Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Explicit isogenies in quadratic time in any characteristic

Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost

Abstract

TODO: Given two elliptic curves and the knowledge of the existence of an isogeny between them, of known degree r, we compute this isogeny by using the structure of the ℓ-torsion of the curves, where ℓ is a prime different from the characteristic p of the base field. say that we are working over a finite field Our algorithm has a complexity of $\tilde{O}(r^2)$ operations in the base field. dependency in $\log(q)$ missing This is to be compared with Couveignes' algorithm, which uses the p-torsion, and has a complexity of $\tilde{O}(r^2 p^{O(1)})$. Our algorithm is therefore an interesting alternative for the medium- and large-characteristic cases.

1. *Introduction*

Isogenies are non-zero morphisms of elliptic curves, that is, non-constant rational maps preserving the point at infinity. They are also algebraic group morphisms. Isogeny computations play a central role in the algorithmic theory of elliptic curves. They are notably used to speed up Schoof's point counting algorithm [**Sch85**, **Atk88**, **Elk92**, **Sch95**, **Elk98**]. They are also widely applied in cryptography, where they are used to speed up point multiplication [**GLV01**, **BS11**], to perform cryptanalysis [**MMT01**], and to construct new cryptosystems [**Tes06**, **CLG09**, **Sto10**, **DFJP11**, **JS14**].

The *degree* of an isogeny is its degree as a rational map. If an isogeny has degree r, we call it an r-isogeny, and we say that two elliptic curves are r-isogenous if there exists an r-isogeny relating them. Accordingly, we say that two field elements j and j' are r-isogenous if there exist r-isogenous elliptic curves E and E' such that $j(E) = j$ and $j(E') = j'$. The *explicit isogeny* problem has many incarnations. In this paper, we are interested in the variant defined below.

Explicit isogeny problem. Given two j-invariants j and j', and a positive integer r, determine if they are r-isogenous. In that case, compute curves E, E' with $j(E) = j$ and $j(E') = j'$, and the kernel of an r-isogeny $\psi : E \to E'$.

Once the kernel of the isogeny is computed, the rational maps associated to it can be computed in optimal time using Velu's formulas [**Vél71**].

This paper focuses on the explicit isogeny problem for *ordinary* elliptic curves over finite fields. A famous theorem by Tate states that two curves are isogenous over a finite field if and only if they have the same cardinality over that field. The explicit isogeny problem stated here appears naturally in the Schoof-Elkies-Atkin point counting algorithm (SEA). There, E is the curve of which we want to compute the cardinality, and E' is an r-isogenous curve, with r a prime of size approximately $\log(\#E)$. For this reason, the explicit isogeny problem is customarily solved without prior knowledge of the cardinality of E. We will abide by this convention here.

A good measure of the computational difficulty of the problem is given by the isogeny degree r. Indeed the output TODO: rational functions? kernel? is represented by $O(r)$ base

---

2000 *Mathematics Subject Classification* 11Y40 (primary), 11G20, 14H52 (secondary).

This work was partially supported by the DIGITEO grant 2013-0531D (ARGC).

field elements, hence an asymptotically optimal algorithm would solve the problem using $O(r)$ field operations. Many algorithms have been suggested over the years to solve the explicit isogeny problem. Early algorithms were due to Atkin [**Atk91**] and Charlap, Coley and Robbins [**CCR91**]. Elkies' [**Elk92**, **Elk98**, **BMSS08**] was the first algorithm targeted to finite fields (of large enough characteristic). Assuming r is prime, its complexity is dominated by the computation of the modular polynomial Φ_r, which is an object of (binary) size $O(r^3 \log(r))$. Later Bröker, Lauter and Sutherland [**BLS10**] optimized the modular polynomial computation in the context of the SEA algorithm. Finally Lercier and Sirvent [**LS08**, **LV16**] generalized Elkies' algorithm to work in any characteristic. Despite these advances, the overall cost of Elkies' algorithm and its variants is still at least cubic in r.

Another line of work to solve the explicit isogeny problem was initiated by Couveignes [**Cou94**, **Cou96**, **Cou00**], and later improved by De Feo and Schost [**DF11**, **DFS12**]. These algorithms use an interpolation approach combined with ad-hoc constructions for towers of finite fields of characteristic p. Their complexity is quasi-quadratic in r, but exponential in $\log(p)$, hence they are only practical for very small characteristic.

In this paper we present a variant of Couveignes' algorithm with complexity polynomial in $\log(p)$ and quasi-quadratic in r. Together with the Lercier-Sirvent algorithm, they are the only polynomial-time isogeny computation algorithms working in any characteristic, hence they are especially relevant for counting points in *medium* characteristic (i.e., counting points over $\mathbb{F}_{p^n}$, when $n \gg p/\log(p)$).

Note that, although Couveignes-type algorithms do not make use of the modular polynomial Φ_r, its computation is still necessary in the context of the SEA algorithm. Thus our new algorithm does not improve the TODO: overall complexity state of the art on point counting. It gives, however, an effective algorithm for solving the explicit isogeny problem, with potential applications in other contexts, e.g., cryptography.

1.1. *Notation*

Throughout this paper: r is a positive integer, p an odd prime, q a power of p, and $\mathbb{F}_q$ is the finite field with q elements. E is an ordinary elliptic curve over $\mathbb{F}_q$, its group of n-torsion points is denoted by $E[n]$, its q-Frobenius endomorphism by π. The endomorphism ring of E is denoted by $\mathcal{O}$, with $K = \mathcal{O} \otimes \mathbb{Q}$ the corresponding number field, $\mathcal{O}_K$ is its maximal order, and d_K the discriminant of $\mathcal{O}_K$. For a prime ℓ different from p and not dividing r, we denote by $E[\ell^k]$ the group of ℓ^k-torsion points of E, $E[\ell^\infty] = \varinjlim E[\ell^k]$ the reunion of all $E[\ell^k]$, and $T_\ell(E) = \varprojlim E[\ell^k]$ the ℓ-adic Tate module [**Sil92**, III.7], which is free of rank two over $\mathbb{Z}_\ell$. The factorization of the characteristic polynomial of π in $\mathbb{Z}_\ell$ is determined by the Kronecker symbol (d_K/ℓ). If $(d_K/\ell) = +1$ then we also define λ, μ as the eigenvalues of π in $\mathbb{Z}_\ell$ and write $h = v_\ell(\lambda - \mu)$, where v_ℓ is the ℓ-adic valuation.

We measure all computational complexities in terms of operations in $\mathbb{F}_q$; the binary costs associated to the algorithms presented next are negligible compared to the algebraic costs, and will be ignored. We use the Landau notation $O(\ )$ to express asymptotic complexities, and the notation $\tilde{O}(\ )$ to neglect (poly)logarithmic factors. We let $\mathsf{M}(n)$ be a function such that polynomials in $\mathbb{F}_q[x]$ of degree less than n can be multiplied using $\mathsf{M}(n)$ operations in $\mathbb{F}_q$, under the assumptions of [**vzGG99**, Chapter 8.3]. Using FFT multiplication, one can take $\mathsf{M}(n) \in O(n \log(n) \operatorname{loglog}(n))$.

1.2. *Couveignes' algorithm*

Couveignes' isogeny algorithm takes as input two *ordinary* elliptic curves E and E' defined over $\mathbb{F}_q$, and given in Weierstrass form TODO: check TODO: Couveignes ne précise pas dans son article, dans l'implantation on se sert des formes de Weierstrass and a positive integer

r not divisible by p, and returns, if it exists, the kernel of an r-isogeny $\psi : E \to E'$.TODO: Aren't we taking only the j-invariants as input? TODO: Couveignes dans son article prend des courbes, donc autant faire pareil It is based on the observation that the isogeny ψ must put $E[p^k]$ in bijection with $E'[p^k]$, in a way that is compatible with their structure of cyclic groups. It proceeds in three steps:

(1) Compute generators P, P' of $E[p^k]$ and $E'[p^k]$ respectively, for k large enough;
(2) Compute the interpolation polynomial L sending $x(P)$ to $x(P')$, and the abscissas of their scalar multiples accordingly;
(3) Deduce a rational fraction $g(x)/h(x)$ that coincides with L at all points of $E[p^k]$, and verify that it defines the first component of an isogeny of degree r. If it does, return it TODO: shouldn't we return h, to be consistent?, otherwise replace P' with a scalar multiple of itself and go back to Step (2).

For this algorithm to succeed, enough interpolation points are required. Given that the isogeny ψ is defined by a rational fraction of degree $(r, r-1)$ TODO: not clear, there should be 2 components; explain better, or give Velu's formulas somewhere, it is necessary that $p^k \in \Omega(r)$. However, most of the time, those points are not going to be defined in the base field $\mathbb{F}_q$, thus Couveignes' algorithm must be based on efficient algorithms to construct and compute in towers of extensions of finite fields. Indeed, Couveignes and his successors go at great length in studying the arithmetic of *Artin-Schreier towers* [**Cou00**, **DFS12**], and the adaptation of the fast interpolation algorithm to that setting [**DF11**]. Using these highly specialized constructions, Steps (1) and (2) are both executed in quasi-linear TODO: ? in what? time $\tilde{O}(p^{k+O(1)}) = \tilde{O}(rp^{O(1)})$. However the last step only succeeds for one pair of torsion points P, P', in general, thus $O(r)$ trials are expected on average.

Hence, the overall complexity of Couveignes' algorithm is $\tilde{O}(r^2 p^{O(1)})$, i.e., quadratic in r^2, but exponential in $\log(p)$. Although the exponent of p is relatively small, Couveignes algorithm quickly becomes impractical as p grows.

1.3. *Our contributions*

In this paper we introduce a variant of Couveignes' algorithm with the same quadratic complexity in r, and **no exponential dependency in** $\log(p)$.

The bottom line of our algorithm is elementary: replace $E[p^k]$ in the algorithm with $E[\ell^k]$, for some small prime ℓ. However a naive application of this idea fails to yield a quadratic-time algorithm. Indeed, in the worst case one has $\ell^{2k} \in \Theta(r)$, with $E[\ell^k] \simeq (\mathbb{Z}/\ell^k\mathbb{Z})^2$. Hence, two generators P, Q of $E[\ell^k]$ must be mapped onto two generators of $E'[\ell^k]$. This can be done in $O(\ell^{4k})$ possible ways, with a best possible cost of $O(\ell^{2k})$ per trial, thus yielding an algorithm of complexity $O(\ell^{6k}) = O(r^3)$ at best.

To avoid this pitfall, we carefully study in Section 2 the structure of $E[\ell^k]$, and its relationship with the Frobenius endomorphism π. With that knowledge, we can put some restrictions on the generators P, Q, as explained in Section 3, thus limiting the number of trials to $O(\ell^{2k})$. In Section 4 we present an interpolation algorithm adapted to the setting of ℓ-adic towers, and in Section 5 we put all steps together and analyze the full algorithm. Finally in Section 6 we discuss our implementation and the performance of the algorithm.

1.4. *Towers of finite fields*

The algorithms presented next operate on elements defined in finite extensions of $\mathbb{F}_q$. Specifically, we will work in a *tower* of finite fields $\mathbb{F}_q = F_0 \subset F_1 \subset \cdots \subset F_n$, with ℓ dividing $\#F_1 - 1$, $d_1 = [F_1 : F_0]$ dividing $\ell - 1$, and $[F_{i+1} : F_i] = \ell$ for any $i > 0$. For $\ell = 2$, we build upon the work of Doliskani and Schost [**DS15**], whereas for general ℓ we use towers of Kummer extensions in a way similar to [**DDS13**, §2]. Both constructions represent elements of F_i as univariate polynomials with coefficients in $\mathbb{F}_q$, thus basic arithmetic operations can be performed with classic modular polynomial arithmetic. While constructing the tower, we also enforce special relations between the generators of each level, so that moving elements up and down the tower, and testing membership, can be done at negligible cost.

We briefly sketch the construction for odd ℓ. We first look for a primitive polynomial $P_1 \in \mathbb{F}_q[x]$ of degree equal to $[F_1 : F_0]$. There are many probabilistic algorithms to compute P_1 in time polynomial in ℓ and $\log(q)$; since their cost does not depend on the height n of the tower, we neglect it. Then, the image x_1 of x in $F_1 = \mathbb{F}_q[x]/P_1(x)$ is an element of multiplicative order $\#F_1 - 1$, and in particular it is not a ℓ-th power. Hence for any $i > 1$ we define F_i as $\mathbb{F}_q[x]/P_1\big(x^{\ell^{i-1}}\big)$, the computation of the polynomials $P_1\big(x^{\ell^{i-1}}\big)$ incurring no algebraic cost. Using this representation, elements of F_i can be expressed as elements of a higher level F_{i+j}, and reciprocally, by a simple rearrangement of the coefficients. Another fundamental operation can be done much more efficiently than in generic finite fields, as the following generalization of [**DS15**, §2.3] shows.

LEMMA 1.1. *Let $F_0 \subset \cdots \subset F_n$ be a Kummer tower as defined above, and let $a \in F_i$ for some $0 \leqslant i \leqslant n$. For any integer j, we can compute the $(\#F_j)$-th power of a using $O(\ell^i \mathsf{M}(\ell) + \mathsf{M}(\ell^i))$ operations in $\mathbb{F}_q$, after a precomputation independent of a that uses $O(\ell \mathsf{M}(\ell)\log(q))$ operations in $\mathbb{F}_q$.*

Proof. Without loss of generality, we can assume that $j < i$; otherwise, the output is simply a itself. Let $\tau = \#F_i$ and $\sigma = \#F_j$. By assumption, a is written as $a = a_0 + a_1 x + \cdots + a_{\tau-1}x^{\tau-1}$, for some x that satisfies $x^{\ell^{i-1}} = x_1$, where $x_1 \in F_1$ is a root of P_1.

The first step, independently of a, is to compute $y = x^\sigma$. Writing $\sigma = u\ell^{i-1} + r$, with $r < \ell^{i-1}$, we see that y is given by $x_1^{u \bmod \#F_1} x^r$. We compute $x_1^{u \bmod \#F_1}$ using $O(\ell \mathsf{M}(\ell)\log(q))$ operations in $\mathbb{F}_q$, and we keep this element as a monomial of $F_1[x]$.

Finally, once we know y, we compute $a(y)$ by a Horner scheme. All powers y^i we need are themselves monomials in $F_1[x]$, each computed from the previous one using $O(\mathsf{M}(\ell))$ operations in $\mathbb{F}_q$, for a total of $O(\ell^i \mathsf{M}(\ell))$. Finally the monomials $a_i y^i$ are combined together to form a polynomial in x of degree $O(\ell^i)$, and then brought to a canonical form in F_i via a modular reduction at a cost of $O(\mathsf{M}(\ell^i))$ operations. TODO: ?? Why do we need a reduction? We compute all y_i's reduced modulo $x^{\ell^{i-1}} - x_1$; they are still monomials after reduction. □

Note that the complexity of the previous algorithm can be significantly improved when $F_1 = F_0$, as shown in [**DS15**] for the case $\ell = 2$ TODO: ?. Summarizing, the following computations can be performed in a Kummer tower at the indicated asymptotic costs, all expressed in terms of operations in $\mathbb{F}_q$.

- basic arithmetic operations (addition, multiplication) in F_i, using $O(\mathsf{M}(\ell^i))$ operations;
- inversion in F_i using $O(\mathsf{M}(\ell^i)\log(\ell^i))$ operations (when $\ell = 2$, a factor of i can be saved here [**DS15**], but we will disregard this optimization for simplicity.)
- mapping elements from F_{i-1} to F_i and *vice versa* at no arithmetic cost;
- multiplication and Euclidean division of polynomials of degree at most d in $F_i[x]$ using $O(\mathsf{M}(d\ell^i))$ operations, via Kronecker's substitution, as already done in e.g. [**vzGS92**];
- computing a $(\#F_j)$-th power in F_i using $O(\ell^i \mathsf{M}(\ell) + \mathsf{M}(\ell^i))$ operations, after a precomputation that uses $O(\ell \mathsf{M}(\ell)\log(q))$ operations.

For one fundamental operation, we only have an efficient algorithm in the case $\ell = 2$, hence we introduce the following notation:

- $\mathsf{R}(i)$ is the cost of finding a root of a polynomial of degree ℓ in $F_i[x]$.

For $\ell = 2$, Doliskani and Schost show that $\mathsf{R}(i) = O(\mathsf{M}(\ell^i)\log(\ell^i q))$. For general ℓ, we have $\mathsf{R}(i) = O(\ell^i \mathsf{M}(\ell^{i+1})\log(\ell)\log(\ell q))$ using the variant of the Cantor-Zassenhaus algorithm described in [**vzGG99**, Chapter 14.5], or $\mathsf{R}(i) = O\big((\ell^{i(\omega+1)/2} + \mathsf{M}(\ell^{i+1}\log(q)))i\log(\ell)\big)$ using [**KS97**]. Here, ω is such that matrix multiplication in size m over any ring can be done in $O(m^\omega)$ base ring operations (so we can take $\omega = 2.38$ using the Coppersmith-Winograd algorithm). In any case, $\mathsf{R}(i)$ is between linear and quadratic in the degree ℓ^i.

2. *The Frobenius and the volcano*

In this section we explore some fundamental properties of ordinary elliptic curves over finite fields: the structure of their isogeny classes, its relationship with the rational ℓ^∞-torsion points, and with the Frobenius endomorphism π.

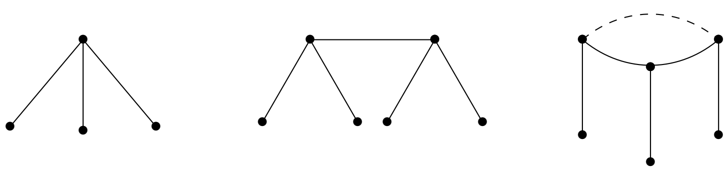
2.1. *Isogeny volcanoes*

For an extensive introduction to isogeny volcanoes we address the reader to [**Sut13**]. We recall here, without their proof, two results about ℓ-isogenies between ordinary elliptic curves.

PROPOSITION 2.1 [**Koh96**, Proposition 21]. *Let $\phi : E \to E'$ be an ℓ-isogeny between ordinary elliptic curves and $\mathcal{O}, \mathcal{O}'$ be their endomorphism rings. Then one of the three following cases is true:*
(i) $[\mathcal{O}' : \mathcal{O}] = \ell$, *in which case we call ϕ* ascending*;*
(ii) $[\mathcal{O} : \mathcal{O}'] = \ell$, *in which case we call ϕ* descending*;*
(iii) $\mathcal{O}' = \mathcal{O}$, *in which case we call ϕ* horizontal.

PROPOSITION 2.2 [**Koh96**, Proposition 23]; [**Sut13**, Lemma 6]. *Let E be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$.*
(i) *If $\mathcal{O}$ is ℓ-maximal then there are $(d_K/\ell) + 1$ horizontal ℓ-isogenies from E (and no ascending ℓ-isogenies).*
(ii) *If $\mathcal{O}$ is not ℓ-maximal then there are no horizontal ℓ-isogenies from E, and one ascending ℓ-isogeny.*

A *volcano of ℓ-isogenies* is a connected component of the graph of rational ℓ-isogenies between curves defined on $\mathbb{F}_q$. The *crater* is the subgraph corresponding to curves having an ℓ-maximal endomorphism ring. The shape of the crater is given by the Kronecker symbol (d_K/ℓ), as per Proposition 2.2. For any $k \geqslant 0$, a ℓ^k-isogeny is *horizontal* if it is the composite of k horizontal ℓ-isogenies. The *depth* of a curve is its distance from the crater. It is also the ℓ-adic valuation of the conductor of $\mathcal{O} = \mathrm{End}(E)$.



"Stromboli": $(d_K/\ell) = -1$ "Vesuvius": $(d_K/\ell) = 0$ "Etna": $(d_K/\ell) = +1$

FIGURE 1. *The three shapes of volcanoes of 2-isogenies*

2.2. *The ℓ-adic Frobenius*

In the rest of this paper we consider only a volcano with a cyclic crater (i.e. we assume $(d_K/\ell) = +1$), so that ℓ is an Elkies prime for these curves. This implies that the Frobenius automorphism on $T_\ell(E)$, which we write $\pi|T_\ell(E)$, has two distinct eigenvalues $\lambda \neq \mu$. The depth of the volcano of $\mathbb{F}_q$-rational ℓ-isogenies is $h = v_\ell(\lambda - \mu)$.

Proposition 2.3. *Let E be an ordinary elliptic curve with Frobenius endomorphism π. Assume that the characteristic polynomial of π has two distinct roots λ, μ in $\mathbb{Z}_\ell$, so that the ℓ-isogeny volcano has a cyclic crater. Then there exists a unique $a \in [\![0, \ell^h - 1]\!]$ such that $\pi|T_\ell(E)$ is conjugate, over $\mathbb{Z}_\ell$, to the matrix $\begin{pmatrix}\lambda & a\\ 0 & \mu\end{pmatrix}$. Moreover $a = 0$ if E lies on the crater, and else $h - v_\ell(a)$ is the depth of E in the volcano.*

Proof. Since the characteristic polynomial of π splits over $\mathbb{Z}_\ell$, the matrix of $\pi|T_\ell(E)$ is trigonalizable. Conjugating the matrix $\begin{pmatrix}\lambda & a\\ 0 & \mu\end{pmatrix}$ by $\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$ replaces a by $a + b(\lambda - \mu)$, so that a is well-defined modulo ℓ^h. Finally, by Tate's theorem [Sil92, Isogeny theorem 7.7 (a)], $\mathcal{O} \otimes \mathbb{Z}_\ell$ is isomorphic to the order in $\mathbb{Q}_\ell[\pi_\ell]$ of matrices with integer coefficients, which is generated by the identity and $\ell^{-\min(h, v_\ell(a))}(\pi_\ell - \lambda)$. □

We now study the action of ℓ-isogenies on the ℓ-adic Frobenius. The isogeny determined by a point R of order ℓ^k only depends on the subgroup $\langle R\rangle$ generated by R in $E[\ell^k]$. Equivalently, this subgroup defines a point in the projective space of $E[\ell^k]$, which is a projective line over $\mathbb{Z}/\ell^k\mathbb{Z}$. There exists a canonical bijection [Ser77, II.1.1] between this projective line and the set of lattices of index ℓ^k in the $\mathbb{Z}_\ell$-module $T_\ell(E)$: it maps a line $\langle R\rangle$ to the lattice $\Lambda_R = \langle R\rangle + \ell^k T_\ell(E)$. This lattice is also the preimage by the isogeny $\phi_R : E \to E_R$ of the lattice $\ell^k T_\ell(E_R)$. TODO: not so clear; ϕ_R and E_R should be defined more precisely

Fix a basis (P, Q) of $E[\ell^k]$ and let $R = xP + yQ$. The lattice Λ_R is generated by the columns of the matrix $L_R = \begin{pmatrix}\ell^k & 0 & x\\ 0 & \ell^k & y\end{pmatrix}$. The Hermite normal form of L_R is $M_R = \begin{pmatrix}\ell^{k-m} & x/y'\\ 0 & \ell^m\end{pmatrix}$, where we write $y = \ell^m y'$ with $\ell \nmid y'$, and its columns also generate the lattice Λ_R. We check that M_R has determinant ℓ^k. Since $\Lambda_R = \phi_R^{-1}(\ell^k T_\ell(E_R))$, there exist bases of $T_\ell(E), T_\ell(E')$ in which Φ_R TODO: Φ_R? has matrix $\ell^k M_R^{-1}$. Therefore, in that basis of $T_\ell(E_R)$, the matrix of $\pi|T_\ell(E_R)$ is $M_R^{-1} \cdot \pi \cdot M_R$. TODO: What is π in the middle of the rhs? Why do we need this discussion here?

Definition 2.4 (Horizontal and diagonal bases). Let E be a curve lying on the crater. We call a basis of $E[\ell^k]$ *diagonal* if π is diagonal in it; we call it *horizontal* if both basis points generate the kernel of horizontal ℓ^k-isogenies. Accordingly, we also call diagonal (resp. horizontal) the generators of a diagonal (resp. horizontal) basis.

The link between horizontal and diagonal bases is given below.

Proposition 2.5. *Let E be a curve lying on the crater and P be a point of $E[\ell^k]$. Then $\ell^h P$ is horizontal if, and only if, P is an eigenvector for π. If $\pi(P) = \lambda P$ then we say that $\ell^h P$ has the direction λ.*

Proof. Fix a basis (R, S) of $E[\ell^k]$ that diagonalizes π. We can write $P = xR + yS$; without loss of generality we may assume $y = 1$. Let E' be the image curve of $\phi_{\ell^h P}$. TODO: we should define this notation $\phi_{\dots}$ somewhere Then $\pi|T_\ell(E')$ has matrix $\begin{pmatrix}\lambda & \ell^{h-k}x(\lambda-\mu)\\ 0 & \mu\end{pmatrix}$. This matrix is diagonalizable only if $v_\ell(x) \geqslant k - h$. On the other hand, we can compute $(\pi - \mu)P = x(\lambda - \mu)R$, so that P is an eigenvector on the same condition $v_\ell(x) \geqslant k - h$. □

While horizontal bases are our main interest, diagonal bases are easier to compute in practice. Algorithms computing both kind of bases are given in Section 3. The main tool for this is the next proposition: given a horizontal point of order ℓ^k, it allows us to compute a horizontal point of order ℓ^{k+1}.

PROPOSITION 2.6. *Let $\psi : E \to E'$ be a horizontal ℓ-isogeny with direction λ. For any point $Q \in E[\ell^\infty]$, if $\ell \cdot Q$ is horizontal with direction μ, then $\psi(Q)$ is horizontal with direction μ.*

(Since Q has direction μ, its image $\psi(Q)$ has the same multiplicative order as Q).

Proof. Let $Q' = \psi(Q)$ and $\widehat{\psi}$ be the isogeny dual to ψ. Since both $\widehat{\psi}$ and $\widehat{\psi}(Q') = \ell Q$ are horizontal with direction μ, Q' is also horizontal. □

PROPOSITION 2.7. *Let $\psi : E \to E'$ be an isogeny of degree r prime to ℓ.*
(i) *The curves E and E' have the same depth in their ℓ-isogeny volcanoes.*
(ii) *For any point $P \in E[\ell^k]$, the isogenies with kernel $\langle P\rangle$ and $\langle \psi(P)\rangle$ have the same type (ascending, descending, or horizontal with the same direction).*
(iii) *If $P \in E[\ell]$ and $P' \in E'[\ell]$ are both ascending, or both horizontal with the same direction, then E/P and E'/P' are again r-isogenous.*

Proof. Points (i) and (ii) are consequences of Proposition 2.3 and of the fact that ψ, being rational and of degree prime to ℓ, induces an isomorphism between the Tate modules of E and E', commuting to the Frobenius endomorphisms. For point (iii), we just note that since there exists a unique point of order ℓ either ascending or horizontal with a given direction, we must have $P' = \psi(P)$. □

2.3. *Galois classes in the ℓ-torsion*

Here we assume that E has a ℓ-maximal endomorphism ring. If ℓ is odd, let $\alpha = v_\ell(\lambda^{\ell-1} - 1)$ and $\beta = v_\ell(\mu^{\ell-1} - 1)$; if $\ell = 2$, let $\alpha = v_2(\lambda^2 - 1) - 1$ and $\beta = v_2(\mu^2 - 1) - 1$, and assume without loss of generality that $\alpha \geqslant \beta$. Since $\lambda \not\equiv \mu \pmod{\ell^{h+1}}$, it is impossible that $\lambda \equiv \mu \equiv 1 \pmod{h}$, so that one at least of the two valuations α, β is $\leqslant h$, and therefore $\beta \leqslant h$.

PROPOSITION 2.8. *For any k, let d_k be the degree of the smallest field extension $F/\mathbb{F}_q$ such that all the points of $E[\ell^k] \subset E(F)$. Then:*
(i) *The order of q in $(\mathbb{Z}/\ell\mathbb{Z})^\times$ divides d_1, and d_1 divides $(\ell - 1)$.*
(ii) *If ℓ is odd then for all $k \geqslant 1$, $d_k = \mathrm{lcm}(d_1, \ell^{k-\beta})$.*
(iii) *If $\ell = 2$ then $d_2 \in \{1, 2\}$ and, for all $k \geqslant 2$, $d_k = \mathrm{lcm}(d_2, \ell^{k-\beta})$.*
(iv) *For any n, the group $E[\ell^\infty](F_n)$ is isomorphic to $(\mathbb{Z}/\ell^{n+\alpha}\mathbb{Z}) \times (\mathbb{Z}/\ell^{n+\beta}\mathbb{Z})$.*
(v) *The group $E[\ell^k]$ contains at most $k \cdot \ell^{k+\beta}$ Galois conjugacy classes over $F_1 = \mathbb{F}_{q^{d_1}}$.*

Proof. The degree d_k is exactly the order of the matrix $\pi|E[\ell^k]$. It is therefore the least common multiple of the multiplicative orders of λ, μ modulo ℓ^k. This proves (i) using the fact that $\lambda \cdot \mu = q$. Note that in general the order of q is a strict divisor of d_1, as is for example the case for $\pi^2 - \pi + 29 = 0$ and $\ell = 7$, where $q = 29 \equiv 1 \pmod 7$ and $d_1 = 6$.

For points (i)–(v) we may assume that $d_1 = 1$. Then, for any n, $v_\ell(\lambda^{2n} - 1) = \alpha + v_\ell(2n)$. Let (P, Q) be a diagonal basis of $E[\ell^k]$. The point $(\pi^n - 1)(xP + yQ) = (\lambda^n - 1)xP + (\mu^n - 1)yQ$ is zero iff $v_\ell(x) + \alpha + v_\ell(n) \geqslant k$ and $v_\ell(y) + \beta + v_\ell(n) \geqslant k$. This shows (iv). The largest Galois classes are those for which $v_\ell(y) = 0$ and their size is $\ell^{k-\beta}$, proving (ii) and (iii). Moreover, for any $i \leqslant k - \beta$ the points in an orbit of size $\leqslant \ell^i$ are those for which $v_\ell(x) \geqslant k - \alpha - i$ and $v_\ell(y) \geqslant k - \beta - i$; there are at most $\ell^{\min(\alpha+i,k)+\min(\beta+i,k)}$ such points, and therefore $\ell^{\min(\alpha+i,k)+\min(\beta,k-i)} \leqslant \ell^{k-i+\beta}$ corresponding classes. Summing this over all i proves (v). □

3. *Computing the action of the Frobenius endomorphism*

We continue here our study on the action of the Frobenius π on $E[\ell^k]$. Given an elliptic curve E with ℓ-maximal endomorphism ring, we explicitly compute diagonal and horizontal bases of $E[\ell^k]$ as defined in the previous section. We will use the latter basis of $E[\ell^k]$ in Section 5.2, to put restrictions on the interpolation problem of our algorithm.

By Proposition 2.8, there exists a Kummer tower $F_0 \subset \cdots \subset F_{k-\beta}$ such that all the points of $E[\ell^k]$ are rational over $F_{k-\beta}$. The algorithms presented next assume that the tower has already been computed.

3.1. *Computation of a diagonal basis*

In Algorithm 1 below, we describe how to compute eigenvalues of the Frobenius $\bmod \ell^k$ and corresponding eigenvectors in the ℓ^k-torsion subgroup. We write $Q \leftarrow \mathsf{divide}(\ell, P)$ for the computation of a preimage of P by multiplication by ℓ.

Algorithm 1 Computing a diagonal basis of $E[\ell^k]$

Input: E: an ordinary, ℓ-maximal elliptic curve; k: an integer.
Output: (P_k, Q_k): a basis of $E[\ell^k]$; $\lambda, \mu \in \mathbb{Z}/\ell^k\mathbb{Z}$ such that $\pi(P_k) = \lambda P_k$, $\pi(Q_k) = \mu Q_k$.

1: Compute (P_1, Q_1), a basis of $E[\ell]$
2: $h := 1, u := 1$
3: **for** $i = 1$ to $k-1$ **do**
4: $\quad P' \leftarrow \mathsf{divide}(\ell, P_i)$; $Q' \leftarrow \mathsf{divide}(\ell, Q_i)$.
5: $\quad$ compute $\pi|(P', Q') = \begin{pmatrix} \lambda + a\ell^i & b\ell^i \\ c\ell^i & \mu + d\ell^i \end{pmatrix} \pmod{\ell^{i+1}}$ with $a, b, c, d \in \mathbb{Z}/\ell\mathbb{Z}$
6: $\quad$ **if** $\lambda \neq \mu$ **then** $u \leftarrow (\lambda - \mu)/\ell^h$ **endif**
7: $\quad (\lambda, \mu) \leftarrow (\lambda + a\ell^i, \mu + d\ell^i)$
8: $\quad (b', c') \leftarrow (-b/u, c/u) \pmod{\ell}$
9: $\quad (P_{i+1}, Q_{i+1}) \leftarrow (P' + \ell^{i-1-h} b' Q',\ Q' + \ell^{i-1-h} c' P')$
10: $\quad$ **if** $\lambda = \mu$ **then** $h \leftarrow h + 1$ **endif**
11: **end for**
12: **return** (P_k, Q_k, λ, μ)

Proposition 3.1. *Algorithm 1 computes a diagonal basis of $E[\ell^k]$ using $O(\mathsf{R}(k-\beta) + \ell^2 \mathsf{M}(\ell^{k-\beta}) + \ell \mathsf{M}(\ell^2) \log(\ell) \log(\ell q))$ operations in $\mathbb{F}_q$.*

Proof. TODO: correctness
To bootstrap the algorithm, we need to compute a basis of $E[\ell]$ over the field F_1. We do this by factoring the ℓ-division polynomial at a cost of $O(\ell \mathsf{M}(\ell^2) \log(\ell) \log(\ell q))$ operations using the Cantor-Zassenhaus algorithm.

Once $E[\ell]$ has been computed, we can factor the multiplication-by-ℓ map as a product of two ℓ-isogenies. Then, for any P defined in $E(F_{i-\beta})$, the computation of $\mathsf{divide}(\ell, P)$ at Step 4 costs $O(\mathsf{R}(i - \beta + 1))$ operations.

Evaluating $\pi(P')$ in Step 5 has a cost of $O(\ell^{i-\beta+1}\mathsf{M}(\ell) + \mathsf{M}(\ell^{i-\beta+1}))$. Writing $\pi(P')$ as a linear combination $\alpha P' + \beta Q'$ needs at most ℓ^2 point additions, with a cost of $\ell^2 \mathsf{M}(\ell^{i-\beta+1})$. Finally, all other steps are negligible.

Since the cost of each loop grows geometrically, the last loop dominates all others, and gives the stated complexity. □

3.2. *Computation of a horizontal basis*

Using the previous algorithm we can compute a diagonal basis of $E[\ell^{h+1}]$. By Proposition 2.5, this gives us a horizontal basis of $E[\ell]$. Thanks to Proposition 2.6, we can use this information to improve horizontal points of $E[\ell^i]$ into horizontal points of $E[\ell^{i+1}]$, as illustrated in Algorithm 2.

Algorithm 2 Computing a horizontal point of order ℓ^k

Input: (P_0, Q_0): a diagonal basis of $E[\ell^{h+1}]$; k: an integer.
Output: R: a horizontal point of $E[\ell^k]$ with direction λ.

1: **for** $i = 1$ to $k-1$ **do**
2: $\quad \phi_i \leftarrow$ isogeny with kernel $\langle \ell^h P_{i-1} \rangle$
3: $\quad Q_i \leftarrow \phi_i(Q_{i-1})$
4: $\quad P' \leftarrow \mathsf{divide}(\ell, \phi_i(P_{i-1}))$.
5: $\quad$ Write $\pi(P') = \lambda P' + bQ_i$ for $b \in \mathbb{Z}/\ell\mathbb{Z}$ and let $P_i \leftarrow P' - (b/\mu)Q_i$.
6: **end for**
7: **return** $R = \widehat{\phi}_1 \circ \ldots \circ \widehat{\phi}_{k-1}(\mathsf{divide}(\ell^{k-(h+1)}, P_{k-1}))$.

Proposition 3.2. *Algorithm 2 is correct and computes its output using $O(\mathsf{R}(k-\beta) + k\mathsf{R}(h-\beta+1) + k\ell^2\mathsf{M}(\ell^{h-\beta+1}))$ operations in $\mathbb{F}_q$.*

Proof. We check that at step i of the loop, the points (P_i, Q_i) form a diagonal basis of $E_i[\ell^{h+1}]$, and ϕ_i has direction λ. The fact that R is horizontal is then a consequence of Proposition 2.6.

The two most expensive operations in the loop are Steps 4 and 5, costing respectively $O(\mathsf{R}(h-\beta+1))$ and $O(\ell^2\mathsf{M}(\ell^{h-\beta+1}))$, as discussed in the proof of Proposition 3.1. They are repeated k times. Finally, Step 7 is dominated by the last divide operation, which costs $O(\mathsf{R}(k-\beta))$. $\square$

One application of Algorithm 1 (with input $k \leftarrow h+1$) and two applications of Algorithm 2 allow us to compute a horizontal basis of $E[\ell^k]$. This could be done directly with Algorithm 1 instead, but that would require computing in an extension $F_{k+h-\beta}$.

4. *Interpolation step*

After constructing bases (P, Q) of $E[\ell^k]$ and (P', Q') of $E'[\ell^k]$ using the algorithms of the previous section, our algorithm computes the polynomial with coefficients in $\mathbb{F}_q$ sending $x(P) \mapsto x(P')$, $x(Q) \mapsto x(Q')$, and the other abscissas accordingly. In this section we give an efficient algorithm for this specific interpolation problem. The algorithm has already appeared in [**DF11**] and [**EM03**]; we recall it here, and adapt the complexity analysis to our setting.

4.1. *Rational interpolation*

We start by tackling a simpler problem. We suppose we have constructed a tower of Kummer extensions $\mathbb{F}_q = F_0 \subset F_1 \subset \cdots \subset F_n$, with $[F_1 : F_0] \mid (\ell - 1)$, and $[F_{i+1} : F_i] = \ell$ for any $i > 0$. Given two elements $v, w \in F_n \setminus F_{n-1}$, we want to compute polynomials T and L such that:

- $T \in \mathbb{F}_q[x]$ is the minimal polynomial of v, of degree $d = \deg T < \ell^n$;
- L is in $\mathbb{F}_q[x]$, of degree less than d, and $L(v) = w$.

Observe that, since $v, w \notin F_{n-1}$, we necessarily have $v_\ell(d) = n - 1$, so that $\ell^{n-1} \leqslant d < \ell^n$.

Using a fast interpolation algorithm [vzGG99, Chapter 10.2], the polynomials T and L could be computed in $O\big(n\mathsf{M}(\ell^{2n})\log(\ell)\big)$ operations in $\mathbb{F}_q$. We can do much better by exploiting the form of the Kummer tower, and the Frobenius algorithm given in Lemma 1.1.

Following [DF11], we first compute T, starting from $T^{(0)} = x - v$. We let σ_i be the map that takes all the coefficients of a polynomial in $F_{n-i}[x]$ to the power $\#F_{n-i-1}$. For $i = 0, \dots, n-2$, suppose we know a polynomial $T^{(i)}$ of degree ℓ^i in $F_{n-i}[x]$. Then, compute the polynomials $T^{(i,j)}$ given by

$$T^{(i,j)} = \sigma_i^j\big(T^{(i)}\big) \quad \text{for } 0 \le j \le \ell - 1,$$

and define

$$T^{(i+1)} = \prod_{j=0}^{\ell-1} T^{(i,j)};$$

one easily sees that $T^{(i+1)}$ is the minimal polynomial of v over F_{n-i+1}. For the last step $i = n-1$, we proceed in a similar way by defining

$$T = T^{(n)} = \prod_{j=0}^{d/\ell^{n-1}} T^{(n-1,j)}.$$

LEMMA 4.1. *The cost of computing $T^{(n)} = T$ is bounded by $O(n\ell\mathsf{M}(\ell^{n+1}))$ operations in $\mathbb{F}_q$.*

Proof. At each step i, from the knowledge of $T^{(i)}$ we compute all $T^{(i,j)}$ using Lemma 1.1. The cost for a single polynomial $T^{(i,j)}$ is of $O\big(\ell^i\big(\ell^{n-i}\mathsf{M}(\ell) + \mathsf{M}(\ell^{n-i})\big)\big)$ operations, which we simplify to a total of $O(\ell\mathsf{M}(\ell^{n+1}))$ for all $O(\ell)$ of them.

From the $T^{(i,j)}$'s we compute $T^{(i+1)}$ using a subproduct tree, as in [vzGG99, Lemma 10.4]. The result has degree $O(\ell^{i+1})$ and coefficients in F_{n-i}, thus the overall cost is $O(\mathsf{M}(\ell^{n+1})\log(\ell))$. After $T^{(i+1)}$ is computed this way, we can convert its coefficients to F_{n-i-1} at no algebraic cost.

Summing over all i, we obtain the stated complexity. □

We can finally proceed with the interpolation itself. First, compute $w' = w/T'(v)$ and let $L^{(0)} = w'$. Next, for $i = 0, \dots, n-2$, suppose we know a polynomial $L^{(i)}$ in $F_{n-i}[x]$ of degree less than ℓ^i. We compute the polynomials $L^{(i,j)}$ given by

$$L^{(i,j)} = \sigma_i^j\big(L^{(i)}\big),$$

for $0 \le j \le \ell - 1$, and

$$L^{(i+1)} = \sum_{j=0}^{\ell-1} L^{(i,j)} \frac{T^{(i+1)}}{T^{(i,j)}}.$$

The last step $i = n-1$ is done analogously. As shown in [DF11], $L^{(n)}$ is the polynomial L we are looking for.

PROPOSITION 4.2. *Given elements $v, w \in F_n \setminus F_{n-1}$, the cost of computing the minimal polynomial $T \in \mathbb{F}_q[x]$ of v, and the interpolating polynomial $L \in \mathbb{F}_q[x]$ such that $L(v) = w$, is of $O(n\ell\mathsf{M}(\ell^{n+1}))$ operations in $\mathbb{F}_q$.*

Proof. After the polynomials $T^{(i)}$ have been computed, we need to compute $T'(v)$. This is done by means of successive Euclidean remainders, since $T'(v) = (((T' \bmod T^{(1)}) \bmod T^{(2)}) \cdots \bmod T^{(n)})$. At stage i, we have to compute the Euclidean division of a polynomial of degree $O(\ell^{n-i+1})$ by one of degree $O(\ell^{n-i})$ in $F_i[x]$. Using the complexities from Section 1.4

we deduce that each division can be done in time $O(\mathsf{M}(\ell^{n+1}))$, for a total of $O(n\mathsf{M}(\ell^{n+1}))$ operations. Then, computing $w' = w/T'(v)$ takes $O(\mathsf{M}(\ell^n)\log(\ell^n))$ operations.

Finally, at each step i, the polynomials $L^{(i,j)}$ are computed at a cost of $O(\ell\mathsf{M}(\ell^{n+1}))$, as in the proof of Lemma 4.1. The computation of $T^{(i)}$ requires $O(\ell)$ additions, multiplications and divisions of polynomials of degree $O(\ell^{i+1})$ with coefficients in F_{n-i}, again at a cost of $O(\ell\mathsf{M}(\ell^{n+1}))$. Summing over all i, the complexity statement follows readily. □

We finally go to the general problem of interpolating a polynomial in $\mathbb{F}_q[x]$ at many points of F_n.

PROPOSITION 4.3. *Let $(v_1, w_1), \dots, (v_s, w_s)$ be pairs of elements of F_n, let t_i be the degree of the minimal polynomial of v_i, and let $t = \sum t_i$. The polynomials*

– *$T \in \mathbb{F}_q[x]$ of degree t such that $T(v_i) = 0$ for all i, and*
– *$L \in \mathbb{F}_q[x]$ of degree less than t such that $L(v_i) = w_i$ for all i*

can be computed using $O\big(\mathsf{M}(t)\log(s) + n\ell\mathsf{M}(\ell^2 t)\big)$ operations in $\mathbb{F}_q$.

Proof. The polynomial T is simply the product of all the minimal polynomials T_i. Let $n_i = v_\ell(t_i)$, so that $v_i, w_i \in F_{n_i+1} \setminus F_{n_i}$, and $\ell^{n_i} \leqslant t_i < \ell^{n_i+1}$. We convert (v_i, w_i) to a pair of elements of F_{n_i+1} at no algebraic cost, then we compute T_i as explained previously at a cost of $O(n\ell\mathsf{M}(\ell^{n_i+2}))$ operations. Bounding ℓ^{n_i} by t_i, summing over all i, and using the superlinearity of M, we obtain a total cost of $O(n\ell\mathsf{M}(\ell^2 t))$ operations. Simultaneously, we compute all the polynomials L_i such that $L_i(v_i) = w_i$, at the same cost.

Then we arrange the T_i's into a binary subproduct tree and multiply them together. A balanced binary tree, though not necessarily optimal, has a depth of $O(\log(s))$, and requires $O(\mathsf{M}(t))$ operations per level. Thus we can bound the cost of computing T by $O(\mathsf{M}(t)\log(s))$.

Finally, using the same subproduct tree structure, we apply the Chinese remainder algorithm of [**vzGG99**, Chapter 10] to compute the polynomial L at the same cost $O(\mathsf{M}(t)\log(s))$. □

5. *The complete algorithm*

We finally come the description of the full algorithm. As stated in the introduction, we are given two elliptic curves E and E', and an integer r, and we want to compute an isogeny $\psi : E \to E'$ of degree r.

Since the algorithms of Section 3 only apply to curves on top of volcanoes with cyclic crater, we first need to determine a small Elkies prime ℓ for E and E', and then reduce to an explicit isogeny problem on the crater of the ℓ-volcanoes. These steps are discussed and analyzed next.

5.1. *Finding a suitable ℓ-volcano*

Our algorithm uses an Elkies prime ℓ. According to Chebotarev's density theorem, the density of primes ℓ such that $(d_K/\ell) = +1$ is asymptotically $1/2$, so that we need only try a $O(1)$ number of primes ℓ. Since d_K is not assumed to be known yet, we need to be able to compute the height h of the volcano, the shape of its crater, as well as the shortest ℓ-isogeny chain from E to the crater.

The algorithms of Fouquet and Morain [**FM02**] compute the height h and find a curve $E_{\max}$ on the crater at the cost of $O(\ell h^2)$ factorizations of the ℓ-th modular polynomial Φ_ℓ. The polynomial Φ_ℓ is computed using $\tilde{O}(\ell^3 \log \ell)$ binary operations and $O(\mathsf{M}(\ell^2)\log q)$ operations in $\mathbb{F}_q$, then each factorization costs $O(\mathsf{M}(\ell)\log(\ell)\log(\ell q))$ operations using the Cantor-Zassenhaus algorithm. More efficient methods for special instances of volcanoes are presented in [**MMRV05**] and in [**IJ10**], but we ignore them .

Once we know a curve on the crater, we still have to determine the shape of the crater. Since the height h of the volcano is known, using Algorithm 1 we can compute a matrix of $\pi|E[\ell^{h+1}]$. If this matrix has two distinct eigenvalues then the crater is cyclic, otherwise it is not.

By Proposition 2.7, the depth of E and E' below their respective craters is the same. Using the methods of Section 5.1, we can compute the shortest path of ℓ-isogenies $\alpha : E \to E_{\max}$, $\alpha' : E' \to E'_{\max}$ linking the curves E, E' to the craters. By Proposition 2.7 (iii), the curves $E_{\max}$ and $E'_{\max}$ are again r-isogenous; we can use our algorithm to compute such an isogeny $\psi_{\max}$. Then $\psi = (\alpha')^{-1} \circ \psi_{\max} \circ \alpha$ is the required r-isogeny; its kernel can be computed in $O(h\mathsf{M}(r)\log(r))$ operations by evaluating α^{-1} on the kernel of $\psi_{\max}$ via a sequence of resultants.

5.2. *Interpolating the isogeny*

We now assume that both curves E, E' have ℓ-maximal endomorphism rings. We fix bases of $E[\ell^k]$, $E'[\ell^k]$ and write π, π' for the matrices of the Frobenius. Since ψ is rational, its matrix satisfies the relation $\pi' \cdot \psi = \psi \cdot \pi$ in $\mathbb{Z}_\ell^{2\times 2}$ and hence in $(\mathbb{Z}/\ell^k\mathbb{Z})^{2\times 2}$.

If diagonal bases of $E[\ell^k], E'[\ell^k]$ are used, then, since π is a cyclic endomorphism of $\mathbb{Z}_\ell^2$, this condition seems to ensure that ψ is a diagonal matrix; however, $\mathbb{Z}/\ell^k\mathbb{Z}$ is not an integral domain and π is congruent, modulo ℓ^h, to the scalar matrix λ, so we can only say that $\psi \pmod{\ell^{k-h}}$ is diagonal. If on the other hand we choose *horizontal* bases of $E[\ell^k], E'[\ell^k]$ then, by Proposition 2.7 (ii), we know that ψ is a diagonal matrix.

We then enumerate all the ℓ^{2k-2} invertible diagonal matrices; for each matrix M, we interpolate the action of M on $E[\ell^k]$ as a rational fraction, and verify that it is an r-isogeny. The successful interpolation will be our explicit isogeny ψ.

We interpolate using the abscissas of non-zero points of $E[\ell^k]$; there are $(\ell^{2k}-1)/2$ distinct such abscissas (or $2^{2k-1}+1$ when $\ell = 2$). Since the isogeny ψ is a rational fraction of degrees $(r, r-1)$, it is defined by $2r$ coefficients. For this method to work, we therefore select the smallest $k \geqslant h+1$ such that $\ell^{2k} - 1 > 4r$.

Summarizing, our algorithm for two curves having ℓ-maximal endomorphism ring proceeds as follows:

(1) Use Algorithms 1 and 2 to compute horizontal bases (P, Q) of $E[\ell^k]$ and (P', Q') of $E'[\ell^k]$;
(2) Compute the polynomial T vanishing on the abscissas of $\langle P, Q\rangle$ using the method of Section 4;
(3) For each invertible diagonal matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ in $(\mathbb{Z}/\ell^k\mathbb{Z})^{2\times 2}$:
   (i) compute the interpolation polynomial $L_{a,b}$ such that $L_{a,b}(x(uP + vQ)) = x(a\,u\,P' + b\,v\,Q')$ for all $u, v \in \mathbb{Z}/\ell^k\mathbb{Z}$;
   (ii) Use the *Cauchy interpolation algorithm* of [**vzGG99**, Chapter 5.8] to compute a rational fraction $F_{a,b} \equiv L_{a,b} \pmod{T}$ of degrees $(r, r-1)$;
   (iii) If $F_{a,b}$ defines an isogeny of degree r, return it and stop.

Theorem. *It is possible to solve the "Explicit Isogeny Problem" using at most*

$$O(r \cdot \mathsf{M}(r) \cdot \log^2(r) + r \cdot \log(r) \cdot \log(q))$$

operations in $\mathbb{F}_q$.

Proof. We expect to find a small Elkies prime ℓ after $O(1)$ trials. Also note that the height h of the volcano of ℓ-isogenies is small with very high probability; in case it is not, we can simply discard ℓ and choose another one. Hence, we treat both h and ℓ as constants for the purpose of this theorem.

First we reduce the problem to one on ℓ-maximal curves. This costs $O(\log(q) + \mathsf{M}(r)\log(r))$, as outlined in Section 5.1. Then we pick k with $\ell^{2k} \in O(r)$, and we apply the algorithm outlined above. By Proposition 2.8, there is a $\beta < h$ such that $E[\ell^k]$ is contained in $E(F_n)$ with $n = k - \beta$. We thus construct the Kummer tower $F_0 \subset \cdots \subset F_n$, and we do the precomputations required by Lemma 1.1 at a cost of $O(\log(r)\log(q))$.

Step (1) costs $O(k\mathsf{R}(k-\beta))$ according to Propositions 3.1 and 3.2. Using the estimates of Section 1.4, we see that this cost is bounded by $O(\mathsf{M}(\sqrt{r})\log(rq))$ if $\ell = 2$, or by $O(r + \mathsf{M}(\sqrt{r}\log(q))\log(r))$ otherwise.

By Proposition 2.8 (v), there are at most $O(k \cdot \ell^{k+\beta})$ Galois classes in $E[\ell^k]$. In order to apply the algorithms of Section 4, we need to compute a representative for each class. Each representative is computed from the basis (P, Q) using point multiplication by two scalars $\leqslant \ell^k$ in the field F_n, which costs $O(\mathsf{M}(\ell^n)\log(\ell^k))$ operations. We thus have a total cost of $O(k\mathsf{M}(\ell^{2k})\log(\ell^k)) \subset O(\mathsf{M}(r)\log^2(r))$ to compute all such representatives.

Then, using proposition 4.3, where the total degree is $t = (\ell^{2k}-1)/2 \in O(r)$, and the number of interpolation points is $s \in O(k \cdot \ell^{k+\beta})$, we can compute the polynomials T and $L_{a,b}$ at a cost of $O(\mathsf{M}(r)\log^2(r))$. The cost of computing $F_{a,b}$, and identifying the isogeny is dominated by that of computing $L_{a,b}$ [**DF11**, §3.3]. Finally, in general approximately $\ell^{2k} \approx r$ candidate matrices must be tried before finding the isogeny. □

6. *Experimental results*

We implement the algorithm on SageMath, we run the test on SageMath v7.0 only for $\ell = 2$. We place ourselves in the optimal case of [**DS15**] with $p = 1 \bmod 4$. Since the main cost of the algorithm comes from the repetition of the interpolation, we observe some floor for the r-isogenies with the same k such that $2^{2k-2}/3 > 4r$. Moreover with curves with a great rational torsion for $p = 1033$ and $p = 521$ we observes also some floor due to the fact that we need to repeat $O(h)$ times the interpolation. TODO: Describe implementation and show benchmarks. Possibly compare with Lercier-Sirvent (Luca has an implementation somewhere).

Acknowledgements. We thank many people.

References

Atk88 A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. 1988.

Atk91 A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. 1991.

BLS10 Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes, January 2010.

BMSS08 Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 77(263), 2008.

BS11 Peter Birkner and Francesco Sica. Four-dimensional Gallant-Lambert-Vanstone scalar multiplication. June 2011.

CCR91 Leonard S Charlap, Raymond Coley, and David P Robbins. Enumeration of rational points on elliptic curves over finite fields, 1991.

CLG09 Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, January 2009.

Cou94 Jean-Marc Couveignes. *Quelques calculs en théorie des nombres*. PhD thesis, Université de Bordeaux, 1994.

Cou96 Jean-Marc Couveignes. Computing l-Isogenies using the p-Torsion. In *ANTS-II: Proceedings of the Second International Symposium on Algorithmic Number Theory*, pages 59–65, London, UK, 1996. Springer-Verlag.

Cou00 J.-M. Couveignes. Isomorphisms between Artin-Schreier towers. *Math. Comp.*, 69(232):1625–1631, 2000.

DDS13 L. De Feo, J. Doliskani, and É. Schost. Fast algorithms for ℓ-adic towers over finite fields. In *ISSAC'13*, pages 165–172. ACM, 2013.

DF11 Luca De Feo. Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic. *Journal of Number Theory*, 131(5):873–893, May 2011.

DFJP11 Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506, September 2011.

DFS12 L. De Feo and É. Schost. Fast arithmetics in Artin-Schreier towers over finite fields. *J. Symbolic Comput.*, 47(7):771–792, 2012.

DS15 J. Doliskani and É. Schost. Computing in degree 2^k-extensions of finite fields of odd characteristic. *Des. Codes Cryptogr.*, pages 559–569, 2015.

Elk92 Noam D. Elkies. Explicit isogenies. 1992.

Elk98 Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *Studies in Advanced Mathematics*, pages 21–76, Providence, RI, 1998. AMS International Press.

EM03 Andreas Enge and François Morain. Fast decomposition of polynomials with known galois group. In *AAECC'03: Proceedings of the 15th international conference on Applied algebra, algebraic algorithms and error-correcting codes*, pages 254–264, Berlin, Heidelberg, 2003. Springer-Verlag.

FM02 M. Fouquet and F. Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2002.

GLV01 Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 190–200, London, UK, 2001. Springer-Verlag.

IJ10 Sorina Ionica and Antoine Joux. Pairing the volcano. In *ANTS*, pages 201–218, 2010.

JS14 David Jao and Vladimir Soukharev. *Post-Quantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, chapter Isogeny-Based Quantum-Resistant Undeniable Signatures, pages 160–179. Springer International Publishing, Cham, 2014.

Koh96 David Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California at Berkley, 1996.

KS97 Erich Kaltofen and Victor Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. In *ISSAC '97: Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, pages 184–188, New York, NY, USA, 1997. ACM.

LS08 Reynald Lercier and Thomas Sirvent. On Elkies subgroups of ℓ-torsion points in elliptic curves defined over a finite field. *Journal de théorie des nombres de Bordeaux*, 20(3):783–797, 2008.

LV16 Pierre Lairez and Tristan Vaccon. On p-adic differential equations with separation of variables, 2016.

MMRV05 Josep M. Miret, Ramiro Moreno, A. Rio, and Magda Valls. Determining the 2-sylow subgroup of an elliptic curve over a finite field. *Math. Comput.*, 74(249):411–427, 2005.

MMT01 Markus Maurer, Alfred Menezes, and Edlyn Teske. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. In *INDOCRYPT '01: Proceedings of the Second International Conference on Cryptology in India*, pages 195–213, London, UK, 2001. Springer-Verlag.

Sch85 René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

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

Ser70 Jean-Pierre Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1970.

Ser77 Jean-Pierre Serre. *Arbres, amalgames, SL_2*, volume 46 of *Astérisque*. Société Mathématique de France, 1977.

Sil92 Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

Sto10 Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. Math. Commun.*, 4(2), 2010.

Sut13 Andrew Sutherland. Isogeny volcanoes. In *ANTS X: Proceedings of the Algorithmic Number Theory 10th International Symposium*, volume 1, pages 507–530. Mathematical Sciences Publishers, 2013.

Tes06 Edlyn Teske. An elliptic curve trapdoor system. *Journal of Cryptology*, 19(1):115–133, January 2006.

Vél71 Jean Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238–241, 1971.

vzGG99 Joachim von zur Gathen and Jurgen Gerhard. *Modern Computer Algebra.* Cambridge University Press, New York, NY, USA, 1999.

vzGS92 Joachim von zur Gathen and Victor Shoup. Computing Frobenius maps and factoring polynomials. In *STOC '92: Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 97–105, New York, NY, USA, 1992. ACM.

Appendix A. *Galois classes in $E[\ell^k]$*

We give here the full decomposition of $E[\ell^k]$ in Galois classes. This is a more precise form of Proposition 2.8 (v).

Proposition A.1. *Let E be an elliptic curve with ℓ-maximal endomorphism ring. Assume $\ell \neq 2$, $\lambda \equiv \mu \equiv 1 \pmod{\ell}$ and let $\alpha = v_\ell(\lambda - 1), \beta = v_\ell(\mu - 1)$. Write $\nu(x, y) = \min(x + y, x +$*

$\beta - 1, y + \alpha - 1)$ *and* $\rho(x, y) = x + y - \nu(x, y) = \max(0, x - \alpha + 1, y - \beta + 1)$. *The decomposition of the group* $E[\ell^k]$ *in Galois classes is as follows:*

(i) *for* $i, j = 1, \ldots, k-1$: $(\ell - 1)^2 \cdot \ell^{\nu(i,j)}$ *classes of size* $\ell^{\rho(i,j)}$;
(ii) *for* $i = 1, \ldots, k-1$: $(\ell - 1) \cdot \ell^{\min(i,\alpha-1)}$ *classes of size* $\ell^{\max(0,i-\alpha+1)}$, *and* $(\ell - 1) \cdot \ell^{\min(i,\beta-1)}$ *classes of size* $\ell^{\max(0,i-\beta+1)}$;
(iii) *the* ℓ^2 *singleton classes of* $E[\ell]$.

Proof. Fix a basis (P, Q) of $E[\ell^k]$ such that $\pi(P) = \lambda P$, $\pi(Q) = \mu Q$. Studying the Galois orbits of $E[\ell^k]$ means studying the map $\mathbb{Z}_\ell^2 \to \mathbb{Z}_\ell^2, (x, y) \mapsto (\lambda x, \mu y)$. In other words, the orbits correspond to elements of $\mathbb{Z}_\ell^2$ modulo the *multiplicative* subgroup generated by (λ, μ). An easy way to describe this is to consider a *multiplicative lattice* in $(\mathbb{Q}_\ell^\times)^2$.

Let ξ be a primitive $(\ell - 1)$-th root of unity in $\mathbb{Z}_\ell$. Then by [**Ser70**, Théorème II.3.2], the map $f(x, y, z) = \ell^x \cdot \xi^y \cdot \exp(\ell z)$ is a group isomorphism between $\mathbb{Z} \times (\mathbb{Z}/(\ell - 1)\mathbb{Z}) \times \mathbb{Z}_\ell$ and $\mathbb{Q}_\ell^\times$. For $i \in [\![0, k-1]\!]$ and $c \in \mathbb{Z}/(\ell - 1)\mathbb{Z}$, let $V(i, c)$ be the image in $\mathbb{Z}/\ell^k\mathbb{Z}$ of the map $f(k - 1 - i, c, -)$: then the multiplicative structure of $V(i, c)$ is that of a principal homogeneous space under $\mathbb{Z}/\ell^i\mathbb{Z}$. We also define $W(i, j, c, d) = V(i, c) \cdot P + V(j, d) \cdot Q \subset E[\ell^k]$.

Since $\lambda \equiv 1 \pmod{\ell}$, we may write $\lambda = f(0, 0, u\,\ell^{\alpha-1})$ and $\mu = f(0, 0, v\,\ell^{\beta-1})$ for some $u, v \in \mathbb{Z}_\ell^\times$. This implies that the set $W(i, j, c, d)$ is stable under Galois. Moreover, the orbits of $W(i, j, c, d)$ correspond bijectively to points of a fundamental domain of the lattice $\Lambda_{i,j}$ generated by the columns of $\begin{pmatrix} \ell^i & 0 & u\ell^{\alpha-1} \\ 0 & \ell^j & v\ell^{\beta-1} \end{pmatrix}$, whereas the size of each orbit is $[(\mathbb{Z}/\ell^i\mathbb{Z}) \times (\mathbb{Z}/\ell^j\mathbb{Z}) : \Lambda_{i,j}]$. By using elementary column manipulations, we find that the covolume of $\Lambda_{i,j}$ is $\ell^{\nu(i,j)}$, hence the point (i) of the proposition. (The case $i = j = 0$ yields singleton classes in $E[\ell]$).

The reunion of all the sets $W(j, i, c, d)$ is exactly the set of all $xP + yQ$ for $x, y \neq 0$. We obtain the classes of (ii) by considering the sets $V(i, c) \cdot P$ and $V(j, d) \cdot Q$. □

We now state the equivalent proposition when $\ell = 2$. The proof is much the same as in the odd case.

Proposition A.2. *Let* E *be an elliptic curve with* 2*-maximal endomorphism ring. Assume* $\lambda \equiv \mu \equiv 1 \pmod 4$ *and let* $\alpha = v_2(\lambda - 1), \beta = v_2(\mu - 1)$. *Write* $\nu_2(x, y) = \min(x + y, x + \beta - 2, y + \alpha - 2)$ *and* $\rho_2(x, y) = x + y - \nu_2(x, y) = \max(0, x - \alpha + 2, y - \beta + 2)$. *The decomposition of the group* $E[2^k]$ *in Galois classes is as follows:*

(i) *for* $i, j = 1, \ldots, k-2$: $4 \cdot 2^{\nu_2(i,j)}$ *classes of size* $2^{\rho_2(i,j)}$;
(ii) *for* $i = 1, \ldots, k-2$: $4 \cdot 2^{\min(i,\alpha-2)}$ *classes of size* $2^{\max(0,i-\alpha+2)}$, *and* $4 \cdot 2^{\min(i,\beta-2)}$ *classes of size* $2^{\max(0,i-\beta+2)}$.
(iii) *the 16 singleton classes of* $E[4]$.

Note that if λ or $\mu \equiv -1 \pmod 4$ then by replacing the base field by a quadratic extension, we can always ensure that the condition $\lambda \equiv \mu \equiv 1 \pmod 4$ is satisfied.

TODO: Luca et Cyril

Jérôme Plût
ANSSI
51, boulevard de La Tour-Maubourg
75007 Paris
France

TODO: Éric