ÉCOLE POLYTECHNIQUE

LIX

Isogeny volcanoes and the SEA algorithm

M. Fouquet, F. Morain

LIX/RR/00/05

28 juin 2000

LABORATOIRE D'INFORMATIQUE
Unité mixte CNRS n°7650
École polytechnique 91128 Palaiseau Cedex FRANCE

ISOGENY VOLCANOES AND THE SEA ALGORITHM

M. FOUQUET AND F. MORAIN

ABSTRACT. In 1985, Schoof gave a deterministic polynomial time algorithm to compute the cardinality of an elliptic curve over a finite field. His algorithm computes the cardinality modulo small primes and builds the answer using the Chinese Remaindering Theorem. The improvements of Atkin and Elkies made the computations easier and practical. Couveignes and Morain showed how to extend the ideas of Elkies to the case of prime powers, in effect walking through the Tate module associated to the curve, via rational isogenies. This latter algorithm works well if the Frobenius of the curve has two distinct eigenvalues and there remained to tackle the case of repeated eigenvalues. The purpose of this work is to solve this problem, explaining how this relates to the computation of the endomorphism ring of the curve, as worked out by Kohel.

1. INTRODUCTION

Let E be an elliptic curve defined 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 [7] 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). Computing $\chi(T)$ is essential for computing the cardinality of the group of points of E over $\mathbb{F}_q$, since $\chi(1) = q + 1 - t$.

Schoof [23] gave a deterministic polynomial time algorithm to compute $\chi(T)$. The idea is to compute $\chi(T)$ modulo small primes ℓ using the ℓ-torsion points of E and to reconstruct the coefficients using the Chinese Remaindering Theorem. The original algorithm used division polynomials that have a large degree and was therefore difficult to implement directly. Significant improvements were given by Atkin and Elkies (see [24, 9, 19]) and completed for the small characteristic case in [16, 17, 3, 4, 14] (see also [15] for a survey of these and [22, 10] for a completely different approach). Since computing the cardinality of supersingular elliptic curves (because in that case, $p \mid t$) is rather easy, especially when p is small [18, 20], we will not be concerned with this problem in the present article. We suppose from now on that we are concerned with ordinary curves.

Elkies's idea is to use rational isogenies of degree ℓ to find a factor of the ℓ-th division polynomial of degree $O(\ell)$ when it exists, that is when the Frobenius has rational eigenvalues, or equivalently when the discriminant $d_\pi = t^2 - 4q$ is a square modulo ℓ. Rational isogenies correspond to the roots of the modular polynomial $\Phi_\ell(X, j(E))$ where $j(E)$ is the invariant of E. Couveignes and Morain [6] showed how to use isogeny cycles to compute a suitable factor of the ℓ^k-th division polynomial by composing intermediate isogenies, in the case where π has two *distinct* rational eigenvalues, that is when d_π is a non-zero square modulo ℓ. If the discriminant is not a square, then we can sometimes find a small degree extension of the base field that can be used [8].

When $d_\pi \equiv 0 \bmod \ell$, the Frobenius has only one double eigenvalue and one eigenspace and the theory of isogeny cycles cannot be used *mutatis mutandis*. In [5], an attempt was made to replace isogeny cycles by trees, but the answer was not satisfactory at all. The key to our understanding of

Date: June 28, 2000.

The second author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

the situation came from Kohel's work [12] on the explicit computation of the endomorphism ring of E, which is an order in an imaginary quadratic field. Finding this order boilds down to finding its conductor f. If ℓ is a prime dividing d_π, then the modular polynomial $\Phi_\ell(X, j(E))$ will have either 1 or $\ell+1$ roots and Kohel is able to relate this number of roots to the ℓ-adic valuation of f. We will work the other way round, since we do not know d_π, but want to find it. Computing the roots of $\Phi_\ell(X, j(E))$ will give us the ℓ-adic valuation ν of f, from which we will deduce $t \bmod \ell^\nu$.

After introducing some basic notations, we will recall the relevant facts about Kohel's work that describe the structure that grows "under" the cycles, forming a volcano. Then we recall the relevant theory of modular polynomials and we are ready to "invert" Kohel's theorem to see the situation from the modular side, which will lead to our algorithm. Also, we relate the new structure to the trees that were invented in [5] and solve a problem raised by Lercier in his thesis. 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 to be used to compute 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 the ring of endomorphisms of the curve 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 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 $\mathcal{O}(E)$ of E. These orders are such that $\mathbb{Z}[\pi] \subseteq \mathcal{O}(E) \subseteq \mathcal{O}_K$ or equivalently, with f the conductor of $\mathcal{O}(E)$ and g that of $\mathbb{Z}[\pi]$:

$$\begin{array}{ll} \mathcal{O}_K & \\ \quad | & \quad f \\ \mathcal{O}(E) & \\ \quad | & \quad g/f \\ \mathbb{Z}[\pi] & \end{array}$$

In his thesis [12], Kohel wants to compute $\mathcal{O}(E)$ starting from the known value of $d_\pi = t^2 - 4q = g^2 d_K$, where t was computed using Schoof's algorithm for instance. The idea to determine f is to place $\mathcal{O}(E)$ with respect to $\mathbb{Z}[\pi]$ and $\mathcal{O}_K$ in the preceding graph. He can do that by a variety of methods, all based on the properties of isogenies. In our case, we will work the other way round: we want to determine $t \bmod \ell^\nu$ in the case where $\ell \mid t^2 - 4q$. We will compute f by first finding the relative place of $\mathcal{O}(E)$ w.r.t. $\mathbb{Z}[\pi]$ and then that of $\mathcal{O}(E)$ w.r.t. $\mathcal{O}_K$.

Let us first 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 ℓ be a prime different from p. Let $\mathcal{O}$ be the endomorphism ring of E, D its discriminant and f its conductor. We will need other ordinary elliptic curves defined over the same finite field. Therefore, we will introduce the same kind of notations. Let E' (resp.

Case		*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 isogenies depending on $[\mathcal{O}_K : \mathcal{O}]$ and $[\mathcal{O} : \mathbb{Z}[\pi]]$.

E_i) be an ordinary elliptic curve and j' (resp. j_i) its j-invariant; we will denote its endomorphism ring by $\mathcal{O}'$ (resp. $\mathcal{O}_i$), its discriminant by D' (resp. D_i) and its conductor by f' (resp. f_i).

Since we are only interested in the factor ℓ^k of the conductor f that we are considering, we will only look at the reduced conductor $\tilde{f}$ w.r.t. ℓ, i.e. $f = c\tilde{f}$ with $\ell \nmid c$ and $\tilde{f} = \ell^k$. With this definition, let n be such that $\tilde{g} = \ell^n$. We also define the reduced order $\tilde{\mathcal{O}}$ w.r.t. ℓ to be the order of conductor the reduced conductor of $\mathcal{O}$. The reduced order $\tilde{\mathcal{O}}$ w.r.t. ℓ and $\mathcal{O}$ have the same reaction with respect to ℓ-isogenies, but reduced orders are much simpler to consider.

Since we only consider rational ℓ-isogenies in the rest of the paper, to simplify the notations, we will call them "isogenies".

2.2. **Kohel's theorem.** The following proposition justifies the fact that we can use the isogenies of an elliptic curve to determine its endomorphism ring $\mathcal{O}$ (and overall its reduced conductor $\tilde{f}$).

Proposition 2.1. *Let $\alpha : E \rightarrow E'$ 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.*

Proof: Kohel [12, Proposition 21]. □

This is equivalent to saying $[\mathcal{O} : \mathcal{O}'] = 1$, ℓ or $\frac{1}{\ell}$.

With the restrictions on the conductors, we have the following graph concerning the orders $\mathcal{O}_K$, $\mathcal{O}$ and $\mathbb{Z}[\pi]$:

$$\begin{array}{c} \tilde{\mathcal{O}}_K \\ | \qquad \tilde{f} = \ell^r \\ \tilde{\mathcal{O}} \\ | \quad \tilde{g}/\tilde{f} = \ell^m = \ell^{(n-r)} \\ \widetilde{\mathbb{Z}[\pi]} \end{array}$$

Let us introduce Kohel's language. An isogeny "down", denoted by $\downarrow$, is an isogeny $\alpha : E_1 \rightarrow E_2$ such that $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$ whilst an isogeny "up", denoted by $\uparrow$, is an isogeny $\alpha : E_1 \rightarrow E_2$ such that $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$. In the case where the endomorphim rings are preserved we call the isogeny "horizontal", denoted by $\rightarrow$. We say that E is "on the floor at ℓ" if $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ and E is "at the surface w.r.t. ℓ" if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. We might also say that E is "of level r at ℓ" if $\ell^r \parallel [\mathcal{O}_K : \mathcal{O}]$, i.e. $\tilde{f} = \ell^r$. Since the algorithm runs for a fixed ℓ, when speaking of "level", of "floor" or of "surface", we omit the reference to ℓ.

Theorem 2.1. *Table 1 classifies the possibilities for the rational isogenies of E defined over $\mathbb{F}_q$.*

Proof: See Kohel [12, Proposition 23]. □

2.3. **Some lemmas about the classification of 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 isogeny α and its dual denoted by $\hat{\alpha}$.

Lemma 2.1. *Let $\alpha : E \to E'$ be an isogeny and $\hat{\alpha}$ its dual. Then*

- *α is $\uparrow$ if and only if $\hat{\alpha}$ is $\downarrow$;*
- *α is $\to$ if and only if $\hat{\alpha}$ is $\to$.*

Proof: If α is $\uparrow$, then $[\mathcal{O}' : \mathcal{O}] = \ell$. Since $\hat{\alpha} : E' \to E$, then, by definition of being $\downarrow$, $\hat{\alpha}$ is $\downarrow$.

If α is $\to$, then $\mathcal{O} \simeq \mathcal{O}'$. Immediately, we have that $\hat{\alpha}$ is $\to$. □

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 isogeny. With respect to ℓ, we distinguish two cases for the endomorphism rings: the static case and the non-static one.

Definition 2.1. *We say that the endomorphism ring $\mathcal{O}$ is* static *with respect to ℓ if we have the two following relations: $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, or equivalently $\tilde{f} = 1$.*

If any of these conditions is not satisfied, we say that the endomorphism ring is non-static *w.r.t. ℓ.*

In the rest of the paper, whenever we say that $\mathcal{O}$ is static, we will mean $\mathcal{O}$ is static w.r.t. ℓ, and whenever we say that a curve is static, we mean that its endomorphism ring is static.

The first lemmas will treat the static case.

Lemma 2.2. *Let E and E' be two isogenous elliptic curves. $\mathcal{O}$ is static if and only if $\mathcal{O}'$ is static.*

Proof: Let $\mathcal{O}$ be static. Referring to Table 1, we can see that if there is any isogeny from E to another curve E', then this isogeny is $\to$. Therefore, $\mathcal{O} \simeq \mathcal{O}'$. Thus the relation of $\mathcal{O}'$ with $\mathcal{O}_K$ and $\mathbb{Z}[\pi]$ is that of $\mathcal{O}$. □

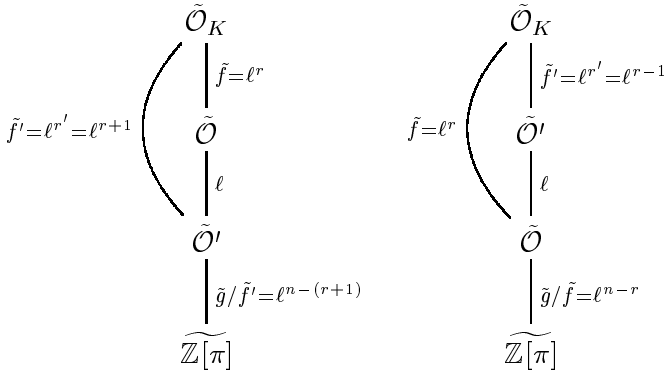
In the following lemma, we will keep the same hypothesis and add one more to show the existence of a two-cycle of isogenies.

Lemma 2.3. *If $\mathcal{O}$ is static and $\left(\frac{D}{\ell}\right) = 0$, then there exists a two-cycle of isogenies $(\alpha, \hat{\alpha})$, such that $\alpha : E \to E'$ and $\hat{\alpha} : E' \to E$ and α (resp. $\hat{\alpha}$) is the only isogeny of E (resp. E'). Therefore we get the following graph of isogenies:*

$$E \rightleftarrows E'.$$

Proof: We denote by α the unique isogeny $\to$ of E given by Theorem 2.1. Let E' be such that $\alpha : E \to E'$. By Lemma 2.2, $\mathcal{O}'$ is static, so $D' = D$, therefore, $\left(\frac{D'}{\ell}\right) = \left(\frac{D}{\ell}\right) = 0$. Hence there exists a unique isogeny $\to$ of E' which must be $\hat{\alpha}$. □

Suppose now that $\mathcal{O}$ is non-static. We state two lemmas about the isogenies of E to distinguish the two possible cases for the endomorphism ring $\mathcal{O}'$. These two different situations are summarized in the following graphs:



We will first study the case where $\tilde{\mathcal{O}} \simeq \widetilde{\mathbb{Z}[\pi]}$ and then we will look at a more general case.

Lemma 2.4. *If $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, i.e. $\tilde{f} = \tilde{g} = \ell^n$ with $n \geq 1$, then the only isogeny $\alpha : E \to E'$ is such that $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$, i.e. $\tilde{f}' = \ell^{n-1}$.*

Proof: Referring to Table 1, the only isogeny of E, denoted by α is $\uparrow$. Then we know that $[\mathcal{O}' : \mathcal{O}] = \ell$, i.e. $\tilde{f}/\tilde{f}' = \ell$. But the hypothesis that $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ tells us that if n is such that $\ell^n = \tilde{g}$ then $\ell^n = \tilde{f}$. Therefore, $\ell \mid (\tilde{g}/\tilde{f}')$, thus $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$ and $\tilde{f}' = \tilde{f}/\ell = \ell^{n-1}$. □

Lemma 2.5. *If $\alpha : E_1 \to E_2$ is an isogeny $\downarrow$ 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 $\downarrow$. Moreover, there are ℓ such isogenies.*

Proof: First of all, since α is $\downarrow$, one has $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, i.e. $\tilde{f}_2/\tilde{f}_1 = \ell$, thus $\ell \mid [\mathcal{O}_K : \mathcal{O}_2]$. From Table 1, we see that there is one isogeny $\uparrow$ and ℓ isogenies $\downarrow$ of E_2.

Let $\gamma : E_2 \to E_3$ be the isogeny $\uparrow$. Since γ is $\uparrow$, $[\mathcal{O}_3 : \mathcal{O}_2] = \ell$, i.e. $\tilde{f}_2/\tilde{f}_3 = \ell$. But we have seen that $\tilde{f}_2/\tilde{f}_1 = \ell$, thus $\tilde{f}_3 = \tilde{f}_1$. Therefore, $\mathcal{O}_3 \simeq \mathcal{O}_1$, which contradicts the hypothesis of the lemma.

Let $\beta : E_2 \to E_3$ be an isogeny $\downarrow$. Since β is $\downarrow$, $[\mathcal{O}_2 : \mathcal{O}_3] = \ell$, i.e. $\tilde{f}_3/\tilde{f}_2 = \ell$. But we have seen that $\tilde{f}_2/\tilde{f}_1 = \ell$, thus $\tilde{f}_3 = \ell^2\tilde{f}_1$ and $\mathcal{O}_3 \not\simeq \mathcal{O}_1$. Therefore every isogeny satisfying the hypothesis of the lemma is $\downarrow$ and there are ℓ of them. □

In other words, if $\beta \neq \hat{\alpha}$, then β is $\downarrow$. Since E_2 has $\ell + 1$ isogenies, $\hat{\alpha}$ is $\uparrow$ and the ℓ others are $\downarrow$.

Let us now describe a very particular case.

Lemma 2.6. *If there exist two different isogenies $\alpha : E \to E'$ and $\beta : E \to E'$, then they are both $\to$. We can also conclude that $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, $\mathcal{O} \simeq \mathcal{O}'$ and $\left(\frac{D}{\ell}\right) = +1$.*

Proof: First of all, we will show that if $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ then we cannot have two such isogenies. If $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, we have this conclusion immediately since there is only one isogeny of E (see Table 1). If $\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$, then if these two isogenies exist, they have to be $\downarrow$. Otherwise, since there is only one isogeny $\uparrow$ (see Table 1), one should be $\uparrow$ and the other $\downarrow$, i.e. $[\mathcal{O}' : \mathcal{O}] = \ell$ and $[\mathcal{O} : \mathcal{O}'] = \ell$: this is impossible. Now if we look at $\mathcal{O}'$, then we know that $[\mathcal{O} : \mathcal{O}'] = \ell$, thus $\ell \mid [\mathcal{O}_K : \mathcal{O}']$. Therefore, E' has exactly one isogeny $\uparrow$ and depending on whether $\ell \mid [\mathcal{O}' : \mathbb{Z}[\pi]]$ or not, ℓ isogenies $\downarrow$. But $\hat{\alpha}$ and $\hat{\beta}$ are $\uparrow$ from Lemma 2.1 and different, which contradicts the fact that there is only one isogeny $\uparrow$. □

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

Theorem 2.2. [24] *Suppose there are two ℓ-isogenies α and β from E to the same curve E'. Then the discriminant D of the endomorphism $\mathcal{O}$ of E is such that $|D| \leq 4\ell^2$.*

Proof: The isogeny $\hat{\alpha}\beta$ is an endomorphism of E and is cyclic of degree ℓ^2 not equal to ℓ times an automorphism. Therefore, there exists an algebraic integer of $\mathcal{O}$ of norm ℓ^2 or equivalently $4\ell^2 = x^2 + |D|y^2$ is solvable in integers x and y. The conclusion follows. □

This set of lemmas gives us an idea of the graph of 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 isogenies that we can find when $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ using Table 1 and the rest of the volcanic structure comes from the fact that by Lemmas 2.4 and 2.5, we see that if $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ then E does not have any horizontal isogeny. In the case where $\left(\frac{D}{\ell}\right) = -1$, there is no such isogeny, we will say that the case is degenerated. The case where $\left(\frac{d_\pi}{\ell}\right) = \pm 1$ gives us another degenerated case, since we can only find horizontal isogenies by Lemmas 2.2 and 2.3. To summarize these ideas, we get the graph of Figure 1 in the general case.

3. Modular equations and isogenies

3.1. **The modular polynomial.** Elkies's algorithm tests the existence of rational ℓ-isogenies efficiently via modular equations. 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 only if $\Phi_\ell(j(E), j(E')) = 0$. (Note that

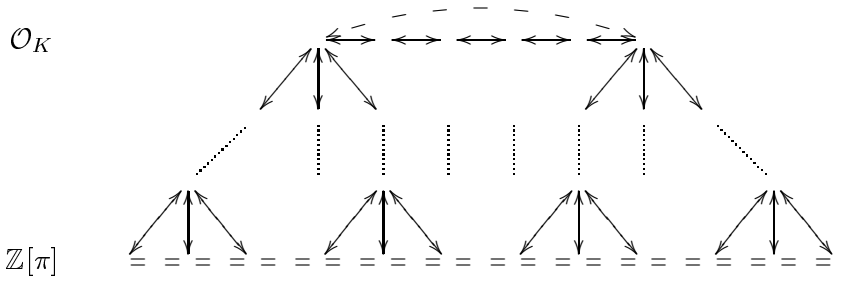


FIGURE 1. Volcano of the isogenies.

two curves may have the same invariant without being isogenous, e.g. in the case where they are twists.)

For instance

$$\Phi_2(X,Y) = X^3+Y^3-157464000000000+8748000000X-162000X^2+8748000000Y+40773375XY$$
$$+1488X^2Y-162000Y^2+1488XY^2-X^2Y^2,$$
$$\Phi_3(X,Y) = X^4+Y^4+1855425871872000000000X+452984832000000X^2+36864000X^3$$
$$+1855425871872000000000Y-770845966336000000XY+8900222976000X^2Y$$
$$-1069956X^3Y+452984832000000Y^2+8900222976000XY^2+2587918086X^2Y^2$$
$$+2232X^3Y^2+36864000Y^3-1069956XY^3+2232X^2Y^3-X^3Y^3.$$

More generally, the coefficients of Φ_ℓ tend to explode [2]. In the most optimized versions of Elkies's algorithm, special modular equations are used, that have smaller coefficients. We are not concerned by this aspect here and refer the reader to [19, 21] for more details. Note that in real life, it is easy to use these alternative equations to perform the computations described below.

3.2. **Finding isogenous curves.** 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 [24]. We suppose that E has equation $Y^2 = X^3 + AX + B$ (resp. $E^* : Y^2 = X^3 + A^*X + B^*$) and invariant j (resp. j^*) and we write $\Phi_X = \partial\Phi_\ell/\partial X$ (resp. $\Phi_Y = \partial\Phi_\ell/\partial Y$). We must suppose that neither j nor j^* belong to $\{0, 1728\}$.

Theorem 3.1. *Assume Φ_X and Φ_Y are non-zero. Define*

$$\kappa = -\frac{18}{\ell}\,\frac{B}{A}\quad\frac{\Phi_X(j,j^*)}{\Phi_Y(j,j^*)}\,j.$$

Then

$$A^* = \frac{3j^*}{1728-j^*}\left(\frac{\kappa}{12j^*}\right)^2\ell^4,\quad B^* = \frac{2j^*}{1728-j^*}\left(\frac{\kappa}{12j^*}\right)^3\ell^6.$$

We are still left with the case where j or j^* are in $\{0, 1728\}$ or $\Phi_X = \Phi_Y = 0$ for which the preceding theorem does not apply. The case where $\Phi_X(j, j^*) = \Phi_Y(j, j^*) = 0$ corresponds to the case of two isogenies between E and E^* and are covered by Theorem 2.2.

For our needs, this is not a problem, since at this point we know a lot of things on E and E^* and can deduce their cardinality in particular. We will call such a curve E a *special* curve (or having a special endomorphism ring) and have a procedure detecting this, which is costless, since testing whether $\Phi_X = \Phi_Y = 0$ costs one polynomial gcd.

As a side note, when j and j^* do not belong to $\{0, 1728\}$, but $\Phi_X = \Phi_Y = 0$, we can compute $G(Y) = \gcd(\Phi_X(j, Y), \Phi_Y(j, Y))$ and compute Φ_X/Φ_Y as

$$(\Phi_X(j, Y)/G(Y))/(\Phi_Y(j, Y)/G(Y))$$

evaluated at the point $Y = j^*$.

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.

3.3. **The number of isogenous curves and some consequences.** Let us come back to Elkies's algorithm and let E be an elliptic curve. It can be proved that the equation $\Phi_\ell(X, j(E)) = 0$ has 0, 1, 2 or $\ell+1$ roots in the base field (more is known on the factors of Φ_ℓ but we do not need that). In general, there is no repeated roots, unless we are in the particular cases treated in Lemma 2.6, Theorem 2.2 and in Case c of Section 4.6.3. The case of 0 root corresponds to $\left(\frac{d_\pi}{\ell}\right) = -1$, whereas two roots corresponds to $\left(\frac{d_\pi}{\ell}\right) = +1$. When $\Phi_\ell(X, j) = 0$ has either $\ell+1$ or 1 roots, then $\left(\frac{d_\pi}{\ell}\right) = 0$.

Suppose that $\left(\frac{d_\pi}{\ell}\right) = +1$. Let j_1 be a root of $\Phi_\ell(X, j(E))$. The corresponding curve E_1 is isogenous to E, so has the same Frobenius by Tate's theorem and therefore $\Phi_\ell(X, j_1) = 0$ has also two roots, one being the original $j(E)$ by duality. This leaves a single new invariant j_2, etc. In this way, we build a cycle of isogenies $(j, j_1, j_2, \dots, j)$ and a dual cycle starting with the other root j_1' of $\Phi_\ell(X, j(E))$ (see [6] for more details).

4. Our algorithm

4.1. **Inverting Kohel's theorem.** 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 the endomorphism ring $\mathcal{O}$ of E using Theorem 2.1. We summarize them in Table 2.

$\mathcal{N}_\ell(E)$	Type of the 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	$\to$	$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$ and $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$+1$	$+1$
1	case 1: $\to$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ 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': $\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \to \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$ 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 of the number and type of the isogenies of E.

Kohel [12] uses this approach as one of his methods to compute the endomorphism ring of the elliptic curve E. We use it to find more informations about the trace t of the Frobenius map.

4.2. **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 $\mathcal{O}_\mathcal{E}$ be the endomorphism ring of $\mathcal{E}$, $D_\mathcal{E}$ its discriminant and $f_\mathcal{E}$ its conductor.

First, we suppose that $\ell \neq 2$. The algorithm for $\ell = 2$ works in the same way, but needs some remarks that are made in Section 4.7.

If $\mathcal{N}_\ell(\mathcal{E})$ is equal to 1 or $\ell+1$, then we can deduce that $\left(\frac{d_\pi}{\ell}\right) = 0$ 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 $\ell^n \parallel g$, and since $t^2-4q = g^2 d_K$, we will get

$$t^2 \equiv 4q \pmod{\ell^{2n+\delta}} \tag{1}$$

and therefore $\nu_\ell \geq 2n+\delta$. The value of δ in (1) will be 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 Section 4.7).

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

4.3. **Skeleton of the algorithm.** The algorithm is divided into two parts. First, we determine whether the elliptic curve is in a static case or not. If $\mathcal{E}$ is non-static, then we look for a curve E_s in the crater of the volcano of the isogenies (Figure 1) 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 ComputeValuation
Input: An elliptic curve $\mathcal{E}$ and a prime ℓ, $\ell \neq p$.
Output: $\nu_\ell = 2n+\delta$ (or a lower bound for it when $\ell = 2$).

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

   ELIF $\#F = \ell+1$ THEN GOTO 4;
4. $(E_s, \epsilon, \delta, n, fdp) \leftarrow$FindFullDescendingPaths$(\mathcal{E}, \ell)$.
5. RETURN $\nu_\ell = 2n+\delta$.

4.4. **Special curves.**

4.4.1. *The case $j \in \{0, 1728\}$.* If our original curve E has one of these invariants, then it is easy to compute its cardinality, see for example [11]. If such a case is encountered during our quest, then we ordinarily know the level of E and at the same time its reduced conductor ℓ^r. We know that $j = 0$ (resp. $j = 1728$) corresponds to $\#E = q+1-t$ with $4q = t^2+3v^2$ (resp. $4q = t^2+4v^2$). There are 6 (resp. 4) solutions for (t, v), but only one with $\ell \mid v$ (except when $\ell = 2$).

4.4.2. *The case where some $\Phi_\ell(X, j)$ has a double root.* Let E be our initial curve, with order $\mathcal{O}$ and conductor f and let E_s be such that $\Phi_\ell(X, j(E_s))$ has a repeated root. This can only happen when we are computing the ascending path starting from E. By Lemma 2.6 we know that E_s is at the surface at ℓ. The endomorphism ring $\mathcal{O}_s$ of E_s has conductor f_s which is not divisible by ℓ. By computing a full descending path starting from E_s, we can actually compute n such that $g = \ell^n f_s$.

We also know, by Theorem 2.2 that there is an integer in $\mathcal{O}_s$ that has norm ℓ^2, i.e., the equation $4\ell^2 = x^2 + (|d_K| f_s^2) y^2$ has a nontrivial solution in rational integers (x, y). If ℓ is small, which is actually the case in practice, we can loop through the possible d_K's and f_s's prime to ℓ satisfying the norm equation, and find all the possible orders and endomorphism rings. We can eliminate candidates, since we know that at the same time, q must satisfy $4q = t^2 + (|d_K|(\ell^n f_s)^2) v^2$ for some rational integers t and v.

4.5. **The case $\mathcal{N}_\ell(E) \neq \ell+1$.** These cases are treated first because we can easily see either using Lemma 2.2 that the case we are in is static, or using Lemma 2.4 that we can easily go back to the general case.

4.5.1. $\mathcal{N}_\ell(E) = 0$. In this case, if we refer to Table 2, we see that there is no isogeny from E to another elliptic curve and that $\left(\frac{d_\pi}{\ell}\right) = -1$. We can also deduce that $\tilde{\mathcal{O}}_K \simeq \tilde{\mathcal{O}} \simeq \widetilde{\mathbb{Z}[\pi]}$.

4.5.2. $\mathcal{N}_\ell(E) = 2$. Referring to Table 2, we see that $\left(\frac{d_\pi}{\ell}\right) = +1$. This case has already been treated by Couveignes, Dewaghe and Morain ([6], [5]). Using Lemma 2.2, we know that for every elliptic curve E' such that $\alpha : E \to E'$ with α isogeny then $\mathcal{O}'$ has the same properties as $\mathcal{O}$. We can also deduce that $\tilde{\mathcal{O}}_K \simeq \tilde{\mathcal{O}} \simeq \widetilde{\mathbb{Z}[\pi]}$.

4.5.3. $\mathcal{N}_\ell(E) = 1$. In this case, we see that $\left(\frac{d_\pi}{\ell}\right) = 0$ therefore that $t^2 \equiv 4q \pmod{\ell}$. In Table 2, we see that this is a dual case. By dual, we mean that we may be in a static case 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 this case is non-static. Referring to Table 2, we know that $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$, $\ell \mid [\mathcal{O}_K : \mathcal{O}]$ and the isogeny $\alpha : E \to E'$ is $\uparrow$. Therefore applying Lemma 2.4, 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, E is in a static case.

In this case, we can also deduce that $\ell \parallel d_\pi$. Therefore, $t^2 \equiv 4q \pmod{\ell}$.

Case 2: $\mathcal{N}_\ell(E') = \ell+1$. Suppose that this case is static, i.e. $\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$ and $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. Referring to Table 2, we know that the isogeny $\alpha : E \to E'$ is $\to$ and $(D/\ell) = 0$. Therefore $\mathcal{O}'$ has the same properties as $\mathcal{O}$, 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, E is in a non-static case.

In this case, we can already make some conclusion about $\mathcal{O}$: $\tilde{\mathcal{O}}_K \not\simeq \tilde{\mathcal{O}}$ and $\tilde{\mathcal{O}} \simeq \widetilde{\mathbb{Z}[\pi]}$, i.e. if n is such that $\tilde{g} = \ell^n$ then $\tilde{f} = \ell^n$.

4.6. **The general case $\mathcal{N}_\ell(E) = \ell+1$.** By looking at the skeleton of the algorithm in Section 4.3, 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 at the surface, using *descending paths*. Therefore, we first precise this notion.

4.6.1. *Descending paths.*

Definition 4.1. *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 an isogeny $\downarrow$ and $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$.*

We will say that we have a full descending path *if E is at the surface.*

Lemma 4.1. *With the notations of Definition 4.1, 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 an isogeny $\downarrow$. 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 an isogeny $\downarrow$, 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 $\widetilde{\mathbb{Z}[\pi]}$.

Lemma 4.2. *Let $\mathcal{P}$ be a descending path starting from E and let $m = \#\mathcal{P} - 1$. Then E is of level $(n - m)$.*

Proof: From the definition, $\mathcal{P}$ is a path $E = E_0 \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$. Let E be at level r. Therefore from Lemma 4.1, E_m is of level $r + m$. We also know that $\ell \nmid [\mathcal{O}_m : \mathbb{Z}[\pi]]$, i.e. $\ell^n \parallel f_m$. Therefore $n = r + m$. Thus $r = n - m$. □

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) $P[i] \leftarrow \{E\} \cup \{F[i]\}$;
   (b) $G[i] \leftarrow E$;
   (c) $G'[i] \leftarrow F[i]$;
   (d) 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 floor)$\}$
   ELSE
   (a) IF $(j(S[i][1]) = j(G[i]))$ THEN {(we must not come back to the preceding curve) $G[i] \leftarrow G'[i]$; $G'[i] \leftarrow S[i][2]$;};
   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 $P[i_0]$.

Lemma 2.5 ensures us that whenever we have an isogeny $\alpha : E \to E'$ such that α is $\downarrow$, every isogeny $\beta : E' \to E''$ such that $E'' \not\simeq E$ is $\downarrow$. Therefore, inductively, if we start a path of isogenies with an isogeny $\downarrow$, we will get a descending path.

To find such an isogeny to start the path, we will compute in parallel three different paths starting from any three different curves isogenous to E. We need three of them because if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, there can be two isogenies $\to$ (see Table 1) and if we look at those two, the paths will not start with an isogeny $\downarrow$ and might become empty. The third one will ensure the fact of having a path starting with an isogeny $\downarrow$ and therefore a non-empty path. In the case that $\ell \mid [\mathcal{O}_K : \mathcal{O}]$, there is only one isogeny $\uparrow$ (see Table 1), therefore at least two of the paths we consider are descending and therefore these ensures us to have a non-empty path. Since a non-descending path is composed of a path of isogenies that are not $\downarrow$ 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 4.3. *The complexity of the algorithm* FindDescendingPath *is $O(m\mathcal{F}(\ell))$, where m is the level of E w.r.t. $\mathbb{Z}[\pi]$ 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. □

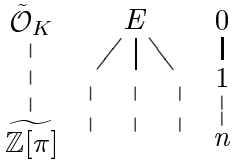
4.6.2. *Why do we need a curve at the surface?* If we have a curve E_s at the surface and a full descending path $E_s \to E_1 \to E_2 \to \cdots \to E_{m-1} \to E_m$, from Lemma 4.1, we find $n = m$ such that $\tilde{g} = \ell^n$. To find E_s, we need to know how to recognize it.

4.6.3. *Detecting the surface and thus determining δ.* From Table 2, we see that there are three different cases that will be detected in three different ways. In fact, these three different cases have the common relation about the isogenies of the curve:

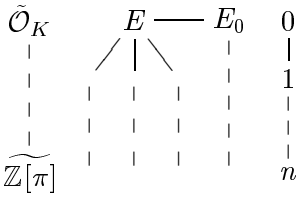
$$\begin{cases} 1 + \left(\frac{D}{\ell}\right) & \to \\ \ell - \left(\frac{D}{\ell}\right) & \downarrow \end{cases}. \tag{2}$$

Suppose E is at the surface. Then one of the following conditions will be met.

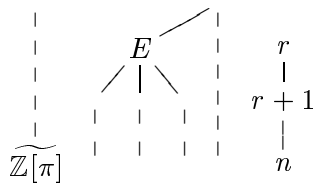
- Case a: There is no isogeny $\to$. Considering the fact that we are at the surface, we have $\ell + 1$ isogenies $\downarrow$ from (2). Then all the descending paths starting from the $\ell + 1$ isogenous curves to E have the same length. The following graph characterizes this situation.



  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 $\left(\frac{d_K}{\ell}\right) = -1$ and therefore $\delta = 0$. This is one of the degenerated structures we talked about when introducing the volcanic structure.
- Case b: There is exactly one isogeny $\to$. There are also ℓ isogenies $\downarrow$ from (2). 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.

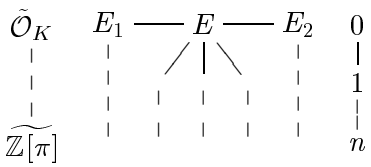


Horizontal case



"Normal" case

  We cannot confuse this case with the "normal" case of one isogeny $\uparrow$ and ℓ $\downarrow$, 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 $\left(\frac{d_K}{\ell}\right) = 0$ and therefore $\delta = 1$.
- Case c: There are two isogenies $\to$. There are also $\ell - 1$ isogeny $\downarrow$ from (2). 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 $\left(\frac{d_K}{\ell}\right) = +1$ and therefore $\delta = 0$.

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

Definition 4.2. *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 isogeny $\uparrow$ and $\ell \nmid [\mathcal{O}_K : \mathcal{O}_{-s}]$.*

We will say that we have a full ascending path *if E is of level n.*

Lemma 4.4. *Using the same notations as in Definition 4.2, if E is of level r then E_{-i} is of level $r - i$.*

Proof: The proof is similar to the proof of Lemma 4.1. □

Corollary 4.1. *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 the one of the curve that we consider. In this case, we will need to consider the $\ell + 1$ isogenies of E and to determine which one of those is $\uparrow$. To do so, we will compute a descending path for every curve isogenous to E and the longer path will be the one of the isogeny $\uparrow$. We reiterate this until we detect a curve at the surface.

Before giving the algorithm describing how to find a curve at the surface, we need an algorithm detecting if we are already at the surface and if not, giving a curve at an inferior level.

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

- $\epsilon = 0$, i_{max} such that $\#\mathfrak{P}[i_{max}]$ is maximal, $\delta = -1$ and λ the level of the curve at an inferior level w.r.t. $\mathbb{Z}[\pi]$
- OR $\epsilon = (d_K/\ell)$, $i_{max} = -1$, δ and $\lambda = n$ if we detect a curve at the surface;
- fdp is a list of (some) full descending paths.

1. $\delta \leftarrow -1$; $\epsilon \leftarrow 0$; $fdp \leftarrow \emptyset$;
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 surface is detected and $\left(\frac{d_K}{\ell}\right) = -1$ (case a) */
   IF $\#I = \ell$ THEN $\{\epsilon \leftarrow -1$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}]$; $i_{max} \leftarrow -1$; $\delta \leftarrow 0$; $fdp \leftarrow \{\{E_{cur}, \mathfrak{P}[1]\}\}$; $\}$
5. /* Case where the surface is detected and $\left(\frac{d_K}{\ell}\right) = +1$ (case c)*/
   IF $\#I = 1$ THEN $\{$ $i_{max2} \leftarrow I[1]$; $\epsilon \leftarrow 1$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $\delta \leftarrow 0$; $i_0 \leftarrow$ any index distinct from i_{max} and i_{max2}; $fdp \leftarrow \{\{E_{cur}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}], \mathfrak{P}[i_{max2}]\}$; $i_{max} \leftarrow -1$; $\}$
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 surface is detected and $\left(\frac{d_K}{\ell}\right) = 0$ (case b) */
   THEN $\{\epsilon \leftarrow 0$; $\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1$; $\delta \leftarrow 1$; $fdp \leftarrow \{\{E_{cur}, \mathfrak{P}[i_0]\}, \mathfrak{P}[i_{max}]\}$; $i_{max} \leftarrow -1$; $\}$
   ELSE $\{\lambda \leftarrow \#\mathfrak{P}[i_{max}] - 1;\}$
7. RETURN $(\epsilon, i_{max}, \delta, \lambda, fdp)$.

The following algorithm returns an isogenous curve to E at the surface by computing an ascending path starting from E using the preceding algorithm.

Procedure FindFullDescendingPaths
Input: A non-special elliptic curve E such that $\ell \mid [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
Output: $(E_s, \epsilon, \delta, n, fdp)$ such that E_s is at the surface, isogenous to E, δ, $\epsilon = (d_K/\ell)$, n and fdp 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) $(\epsilon, i_0, \delta, \lambda, fdp) \leftarrow$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 $(E_s, \epsilon, \delta, \lambda, fdp)$;

Lemma 4.5. *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.

Theorem 4.1. *It takes* $O(n^2\ell\mathcal{F}(\ell))$ *operations to compute the valuation of* ℓ *in* g, *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 $\mathcal{E}$. □

4.7. **Remarks on the case $\ell = 2$.** Some minor modifications are to be made. First, if $\left(\frac{d_K}{\ell}\right) = 0$, it means that $\ell \mid d_K$. When $\ell = 2$, by definition of the discriminant of a quadratic field, it we have $4 \mid d_K$. Therefore, whenever $\left(\frac{d_K}{2}\right) = 0$, δ equals 2. This remark applies also when $\tilde{\mathcal{O}}_K \simeq \widetilde{\mathbb{Z}[\pi]}$ and $\mathcal{N}_\ell(j) = 1$, i.e. we directly know that $t^2 \equiv 4q \pmod 4$.

It could be that $\nu_\ell = 2n + \delta + 1$, since, by definition of the discriminant of a quadratic field $d_K/4$ may be divisible by 2. But we do not know how to "catch" this factor of d_K and in this case, we may obtain a partial result.

5. Complementary remarks

5.1. Application to point counting.

5.1.1. *Finding t mod ℓ^ν.* In general (that is except in the cases where we happened to find a special curve somewhere), 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 $t_1 \equiv t \bmod \ell$: Only one of the roots of the equation modulo ℓ^ν will reduce to t_1 modulo ℓ. Finding t_1 is done via the determination of an eigenspace of π and the associated

eigenfactor of the ℓ-th division polynomial f_ℓ *à la* Elkies. This will determine the eigenvalue, which turns out to be $t_1/2 \bmod \ell$ in that case.

The case $\ell = 2$ is almost hopeless. On the one hand, the equation $t^2 \equiv 4q \bmod 2^\nu$ gives us $t \bmod 2^{\nu-1}$. On the other hand, there are four possible values of t (at least when $\nu > 2$) that we cannot distinguish without computing the corresponding factor of some $f_{2^{\nu-1}}$.

5.1.2. *Finding* $t \bmod \ell^{\nu+1}$. 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 [6] apply there too. In that case, we have found three curves E_s, E_1 and E_1^* and horizontal isogenies between them. Starting for example from $I_1 : E_s \to E_1$, we can find the unique horizontal isogeny $I_2 : E_1 \to E_2$ which is not the dual of I_1 (and therefore E_2 not isomorphic to E_s) by using procedure FindFullDescendingPaths. In this way, we build a sequence of isogenous curves, from which we can deduce factors of $f_{\ell^d}(E_s)$ or of some $f_{\ell^d}(E)$, depending on whether we compute the isogenies forward as originally proposed in [6] or backwards, which is more efficient (see [5]). See example 3 below.

5.2. **Relations with isogeny trees.** In [5], the authors tried to describe the situation where the Frobenius has repeated roots via a tree. This tree corresponds to successive calls to the routine that builds isogenous curves. This tree is in fact a special view of the volcano. Once the surface of the volcano is found in the tree, we can balance it so as to recover a volcano. See example 5 that illustrates the idea.

5.3. **Solving a problem of Lercier.** In his thesis [15, p. 137], Lercier needs to find an elliptic curve E' isogenous to a given curve E having three 2-torsion points, with the property that E' has only one 2-torsion point. Such a curve may exist, since two isogenous curves may not have the same group structure (see [13]). Using our approach, this phenomenon can be explained and an algorithm for finding E' given.

First note that 2-torsion points on E correspond exactly to isogenies of degree 2. For instance, when $p > 2$, the curve $E : Y^2 = (X - x_0)(X^2 + aX + b)$ of invariant

$$j = 256\frac{(w + a^2 - 4b)^3}{w^2(a^2 - 4b)}$$

(with $w = x_0^2 + ax_0 + b$) has $(x_0, 0)$ as a 2-torsion point and a simple calculation shows that

$$j^* = 16\frac{(16w + a^2 - 4b)^3}{w(a^2 - 4b)^2}$$

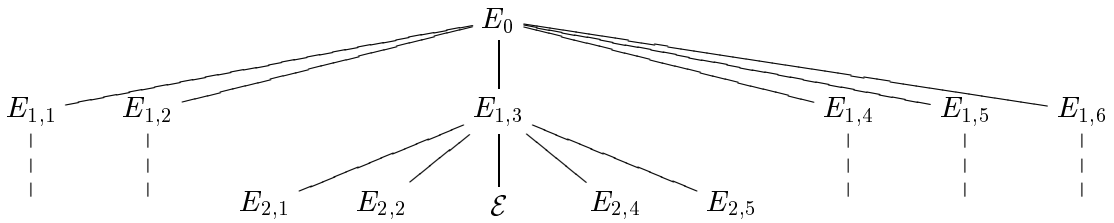
is the invariant of a 2-isogenous curve.

As a consequence, the number of 2-torsion points equals the number of 2-isogenies, that is $\mathcal{N}_2(E)$. From our algorithm, we know that curves on the floor at 2 satisfy $\mathcal{N}_2 = 1$. To find one of these, it is enough to find a descending path starting from E, and indeed, this is a byproduct of the computation of ν_2. The complexity of the computations is bounded by the height of the isogeny tree, which is polynomial in $\log |d_K|$. Moreover, on average, the ν_2 is small, hence the search is quite fast.

6. Numerical examples

Notation: $E = [a, b]$ stands for the equation $y^2 = x^3 + ax + b$ of the curve E.

Example 1 (Normal case $\left(\frac{d_K}{\ell}\right) = -1$): Let $p = 5081$ and $\mathcal{E} = [3290, 3887]$. The j-invariant of $\mathcal{E}$ is $j_\mathcal{E} = 1765$. For $\ell = 5$, we find:

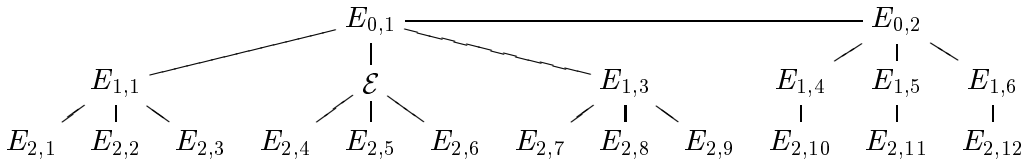


where

curve	equation	curve	equation	curve	equation	curve	equation
E_0	$[1355, 2505]$	$E_{1,3}$	$[3688, 3542]$	$E_{1,6}$	$[3211, 3432]$	$E_{2,4}$	$[1282, 1856]$
$E_{1,1}$	$[3623, 3418]$	$E_{1,4}$	$[2104, 4311]$	$E_{2,1}$	$[4192, 3469]$	$E_{2,5}$	$[2979, 436]$
$E_{1,2}$	$[2761, 2991]$	$E_{1,5}$	$[279, 3638]$	$E_{2,2}$	$[3332, 4679]$		

Therefore, $n = 2$, $\left(\frac{d_K}{\ell}\right) = -1$ thus $\delta = 0$ and $t^2 \equiv 4p \pmod{5^4}$. We use the isogeny $E_0 \to E_{1,1}$ to find the factor $X^2 + 1448X + 1478$ of $f_5(E_0)$ which is associated to the eigenvalue 1 of the Frobenius modulo 5. We deduce that $t \equiv 607 \equiv -18 \bmod 5^4$. As a matter of fact, $t = -18$.

Example 2 (Normal case $\left(\frac{d_K}{\ell}\right) = 0$): Let $p = 5059$ and $\mathcal{E} = [4646, 1411]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 1790$. For $\ell = 3$, one has:

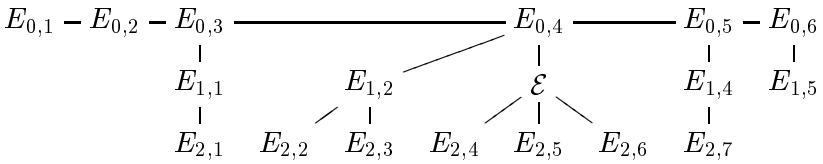


where

curve	equation	curve	equation	curve	equation	curve	equation
$E_{0,1}$	$[4307, 2079]$	$E_{1,5}$	$[1701, 548]$	$E_{2,4}$	$[4770, 1483]$	$E_{2,9}$	$[1724, 4275]$
$E_{0,2}$	$[2746, 1513]$	$E_{1,6}$	$[1105, 3273]$	$E_{2,5}$	$[3968, 2595]$	$E_{2,10}$	$[3571, 1957]$
$E_{1,1}$	$[2072, 3214]$	$E_{2,1}$	$[4021, 3717]$	$E_{2,6}$	$[2853, 4777]$	$E_{2,11}$	$[2543, 1941]$
$E_{1,3}$	$[880, 2818]$	$E_{2,2}$	$[3348, 2041]$	$E_{2,7}$	$[1273, 1362]$	$E_{2,12}$	$[2544, 3362]$
$E_{1,4}$	$[407, 2942]$	$E_{2,3}$	$[4995, 1623]$	$E_{2,8}$	$[301, 235]$		

Therefore, $n = 2$, $\left(\frac{d_K}{\ell}\right) = 0$ thus $\delta = 1$ and $t^2 \equiv 4p \pmod{3^5}$. As a matter of fact, $t = -124$.

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

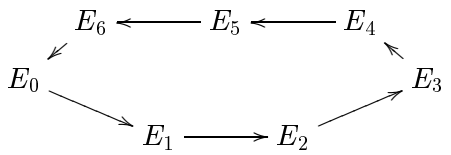


where

curve	equation	curve	equation	curve	equation	curve	equation
$E_{0,1}$	$[1336, 8702]$	$E_{0,6}$	$[352, 4401]$	$E_{2,1}$	$[5412, 9972]$	$E_{2,6}$	$[6203, 3741]$
$E_{0,2}$	$[56, 8167]$	$E_{1,1}$	$[9166, 9156]$	$E_{2,2}$	$[9899, 274]$	$E_{2,7}$	$[2728, 8215]$
$E_{0,3}$	$[7418, 8055]$	$E_{1,2}$	$[5138, 6736]$	$E_{2,3}$	$[6796, 2230]$		
$E_{0,4}$	$[7778, 9421]$	$E_{1,4}$	$[6435, 570]$	$E_{2,4}$	$[8899, 8303]$		
$E_{0,5}$	$[5051, 4157]$	$E_{1,5}$	$[3659, 6441]$	$E_{2,5}$	$[4732, 4541]$		

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:

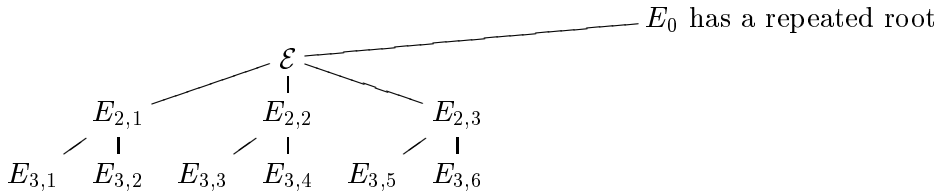


where

curve	equation	curve	equation	curve	equation	curve	equation
E_0	$[7778, 9421]$	E_2	$[56, 8167]$	E_4	$[616, 274]$	E_6	$[5051, 4157]$
E_1	$[7418, 8055]$	E_3	$[1336, 8702]$	E_5	$[352, 4401]$		

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

Example 4 (Case of repeated roots $\left(\frac{d_K}{\ell}\right) = +1$): Let $p = 10039$ and $\mathcal{E} = [7372, 8261]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 102$. Consider the case $\ell = 3$ for which



where

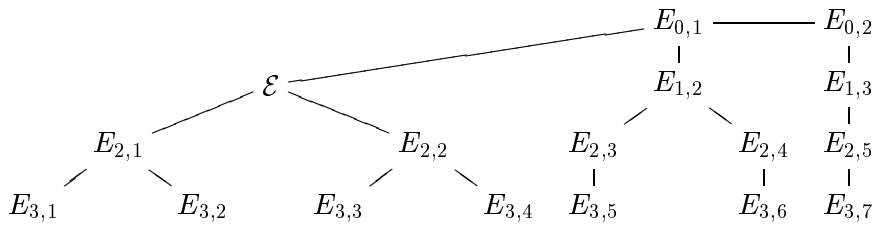
curve	equation	curve	equation	curve	equation	curve	equation
E_0	$[3273, 8056]$	$E_{2,3}$	$[7337, 5253]$	$E_{3,3}$	$[7330, 392]$	$E_{3,6}$	$[3853, 5654]$
$E_{2,1}$	$[8850, 7741]$	$E_{3,1}$	$[9062, 3199]$	$E_{3,4}$	$[3523, 8744]$		
$E_{2,2}$	$[7787, 2602]$	$E_{3,2}$	$[4544, 8271]$	$E_{3,5}$	$[4370, 7215]$		

Therefore, $n = 3$, $\left(\frac{d_K}{\ell}\right) = 1$ thus $\delta = 0$ and $t^2 \equiv 4p \pmod{3^6}$. In that case, we also know that $\mathcal{E}$ has CM by an order of conductor $3^3 f_s$ for some quadratic field $K = \mathbb{Q}(\sqrt{d_K})$ such that the two equations

$$4 \times 3^2 = x^2 + (|d_K| f_s^2) y^2, \quad 4p = t^2 + (|d_K| (3^3 f_s)^2) v^2$$

have a solution in rational integers x, y, t, v. The only possible solution is $d_K = -35$, $f_s = 1$, yielding $|t| = 121$ and as a matter of fact, $t = 121$.

Example 5 (Incomplete case for $\ell = 2$ from [5]): Let $p = 1009$ and $\mathcal{E} = [1, 3]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 269$. For $\ell = 2$, one gets



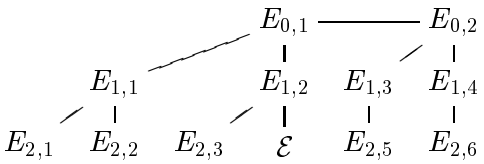
where

curve	equation	curve	equation	curve	equation	curve	equation
$E_{0,1}$	$[241, 990]$	$E_{2,1}$	$[502, 692]$	$E_{2,5}$	$[763, 476]$	$E_{3,4}$	$[65, 785]$
$E_{0,2}$	$[481, 611]$	$E_{2,2}$	$[284, 534]$	$E_{3,1}$	$[978, 971]$	$E_{3,5}$	$[917, 988]$
$E_{1,2}$	$[814, 970]$	$E_{2,3}$	$[309, 338]$	$E_{3,2}$	$[979, 113]$	$E_{3,6}$	$[46, 408]$
$E_{1,3}$	$[427, 373]$	$E_{2,4}$	$[397, 322]$	$E_{3,3}$	$[995, 970]$	$E_{3,7}$	$[1000, 782]$

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 6 (Complete case for $\ell = 2$): Let $p = 10009$ and $\mathcal{E} = [7171, 8117]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 14$. With $\ell = 2$:



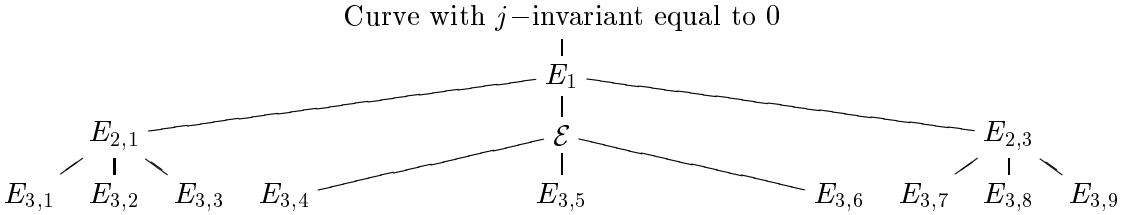
where

curve	equation	curve	equation	curve	equation	curve	equation
$E_{0,1}$	$[2275, 6698]$	$E_{1,2}$	$[201, 7055]$	$E_{2,1}$	$[3135, 4043]$	$E_{2,5}$	$[6160, 1295]$
$E_{0,2}$	$[932, 23]$	$E_{1,3}$	$[654, 573]$	$E_{2,2}$	$[2343, 2889]$	$E_{2,6}$	$[7890, 2646]$
$E_{1,1}$	$[6775, 534]$	$E_{1,4}$	$[9749, 2660]$	$E_{2,3}$	$[4637, 9029]$		

Therefore, $n = 2$, $\left(\frac{d_K}{\ell}\right) = 0$ thus $\delta = 2$ and $t^2 \equiv 4p \pmod{2^6}$.

As a matter of fact, $t = 70$, therefore $d_K = -2^2 \times 61$, $g = 2^2 \times 3$ and $(-70)^2 \equiv 4 \times 10009 \pmod{2^6}$. In this case, we get the valuation.

Example 7 (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 $\ell = 3$:

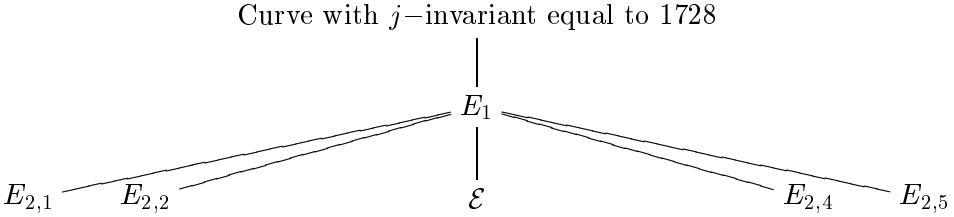


where

curve	equation	curve	equation	curve	equation	curve	equation
E_1	$[45, 30]$	$E_{3,1}$	$[677, 347]$	$E_{3,4}$	$[917, 182]$	$E_{3,7}$	$[901, 228]$
$E_{2,1}$	$[178, 159]$	$E_{3,2}$	$[608, 155]$	$E_{3,5}$	$[595, 887]$	$E_{3,8}$	$[155, 198]$
$E_{2,3}$	$[212, 23]$	$E_{3,3}$	$[941, 179]$	$E_{3,6}$	$[110, 848]$	$E_{3,9}$	$[999, 594]$

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, $t = 43$.

Example 8 (Case where the curve E_s has j-invariant equal to 1728): Let $p = 7349$ and $\mathcal{E} = [6871, 2131]$. The j-invariant of $\mathcal{E}$ is $j_{\mathcal{E}} = 331$. For $\ell = 5$:



where

curve	equation	curve	equation	curve	equation	curve	equation
E_1	$[4255, 5418]$	$E_{2,2}$	$[3272, 6926]$	$E_{2,4}$	$[7104, 2664]$	$E_{2,5}$	$[329, 4771]$
$E_{2,1}$	$[1316, 2594]$						

Therefore, $n = 2$, $\left(\frac{d_K}{\ell}\right) = +1$ thus $\delta = 0$ and $t^2 \equiv 4p \pmod{5^4}$. As a matter of fact, $t = 164$.

7. Conclusion

We have solved the problem of computing the cardinality of an elliptic curve modulo small prime powers ℓ^n in the case where ℓ divides the discriminant of the endomorphism ring of the curve, thereby giving a satisfying conclusion to [5]. We also had the opportunity of answering a question of Lercier raised in his thesis. Our work shows also the relevance of the computation of the endomorphism ring of a curve, in the sequel of the work of Kohel.

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] P. Cohen. On the coefficients of the transformation polynomials for the elliptic modular function. *Math. Proc. Cambridge Philos. Soc.*, 95:389–402, 1984.
[3] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. Thèse, Université de Bordeaux I, July 1994.
[4] J.-M. Couveignes. Computing l-isogenies using the p-torsion. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.
[5] 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/`.
[6] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In *ANTS-I*, 1994.
[7] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, 14:197–272, 1941.
[8] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.*, 67(223):1247–1252, July 1998.
[9] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.
[10] M. Fouquet, P. Gaudry, and R. Harley. On satoh's algorithm and its implementation. In preparation, 2000.
[11] S. A. Katre. Jacobsthal sums in terms of quadratic partitions of a prime. In K. Alladi, editor, *Number Theory*, volume 1122 of *Lecture Notes in Math.*, pages 153–162. Springer-Verlag, 1985. Proceedings of the 4th Matscience Conference held at Ootacamund, India, January 5-10, 1984.
[12] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Phd thesis, University of California, Berkeley, 1996.
[13] H. W. Lenstra, Jr. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56:227–241, 1996.
[14] R. Lercier. Computing isogenies in F_{2^n}. In H. Cohen, editor, *Algorithmic Number Theory*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 197–212. Springer Verlag, 1996. Second International Symposium, ANTS-II, Talence, France, May 1996, Proceedings.
[15] R. Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. Thèse, École polytechnique, June 1997.
[16] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 77–96. American Mathematical Society, International Press, 1998.
[17] R. Lercier and F. Morain. Computing isogenies between elliptic curves over F_{p^n} using Couveignes's algorithm. *Math. Comp.*, 69(229):351–370, January 2000.
[18] A. Menezes and S. Vanstone. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math.*, 38:135–153, 1990.
[19] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux*, 7:255–282, 1995.
[20] F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique ≥ 3. *Utilitas Math.*, 52:241–253, December 1997.

[21] V. Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Technischen Fakultät der Universität des Saarlandes, 1995.
[22] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. Preprint, 1999.
[23] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.
[24] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 1995.

E-mail address, M. Fouquet: `fouquet@lix.polytechnique.fr`

E-mail address, F. Morain: `morain@lix.polytechnique.fr`

Laboratoire d'Informatique, École Polytechnique, F-91128 Palaiseau Cedex, France