Journal of Computer Science and Engineering*, 2(2):7–13, 2010.

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

[IJ13] S. Ionica and A. Joux. Pairing the volcano. *Mathematics of Computation*, 82(281):581–603, 2013.

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

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

[MMS+06] J. M. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. An algorithm to compute volcanoes of 2–isogenies of elliptic curves over finite fields. *Applied Mathematics and Computation*, 176(2):739–750, 2006.

[MMS+08] J. M. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of ℓ–isogenies of elliptic

curves over finite fields. *Applied Mathematics and Computation*, 196(1):67–76, 2008.

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

[MPV15] J. M. Miret, J. Pujolàs, and J. Valera. On the ℓ–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$. *Archiv der Mathematik*, 105(3):261–269, 2015.

[MPV17] J. M. Miret, J. Pujolàs, and J. Valera. On the 2–adic valuation of the cardinality of elliptic curves over finite extensions of $\mathbb{F}_q$, 2017. Submitted.

[MST+07] J. M. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls. Volcanoes of ℓ–isogenies of elliptic curves over finite fields: the case $\ell = 3$. *Publicacions Matemàtiques*, EXTRA:165–180, 2007.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.

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

[Sut11] A. V. Sutherland. Computing Hilbert class polynomials with the Chinese Remainder Theorem. *Mathematics of Computation*, 80(273):501–538, 2011.

[Sut13] A. V. Sutherland. Isogeny volcanoes. In *ANTS X*, volume 1 of *The Open Book Series*, pages 507–530. Mathematical Sciences Publishers, 2013.

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