Isogeny volcanoes and the SEA algorithm

M. Fouquet and F. Morain*

Laboratoire d'Informatique (CNRS / UMR 7650), École Polytechnique, F-91128 Palaiseau Cedex, France

Abstract. Recently, Kohel gave algorithms to compute the conductor of the endomorphism ring of an ordinary elliptic curve, given the cardinality of the curve. Using his work, we give a complete description of the structure of curves related via rational ℓ-degree isogenies, a structure we call a volcano. We explain how we can travel through this structure using modular polynomials. The computation of the structure is possible without knowing the cardinality of the curve, and that as a result, we deduce information on the cardinality.

1 Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where $q = p^r$ with p prime. By Hasse's theorem, the Frobenius π of the curve is an endomorphism of degree 2 with characteristic polynomial $\chi(T) = T^2 - tT + q$ where $|t| \leq 2\sqrt{q}$. It is also known since Deuring [6] that the endomorphism ring of E is either an order in an imaginary quadratic field (the *ordinary* case) or an order in a quaternion algebra (the *supersingular* case). Suppose that E is ordinary and let $d_\pi = t^2 - 4q$ be the discriminant of π. We can write $d_\pi = g^2 d_K$ where d_K is the discriminant of the associated imaginary quadratic field K. To each $f \mid g$ corresponds an order of K and to each such order corresponds an isogeny class of elliptic curves having this particular order as endomorphism ring.

Kohel has shown in his thesis [10] how all these curves are related via isogenies of degree dividing g. Studying this correspondance more closely, we introduce the complete structure of isogenies that we call a *volcano*. Kohel's approach starts from g and finds the conductor f of $\mathrm{End}(E)$, using modular polynomials. We revert this algorithm, using modular polynomials to find g and f. As a consequence, we can come up with an algorithm for computing an elliptic curve of any prescribed conductor $k \mid g$ and in particular the maximal endomorphism ring ($k = 1$), algorithm that is needed in [9].

After introducing some basic notations, we will recall the relevant facts about Kohel's work that describe the structure that grows "under" the isogeny cycles introduced by Couveignes and Morain in [4], forming a volcano. Then we recall the relevant theory of modular polynomials and we are ready to "invert"

* The second author is on the leave from the French Department of Defense, Délégation Générale pour l'Armement. This research was partially supported by the French Ministry of Research – ACI Cryptologie.

Kohel's theorem to see the situation from the modular side, which will lead to our algorithm. We then give some applications. The first one is related to the computation of t. For a prime $\ell \mid g$, our algorithm gives the ℓ-adic valuation of t and this information can be used in Schoof's algorithm. Also, we relate the new structure to the trees that were invented in [3] and solve a problem raised by Lercier in his thesis. We can also use this structure in the algorithm given in [2] to compute the equation class of an order $\mathcal{O}$. This method is based on the computation of all the j-invariants of curves satisfying certain conditions. The problem is that they never distinguish the curves having an endomorphism ring equal to $\mathcal{O}$ from the others, problem that can be solved using the structure of the volcanoes. Numerical examples are given to illustrate our work.

Although the general theory works for any characteristic, we concentrate on examples where the characteristic is not 2 or 3. The modifications to be made concern formulas for computing isogenous curves, but we do not insist on these in this article.

2 Extending Kohel's work

2.1 Prerequisites and notations

If an elliptic curve is not supersingular, then it is known that its ring of endomorphisms is an order in an imaginary quadratic field. Isogenous curves share the same underlying field. In this article, we will consider a set of isogenous curves and the relations between them, so that we can assume that we are dealing with a fixed imaginary quadratic field K of discriminant d_K and maximal order $\mathcal{O}_K$, which can be written as $\mathbb{Z}[\omega_K]$ with $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$. As is well known [1], an order $\mathcal{O}$ in K is completely characterized by its conductor f or equivalently its discriminant. As a matter of fact, $\mathcal{O}$ has finite index in $\mathcal{O}_K$ equal to f and $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$. The discriminant of $\mathcal{O}$ is simply $D = f^2 d_K$. Remember also that if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two orders in K of respective discriminants D_1 and D_2, then $\mathcal{O}_1 \subseteq \mathcal{O}_2$ iff there exists a positive integer k such that $D_1 = k^2 D_2$.

The main focus of the article is the relationship between three orders in K related to a given elliptic curve E: $\mathcal{O}_K$, the order $\mathbb{Z}[\pi]$ generated by the Frobenius map π and the endomorphism ring $\mathrm{End}(E)$ of E. These orders are such that $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$ or equivalently, $[\mathcal{O}_K : \mathcal{O}] = f$, $[\mathcal{O} : \mathbb{Z}[\pi]] = g$ et $[\mathcal{O}_K : \mathbb{Z}[\pi]] = g/f$.

In his thesis [10], Kohel computes $\mathrm{End}(E)$ starting from the known value of $d_\pi = t^2 - 4q = g^2 d_K$, where t was computed using a polynomial algorithm for point counting [11, 13, 12, 8]. In our case, we deduce from Kohel's work a structure that describes the relations between isogenous curves and their endomorphism rings.

Let us fix the notations that will be used in the rest of the paper. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve and j its j-invariant. Let $\mathcal{O}$ be the endomorphism ring of E, D its discriminant and f its conductor. Let ℓ be a prime different from p.

2.2 Kohel's theorem

The following proposition justifies the use of ℓ-isogenies of an elliptic curve to determine its endomorphism ring $\mathcal{O}$ (and overall its conductor f).

Proposition 21 *[10, Proposition 21] Let $\alpha : E \to E'$ be an isogeny of prime degree ℓ. Then $\mathcal{O}$ contains $\mathcal{O}'$ or $\mathcal{O}'$ contains $\mathcal{O}$ in K and the index of one in the other divides ℓ.*

This is equivalent to saying $[\mathcal{O} : \mathcal{O}'] = 1$, ℓ or $\frac{1}{\ell}$. We will use the following language when speaking about ℓ-isogenies. A "descending" ℓ-isogeny, denoted by $\downarrow$, is an ℓ-isogeny $\alpha : E_1 \to E_2$ such that $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$ whilst an "ascending" ℓ-isogeny, denoted by $\uparrow$, is an ℓ-isogeny $\alpha : E_1 \to E_2$ such that $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$. In the case where the endomorphim ring is preserved we say that we have an "horizontal" ℓ-isogeny, denoted by $\rightarrow$.

Theorem 21 *[10, Proposition 23] Table 1 classifies the possibilities for the rational ℓ-isogenies of E defined over $\mathbb{F}_q$.*

Case		*Number and type*	*Total number*
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D}{\ell}\right)$ $\rightarrow$	$1 + \left(\frac{D}{\ell}\right)$
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \rightarrow \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell + 1$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	1 $\uparrow$	*1*
	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell + 1$

Table 1. *Number and type of the ℓ-isogenies depending on $[\mathcal{O}_K : \mathcal{O}]$ and $[\mathcal{O} : \mathbb{Z}[\pi]]$.*

2.3 Some lemmas about the classification of ℓ-isogenies.

Table 1 gives the keys to understand how the endomorphism rings of isogenous curves are related. We first deduce from these results the relation between an ℓ-isogeny α and its dual denoted by $\hat{\alpha}$.

Lemma 21 *Let $\alpha : E \to E'$ be an ℓ-isogeny and $\hat{\alpha}$ its dual. Then α is an ascending ℓ-isogeny iff $\hat{\alpha}$ is a descending ℓ-isogeny and α is an horizontal ℓ-isogeny iff $\hat{\alpha}$ is an horizontal ℓ-isogeny.*

From these results, we can deduce some properties of the endomorphism rings $\mathcal{O}$ and $\mathcal{O}'$ such that $\alpha : E \to E'$ is an ℓ-isogeny. With respect to ℓ, we distinguish two cases for the endomorphism rings: the case $\mathbb{Z}[\pi]$ maximal at ℓ, i.e. $\ell \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ or not.

The following lemma ensures that if $\mathbb{Z}[\pi]$ maximal at ℓ, we can only find horizontal ℓ-isogenies.

Lemma 22 *Let E be an elliptic curve such that $\mathbb{Z}[\pi]$ is maximal at ℓ. If there exists an ℓ-isogeny of E, then this ℓ-isogeny is an horizontal ℓ-isogeny.*

We suppose now that $\mathbb{Z}[\pi]$ is non-maximal at ℓ.

Lemma 23 *[7] If $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, i.e. if $\ell^n \parallel g$ with $n \geq 1$ then $\ell^n \parallel f$, then the only ℓ-isogeny $\alpha : E \to E'$ is such that $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$, i.e. $\ell^{n-1} \parallel f'$.*

Lemma 24 *[7] If $\alpha : E_1 \to E_2$ is a descending ℓ-isogeny and $\ell \mid [\mathcal{O}_2 : \mathbb{Z}[\pi]]$, then for every $\beta : E_2 \to E_3$ such that $\mathcal{O}_3 \not\simeq \mathcal{O}_1$, β is a descending ℓ-isogeny. Moreover, there are ℓ such ℓ-isogenies.*

In other words, if $\beta \neq \hat{\alpha}$, then β is a descending ℓ-isogeny. Since E_2 has $\ell + 1$ ℓ-isogenies, $\hat{\alpha}$ is an ascending ℓ-isogeny and the ℓ others are descending ℓ-isogenies.

Let us now describe a very particular case.

Lemma 25 *[7] If there exist two ℓ-isogenies different up to isomorphism from a curve E to a curve E', then they are both horizontal ℓ-isogenies. We can also conclude that ℓ splits in $\mathcal{O}$.*

This peculiar case gives us some informations about the imaginary quadratic field the endomorphism ring is in.

Theorem 22 *[13] Suppose there are two ℓ-isogenies α and β distinct up to isomorphism from E to the same curve E'. Then the discriminant D of the endomorphism ring of E is such that $|D| \leq 4\ell^2$.*

This set of lemmas gives us an idea of the graph of ℓ-isogenies of the elliptic curves having the same Frobenius map. It has a structure of a volcano truncated at the level of $\mathbb{Z}[\pi]$. The crater comes from the horizontal ℓ-isogenies (if they exist) that we can find when $\mathcal{O}$ is maximal at ℓ using Table 1 and the rest of the volcanic structure comes from the fact that by Lemmas 23 and 24, we see that if $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ then E does not have any horizontal ℓ-isogeny. Figure 1 summarizes these ideas.

The level of an elliptic curve in the volcano is the ℓ-adic valuation of its conductor. The height of the volcano is equal to the level of a curve with endomorphism ring isomorphic to $\mathbb{Z}[\pi]$ locally at ℓ.

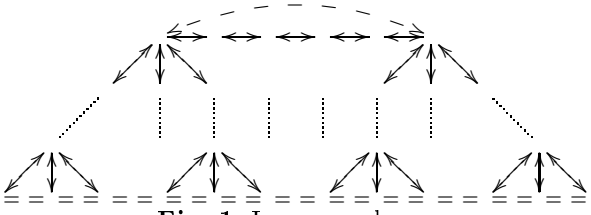


Fig. 1. Isogeny volcano

3 Modular equations and isogenies

We remind the reader that there exists a bivariate polynomial $\Phi_\ell(X,Y)$ with integer coefficients with the following property. Two elliptic curves E and E' defined over $\mathbb{F}_q$, are related via a cyclic isogeny α of degree ℓ if and only if $\#E = \#E'$ and $\Phi_\ell(j(E), j(E')) = 0$.

To find the curves related to E via an ℓ-isogeny, we must solve the equation $\Phi_\ell(X, j(E)) = 0$, which gives us their potential invariants. Suppose j^* is one of these roots. The curve E^* we are looking for is known up to twist and we must find an equation for it. Formulas for computing an equation of E^* are given in [13]. These formulas do not work in the case where j or j^* are in $\{0, 1728\}$ or $\partial\Phi_\ell/\partial X(j,j^*) = \partial\Phi_\ell/\partial Y(j,j^*) = 0$. We will call such a curve a *special* curve (or having a special endomorphism ring) and have a procedure detecting this, which is costless, since testing whether $\partial\Phi_\ell/\partial X(j,j^*) = \partial\Phi_\ell/\partial Y(j,j^*) = 0$ costs one polynomial gcd.

For later use, we will suppose that we have a procedure IsogenousCurves(E, ℓ) that gives us the list of curves that are ℓ-isogenous to a given curve E when E is not special.

4 Our algorithm

Let ℓ be a prime number different from p and $\mathcal{N}_\ell(E)$ denote the number of roots of $\Phi_\ell(X, j(E))$ in $\mathbb{F}_q$. Depending on $\mathcal{N}_\ell(E)$, we can determine some properties of $\mathrm{End}(E)$ using Table 1. We summarize them in Table 2.

$\mathcal{N}_\ell(E)$	Type of the ℓ-isogenies		$\left(\frac{D}{\ell}\right)$	$\left(\frac{d_\pi}{\ell}\right)$
0	none	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	-1	-1
2	$\rightarrow$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$+1$	$+1$
1	case 1: $\rightarrow$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	0	0
	case 2: $\uparrow$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ and $\ell \mid [\mathcal{O}_K : \mathcal{O}]$	0	0
$\ell+1$	case 1': $\begin{cases} 1+\left(\frac{D}{\ell}\right) & \rightarrow \\ \ell-\left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	nothing known	0
	case 2': $\begin{cases} 1 & \uparrow \\ \ell & \downarrow \end{cases}$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ and $\ell \mid [\mathcal{O}_K : \mathcal{O}]$	0	0

Table 2. Properties of $\mathcal{O}$ depending on the number and type of the ℓ-isogenies of E.

Kohel [10] uses this approach as one of his methods to compute the endomorphism ring of the elliptic curve E. We use it to compute isogeny volcanoes.

4.1 Goal of the algorithm

Let $\mathcal{E}$ be a given ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ and $j(\mathcal{E})$ its j-invariant. Let ℓ be a prime different from p. Starting from $\mathcal{E}$, we want to

construct a partial isogeny volcano, that is we want to determine the type of the crater of the isogeny volcano and determine a part of the volcano containing $\mathcal{E}$, plus a set of isogenous curves to $\mathcal{E}$ containing a curve with endomorphism ring isomorphic to $\mathbb{Z}[\pi]$ locally at ℓ and one with endomorphism ring isomorphic to $\mathcal{O}_K$ locally at ℓ.

We first give the skeleton of the algorithm and then detail every step.

4.2 Skeleton of the algorithm

The algorithm is divided into two parts. First, we determine whether $\mathbb{Z}[\pi]$ is maximal at ℓ or not. If not, then we look for a curve E_s in the crater of the isogeny volcano (Figure 1), determine the type of the crater by determining $\epsilon = \left(\frac{d_K}{\ell}\right)$ and then find the height of the volcano using what we call *a full descending path*. Since special curves need a careful treatment, we signal these with an EXIT statement, so as to ligthen the exposition.

Procedure ComputePartialVolcano
Input: An elliptic curve $\mathcal{E}$ and a prime ℓ, $\ell \neq p$.
Output: $\epsilon = \left(\frac{d_K}{\ell}\right)$ and a list $\mathcal{F}$ of full descending paths of the volcano.

1. IF $\mathcal{E}$ is special THEN EXIT;
2. $F \leftarrow$IsogenousCurves$(\mathcal{E}, \ell)$;
3. IF $\#F = 0$ THEN $\{\epsilon \leftarrow -1$; $\mathcal{F} \leftarrow \{\mathcal{E}\}$; GOTO 5$\}$
   ELIF $\#F = 2$ THEN $\{\epsilon \leftarrow +1$; $\mathcal{F} \leftarrow \{\mathcal{E}\}$; GOTO 5$\}$
   ELIF $\#F = 1$ THEN
   - $E' \leftarrow F[1]$;
   - IF E' is special THEN EXIT;
     ELIF $\mathcal{N}_\ell(E') = 1$ THEN $\{\epsilon \leftarrow 0$; $\mathcal{F} \leftarrow \{\mathcal{E}\}$; GOTO 5$\}$
     ELSE GOTO 4;

   ELIF $\#F = \ell + 1$ THEN GOTO 4;
4. $(E_s, P, \epsilon, n, \mathcal{F}) \leftarrow$FindFullDescendingPaths$(\mathcal{E}, \ell)$.
5. RETURN $(\epsilon, \mathcal{F})$.

4.3 Special curves.

If our original curve $\mathcal{E}$ has its j-invariant equal to 0 or 1728, then we cannot build any part of the volcano. We do not know how to distinguish the curves that are isogenous to $\mathcal{E}$ over $\mathbb{F}_q$ from the ones which are only isogenous to $\mathcal{E}$ over the algebraic closure of $\mathbb{F}_q$. If we encounter such a curve during the construction of the volcano, we know that this curve is in the crater of the volcano and we can deduce from this a full descending path and ϵ. But we will not be able to construct the whole volcano.

If at any moment in the construction, we encounter a curve E having two distinct ℓ-isogenies to a curve E', then we deduce that E is in the crater and the type of the crater. We will not be able to construct the entire volcano since we do not have the equation of E' but we can still get the complete subtree below E and therefore a full descending path.

4.4 The case $\mathcal{N}_\ell(\mathcal{E}) \neq \ell + 1$.

• $\mathcal{N}_\ell(\mathcal{E}) = 0$**:** In this case, if we refer to Table 2, we see that there is no ℓ-isogeny from $\mathcal{E}$ to another elliptic curve and that ℓ is inert in $\mathbb{Z}[\pi]$. We can also deduce that $\mathcal{O}_{K_\ell} \simeq \mathrm{End}(\mathcal{E})_\ell \simeq \mathbb{Z}[\pi]_\ell$.
• $\mathcal{N}_\ell(\mathcal{E}) = 2$**:** Referring to Table 2, we see that ℓ splits in $\mathbb{Z}[\pi]$. This case has already been treated by Couveignes, Dewaghe and Morain ([4], [3]). Using Lemma 22, we know that for every elliptic curve E' such that $\alpha : \mathcal{E} \to E'$ with α ℓ-isogeny then $\mathcal{O}' \simeq \mathrm{End}(\mathcal{E})$. We can also deduce that $\mathcal{O}_{K_\ell} \simeq \mathrm{End}(\mathcal{E})_\ell \simeq \mathbb{Z}[\pi]_\ell$.
• $\mathcal{N}_\ell(\mathcal{E}) = 1$**:** In this case, ℓ ramifies in $\mathbb{Z}[\pi]$. In Table 2, we see that this is a dual case. By dual, we mean that we may be in a case where $\mathbb{Z}[\pi]$ is maximal at ℓ or not. We need to distinguish those two cases. In order to do so, we will need its isogenous curve E' and $\mathcal{N}_\ell(E')$.

Case 1: $\mathcal{N}_\ell(E') = 1$**.** Suppose that $\mathbb{Z}[\pi]$ is not maximal at ℓ. Referring to Table 2, we know that $\ell \nmid [\mathrm{End}(\mathcal{E}) : \mathbb{Z}[\pi]]$, $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ and the ℓ-isogeny $\alpha : \mathcal{E} \to E'$ is an ascending ℓ-isogeny. Therefore applying Lemma 23, we have $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$. Thus, referring to Table 1, $\mathcal{N}_\ell(E') = \ell + 1$, which contradicts what we first found for $\mathcal{N}_\ell(E')$. Therefore, $\mathbb{Z}[\pi]$ is maximal at ℓ.

Case 2: $\mathcal{N}_\ell(E') = \ell + 1$**.** Suppose that $\mathbb{Z}[\pi]$ is maximal at ℓ, i.e. $\ell \nmid [\mathrm{End}(\mathcal{E}) : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O}_K : \mathrm{End}(\mathcal{E})]$. Referring to Table 2, we know that the ℓ-isogeny $\alpha : \mathcal{E} \to E'$ is an horizontal ℓ-isogeny and $(D_\mathcal{E}/\ell) = 0$. Therefore $\mathcal{O}'$ has the same conductor as $\mathrm{End}(\mathcal{E})$, i.e. $\ell \nmid [\mathcal{O}' : \mathbb{Z}[\pi]]$, $\ell \nmid [\mathcal{O}_K : \mathcal{O}']$ and $(D'/\ell) = 0$. Referring to Table 1, we see that $\mathcal{N}_\ell(E') = 1 + \left(\frac{D'}{\ell}\right) = 1$ which contradicts the result we first found for $\mathcal{N}_\ell(E')$. Therefore, $\mathbb{Z}[\pi]$ is not maximal at ℓ.

In this case, we can already make some conclusion about $\mathcal{O}$: $\mathcal{O}_{K_\ell} \not\simeq \mathrm{End}(\mathcal{E})_\ell$ and $\mathrm{End}(\mathcal{E})_\ell \simeq \mathbb{Z}[\pi]_\ell$, i.e. there exists an $n > 1$ such that $\ell^n \parallel g$ and $\ell^n \parallel f$.

4.5 The general case $\mathcal{N}_\ell(\mathcal{E}) = \ell + 1$.

By looking at the skeleton of the algorithm in Section 4.2, we see that this case is the most interesting one.

From now on, we assume that E is of level r, $r \in \mathbb{N}$, and $\mathcal{N}_\ell(E)$ equals $\ell + 1$. In fact, we have the equality $\mathcal{N}_\ell(E_i) = \ell + 1$ until we find the ending point of our recurrence that we recognize by $\mathcal{N}_\ell(E_i) = 1$.

This part of the algorithm is based on finding an elliptic curve E_s such that E_s is in the crater, using *descending paths*. First we precise this notion.

Descending paths.

Definition 41 *A* descending path *of an elliptic curve E is a path $E = E_0 \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$ of elliptic curves such that the map $E_i \to E_{i+1}$, for $i \in [0, \ldots, m[$, is a descending ℓ-isogeny and $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$. We will say that we have a* full descending path *if E is in the crater of the volcano.*

Lemma 41 *With the notations of Definition 41, if E is of level r then E_i is of level $r + i$.*

Proof: We prove this lemma by induction. $E_0 = E$ is of level r. Let us suppose that the result is true for E_j, with $0 \leq j < m$. We know that the map $E_j \to E_{j+1}$ is a descending ℓ-isogeny. Therefore, since the level of E_j is $r+j$, i.e. $\ell^{r+j} \parallel [\mathcal{O}_K : \mathcal{O}_j]$ and by definition of a descending ℓ-isogeny, then $\ell^{r+j+1} \parallel [\mathcal{O}_K : \mathcal{O}_{j+1}]$. Thus E_{j+1} is of level $r + (j+1)$. □

The main goal of finding a descending path starting from an elliptic curve E is to locate the endomorphism ring of E in the volcanic structure (see Figure 1) with respect to $\mathbb{Z}[\pi]$.

Corollary 41 *Let $\mathcal{P}$ be a descending path starting from E and let $m = \#\mathcal{P} - 1$. Then E is of level $(n - m)$ where n is the height of the volcano.*

Now that we have defined this notion and its interest, we will show how to compute a descending path. We first give the algorithm and then prove its correctness.

Procedure FINDDESCENDINGPATH
Input: A non special elliptic curve E such that $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
Output: A descending path starting from E.

1. $F \leftarrow$ISOGENOUSCURVES(E, ℓ);
2. IF $\#F = 1$ THEN $\{P[1] \leftarrow \{E\}$; $i_0 \leftarrow 1$; GOTO 6$\}$;
3. FOR $i := 1$ TO 3 DO
   (a) $P[i] \leftarrow \{E\} \cup \{F[i]\}$; $G[i] \leftarrow E$; $G'[i] \leftarrow F[i]$;
   (b) IF $G'[i]$ is special THEN $S[i] \leftarrow \emptyset$ ELSE $S[i] \leftarrow$ISOGENOUSCURVES$(G'[i], \ell)$;
4. $i_0 \leftarrow -1$
5. WHILE $(i_0 = -1)$ DO
   FOR $i := 1$ TO 3 DO (at this point, $G'[i]$ is one of the curves isogenous to $G[i]$ and $S[i]$ contains a list of curves isogenous to $G'[i]$)
   IF $S[i] = \emptyset$ THEN use next i;
   IF $\#S[i] = 1$ THEN $\{i_0 \leftarrow i$; (we have found the base of the volcano)$\}$
   ELSE
   (a) IF $(j(S[i][1]) = j(G[i]))$ THEN {(we must not use the dual of the preceding isogeny) $G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][2]$;};
   ELSE $\{G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][1]$;$\}$;
   (b) $P[i] \leftarrow P[i] \cup \{G'[i]\}$;
   (c) IF $G'[i]$ is special THEN $S[i] \leftarrow \emptyset$ ELSE $S[i] \leftarrow$ISOGENOUSCURVES$(G'[i], \ell)$;
6. RETURN $P[i_0]$.

By Lemma 24, we know that whenever we have an ℓ-isogeny $\alpha : E \to E'$ that is a descending ℓ-isogeny, every ℓ-isogeny $\beta : E' \to E''$ such that $\mathrm{End}(E'') \not\simeq \mathrm{End}(E)$ is a descending ℓ-isogeny. Therefore, inductively, if we start a path of ℓ-isogenies with a descending ℓ-isogeny, we will get a descending path.

To find such an ℓ-isogeny to start the path, we will compute in parallel three different paths starting from any three different curves isogenous to E. Having three different starting curves ensures us of having a path starting with

a descending ℓ-isogeny and therefore a non-empty path. Since a non-descending path is composed of a path of non-descending ℓ-isogenies and a descending path, a non-descending path is longer than a descending path. Therefore, the first path that stops is a descending path.

Lemma 42 *The complexity of the algorithm* FINDDESCENDINGPATH *is* $O(m\mathcal{F}(\ell))$, *where* m *is the height of* E *and* $\mathcal{F}(\ell)$ *the time to find three roots of a modular polynomial.*

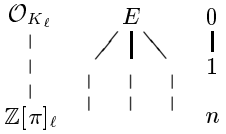
Proof: To calculate each one of the three paths, it takes $m+1$ partial factorizations of the modular equation. □

Why do we need a curve in the crater? If we have a curve E_s in the crater and a full descending path $E_s \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$, we get the height of the volcano and then using the algorithms that are given to find a partial volcano, we can move easily in the volcano and construct the rest of it if we want. To find such a curve E_s we need to know how to recognize that a curve is in the crater.

Detecting the crater and thus determining ϵ. From Table 2, we see that a curve in the crater has $1+\left(\frac{D}{\ell}\right)$ horizontal ℓ-isogenies and $\ell-\left(\frac{D}{\ell}\right)$ descending ℓ-isogenies. We detect these three different cases in three different ways.

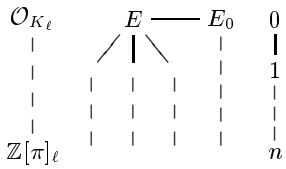
Suppose E is in the crater and let n be the height of the volcano. Then one of the following conditions will be met.

• Case a: There is no horizontal ℓ-isogeny. Considering the fact that we are in the crater, we have $\ell+1$ descending ℓ-isogenies. Then all the descending paths starting from the $\ell+1$ isogenous curves to E have the same length. The following graph characterizes this situation.

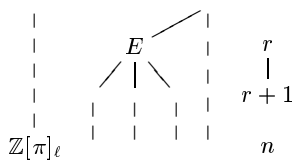


The length of the descending paths is $n-1$ because all the curves corresponding to the $\ell+1$ roots of $\Phi_\ell(X,j)$ are at level 1. We can also deduce that ℓ is inert in $\mathcal{O}_K$ and thus $\epsilon=-1$.

• Case b: There is exactly one horizontal ℓ-isogeny and there are also ℓ descending ℓ-isogenies. Then one of the descending paths starting from the $\ell+1$ isogenous curves to E is of length n (let us say that this path starts on E_0) and the other ℓ ones are of length $(n-1)$. The following graph characterizes this situation and makes the parallel with the normal situation.



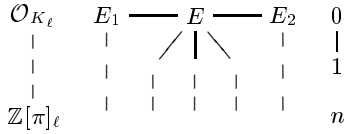
Horizontal case



"Normal" case

We cannot confuse this case with the "normal" case of one ascending ℓ-isogeny and ℓ descending ℓ-isogenies, because in the horizontal case, the difference between the length of the path starting on E_0 and the other paths is 1 whereas in the "normal" case this difference is 2. We know also that ℓ ramifies in $\mathcal{O}_K$ and therefore $\epsilon = 0$.

• Case c: There are two horizontal ℓ-isogenies and there are also $\ell - 1$ descending ℓ-isogenies. Then two of the descending paths starting from the $\ell + 1$ isogenous curves to E are of length n (let us say that these two paths start on E_1 and E_2) and the other $\ell - 1$ ones are of length $n - 1$. The following graph characterizes this situation.



The difference with the preceding case is that we find two paths longer than the others instead of just one. So no confusion with the "normal" case is possible. We know also that ℓ splits in $\mathcal{O}_K$ and therefore $\epsilon = +1$.

How to find a curve in the crater. The algorithm finding a curve in the crater is exactly the inverse of the one finding a descending path. We want to construct an *ascending path* starting from $\mathcal{E}$.

Definition 42 *An* ascending path *of an elliptic curve E is a path $E = E_0 \to E_{-1} \to E_{-2} \to \cdots \to E_{-(s-1)} \to E_{-s}$ of elliptic curves such that the map $E_{-i} \to E_{-(i+1)}$, for $i \in [0, \ldots, s-1[$, is an ascending ℓ-isogeny and $\ell \nmid [\mathcal{O}_K : \mathcal{O}_{-s}]$.*

We will say that we have a full ascending path *if $\mathcal{O}_\ell \simeq \mathbb{Z}[\pi]_\ell$.*

Lemma 43 *Using the same notations as in Definition 42, if E is of level r then E_{-i} is of level $r - i$.*

Corollary 42 *If the length of the ascending path starting on E is $r+1$, then E is at level r.*

At every step of this algorithm, we want to find a curve at an inferior level than E i.e. the unique ascending ℓ-isogeny of E. To do so, we will compute a descending path for every curve isogenous to E and compare their sizes. We reiterate this until we detect a curve in the crater.

Procedure DetectSurface
Input: A list of descending paths $\mathfrak{P}$ and the curve E_{cur}.
Output: $(\epsilon, i_{max}, \lambda, \mathcal{F})$ such that

- $\epsilon = 0$, i_{max} such that $\#\mathfrak{P}[i_{max}]$ is maximal and $\lambda = \#\mathfrak{P}[i_{max}]$
- OR $\epsilon = (d_K/\ell)$, $i_{max} = -1$ and λ is the height of the volcano if we detect that E_{cur} is in the crater;
- $\mathcal{F}$ is a list of (some) full descending paths.

1. $\epsilon \leftarrow 0$; $\mathcal{F} \leftarrow \emptyset$;

2. Find i_{max} such that $\#\mathfrak{P}[i]$ is maximal;
3. $I \leftarrow \{i$ s.t. $i \neq i_{max}$ and $\#\mathfrak{P}[i] = \#\mathfrak{P}[i_{max}]\}$;
4. /* Case where the crater is detected and $\left(\frac{d_K}{\ell}\right) = -1$ (case a) */
   IF $\#I = \ell$ THEN $\{\epsilon \leftarrow -1; \lambda \leftarrow \#\mathfrak{P}[i_{max}]; i_{max} \leftarrow -1; \mathcal{F} \leftarrow \{\{E_{cur}, \mathfrak{P}[1]\}\};$
   $\}$
5. /* Case where the crater is detected and $\left(\frac{d_K}{\ell}\right) = +1$ (case c)*/
   IF $\#I = 1$ THEN $\{$ $i_{max2} \leftarrow I[1]$; $\epsilon \leftarrow 1$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $i_0 \leftarrow$ any index distinct from i_{max} and i_{max2}; $\mathcal{F} \leftarrow \{\{E_{cur}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}], \mathfrak{P}[i_{max2}]\}$; $i_{max} \leftarrow -1$; $\}$
6. IF $\#I = 0$ THEN
   (a) IF $i_{max} = 1$ THEN $i_0 \leftarrow 2$; ELSE $i_0 \leftarrow 1$;
   (b) IF $\#\mathfrak{P}[i_{max}] - \#\mathfrak{P}[i_0] = 1$ /* Case where the crater is detected and $\left(\frac{d_K}{\ell}\right) = 0$ (case b) */
   THEN $\{\epsilon \leftarrow 0$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $\mathcal{F} \leftarrow \{\{E_{cur}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}]\}$; $i_{max} \leftarrow -1$; $\}$
   ELSE $\{\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1;\}$
7. RETURN $(\epsilon, i_{max}, \lambda, \mathcal{F})$.

Procedure FindFullDescendingPaths
Input: A non-special elliptic curve E such that $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
Output: $(E_s, P, \epsilon, n, \mathcal{F})$ such that E_s is in the crater, isogenous to E, P is an ascendin path from E to E_s, $\epsilon = (d_K/\ell)$, n the height of the volcano and $\mathcal{F}$ is a list of (some) full descending paths.

1. $E_{cur} \leftarrow E$;
2. $F \leftarrow$IsogenousCurves(E_{cur}, ℓ);
3. $P \leftarrow \{E_{cur}\}$;
4. IF $\#F = 1$ THEN $\{E_{cur} \leftarrow F[1]$; IF E_{cur} is special THEN EXIT; ELSE $\{P \leftarrow P \cup \{F[1]\};\}\}$
5. $i_0 \leftarrow 0$;
6. WHILE $i_0 \neq -1$ DO
   (a) $F \leftarrow$IsogenousCurves(E_{cur}, ℓ);
   (b) FOR $i := 1$ TO $\ell + 1$ DO
   IF $F[i]$ is special THEN EXIT;
   $\mathfrak{P}[i] \leftarrow$ FindDescendingPath$(F[i])$;
   (c) $(\epsilon, i_0, \lambda, \mathcal{F}) \leftarrow$DetectSurface$(\mathfrak{P})$;
   (d) IF $i_0 \neq -1$ THEN $\{E_{cur} \leftarrow F[i_0]$; $P \leftarrow P \cup \{E_{cur}\};\}$
7. $E_s \leftarrow E_{cur}$;
8. RETURN $(E_s, P, \epsilon, \lambda, \mathcal{F})$;

Lemma 44 *The complexity of the algorithm* FindFullDescendingPaths *is* $O(n^2 \ell \mathcal{F}(\ell))$*, with* $\mathcal{F}(\ell)$ *the time to calculate all the roots of a modular polynomial.*

Proof: To go from level μ to level $\mu - 1$, we need to calculate $\ell + 1$ descending paths. This takes $O(\mu \ell \mathcal{F}(\ell))$ operations, for a total of $\Sigma_{\mu=1}^{n} \mu \mathcal{F}(\ell) = \frac{n(n+1)}{2} \mathcal{F}(\ell)$. Therefore it takes $O(n^2 \ell \mathcal{F}(\ell))$ operations to compute an ascending path. □

The following theorem gives the complexity of the algorithm to compute a partial volcano.

Theorem 41 *It takes $O(n^2\ell\mathcal{F}(\ell))$ operations to compute a partial volcano of ℓ-isogenies, with $n \leq \frac{\log_2(|d_K|)}{\log_2(\ell)}$ and $\mathcal{F}(\ell)$ the time to calculate all the roots of a modular polynomial.*

Proof: The whole algorithm is based on the computation of an ascending path starting from $\mathcal{E}$. □

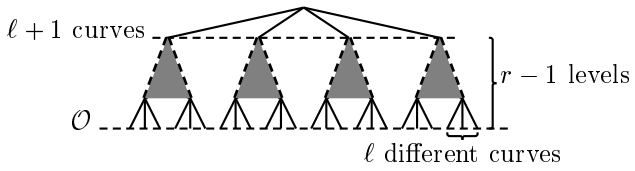
5 Number of isogeny volcanoes

We define the endomorphism class of E denoted by $\mathcal{C}(E)$ to be a set of curves isogenous but non isomorphic having the same endomorphism ring $\mathcal{O}$. There exists a bijection between $C(\mathcal{O})$ and $\mathcal{C}(E)$. If there exists a unique ℓ-isogeny volcano then we can compute the set of $h(\mathcal{O})$ elliptic curves in $\mathcal{C}(E)$ using this volcano. Therefore we use properties of $h(\mathcal{O})$ to compute the number of ℓ-isogeny volcanoes.

Theorem 51 *The number of different volcanoes of ℓ-isogenies is $h(f'^2 d_K)/\mathrm{ord}(\mathfrak{l})$ where $\mathrm{ord}(\mathfrak{l})$ is the order of the ideal $\mathfrak{l}$ which is a prime ideal of norm ℓ.*

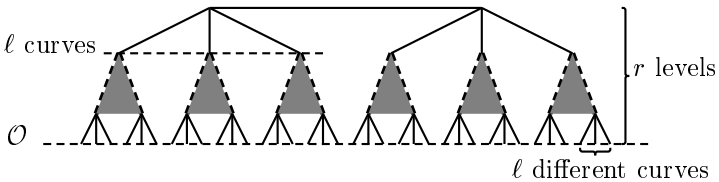
Proof: We treat separately the different types of volcanoes.

Case where $\left(\frac{d_K}{\ell}\right) = -1$. In this situation, every ℓ-isogeny volcano is of the form:



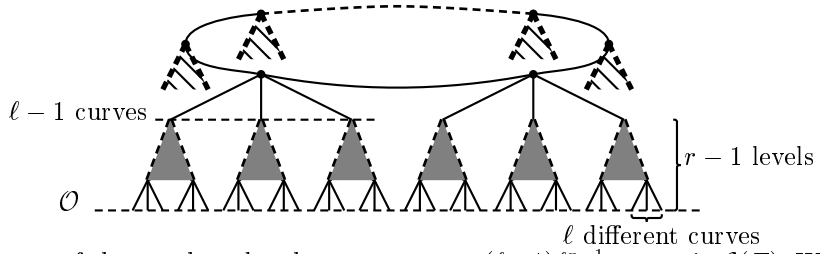
In this type of volcano we have found $\ell^r + \ell^{r-1}$ of the $h(\mathcal{O})$ curves isogenous to E having the same endomorphism ring $\mathcal{O}$. We have $h(m^2 D) = \frac{h(D)m}{[\mathcal{O}_1^* : \mathcal{O}_2^*]} \prod_{p|m} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)$ where $\mathcal{O}_1$ and $\mathcal{O}_2$ are the orders of discriminant D and $m^2 D$ ([5, Coro 7.28]) and when D is different from -4 and -3, $[\mathcal{O}_1^* : \mathcal{O}_2^*]$ is equal to 1. In our case we consider $m = \ell^r$ where r is the ℓ-adic valuation of the conductor f of $\mathcal{O}$. We set $f = f'\ell^r$. Then $h(f^2 d_K) = h(f'^2 D)\ell^r \left(1 - \left(\frac{D}{\ell}\right)\frac{1}{\ell}\right) = h(f'^2 D)\ell^r(1 + 1/\ell) = h(f'^2 D)(\ell^r + \ell^{r-1})$. Then there are $h(f'^2 D)$ distinct volcanoes of this type.

Case where $\left(\frac{d_K}{\ell}\right) = 0$. In this situation, every ℓ-isogeny volcano is of the form:



In such a volcano, we get $2\ell^r$ curves in $\mathcal{C}(E)$. In this case, it is also clear that there are $h(f'^2 D_K)/2$ distinct volcanoes (reusing the preceding notations).

Case where $\left(\frac{d_K}{\ell}\right) = 1$. We get a volcano of the form:



For each one of the graph under the crater we get $(\ell-1)\ell^{r-1}$ curves in $\mathcal{C}(E)$. We now have to determine the size of the crater. If we consider the set of the curves in the crater lifted in $\mathbb{C}$, we get the following cycle $\mathcal{E}_0 \to \mathcal{E}_1 \to \cdots \mathcal{E}_{s-1} \to \mathcal{E}_s \simeq \mathcal{E}_0$ where $\mathcal{E}_i \simeq \mathbb{C}/\mathfrak{a}_i$. Since we consider ℓ-isogenies we have $\mathfrak{a}_i = \mathfrak{a}_{i+1}\mathfrak{l}$ where $\mathfrak{l}$ is a prime ideal of norm ℓ. Therefore $\mathfrak{a}_0 = \mathfrak{a}_s = \mathfrak{l}^s\mathfrak{a}_0$ i.e. $\mathfrak{l}^s$ is a principal ideal of $\mathcal{O}_K$ and thus s is the order of $\mathfrak{l}$ in $\mathcal{O}_K$ and s is the size of the crater. Therefore the number of different volcanoes we can build is $h(f'^2 d_K)/\mathrm{ord}(\mathfrak{l})$ where $\mathrm{ord}(\mathfrak{l})$ is the order of the ideal $\mathfrak{l}$ which is a prime ideal of norm ℓ.

Using the type of decomposition of the ideal $\ell\mathcal{O}_K$, we can generalise this last formula to all the types of volcanoes. □

6 Application to point counting

First, we suppose that $\ell \neq 2$ and that we have not encountered a special curve (for these cases see [7]).

If $\mathcal{N}_\ell(\mathcal{E})$ is equal to 1 or $\ell+1$, then we can deduce that ℓ ramifies in $\mathbb{Z}[\pi]$ i.e. $\left(\frac{d_\pi}{\ell}\right) = 0$ and therefore we immediately know that $t^2 \equiv 4q \pmod{\ell}$. Our idea is to explain how a more precise result can be found, namely the ℓ-adic valuation of $t^2 - 4q$ that we note ν_ℓ. We will determine n such that $\ell^n \parallel g$, i.e. the height of the isogeny volcano, and since $t^2 - 4q = g^2 d_K$, we get $t^2 \equiv 4q \pmod{\ell^{2n+\delta}}$ and therefore $\nu_\ell \geq 2n+\delta$. The value of δ is determined by the Legendre symbol $\left(\frac{d_K}{\ell}\right)$. If it is equal to 0, then we deduce that $\ell \mid d_K$, therefore $\delta = 1$. Otherwise, $\delta = 0$. By definition of the fundamental discriminant d_K, we have in fact $\nu_\ell = 2n + \delta$ (except maybe in the case $\ell = 2$, see [7]).

6.1 Finding t mod ℓ^ν

In general (that is except in the cases where we happened to find a special case), our algorithm has given us $t^2 \equiv 4q \bmod \ell^\nu$, we may want $t \bmod \ell^\nu$. Suppose $\ell \neq 2$. Then there are only two squareroots of $4q$ modulo ℓ^ν. To find the sign of t, it is enough to find the sign of $t_1 \equiv t \bmod \ell$. Finding t_1 is done via the determination of an eigenspace of π and the associated eigenfactor of the ℓ-th division polynomial Ψ_ℓ *à la* Elkies. This will determine the eigenvalue, which turns out to be $t_1/2 \bmod \ell$ in that case.

6.2 Finding t mod $\ell^{\nu+1}$

Now that we have $t \bmod \ell^\nu$, is it possible to find $t \bmod \ell^{\nu+1}$? When $(d_K/\ell) \neq +1$, we cannot do anything, since we already explored all possible isogenies. In the

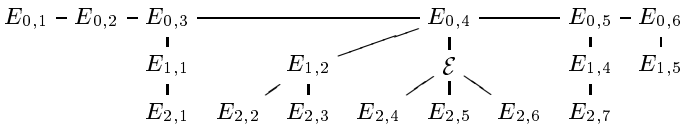
case where $(d_K/\ell) = +1$, the head of the volcano is an isogeny cycle and the ideas of [4] apply there too (see [7]).

Further applications are given in [7]. In particular, we solve a problem of Lercier encountered in [11].

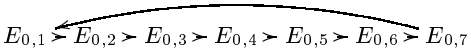
7 Numerical examples

The reader can find a more complete set of examples in [7].

Example 1 (Normal case, ℓ splits in $\mathcal{O}_K$ i.e. $\left(\frac{d_K}{\ell}\right) = +1$): Let $p = 10009$ and $\mathcal{E} = [7478, 1649]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 83$. Using $\ell = 3$, we find

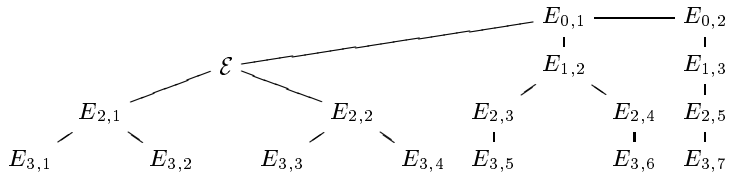


Therefore, $n = 2$, $\left(\frac{d_K}{\ell}\right) = 1$ thus $\delta = 0$ and $t^2 \equiv 4p \pmod{3^4}$ and in fact $t \equiv 34 \bmod 3^4$. Moreover, in this case, we are able to construct at the surface a cycle of isogenies. We get the following graph:



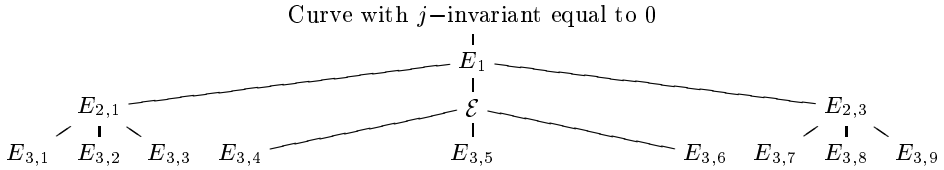
Using this cycle, we find that $t \equiv -47 \bmod 3^5$. As a matter of fact, $t = -47$.

Example 2 (Incomplete case for $\ell = 2$ from [3]): Let $p = 1009$ and $\mathcal{E} = [1, 3]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 269$. For $\ell = 2$, one gets



Therefore, $n = 3$, $\left(\frac{d_K}{\ell}\right) = 0$ thus $\delta = 2$ and $t^2 \equiv 4p \pmod{2^8}$. As a matter of fact, $t = -50$, therefore $d_K = -24$, $g = 2^3$ and $(-50)^2 \equiv 4 \times 1009 \pmod{2^9}$. In this case, we only get a lower bound of the valuation.

Example 3 (Case where the curve E_s has j-invariant equal to 0): Let $p = 1009$ and $\mathcal{E} = [363, 690]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 433$. Consider $\ell = 3$:



Therefore, $n = 3$, $\left(\frac{d_K}{\ell}\right) = 0$ thus $\delta = 1$ and $t^2 \equiv 4p \pmod{3^7}$. As a matter of fact, $t = 43$.

8 Conclusion

We have found an answer to several problems encountered while implementing various algorithms for elliptic curves over finite fields. The volcanon structure is an important point of view on the isogeny class of a curve and may therefore become an important tool for that type of studies. It would be interesting to study more closely the relationships between distinct volcanoes of same prime ℓ. Another direction would be to look at volcanoes of composite indices.

Acknowledgments. We would like to thank D. Kohel for useful discussions on isogenies and for anticipating some of the results on the volcano structure. Special thanks also to P. Gaudry for useful remarks concerning this work.

References

1. Z. I. Borevitch and I. R. Chafarevitch. *Théorie des nombres.* Gauthiers-Villars, Paris, 1967.
2. J. Chao, O. Nakamura, K. Sobataka, and S. Tsujii. Construction of secure elliptic cryptosystems using CM tests and liftings. In K. Ohta and D. Pei, editors, *Advances in Cryptology – ASIACRYPT'98*, volume 1514 of *Lecture Notes in Comput. Sci.*, pages 95–109. Springer-Verlag, 1998. Beijing, China.
3. J.-M. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03, LIX, April 1996. Available at `http://www.lix.polytechnique.fr/Labo/Francois.Morain/`.
4. J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In *ANTS-I*, 1994.
5. D. H. Cox. *Primes of the Form* $x^2 + ny^2$. Wiley-Interscience, 1989.
6. M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.
7. M. Fouquet. *Anneau d'endomorphismes et cardinalité des courbes elliptiques : aspects algorithmiques.* Thèse, École polytechnique, December 2001. Available at `http://www.lix.polytechnique.fr/Labo/Mireille.Fouquet/`.
8. M. Fouquet, P. Gaudry, and R. Harley. An extension of Satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, December 2000.
9. S.D. Galbraith, F. Hess, and N.P. Smart. Extending the GHS weil descent attack. `http://eprint.iacr.org/`, 2001.
10. D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* Phd thesis, University of California, Berkeley, 1996.
11. R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis.* Thèse, École polytechnique, June 1997.
12. T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15:247–270, December 2000.
13. R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 1995.