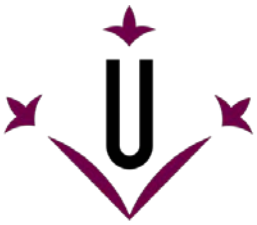


Distorting the volcano

Mireille Fouquet Josep M. Miret Javier Valera

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.

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 [16] or computing its group order in the SEA algorithm [22].

In a volcano of ℓ–isogenies the vertices are distributed in levels and the arcs represent ℓ–isogenies [12, 16]. 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 [12] gave an algorithm to compute the height of a volcano of ℓ–isogenies using an exhaustive search of several paths in the volcano. As a consequence, some computational improvements were obtained for the SEA algorithm. Later, Ionica and Joux [15], using a symmetric pairing on the ℓ–Sylow subgroup of an elliptic curve, proposed a method to determine the direction of an ℓ–isogeny, that is, descending, horizontal or ascending. This allows us to calculate the height of a volcano more efficiently. Volcanoes of ℓ–isogenies have also been used by Sutherland [24] for the computation of Hilbert class polynomials. Other applications have been provided by Bisson and Sutherland [1] to compute the endomorphism ring of an ordinary elliptic curve and by Bröker, Lauter and Sutherland [3] to compute modular polynomials. Recently, Moody

[20] has studied how to compute a volcano of ℓ–isogenies from the knowledge of volcanoes of m–isogenies, $m \neq \ell$.

In this paper, given an ordinary elliptic curve E over $\mathbb{F}_q$, we give a condition for determining which ℓ–isogenies of E are non-descending. For this purpose we consider an endomorphism of E which acts as a distortion map. As a consequence, we present an algorithm which returns an ascending path from E in the volcano of ℓ–isogenies where it belongs.

The paper is structured as follows. Section 2 introduces some concepts and notations about volcanoes of ℓ–isogenies. Section 3 provides some preliminary results concerning the existence and direction of isogenies. In Section 4 we give a characterization for the kernels of the non-descending ℓ–isogenies. In Section 5 we present some relationships among the crater sizes of volcanoes of m–isogenies whose elliptic curves belong to a volcano of ℓ–isogenies. In Section 6 we propose an algorithm for computing an ascending path in a volcano of ℓ–isogenies and we study its complexity. Section 7 is devoted to showing several examples. Finally, in Section 8 we give our conclusions about this paper.

Throughout this paper we consider elliptic curves over a finite field $\mathbb{F}_q$ of characteristic p, with j–invariant different from 0 and 1728. Furthermore, we denote by ℓ and m two distinct primes different from p.

2 Volcanoes of ℓ–isogenies

In this section we introduce the concept of volcano of ℓ–isogenies and we provide some notations and some of their properties.

We denote by $E/\mathbb{F}_q$ an elliptic curve over $\mathbb{F}_q$, by $E(\mathbb{F}_q)$ its group of rational points with O_E its neutral element and by $j(E)$ its j–invariant.

Given an ordinary elliptic curve $E/\mathbb{F}_q$ with group order $N = q + 1 - t$, where t is the trace of the Frobenius endomorphism of $E/\mathbb{F}_q$, its endomorphism ring $\mathrm{End}(E)$ can be identified with an order of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{t^2 - 4q})$ (see [23]). The order $\mathcal{O} \simeq \mathrm{End}(E)$ satisfies [6]

$$\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K,$$

where $\mathcal{O}_K$ is the ring of integers of K and π is the Frobenius endomorphism of $E/\mathbb{F}_q$. Writing

$$t^2 - 4q = g^2 d_K,$$

where d_K is the discriminant of K, it turns out that g is the conductor of the order $\mathbb{Z}[\pi]$ in the maximal order $\mathcal{O}_K$. Then the conductor f of $\mathcal{O}$ divides g.

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 given an isogeny $\mathcal{I} : E \to E'$ of degree a prime ℓ such that $\ell \nmid q$, Kohel [16] introduces the notion of direction of an ℓ–isogeny. The ℓ–isogeny $\mathcal{I}$ is ascending, horizontal or descending whether the index $[\mathcal{O}' : \mathcal{O}]$ is ℓ, 1 or $1/\ell$ respectively. With this notion of direction for the ℓ–isogenies, the set of isomorphism classes of ordinary elliptic curves over $\mathbb{F}_q$ with a given cardinality can be represented as a directed graph whose vertices

are the isomorphism classes and whose arcs represent ℓ–isogenies. It is worth remarking that if two vertices are connected by an arc, the corresponding dual ℓ–isogeny is represented as an arc in the other direction.

Each connected component of this graph is called a volcano of ℓ–isogenies. The vertices of a volcano can be stratified into levels so that the curves in each level have isomorphic endomorphism rings. A volcano consists of a unique cycle at the top level, called crater, and from each vertex of the cycle hangs $\ell+1$, ℓ or $\ell-1$ ℓ–ary isomorphic complete trees except in the case where the volcano is reduced to the crater. When a volcano has more than one level, the vertices on the floor, that is, at the bottom level, only have one ascending outgoing arc. In the other levels each vertex has $\ell+1$ outgoing arcs: for the vertices between the floor and the crater one is ascending and ℓ are descending while for the vertices on the crater $\left(\frac{D}{\ell}\right)+1$ are horizontal and $\ell-\left(\frac{D}{\ell}\right)$ are descending, being D the discriminant of the order isomorphic to the endomorphism rings of the curves located in the crater. Just as a remark, the case where there is a vertex with j–invariant $j=0$ or $j=1728$ is slightly different (see [25]).

We denote by $V_\ell(E/\mathbb{F}_q)$ the volcano of ℓ–isogenies where $E/\mathbb{F}_q$ belongs. We notice that if $E'/\mathbb{F}_q$ is another curve on the volcano, $V_\ell(E'/\mathbb{F}_q)=V_\ell(E/\mathbb{F}_q)$. The height of $V_\ell(E/\mathbb{F}_q)$ is defined as the ℓ–adic valuation of the conductor g of $\mathbb{Z}[\pi]$. This value, denoted by $h(V_\ell(E/\mathbb{F}_q))$, coincides with the number of levels of $V_\ell(E/\mathbb{F}_q)$ minus one. The number of vertices in the crater of $V_\ell(E/\mathbb{F}_q)$ is denoted by $c(V_\ell(E/\mathbb{F}_q))$. Concerning this parameter, from [10] we have the following result:

Proposition 2.1. *Let E and E' be two ordinary elliptic curves over $\mathbb{F}_q$. If $\mathrm{End}(E)\simeq\mathrm{End}(E')$, then $c(V_\ell(E/\mathbb{F}_q))=c(V_\ell(E'/\mathbb{F}_q))$.*

Lenstra [17] proved that $E(\mathbb{F}_q)\simeq\mathcal{O}/(\pi-1)$ as $\mathcal{O}$–modules, from which one can deduce that $E(\mathbb{F}_q)\simeq\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$. By writing $\pi=a+g\omega$ with

$$a=\begin{cases}(t-g)/2\\ t/2\end{cases}\qquad\text{and}\qquad\omega=\begin{cases}\frac{1+\sqrt{d_K}}{2} & \text{if } d_K\equiv 1 \pmod 4\\ \sqrt{d_K} & \text{if } d_K\equiv 2,3 \pmod 4\end{cases}$$

we obtain [26] that $n_2=\gcd(a-1,g/f)$, $n_2\mid n_1$, $n_2\mid q-1$ and $\#E(\mathbb{F}_q)=n_1n_2$. This implies that on a volcano of ℓ–isogenies the group structure of all the curves with isomorphic endomorphism rings, i.e. at the same level, is identical.

From this classification of the elliptic curves, Miret et al. [19] deduced the relationship between the structure of the ℓ–Sylow subgroup $E[\ell^\infty](\mathbb{F}_q)$ and its location in the volcano of ℓ–isogenies $V_\ell(E/\mathbb{F}_q)$ (see [18] to determine $E[\ell^\infty](\mathbb{F}_q)$).

Proposition 2.2. *Let $E/\mathbb{F}_q$ be an elliptic curve whose ℓ–Sylow subgroup is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z}\times\mathbb{Z}/\ell^s\mathbb{Z}$, $r\geq s\geq 0$, $r+s\geq 1$.*

- *If $s<r$ then E is at level s in $V_\ell(E/\mathbb{F}_q)$;*
- *If $s=r$ then E is at least at level s in $V_\ell(E/\mathbb{F}_q)$.*

We call stability level that which, when going downwards, the structure of the ℓ–Sylow subgroup is different at each level and, when going upwards if possible, the structure of the ℓ–Sylow subgroup does not change. A volcano whose crater is equal to the stability level is called a regular volcano (see [19]). For a regular volcano of ℓ–isogenies $V_\ell(E/\mathbb{F}_q)$, Ionica and Joux [15] determine which ℓ–isogenies of $E/\mathbb{F}_q$ are non-descending. In the case that $V_\ell(E/\mathbb{F}_q)$ is not regular, they define a second level of stability which is equal to $\min(v_\ell(\#E(\mathbb{F}_q)) - 1, h(V_\ell(E/\mathbb{F}_q)))$. Up to that level, they find the non-descending ℓ–isogenies of $E/\mathbb{F}_q$ by using a symmetric pairing.

The set of all volcanoes of ℓ–isogenies whose elliptic curves have a given group order over $\mathbb{F}_q$ constitutes an ℓ–cordillera. Recently, Moody [20] gave several relationships between different cordilleras. In his paper he introduces the notion of associated elliptic curves: two elliptic curves E_1 and E_2 are ℓ–associated if both have an ascending ℓ–isogeny to a same elliptic curve E.

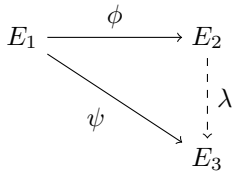
Proposition 2.3 (Proposition 5 of [20])**.** *Let n be a prime number. If n j–invariants of curves are equally spaced around a cycle of length a multiple of n in a volcano of ℓ–isogenies, then in any other cordillera they are either associates, equally spaced vertices around a cycle (or cycles), or are on the same level (but are not associates and are not on the crater).*

These relationships allow us to compute an ℓ–cordillera from the knowledge of an m–cordillera.

3 Preliminary results

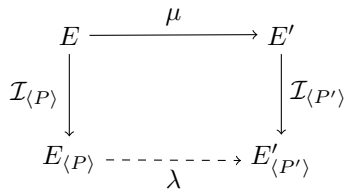
Let E be an ordinary elliptic curve over $\mathbb{F}_q$. If G is a cyclic subgroup of E, we denote by $\mathcal{I}_G$ the isogeny of kernel G and by E_G the isogenous curve to E under $\mathcal{I}_G$.

Lemma 3.1 (Corollary 4.11 of [23])**.** *Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be non constant isogenies, and assume that ϕ is separable. If $\ker\phi \subset \ker\psi$, then there exists a unique isogeny $\lambda : E_2 \to E_3$ such that the following diagram*



is commutative, that is, $\psi = \lambda \circ \phi$.

Proposition 3.2. *Let $\mu : E \to E'$ be an isogeny of degree m. Let P be a point of order ℓ of E and let $P' = \mu(P)$. Then there exists a unique isogeny $\lambda : E_{\langle P\rangle} \to E'_{\langle P'\rangle}$ of degree m such that the following diagram*



is commutative, that is, $\mathcal{I}_{\langle P'\rangle} \circ \mu = \lambda \circ \mathcal{I}_{\langle P\rangle}$.

Proof. Since $(\mathcal{I}_{\langle P'\rangle} \circ \mu)(P) = \mathcal{I}_{\langle P'\rangle}(P') = O_{E'_{\langle P'\rangle}}$, $\ker \mathcal{I}_{\langle P\rangle} \subset \ker(\mathcal{I}_{\langle P'\rangle} \circ \mu)$. From Lemma 3.1, there exists a unique isogeny $\lambda : E_{\langle P\rangle} \to E'_{\langle P'\rangle}$ such that $\mathcal{I}_{\langle P'\rangle} \circ \mu = \lambda \circ \mathcal{I}_{\langle P\rangle}$. By looking at the degrees of μ, $\mathcal{I}_{\langle P\rangle}$ and $\mathcal{I}_{\langle P'\rangle}$, it turns out that λ has degree m. □

Corollary 3.3. *Let $\mu : E \to E'$ be an isogeny of degree m. Let P be a point of order ℓ of E and let $P' = \mu(P)$. Then respectively the isogenies $\mathcal{I}_{\langle P\rangle}$ and $\mathcal{I}_{\langle P'\rangle}$ and the isogenies μ and λ, being λ defined as in Proposition 3.2, have the same direction in terms of volcanoes (ascending, descending or horizontal).*

Proof. Let f and g be the conductors of $\mathrm{End}(E)$ and $\mathrm{End}(E'_{\langle P'\rangle})$ respectively. These conductors might change by a factor ℓ or a factor m. These changes depend on the direction of $\mathcal{I}_{\langle P'\rangle}$ and μ. Since $\mathcal{I}_{\langle P'\rangle} \circ \mu = \lambda \circ \mathcal{I}_{\langle P\rangle}$ and $\ell \neq m$, the direction of $\mathcal{I}_{\langle P\rangle}$ and λ are the same. □

4 Determining the direction of an ℓ–isogeny using a distortion map

In this section we propose a method to determine if an ℓ–isogeny of an ordinary elliptic curve E is descending or non-descending, based on the behaviour of an appropriate endomorphism of E.

From now on, in the rest of the paper, we suppose that $\ell \neq 2, 3$, $E[\ell] \subseteq E(\mathbb{F}_q)$, and $\left(\frac{d_K}{m}\right) = 1$, with $m \neq \ell$.

We consider a volcano of m–isogenies where E belongs to its crater. The elliptic curves of the crater of $V_m(E/\mathbb{F}_q)$ has two horizontal m–isogenies since $\left(\frac{d_K}{m}\right) = 1$. Let

$$E = E_0 \xrightarrow{\mu_1} E_1 \xrightarrow{\mu_2} \cdots \xrightarrow{\mu_{c-1}} E_{c-1} \xrightarrow{\mu_c} E_c \simeq E_0 \tag{4.1}$$

be one of the two cycles of m–isogenies of the crater. Let π_i be the Frobenius endomorphism of $E_i/\mathbb{F}_q$, $0 \leq i \leq c-1$. If $h(V_m(E_i/\mathbb{F}_q)) = 0$, then π_i has two different eigenvalues τ_1 and τ_2 in $\mathbb{F}_m$. Let $P_{i,1}$ and $P_{i,2}$ be two points corresponding to the eigenvectors of π_i, that is, $\pi_i(P_{i,1}) = \tau_1 P_{i,1}$ and $\pi_i(P_{i,2}) = \tau_2 P_{i,2}$. Then $\mathcal{I}_{\langle P_{i,1}\rangle}$ and $\mathcal{I}_{\langle P_{i,2}\rangle}$ are the two horizontal m–isogenies of E_i. Moreover, either $\mu_{i+1} = \mathcal{I}_{\langle P_{i,1}\rangle}$ for all $i \in \{0, \ldots, c-1\}$ or $\mu_{i+1} = \mathcal{I}_{\langle P_{i,2}\rangle}$ for all $i \in \{0, \ldots, c-1\}$.

If $h(V_m(E_i/\mathbb{F}_q)) > 0$, then π_i has a unique eigenvalue in $\mathbb{F}_m$. Let $T_m(E_i)$ be the m–adic Tate module (see III.7 of [23]). The characteristic polynomial of π_i on $T_m(E_i)$ has two different roots τ_1 and τ_2 in $\mathbb{Z}_m$. Then there exist two eigenspaces $S_{i,1}$ and $S_{i,2}$ of eigenvalues τ_1 and τ_2, respectively. The images of $S_{i,1}$ and $S_{i,2}$ in $E_i[m]$ determine the kernels of the two horizontal m–isogenies of E_i, kernels that can be computed using [8] . As in the former case, the cycle of m–isogenies (4.1) is determined by one of the two eigenvalues. See [5, 9] for more information.

Consider the cycle of m–isogenies (4.1). Taking an isomorphism

$$\gamma : E_c \to E_0,$$

we can build the following endomorphism of E:

$$\varphi = \gamma \circ \mu_c \circ \cdots \circ \mu_1. \tag{4.2}$$

This endomorphism can be a distortion map for a subgroup of order ℓ of E. A distortion map for a subgroup G of E is an endomorphism f of E such that $f(G) \neq G$. For ordinary elliptic curves, we have the following result:

Lemma 4.1 (Theorem 2.1 of [4])**.** *Let E be an ordinary elliptic curve over $\mathbb{F}_q$ such that $E[\ell] \subseteq E(\mathbb{F}_q)$. If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and ℓ is split in $\mathcal{O}_K$, then all but two subgroups of $E[\ell]$ have distortion maps.*

The next proposition generalizes the results of the previous section for the endomorphism φ defined in (4.2).

Proposition 4.2. *Let P be a point of order ℓ of E and let $Q = \varphi(P)$. Then there exists a unique isogeny $\psi : E_{\langle P \rangle} \to E_{\langle Q \rangle}$ of degree m^c such that the following diagram*

$$\begin{array}{ccc} E & \xrightarrow{\quad\varphi\quad} & E \\ {\scriptstyle \mathcal{I}_{\langle P \rangle}}\downarrow & & \downarrow{\scriptstyle \mathcal{I}_{\langle Q \rangle}} \\ E_{\langle P \rangle} & \xrightarrow[\psi]{\quad\quad} & E_{\langle Q \rangle} \end{array}$$

is commutative, that is, $\mathcal{I}_{\langle Q \rangle} \circ \varphi = \psi \circ \mathcal{I}_{\langle P \rangle}$. The isogenies $\mathcal{I}_{\langle P \rangle}$ and $\mathcal{I}_{\langle Q \rangle}$ have the same direction while the isogeny ψ is a composition of horizontal isogenies of degree m.

Proof. Using iteratively Proposition 3.2 and Corollary 3.3 the claim follows. □

Remark 4.3. If $\mathcal{I}_{\langle P \rangle}$ and $\mathcal{I}_{\langle Q \rangle}$ are descending, then the composition ψ given in Proposition 4.2 never takes a dual nor goes through $E_{\langle P \rangle}$ although it can finish in $E_{\langle P \rangle}$ when $Q \in \langle P \rangle$. Indeed, if we consider the elliptic curve E over $\mathbb{C}$, it can be represented as $\mathbb{C}/\Lambda$ where $\Lambda \subseteq \mathcal{O}$ is an invertible ideal. Then, taking into account that μ_1 and $\mathcal{I}_{\langle P \rangle}$ are represented by two invertible ideals $\mathfrak{a}$ and $\mathfrak{b}$ respectively, the claim can be deduced from the following diagram:

$$\begin{array}{ccccccccc}
\mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{a}^{-1} & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{a}^{-2} & \longrightarrow & \cdots & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{a}^{-c} \simeq \mathbb{C}/\Lambda \\
\downarrow & & \downarrow & & \downarrow & & & & \downarrow \\
\mathbb{C}/\Lambda\mathfrak{b}^{-1} & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{b}^{-1}\mathfrak{a}^{-1} & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{b}^{-1}\mathfrak{a}^{-2} & \longrightarrow & \cdots & \longrightarrow & \mathbb{C}/\Lambda\mathfrak{b}^{-1}\mathfrak{a}^{-c}
\end{array}$$

We now give a condition which must be satisfied by a point $P \in E[\ell]$ in order to guarantee that the ℓ–isogeny $\mathcal{I}_{\langle P\rangle}$ is non-descending. This condition is related with the behaviour of the endomorphism φ given in (4.2) over P. More precisely, it is necessary that φ be a distortion map for $\langle P\rangle$.

Theorem 4.4. *Let P be a point of order ℓ of $E(\mathbb{F}_q)$. If $\varphi(P) \notin \langle P\rangle$, then $\mathcal{I}_{\langle P\rangle}$ is descending.*

Proof. We first assume that E is not located in the crater of $V_\ell(E/\mathbb{F}_q)$. In this case, as is known, E has one ascending and ℓ descending ℓ–isogenies. Therefore, we must prove that $\mathcal{I}_{\langle P\rangle}$ is not ascending. Suppose that it is. Let $Q = \varphi(P)$. From Proposition 4.2 we have that $\mathcal{I}_{\langle Q\rangle}$ is ascending. Since $Q \notin \langle P\rangle$, it turns out that $\ker \mathcal{I}_{\langle P\rangle} \neq \ker \mathcal{I}_{\langle Q\rangle}$, that is, E have two ascending ℓ–isogenies, which is a contradiction.

Assume now E is located in the crater of $V_\ell(E/\mathbb{F}_q)$. Under this assumption, the trivial case is when E does not have horizontal ℓ–isogenies. When E has one horizontal ℓ–isogeny, the proof is similar to the one given at the beginning when E had one ascending ℓ–isogeny. Hence we will focus on the case that E has two horizontal ℓ–isogenies. Besides these two ℓ–isogenies, E has $\ell - 1$ descending. Assume $\mathcal{I}_{\langle P\rangle}$ is a descending one. Let $Q = \varphi(P)$. Since $Q \notin \langle P\rangle$ and $j(E) \neq 0, 1728$, it turns out that $E_{\langle P\rangle} \not\simeq E_{\langle Q\rangle}$. Then, taking into account Proposition 4.2 and Remark 4.3, we get $c(V_m(E_{\langle P\rangle}/\mathbb{F}_q)) = c(V_m(E_{\langle Q\rangle}/\mathbb{F}_q)) > c$. Let $R \in E(\mathbb{F}_q)$ be a point of order ℓ such that $R \notin \langle P\rangle \cup \langle Q\rangle$ and suppose that $\mathcal{I}_{\langle R\rangle}$ is descending. Let $S = \varphi(R)$. If $S \in \langle R\rangle$, then $E_{\langle R\rangle} \simeq E_{\langle S\rangle}$. Again taking into account Proposition 4.2 and Remark 4.3, we get $c(V_m(E_{\langle R\rangle}/\mathbb{F}_q)) = c$. But this is a contradiction with Proposition 2.1. Therefore, for any R such that $\mathcal{I}_{\langle R\rangle}$ is descending we have that $\varphi(R) \notin \langle R\rangle$. Then, from Lemma 4.1, E must have two different subgroups G of order ℓ such that $\varphi(G) = G$, which are the kernels of the horizontal ℓ–isogenies. □

Corollary 4.5. *Let $G_1, \ldots, G_k$ be the kernels of the descending ℓ–isogenies of E. Then either $\varphi(G_i) = G_i$ for all G_i or $\varphi(G_i) \neq G_i$ for all G_i.*

Proof. It follows from the proof of Theorem 4.4. □

Corollary 4.6. *Assume there exists a descending ℓ–isogeny of E of kernel G such that $\varphi(G) \neq G$.*

- *If E is not located in the crater of $V_\ell(E/\mathbb{F}_q)$, then all subgroups G of E of order ℓ, except one subgroup, satisfy $\varphi(G) \neq G$. The subgroup that does*

not satisfy this condition is the kernel of the only ascending ℓ–isogeny of E.

- *If E is located in the crater of $V_\ell(E/\mathbb{F}_q)$, then all subgroups G of E of order ℓ, except $0, 1$ or 2 subgroups, satisfy $\varphi(G) \neq G$. The subgroups that do not satisfy this condition are the kernels of the horizontal ℓ–isogenies of E.*

Proof. It follows from Theorem 4.4 and Corollary 4.5. □

5 Relationships between volcanoes of isogenies of different degrees

In this section we give a result of the crater sizes of volcanoes of m–isogenies of elliptic curves belonging to a given volcano of ℓ–isogenies. This result extends Proposition 5 given by Moody in [20] (see Proposition 2.3).

Proposition 5.1. *Let $E = E_{1,1}, E_{1,2}, \ldots, E_{1,c}$ be the elliptic curves in the crater of $V_m(E/\mathbb{F}_q)$. Let E' be an elliptic curve ℓ–isogenous to E under a descending ℓ–isogeny of kernel $\langle P\rangle$ with $P \in E(\mathbb{F}_q)$. Let $E' = E_{2,1}, E_{2,2}, \ldots, E_{2,c'}$ be the elliptic curves in the crater of $V_m(E'/\mathbb{F}_q)$. Then*

- *$c' = c$ if and only if $\varphi(P) \in \langle P\rangle$;*
- *$c' = nc$ if and only if $\varphi(P) \notin \langle P\rangle$ being n an integer such that $n \neq 1$ and $n \mid \left(\ell - \left(\frac{D}{\ell}\right)\right)$ where D is the discriminant of $\mathcal{O} \simeq \mathrm{End}(E)$.*

In the second case, $E_{2,ic+j}$ is ℓ–isogenous to $E_{1,j}$ for all $i \in \{0, \ldots, n-1\}$.

Proof. Let $\mathcal{I} : E \to E'$ be the isogeny of kernel $\langle P\rangle$ and let $Q = \varphi(P)$. From Proposition 4.2 and Remark 4.3 we have that $c' \geq c$. We prove the first equivalence.

- $c' = c \Longrightarrow Q \in \langle P\rangle$: Assume $Q \notin \langle P\rangle$. Then $\ker \mathcal{I} \neq \ker \mathcal{I}_{\langle Q\rangle}$, and since $j(E) \neq 0, 1728$, $E' \not\simeq E_{\langle Q\rangle}$. Hence, from Proposition 4.2 and Remark 4.3 we have $c' > c$, which is a contradiction.
- $Q \in \langle P\rangle \Longrightarrow c' = c$: Since $Q \in \langle P\rangle$, it turns out $E' \simeq E_{\langle Q\rangle}$. Then, from Proposition 4.2 and Remark 4.3 we have $c' = c$.

The equivalence $c' > c \iff \varphi(P) \notin \langle P\rangle$ can be deduced from the first one. In order to prove that $c \mid c'$ we consider the smallest integer n such that $\varphi^n(P) \in \langle P\rangle$. In this situation we have

$$E_{2,1} = E_{\langle P\rangle}, E_{2,c+1} = E_{\langle \varphi(P)\rangle}, \ldots, E_{2,nc+1} = E_{\langle \varphi^n(P)\rangle} \simeq E_{2,1}.$$

More generally, if μ_j is the isogeny of degree m^{j-1} between $E_{1,1}$ and $E_{1,j}$, $j > 1$, we have

$$E_{2,j} = E_{\langle \mu_j(P)\rangle}, E_{2,c+j} = E_{\langle \mu_j(\varphi(P))\rangle}, \ldots, E_{2,nc+j} = E_{\langle \mu_j(\varphi^n(P))\rangle} \simeq E_{2,j}.$$

Hence $c' = nc$ and the curves $E_{2,ic+j}$ are ℓ–isogenous to $E_{1,j}$. Finally, since the craters of the volcanoes of m–isogenies of the ℓ–isogenous curves to $E_{1,j}$ under descending ℓ–isogenies must have the same size (Proposition 2.1) and since in each crater there are a total of n of these curves, it turns out that n divides the number of descending ℓ–isogenies of $E_{1,j}$, that is, $n \mid \left(\ell - \left(\frac{D}{\ell}\right)\right)$. □

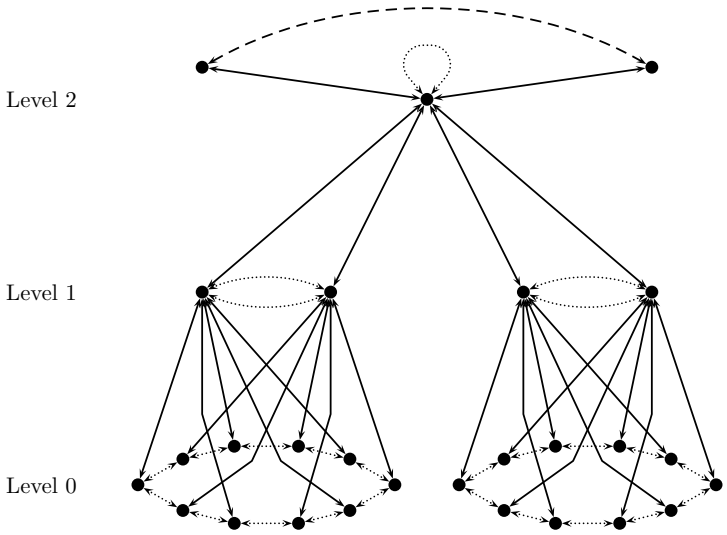


Figure 1: A volcano of 5–isogenies together with volcanoes of m–isogenies which only have crater.

In Figure 1 we show the relationships among the crater sizes of volcanoes of m–isogenies whose vertices belong to a volcano of 5–isogenies of height 2 and size crater > 2. The vertices in level 0 are distributed in volcanoes of m–isogenies of crater size 10. The vertices in level 1 are distributed in volcanoes of m–isogenies of crater size 2. Finally, the vertices in level 2 are distributed in volcanoes of m–isogenies of crater size 1.

6 Ascending the volcano

In this section, using the previous results, we propose an algorithm which given an elliptic curve E returns an ascending path from E in its volcano of ℓ–isogenies. This algorithm makes use of a prime number m to find at each level the non-descending ℓ–isogenies according to Corollary 4.6. In order to reach the crater, we can use this algorithm with different primes m.

Firstly, we show how to determine given a point $P \in E(\mathbb{F}_q)$ of order ℓ such that $\varphi(P) \notin \langle P \rangle$ which ℓ–isogenies of E are non-descending. Let $Q = \varphi(P)$ and $R = aP + bQ = \varphi(Q)$, $0 \leq a, b \leq \ell - 1$, $a \neq 0$. Then the action of φ over $E[\ell]$ is

given by the following matrix:

$$M_\varphi = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} \in GL(2, \mathbb{F}_\ell).$$

In order to obtain a and b we can proceed as follows:

- Compute $W_\ell(Q,P)$, $W_\ell(Q,R)$ and $W_\ell(R,P)$, with $W_\ell(*,*)$ the Weil pairing (see III.8 of [23]).
- Solve the following two discrete logarithms: $W_\ell(Q,P)^a = W_\ell(Q,R)$ and $W_\ell(Q,P)^b = W_\ell(R,P)$.

From these values a and b we can determine the non-descending ℓ–isogenies of E. Indeed, considering the characteristic polynomial of M_φ,

$$c_{M_\varphi}(x) = x^2 - bx - a,$$

we compute the eigenvalues α_1 and α_2 of M_φ and thus we obtain the points $S_i = P + \frac{\alpha_i}{a}Q$ such that $\varphi(S_i) \in \langle S_i \rangle$ which determine the kernels of the non-descending ℓ–isogenies from E. For this task, following the former steps, we have the Algorithm 1 which returns the points S_i.

Algorithm 1: Determining the non-descending ℓ–isogenies of an elliptic curve (NonDescending).

Input : $E/\mathbb{F}_q$, ℓ, φ given as in (4.2), $P \in E(\mathbb{F}_q)$ of order ℓ, $Q \in E(\mathbb{F}_q)$ such that $Q = \varphi(P) \notin \langle P \rangle$, and $W_\ell(Q,P)$.
Output: A sequence S that contains a generator of each kernel of the non-descending ℓ–isogenies of E.

$S \leftarrow [\,]$
$R \leftarrow \varphi(Q)$
Compute $W_\ell(Q,R)$ and $W_\ell(R,P)$
Compute $a \in [1, \ell-1]$ such that $W_\ell(Q,P)^a = W_\ell(Q,R)$
Compute $b \in [0, \ell-1]$ such that $W_\ell(Q,P)^b = W_\ell(R,P)$
foreach $\alpha \in \mathbb{F}_\ell$ such that $\alpha^2 - b\alpha - a = 0$ **do** $S[\#S+1] \leftarrow P + \frac{\alpha}{a}Q$
return S

Note that by repeating Algorithm 1 we can find a path of ascending ℓ–isogenies from E. For this goal it is necessary to take into account that if $\langle P + kQ \rangle$ is the kernel of an ascending ℓ–isogeny, then by [11], $\langle \mathcal{I}_{\langle P+kQ \rangle}(P) \rangle$ is the kernel of the dual isogeny of $\mathcal{I}_{\langle P+kQ \rangle}$, and therefore this ℓ–isogeny is descending and we can apply the procedure again. This task is implemented in Algorithm 2.

Given an ascending path $E_0 \to E_1 \to \cdots \to E_h$ in an ℓ–volcano V with height h, the Algorithm 2 will detect the crater of V starting at E_i, $0 < i \leq h$, if and only if the following relations hold:

$$c(V_m(E_{i-1}/\mathbb{F}_q)) > c(V_m(E_i/\mathbb{F}_q)) > \cdots > c(V_m(E_h/\mathbb{F}_q)). \tag{6.1}$$

Algorithm 2: Determining an ascending path in a volcano of ℓ–isogenies.

Input : $E/\mathbb{F}_q$, ℓ, $P \in E(\mathbb{F}_q)$ of order ℓ such that $\mathcal{I}_{\langle P \rangle}$ is descending, and m.

Output: A sequence S that contains an ascending path from E and a boolean `crater` that indicates if we have reached the crater of $V_\ell(E/\mathbb{F}_q)$.

```
S ← [ ]
crater ← false
Compute φ
Q ← φ(P)
W ← W_ℓ(Q, P)
if W ≠ 1 then
    final ← false
    repeat
        U ← NonDescending(E, ℓ, φ, P, Q, W)
        if #U ≠ 1 then
            crater ← true    final ← true
        else
            Compute E_⟨U[1]⟩ and I_⟨U[1]⟩
            E ← E_⟨U[1]⟩    P ← I_⟨U[1]⟩(P)
            Compute φ
            Q ← φ(P)
            W ← W_ℓ(Q, P)
            if W = 1 then
                Compute P' ∈ E[ℓ](F_q) such that P' ∉ ⟨P⟩
                if W_ℓ(P', φ(P')) ≠ 1 then
                    crater ← true
                else
                    S[#S + 1] ← E
                end
                final ← true
            else
                S[#S + 1] ← E
            end
        end
    until final
end
return S, crater
```

If some of these relations do not hold, we can repeat Algorithm 2 with different primes m until reaching the crater.

Theoretically, it is always possible to find a prime m for which Algorithm 2 calls only once Algorithm 1. Let $\phi_1 : E_1 \to E$ and $\phi_2 : E_2 \to E$ be two ascending ℓ–isogenies. Assume $E_1 \not\simeq E_2$. Let $D = f^2 d_K$ be the discriminant of the order

$\mathcal{O}$ isomorphic to $\mathrm{End}(E_i)$, $i \in \{1,2\}$. From Theorem 9.12 of [6] and Proposition 4.1.3 of [21], we obtain that there exist infinitely many primes m which are represented by a quadratic form of discriminant D such that $\left(\frac{D}{m}\right) = 1$. Let m be one of these primes such that $m \nmid f$. From Theorem 7.7 of [6], there exists a horizontal m–isogeny from E_1 to E_2. Taking into account that ϕ_1 and ϕ_2 are the unique ascending ℓ–isogenies of E_1 and E_2, respectively, from Proposition 3.2 and Corollary 3.3, there also exists a horizontal m–isogeny φ from E to itself. Hence,

$$c(V_m(E_1/\mathbb{F}_q)) = c(V_m(E_2/\mathbb{F}_q)) > c(V_m(E/\mathbb{F}_q)) = 1.$$

Therefore, from Proposition 5.1, we can see that Algorithm 1 will be executed inside Algorithm 2 (if $\langle P \rangle = \ker \widehat{\phi_1}$, then $\varphi(P) \notin \langle P \rangle$). Algorithm 1 will be executed only once since $c(V_m(E/\mathbb{F}_q)) = 1$.

6.1 Complexity analysis of Algorithm 1

In this section we assume that $m \neq 2$, $p \gg \ell, m$, and $h(V_m(E/\mathbb{F}_q)) = 0$. We also assume that the modular polynomial $\Phi_m(X,Y) \in \mathbb{F}_p[X,Y]$ is precomputed.

Before studying the cost of Algorithm 1, given an elliptic curve $\mathcal{E}$ belonging to $V_m(E/\mathbb{F}_q)$ of j–invariant j, we need to study the cost of computing a normalized m–isogeny $\mu : \mathcal{E}/\mathbb{F}_q \to \mathcal{E}'/\mathbb{F}_q$ from a root $j' \in \mathbb{F}_q$ of $\Phi_m(X,j)$, and the cost of computing the image of a point under μ.

Let $y^2 = x^3 + Ax + B$ be the equation of $\mathcal{E}$. The coefficients of the elliptic curve $\mathcal{E}' : y^2 = x^3 + A'x + B'$ are given by (see Section 4.1.3 of [10] or Section 25.2.1 of [13])

$$A' = \frac{3j'}{1728 - j'} \left(\frac{\kappa}{12j'}\right)^2 m^4 \quad \text{and} \quad B' = \frac{2j'}{1728 - j'} \left(\frac{\kappa}{12j'}\right)^3 m^6,$$

where

$$\kappa = -\frac{18}{m} \frac{B}{A} \frac{\Phi_X(j,j')}{\Phi_Y(j,j')} j,$$

with $\Phi_X(X,Y)$ and $\Phi_Y(X,Y)$ being the partial derivatives of $\Phi_m(X,Y)$ with respect to X and Y, respectively. Since $\Phi_m(X,Y)$ is a symmetric polynomial of degree $m+1$, the cost of applying these formulas is of $O(m^2)$ operations in $\mathbb{F}_q$.

Regarding the equations of μ, let

$$g(x) = x^d - g_1 x^{d-1} + g_2 x^{d-2} + \cdots + (-1)^d g_d$$

be the polynomial over $\mathbb{F}_q[x]$ of degree $d = (m-1)/2$ whose roots are the abscissas of the points of $\ker \mu \setminus \{O_{\mathcal{E}}\}$. Then (see Section 4.1 of [2])

$$\mu(x,y) = \left(\frac{N(x)}{D(x)}, y\left(\frac{N(x)}{D(x)}\right)'\right),$$

where

$$\frac{N(x)}{D(x)} = mx - 2g_1 - (3x^2 + A)\frac{D'(x)}{D(x)} - 2(x^3 + Ax + B)\left(\frac{D'(x)}{D(x)}\right)',$$

$D(x) = g(x)^2$ and $D'(x)/D(x) = 2g'(x)/g(x)$. In our case, $g(x)$ is unknown, so $N(x)$ and $D(x)$ can be obtained in $O(M(m)\log m)$ operations in $\mathbb{F}_q$, where $M(n) = n\log n \log\log n$, by using $\mathsf{fastElkies}'$ algorithm (see Theorem 2 and Section 4.3 of [2]).

Taking into account that the degrees of $N(x)$ and $D(x)$ are m and $m-1$, respectively, if both polynomials are known, then the cost of computing $\mu(P)$, $P \in \mathcal{E}(\mathbb{F}_q) \setminus \{O_\mathcal{E}\}$, is $O(m)$.

We now study the complexity of Algorithm 1. In order to execute the algorithm, firstly we need to compute the endomorphism φ defined in (4.2), the point $Q = \varphi(P)$, and the Weil pairing $W_\ell(Q, P)$. The cost of these computations is given by the expression $C_1 = c(K_1 + K_2) + K_3$, where $c = c(V_m(E/\mathbb{F}_q))$, K_1 is the cost of computing an m–isogeny without knowing its kernel, K_2 is the cost of computing the image of a point under an m–isogeny, and K_3 is the cost of computing a Weil pairing. The partial cost $c(K_1 + K_2)$ is the cost of walking around the crater of $V_m(E/\mathbb{F}_q)$.

Let $\mathcal{E}$ be an elliptic curve belonging to $V_m(E/\mathbb{F}_q)$ of j–invariant j and let $\lambda : \mathcal{E}/\mathbb{F}_q \to \mathcal{E}''/\mathbb{F}_q$ be an m–isogeny. Given $\mathcal{E}$ and $j'' = j(\mathcal{E}'')$, the cost K_1 of computing an m–isogeny $\mu : \mathcal{E}/\mathbb{F}_q \to \mathcal{E}'/\mathbb{F}_q$, $\mu \neq \lambda$, is determined by the costs of the following steps:

(1) Compute $\Phi_m(X, j)$;

(2) Compute $\Phi_m(X, j)/(X - j'')$;

(3) Compute a root $j' \in \mathbb{F}_q$ of $\Phi_m(X, j)/(X - j'')$;

(4) Compute the curve $\mathcal{E}'$ such that $j(\mathcal{E}') = j'$;

(5) Compute the equations of $\mu : \mathcal{E} \to \mathcal{E}'$.

The cost of step (1) is $O(m^2)$. Step (2) has a cost of $O(m)$. The cost of step (3) is $O(M(m)\log q)$ (see [14]). Finally, as we have seen at the begining of this section, the costs of steps (4) and (5) are $O(m^2)$ and $O(M(m)\log m)$, respectively. Hence, the cost K_1 is $O(m^2 + M(m)\log q)$. Taking into account that K_2 and K_3 are $O(m)$ and $O(\log \ell)$, respectively, the total cost C_1 is $O(c(m^2 + M(m)\log q))$.

In order to compute the cost of Algorithm 1, we assume that the parameter φ is passed by means of the m–isogenies μ_i (a pair $(N_i(x), D_i(x))$ for each μ_i) and the isomorphism γ. Then, considering this, the cost of Algorithm 1 is given by the expression $C_2 = cK_2 + 2K_3 + 2K_4 + K_5$, where K_4 is the cost of computing a discrete logarithm in a subgroup of order ℓ of $\mathbb{F}_q$, and K_5 is the cost of computing the roots of a second degree equation in $\mathbb{F}_\ell$. As we have seen before, the costs K_2 and K_3 are $O(m)$ and $O(\log \ell)$, respectively. By using the Pollard's rho method, the cost K_4 is $O(\sqrt{\ell})$. Taking into account that $\ell \ll q$, the cost K_5 is negligible, and hence, the total cost C_2 is $O(cm + \sqrt{\ell})$.

Therefore, the cost of Algorithm 1 together with the computations needed for its performance is $O(c(m^2 + M(m)\log q) + \sqrt{\ell})$.

6.2 Implementation remarks

As we have seen in the previous section, one of the costs that most influence in the complexity of Algorithm 1 is the cost of computing φ. This cost has two critical parameters: m and c. Regarding m, recall that we are assuming the modular polynomials $\Phi_m(X, Y)$ are precomputed modulo p. Nevertheless, there exist limitations for m. According to [3], the running time to compute $\Phi_m(X, Y) \mod p$ is $O(m^3 \log^3 m \log\log m)$ and the required space is $O(m^2 \log mp)$. Moreover, the largest value of m for which the authors were able to compute $\Phi_m(X, Y)$ modulo a 256-bit integer is $m = 20011$.

Regarding c, let $\mathcal{O}$ be the order isomorphic to $\mathrm{End}(E)$ and let I be a prime ideal of $\mathcal{O}$ of norm m. Then c is the order of I. Assume first that $\mathcal{O}$ and the class number $h(\mathcal{O})$ are known. Let E' be isogenous to E via a descending ℓ–isogeny. Let $\mathcal{O}'$ be the order isomorphic to $\mathrm{End}(E')$, let I' be a prime ideal of $\mathcal{O}'$ of norm m, and let c' be the order of I'. Then, for each m, we can decompose the ideal (m) as $(m) = IJ$ and $(m) = I'J'$ in $\mathcal{O}$ and $\mathcal{O}'$, respectively. From the prime factorization of $h(\mathcal{O})$ we can obtain c and check whether $c' > c$. Moreover, we can also check if m and c are small enough to compute φ. Although such a procedure is correct, we can not apply it since $\mathcal{O}$ and $h(\mathcal{O})$ are unknown. Thus, the procedure we use is to compute m–isogenies until either the crater cycle is closed or a stopping bound is reached. In the worst case $c \approx \sqrt{q}\log q$ (see Lemma 10 of [7]), which is unfeasible. Nevertheless, in Example 7.1, $\sqrt{q}\log q \approx 10^9$, whereas $c = 83$. In practice we are able to compute φ for small values of c.

7 Examples

In this section, we present three examples. In the first one, we show how to determine the non-descending ℓ–isogenies of an elliptic curve using Algorithm 1. In the second one, for different values of m, starting from level 1 of an ℓ–volcano, we give the maximum levels reached using Algorithm 2. Finally, in the third one, for different values of m, we show the relationships between the crater sizes of the m–volcanoes determined by two elliptic curves located in two consecutive levels of an ℓ–volcano.

Example 7.1. Consider the elliptic curve

$$E/\mathbb{F}_q : y^2 = x^3 + 183774841409640x + 223980779104549$$

with $q = p = 1000000000008293$ such that

$$\#E(\mathbb{F}_q) = 101^2 \cdot 109363 \cdot 896369 \quad \text{and} \quad t^2 - 4q = -11^2 \cdot 101^4 \cdot 284803.$$

Let $\ell = 101$ and $m = 13$. We consider the point

$$P = (204226152861254, 361336474060208) \in E[\ell]$$

such that $\varphi(P) \notin \langle P \rangle$. From P we obtain the points

$$\begin{aligned} Q &= \varphi(P) = (627772168051878, 646515548692986), \\ R &= \varphi(Q) = aP + bQ = (59765655418718, 513192517511964). \end{aligned}$$

Now we compute the Weil pairings:

$$\begin{aligned} W_\ell(Q,P) &= 513780462755483, \\ W_\ell(Q,R) &= 606324367233648, \\ W_\ell(R,P) &= 514049653346552. \end{aligned}$$

From these values, we obtain $a = 80$ and $b = 69$. Then computing the roots of the characteristic polynomial of M_φ,

$$c_{M_\varphi}(x) = x^2 - bx - a = (x - \alpha_1) \cdot (x - \alpha_2),$$

we get $\alpha_1 = 13$ and $\alpha_2 = 56$. Therefore, the kernels of the non-descending ℓ–isogenies of E are $\langle P + \frac{\alpha_1}{a} Q \rangle = \langle P + 9Q \rangle$ and $\langle P + \frac{\alpha_2}{a} Q \rangle = \langle P + 31Q \rangle$.

Example 7.2. Let $q = p = 46386721$. We consider elliptic curves over $\mathbb{F}_q$ with trace of the Frobenius endomorphism $t = -3$. Hence

$$q + 1 - t = 5^2 \cdot 7 \cdot 11 \cdot 24097 \quad \text{and} \quad t^2 - 4q = (5^5)^2 \cdot (-19).$$

Now, we take a sequence of elliptic curves from the floor to the crater of a volcano of 5–isogenies. In Table 1 we give the j–invariants of these curves and the level where they are located. From different values of m, we show the crater size c_m of the volcanoes of m–isogenies where they belong. Finally, starting from level 1, we give the maximum level reached by using Algorithm 2 and whether the crater has been detected.

In this example, the second stability level coincides with the (first) stability level, which is equal to 1. Note that by using the Ionica-Joux's method we could ascend until level 2, while by using Algorithm 2 we detect the crater for $m = 7, 11$. In both cases, the algorithm reaches the crater because the crater sizes of the volcanoes of m–isogenies in each level are different and, since the volcano of 5–isogenies has two horizontal 5–isogenies, it detects the crater (see relations (6.1)).

Table 1: Crater sizes of m–volcanoes linked to each level of a 5–volcano.

Level	j–invariant	c_7	c_{11}	c_{47}	c_{131}
5	45501985	1	1	1	1
4	24731254	4	2	4	1
3	3250539	20	10	4	5
2	33489323	100	50	20	25
1	25252154	500	250	100	125
0	38756238	2500	1250	500	625
Level reached		5	5	4	5
Crater detected?		Yes	Yes	No	No

Example 7.3. Consider the elliptic curve

$$E/\mathbb{F}_q : y^2 = x^3 + 467177x + 65679$$

with $q = p = 1000033$ such that

$$\#E(\mathbb{F}_q) = 3^2 \cdot 11^2 \cdot 919, \quad t^2 - 4q = -3^3 \cdot 11^2 \cdot 1049 \quad \text{and} \quad \mathrm{End}(E) \simeq \mathcal{O}_K$$

with $K = \mathbb{Q}(\sqrt{-3 \cdot 1049})$. Let $\ell = 11$ such that $\left(\frac{d_K}{\ell}\right) = -1$. Consider the elliptic curve

$$E'/\mathbb{F}_q : y^2 = x^3 + 748468x + 81429$$

ℓ–isogenous to E under the descending ℓ–isogeny with kernel $\langle P \rangle$ with

$$P = (689210, 432856).$$

In Table 2 we show the crater sizes c_m and c'_m of $V_m(E/\mathbb{F}_q)$ and $V_m(E'/\mathbb{F}_q)$, respectively, for different values of m. The ratio between c'_m and c_m is a divisor of $\ell - \left(\frac{d_K}{\ell}\right) = \ell + 1 = 12$ as is proven in Proposition 5.1. Note that all divisors of 12 occur.

Table 2: Relationships between several crater sizes.

m	c_m	c'_m
2	1	$1 = 1 \cdot c_m$
17	10	$20 = 2 \cdot c_m$
47	10	$30 = 3 \cdot c_m$
13	5	$20 = 4 \cdot c_m$
41	10	$60 = 6 \cdot c_m$
19	5	$60 = 12 \cdot c_m$

8 Conclusions

In this paper we have presented a new method to determine the non-descending ℓ–isogenies of an elliptic curve E defined over a finite field $\mathbb{F}_q$. In order to do this, we have made use of the endomorphism φ of E obtained going through the crater of the volcano of m–isogenies where E is located, m being a prime different from ℓ. Our method works when φ is a distortion map for a subgroup of order ℓ of $E(\mathbb{F}_q)$. This method, like the one given by Ionica and Joux, does not need computing ℓ–isogeny paths. Unlike their method, ours can be applied beyond the second stability level. We have also studied the relationships between the crater sizes of volcanoes of m–isogenies whose elliptic curves belong to a volcano of ℓ–isogenies of height ≥ 1.

Acknowledgments

Research of the authors was partially supported by grants MTM2013–46949–P (Spanish MINECO) and 2014 SGR1666 (Generalitat de Catalunya).

References

[1] G. Bisson and A. V. Sutherland. Computing the endomorphism of an ordinary elliptic curve over a finite field, *J. Number Theory* 131, no. 5, 815-831, 2011.

[2] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves, *Math. Comp.* 77, no. 263, 1755-1778, 2008.

[3] R. Bröker, K. Lauter, and A. V. Sutherland. Modular polynomials via isogeny volcanoes, *Math. Comp.* 81, no. 278, 1201-1231, 2012.

[4] D. Charles. On the existence of distortion maps on ordinary elliptic curves, *Cryptology ePrint Archive, Report 2006/128*, 2006.

[5] J. M. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm, *École Polytechnique*, 1996.

[6] D. A. Cox. *Primes of the form $x^2 + ny^2$*, Wiley-Interscience, 1989.

[7] L. De Feo, J. Doliskani, and É. Schost. *Fast algorithms for ℓ–adic towers over finite fields*, ISSAC 2013, 165-172, 2013.

[8] L. De Feo, C. Hugounenq, J. Plût, and É. Schost. Explicit isogenies in quadratic time in any characteristic, *LMS Journal of Computation and Mathematics* 19(A), 267-282, 2016.

[9] N. D. Elkies. Explicit isogenies, Draft, 1991.

[10] M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*, Ph.D. thesis, École Polytechnique, Palaiseau Cedex, 2001.

[11] M. Fouquet, J. Miret, and J. Valera. *Isogeny volcanoes of elliptic curves and Sylow subgroups*, Latincrypt 2014, LNCS 8895, 162-175, 2015.

[12] M. Fouquet and F. Morain. *Isogeny volcanoes and the SEA algorithm*, ANTS V, LNCS 2369, 276-291, 2002.

[13] S. D. Galbraith. *Mathematics of public key criptography*, Cambridge University Press, 2012.

[14] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*, Second edition, Cambridge University Press, 2003.

[15] S. Ionica and A. Joux. Pairing the volcano, *Math. Comp.* 82, no. 281, 581-603, 2013.

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

[17] H. W. Lenstra Jr. Complex multiplication structure of elliptic curves, *J. Number Theory* 56, no. 2, 227-241, 1996.

[18] J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the ℓ–power torsion of an elliptic curve over a finite field, *Math. Comp.* 78, no. 267, 1767-1786, 2009.

[19] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. Computing the height of volcanoes of ℓ–isogenies of elliptic curves over finite fields, *Appl. Math. Comput.* 196, no. 1, 67-76, 2008.

[20] D. Moody. Computing isogeny volcanoes of composite degree, *Appl. Math. Comput.* 218, no. 9, 5249-5258, 2012.

[21] F. Morain. Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm, INRIA, RR-0911, 1988.

[22] R. Schoof. Counting points on elliptic curves over finite fields, *J. Théor. Nombres Bordeaux* 7, no. 1, 219-254, 1995.

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

[24] A. V. Sutherland. Computing Hilbert class polynomials with the chinese remainder theorem, *Math. Comp.* 80, no. 273, 501-538, 2011.

[25] A. V. Sutherland. *Isogeny volcanoes*. ANTS X, 507-530, 2013.

[26] C. Wittmann. Group structure of elliptic curves over finite fields, *J. Number Theory* 88, no. 2, 335-344, 2001.