



Orienteering with One Endomorphism

Sarah Arpin¹  · Mingjie Chen²  · Kristin E. Lauter³  · Renate Scheidler⁴  ·
Katherine E. Stange⁵  · Ha T. N. Tran⁶ 

Received: 19 October 2022 / Revised: 15 March 2023 / Accepted: 18 May 2023 /
Published online: 20 June 2023
© The Author(s) 2023

Abstract

In supersingular isogeny-based cryptography, the path-finding problem reduces to the endomorphism ring problem. Can path-finding be reduced to knowing just one endomorphism? It is known that a small degree endomorphism enables polynomial-time path-finding and endomorphism ring computation (in: Love and Boneh, ANTS XIV-Proceedings of the Fourteenth Algorithmic Number Theory Symposium, volume 4 of Open Book Ser. Math. Sci. Publ., Berkeley, 2020). An endomorphism gives an explicit orientation of a supersingular elliptic curve. In this paper, we use the volcano structure of the oriented supersingular isogeny graph to take ascending/descending/horizontal steps on the graph and deduce path-finding algorithms to an initial curve. Each altitude of the volcano corresponds to a unique quadratic order, called the primitive order. We introduce a new hard problem of computing the primitive order given an arbitrary endomorphism on the curve, and we also provide a sub-exponential quantum algorithm for solving it. In concurrent work (in: Wesolowski, Advances in cryptology-EUROCRYPT 2022, volume 13277 of Lecture Notes in Computer Science. Springer, Cham, 2022), it was shown that the endomorphism ring problem in the presence of one endomorphism with known primitive order reduces to a vectorization problem, implying path-finding algorithms. Our path-finding algorithms are more general in the sense that we don't assume the knowledge of the primitive order associated with the endomorphism.

Katherine E. Stange and Sarah Arpin were supported by NSF-CAREER CNS-1652238. Katherine E. Stange was also supported by Simons Fellowship 822143. Ha T. N. Tran was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and DGEGR-2019-00428). R. Scheidler was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04844). Mingjie Chen was supported by NSF Grants DMS-1844206 and DMS-1802161.

✉ Sarah Arpin
s.a.arpin@math.leidenuniv.nl

Extended author information available on the last page of the article

Keywords Elliptic curve · Endomorphism ring · Supersingular isogeny graph · Orientation · Path-finding · Vectorization

Mathematics Subject Classification Primary 14G50 · 94A60 · 11G05 · 14K04 · 11-04; Secondary 11R52

1 Introduction

The security of isogeny-based cryptosystems depends upon a constellation of hard problems. Central are the path-finding problem introduced in [10] (to find a path between two specified elliptic curves in a supersingular ℓ -isogeny graph), and the endomorphism ring problem (to compute the endomorphism ring of a supersingular elliptic curve). Only exponential algorithms are known for general path-finding, in the absence of information beyond the j -invariants of the desired starting and ending vertices of the path. However, if the endomorphism rings are known, the KLPT algorithm allows for polynomial-time path-finding [35]. In fact, it is known that the path-finding and endomorphism ring problems are equivalent [25, 61]. These are the central problems in isogeny based cryptography, despite the recent complete break of SIDH/SIKE [7, 40, 45]. The hardness of these problems is in no way affected by the attack, and they form the basis of the CGL hash function [10] and CSIDH [8], among others.

A natural question to ask is whether knowledge of a single explicit endomorphism (which generates only a rank 2 subring of the rank 4 endomorphism ring) can be used for path-finding. Answering this question is the goal of this paper: we give explicit algorithms transforming knowledge of one endomorphism into a way-finding tool that can detect ascending, descending and horizontal directions with regards to the corresponding orientation, and use this to walk to $j = 1728$.

By *explicit endomorphism*, we mean one given in some form in which its action on the curve is computable, and its minimal polynomial is known (but note that, given an endomorphism, both its norm and trace are in many cases computable; see Sect. 2.2). For example, such an endomorphism may be given as a rational map, or a composition chain of rational maps, and these are the two cases we focus on in this paper. The data of such an endomorphism is equivalent to the data of an *orientation* of a supersingular elliptic curve E , namely a map $\iota : K \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(E)$, where K is the imaginary quadratic field generated by a root of the minimal polynomial of the endomorphism.

The study of orientations provides some structure to the supersingular isogeny graph, which has recently been exploited [15, 20, 43]. In particular, the ℓ -isogeny graph of *oriented* supersingular elliptic curves over $\overline{\mathbb{F}}_p$ has a volcano structure familiar from the ordinary case: Each connected component consists of a single cycle, called a *rim*, of vertices connected by *horizontal* edges, and *descending* edges connecting the rim the non-rim vertices at lower *altitudes* of the volcano. Non-rim vertices only have ascending/descending edges. This graph maps onto the supersingular ℓ -isogeny graph over $\overline{\mathbb{F}}_p$. Our approach is to use the orientation provided by a given explicit endomorphism to discern ascending, descending and horizontal directions with regards to the volcano. This provides a sort of tool for ‘*orienteering*’. (The sport of *orienteering*

involves finding one’s way to checkpoints across varied terrain using only map and compass.)

The core result of our paper is an algorithm that finds an ℓ -isogeny path from a given supersingular elliptic curve E to an initial curve E_{init} , given a single explicit endomorphism of E . We take E_{init} to be the curve with j -invariant $j = 1728$, but other choices are possible (see Sect. 6.3). The overall plan is as follows. First, climb the oriented volcano from E , oriented by the given endomorphism, to the volcano rim (using the given endomorphism as our ‘orienting tool’). Then, by orienting the curve $j = 1728$ with the same field, we can climb to the rim from there also. Finally, we attempt to meet by circling the rim.

This approach is limited by our ability to traverse a potentially large segment of the rim, or to hit the same rim in a large cordillera of volcanoes, whose size is generally equal to the class number of the corresponding quadratic order. If we simply walk the rim, then, classically, the runtime depends linearly on this class number. Using a quantum computer to solve the vectorization problem (see Sect. 9.1) yields a subexponential algorithm.

1.1 Main Theorems

We rely on a number of heuristic assumptions: (i) The Generalized Riemann Hypothesis (hereafter referred to as GRH). (ii) Powersmoothness in a quadratic sequence or form is as for random integers (a powersmooth analogue of the heuristic assumption underlying the quadratic sieve; see Heuristics 5.10 and 9.3). (iii) The orientations of a fixed j -invariant are distributed reasonably across all suitable volcanoes (Heuristic 3.7). (iv) This distribution is independent of a certain integer factorization (Heuristic 6.7). (v) The aforementioned integer factorization is prime with the same probability as a random integer (Heuristic 6.4; this heuristic is similar to those used in [24] and [35]).

We state our main results here; their proofs can be found in Sect. 11.1. We use the notation $L_x(y) = \exp(O((\log x)^y(\log \log x)^{1-y}))$. Our first theorem gives a classical algorithm for ℓ -isogeny path-finding that is subexponential in $\log p$ times a certain class number, for a wide range of input endomorphisms.

For any endomorphism θ of a supersingular curve E , let Δ' denote the ℓ -fundamental part of the discriminant Δ of θ (obtained¹ by removing the largest even power of ℓ). Let $h_{\Delta'}$ be the class number of the quadratic order of discriminant Δ' . Note that Δ' can be significantly smaller than Δ .

Theorem 1.1 *Assume $|\Delta'| \leq p^{2+\epsilon}$. Under the heuristic assumptions and notation given above, there is a classical algorithm (given explicitly in Sect. 11; see also Algorithm 8.1) that, given an endomorphism θ of sufficiently large degree d which can be efficiently evaluated on points, finds an ℓ -isogeny path of length $O(\log p + h_{\Delta'})$ from E to the curve with $j = 1728$ in runtime $h_{\Delta'} L_d(1/2) \text{ poly}(\log p)$.*

The term ‘sufficiently large’ as applied to the degree d asks that $L_d(1/2) \geq \text{poly}(\log p)$. The term ‘efficiently’ means that the endomorphism can be evaluated

¹ Except when $\ell = 2$, if $\Delta = 2^{2k} \Delta''$ where $4 \nmid \Delta''$ and $\Delta'' \equiv 2, 3 \pmod{4}$, then we set $\Delta' := 4\Delta''$.

on points $P \in E(\mathbb{F}_{p^k})$ in time polynomial in $\log d$, in k and in $\log p$. An example of such an endomorphism is an endomorphism given as a chain of isogenies of small degree, but we can also accommodate less efficient endomorphism representations. The full formal statement given in Theorem 11.1 tracks the cost of this evaluation in the final runtime: it is assumed that the endomorphism θ can be evaluated on points $P \in E(\mathbb{F}_{p^k})$ in time denoted $T_\theta(k, p)$, and the algorithm runtime, more precisely, is $T_\theta(L_d(1/2), p) + h_{\Delta'} L_d(1/2) \text{poly}(\log p)$. The algorithm comes in two phases: the first phase is to represent the given endomorphism as an isogeny chain in runtime $T_\theta(L_d(1/2), p)$ depending on the representation of θ ; the second phase walks the isogeny graph using this representation and always has runtime $h_{\Delta'} L_d(1/2) \text{poly}(\log p)$. Phase one is included to allow for an abstract notion of an input endomorphism (see Sect. 5.1).

Any θ of degree d which is represented in terms of rational maps has $T_\theta(k, p) = \text{poly}(d, k, \log p)$, hence the final runtime would be $\text{poly}(d \log p) + h_{\Delta'} L_d(1/2) \text{poly}(\log p)$. But θ could be represented as a composition chain of isogenies in such a way that $T_\theta(k, p)$ is polynomial in $\log d$. In this case, the final runtime would be $h_{\Delta'} L_d(1/2) \text{poly}(\log p)$. The factor $L_d(1/2)$ in the runtime arises from the need, during the algorithm, to sieve for endomorphisms of powersmooth degree amongst translates $\theta + [d]$, $d \in \mathbb{Z}$.

The algorithm can perform significantly better in some special cases, such as when the endomorphism is presented in an efficient way (in which case the first phase may be skipped), the curve is already at a rim (in which case the sieving is avoided), or the class number $h_{\Delta'}$ is small (in which case the walk is short), etc. Specifically, modifications of the algorithm lead to special cases:

- (1) If the input endomorphism is rationally represented in polynomial space, or the class number is polynomial in $\log p$ (with some conditions on ℓ), the algorithm becomes polynomial in $\log p$ (Theorem 11.3). The cryptographic weaknesses in these cases are already known by other methods [39].
- (2) If ℓ is inert in the field $\mathbb{Q}(\sqrt{\Delta})$, the runtime improves for endomorphisms in suitable form to $L_d(1/2) + h_{\Delta'} \text{poly}(\log p)$, and the path length is improved to $O(\log p)$ (Proposition 8.1).
- (3) If, in addition to (2), $\Delta' = \Delta$, then the runtime improves further to $h_{\Delta'} \text{poly}(\log p)$ (Proposition 8.1).
- (4) If the degree of the endomorphism has $B(p)$ -powersmooth factorization and its discriminant is coprime to ℓ , then the runtime improves to $h_{\Delta'} \text{poly}(B(p) \log p)$ (Theorem 11.5).
- (5) If degree and discriminant have suitable factorizations, then the runtime can improve to $\text{poly}(\log p)$ even for non-small degree endomorphisms (Theorem 11.4). Such endomorphisms exist on all supersingular elliptic curves.

Our second theorem gives a quantum algorithm for finding a smooth isogeny to an initial curve that runs in subexponential time in $\log |\Delta|$, and polynomial in $\log p$.

Theorem 1.2 *Under the heuristic assumptions and notation given above, there is a quantum algorithm (given explicitly in Sect. 11; see also Algorithm 10.1) which, given an endomorphism θ of degree d and discriminant Δ satisfying $d \ll |\Delta| \leq p^{2+\epsilon}$ and*

which can be efficiently evaluated on points, will return an $L_{|\Delta|}(1/2)$ -smooth isogeny of norm $O(\sqrt{|\Delta|})$ from E to the curve of $j = 1728$, and runs in time subexponential in $\log |\Delta|$ and polynomial in $\log p$.

The term ‘efficiently’ is as for Theorem 1.1. In the full formal statement in Theorem 11.2, the runtime, more precisely, is $T_\theta(O(\log^2 d), p)L_{|\Delta|}(1/2)$.

In both theorems, one may use other suitable initial curves besides $j = 1728$; see Sect. 6.3.

1.2 A New Hard Problem

Each altitude of an oriented volcano corresponds to a unique order in K , called the primitive order for the oriented curves at that altitude. The orders get smaller as the altitude gets lower, decreasing in index by ℓ at each step. Given an elliptic curve E oriented by an endomorphism θ , the knowledge of the primitive order \mathcal{O} with respect to (E, θ) plays a vital role in the algorithms: our classical algorithm computes a suborder of \mathcal{O} whose relative index in \mathcal{O} is coprime to ℓ in order to walk horizontally more efficiently; our quantum algorithm requires the full knowledge of \mathcal{O} in order to solve the \mathcal{O} -vectorization problem.

The primitive order \mathcal{O} doesn’t come for free; this is Problem 1.3. To the best of our knowledge, this paper is the first work that introduces this problem as a hard problem and provides a quantum algorithm (Proposition 9.8) for solving it in quantum sub-exponential time.

Problem 1.3 (PRIMITIVEORIENTATION). Given a supersingular elliptic curve E , and an endomorphism $\theta \in \text{End}(E)$, determine the quadratic order \mathcal{O} such that $\mathcal{O} \cong \mathbb{Q}(\theta) \cap \text{End}(E)$.

The importance of Problem 1.3 comes from the increasing interest in orientations on elliptic curves. Given an arbitrary supersingular elliptic curve E , the best known way to define an orientation on E is to perform random walks on the supersingular isogeny graph until a cycle on E is found, whereby an endomorphism on E is obtained by composing the edges along the cycle. In order to take advantage of the associated orientation, it is important to be able to answer Problem 1.3. This most general setting for obtaining orientations on E is the setting our paper works with.

Classically, however, solving Problem 1.3 as discussed in Sect. 9.2 takes time polynomial in the largest prime power factor of f , where f is the conductor of $\mathbb{Z}[\theta]$. Luckily, with our classical path-finding algorithm (Theorem 11.1), we are able to circumvent the issue by computing a specific smaller order instead, which can be done in polynomial time. This is also what makes our path-finding algorithms more general compared to the algorithms in a related paper [60] (See Sect. 1.4).

1.3 Other Algorithms Presented

Some of the explicit building blocks of the results above may have independent applications. In particular, we provide algorithms for the following tasks, among others:

- (1) Section 4 provides methods for detecting ascending, descending and horizontal directions in general.
- (2) Remark 4.9 explains how to adapt the algorithms of this paper to an endomorphism given as an approximate element of the Tate module (i.e. given by its action on ℓ -torsion).
- (3) Section 5.3 presents a technique for obtaining a prime-power powersmooth isogeny chain endomorphism from the same quadratic order as a given endomorphism (Algorithm 5.3).
- (4) Section 6 discusses an algorithm which computes an orientation of the elliptic curve of j -invariant 1728 (or other suitable curves; see Sect. 6.3) by an ℓ -power multiple of a given discriminant (Algorithm 6.1). In other words, given a quadratic order \mathcal{O} , it finds $j = 1728$ somewhere in the cordillera of an order containing \mathcal{O} . In fact, it finds arbitrarily many such orientations, moving gradually further ‘down’ the volcanoes. This algorithm runs in heuristic polynomial time when the discriminant is coprime to p and less than p^2 in absolute value.
- (5) Section 7.2 concerns a method for computing the class group action of $\text{Cl}(\mathcal{O})$ on $\text{SS}_{\mathcal{O}}^{pr}$, the set of curves primitively oriented by \mathcal{O} . In fact, we demonstrate how to navigate $\text{SS}_{\mathcal{O}}^{pr}$ using the class group action of $\text{Cl}(\mathcal{O}')$ for any $\mathcal{O}' \subseteq \mathcal{O}$ such that $\ell \nmid [\mathcal{O} : \mathcal{O}']$.
- (6) Section 9 provides two new quantum algorithms. Namely, an algorithm for vectorization on an oriented volcano rim (Proposition 9.4; prior work includes [11, Section 6.1], [60, Proposition 4]; our approach includes a novel method to evaluate isogenies on oriented curves), and for determining the quadratic order for which a given orientation is primitive (Proposition 9.8). We provide runtime analyses of these algorithms in terms of the degree and presentation of the given orientation and the prime p .
- (7) Given the input of an elliptic curve with orientation, Sect. 10 provides a quantum algorithm (Algorithm 10.1) for finding a smooth isogeny to $j = 1728$. In Proposition 10.1, we analyze the runtime of this algorithm in terms of the degree and presentation of the given orientation and the prime p .
- (8) Section 12 contains an efficient algorithm for dividing an isogeny by $[\ell]$ (Algorithm 12.2), originally outlined by McMurdy. We make McMurdy’s approach explicit for an arbitrary small prime ℓ (he only made explicit the case $\ell = 2$, which is more straightforward).

1.4 Related Work

The question of the security of one endomorphism has recently been ‘in the air,’ for example, with the uber isogeny assumption of [22] (see Remark 9.2). Knowledge of a small explicit endomorphism is known to be a weakness [38, 39].

In a recent preprint [27], the authors design a generic framework for computing the class group actions on oriented supersingular curves. They propose to use an imaginary quadratic order \mathcal{O} of large prime conductor f inside a maximal order of small class number. By carefully choosing parameters such as the conductor f , the finite field characteristic p and the norm of a generator α of \mathcal{O} , they made the computation of the

class group action of arbitrary class group elements on the set of oriented supersingular elliptic curves efficient, leading to a practical signature scheme. The security of their scheme relies on the hardness of the path-finding problem on the associated oriented supersingular isogeny graph. This problem is still hard even with the presence of our path-finding algorithms due to the choice of a large prime conductor f .

The work in this paper was done concurrently with [60], which also provides path-finding algorithms in the setting of oriented curves. However, the two papers are very different in nature. The work in [60] covers a web of reductions between a wide variety of hard problems related to orientations using quaternion algebras, which are of interest both in theory and applications. The path-finding algorithms are not presented in explicit algorithmic form in [60] but implied by several reductions combined with algorithms for solving the vectorization problem for oriented curves classically and quantumly. Our paper, by contrast, focuses on the path-finding problem. Our method is very explicit and works with isogenies and endomorphisms directly. We discuss the practical representations of isogenies and endomorphisms, provide complete algorithms, detailed runtime analysis and concrete numerical examples.

The most important advantage of our path-finding algorithms over those given by [60] is that we deal with orientations in greater generality. In both papers, an orientation is identified with an endomorphism. As discussed in Sect. 1.2, our input is an arbitrary endomorphism θ , and it is a hard problem (Problem 1.3) to find the primitive order with respect to (E, θ) . However, the input endomorphism θ in [60] is one such that the order $\mathbb{Z}[\theta]$ is already the primitive order. Such an endomorphism is unlikely to be found for an arbitrary supersingular elliptic curve.

With due consideration of the added constraints on input for the algorithm in [60], we can more accurately compare runtimes. Let Δ , Δ' and $h_{\Delta'}$ be as in Sect. 1.1. Classically, the runtime of the algorithm in [60] is linear in $h_{\Delta'}^{1/2}$, whereas the runtime of our algorithm is linear in $h_{\Delta'}$. Quantumly, both algorithms run in subexponential time. If we consider the same input endomorphism in [60] as in this work, then the runtime for solving Problem 1.3 should be added to the runtime of [60]. As discussed in Sect. 9.2, solving Problem 1.3 takes time polynomial in the biggest prime power factor of the conductor of $\mathbb{Z}[\theta]$ classically and subexponential time quantumly.

Lastly, the paper [60] assumes the stronger hypothesis that the discriminant of the input endomorphism has a known factorization. We do not assume this. The work [60] is not heuristic beyond a dependence on GRH and the solution to the vectorization problem ([60, Proposition 4]), whereas we rely on a number of heuristic assumptions as given in Sect. 1.1. Our classical algorithm directly produces a path whose length depends on the class number (since it traverses a volcano rim), whereas a reduction to the vectorization problem as in the algorithms implied in [60] and our quantum algorithm produces a path of $\text{poly}(\log p)$ length.

Other related work includes [9, 20]. In [2], the authors of the present article show that appropriately defined closed walks of the isogeny graph are in bijection with the rims of oriented isogeny volcanoes, giving a class number sum for their number.

1.5 Other Contributions

We give careful runtime analyses for various tasks related to endomorphisms represented as rational functions or as composition chains of isogenies, including evaluation, translation, division-by- $[\ell]$, and Waterhouse transfer. Additionally, we provide a review and some modest extensions to the theory of orientations as described in [15, 43]; see Sect. 3, in particular Sect. 3.3.

In a follow-up paper [2], we establish a theoretical bijection between volcano rims and cycles in the ℓ -isogeny graph, and address some of the aforementioned heuristics for oriented supersingular ℓ -isogeny graphs used in this paper.

Throughout the paper we demonstrate our algorithms with a running example first introduced in Example 3.2. The examples are given in more detail in SageMath [54] worksheets with accompanying PDF details, available on GitHub [3].

1.6 Outline

In Sect. 2, we set some notations and conventions and also state a few runtime lemmata. In Sect. 3, we introduce the main object of study, namely oriented ℓ -isogeny graphs and their properties, including some heuristic behaviour. In Sect. 4, the relationship between an endomorphism and an orientation is explained, and we also introduce a few new definitions that aid in navigating the oriented ℓ -isogeny graph. In Sect. 5, we discuss the representation of endomorphisms, along with the basic functionalities for these representations required for later algorithms. We then compute orientations for the supersingular elliptic curve of j -invariant 1728 in Sect. 6. In Sects. 7 and 8, we present algorithms for walking on an oriented ℓ -isogeny graph and for classical path-finding to $j = 1728$ and give detailed runtime analyses and examples for illustration. We then provide quantum algorithms to solve the oriented vectorization and the primitive orientation problems in Sect. 9 and a quantum algorithm for finding a smooth isogeny to $j = 1728$ in Sect. 10. In Sect. 11, we discuss the proofs of our main theorems as well as some special cases. Lastly, we leave to Sect. 12 the technical explanation of McMurdy's division-by- ℓ algorithm and provide its runtime analysis. Throughout the paper, to aid in reading, important assumptions will be rendered in **bold**.

2 Background

2.1 Notations and Conventions

Throughout the paper, let p **be a cryptographically sized prime** (upon which runtimes will depend), and let ℓ **be a small prime** (whose size will be assumed $O(1)$ for runtimes). In particular, $\ell \neq p$. We will assume **both p and ℓ are defined once throughout the paper** (so, for example, they will not be repeated as an input to every algorithm); the only exception being Sects. 9 and 10.

Every elliptic curve considered in the paper is assumed to be a **supersingular curve** over $\overline{\mathbb{F}}_p$. All such curves can be defined over \mathbb{F}_{p^2} . Every isogeny and endomorphism is assumed to have domains and codomains which are curves of this type. We use the notation $\text{End}(E)$ for the endomorphism ring of the elliptic curve E over $\overline{\mathbb{F}}_p$, and $\text{End}^0(E) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(E)$ for the endomorphism algebra of E . We use the notation O_E for the identity element of an elliptic curve E , and $j(E)$ for the j -invariant. We use the variables φ and ψ to denote isogenies, while θ is generally reserved for endomorphisms. The dual isogeny to an isogeny φ is denoted by $\widehat{\varphi}$. Let $E^{(p)}$ denote the curve obtained by the action of Frobenius on E (acting on the Weierstrass coefficients). Let $\pi_p : E \rightarrow E^{(p)}$ denote the Frobenius isogeny, given by $\pi_p(x, y) = (x^p, y^p)$. Note that Frobenius is an endomorphism if E is defined over \mathbb{F}_p . Frobenius also acts on any isogeny $\varphi : E \rightarrow E'$ (acting on its coefficients) to give $\varphi^{(p)} : E^{(p)} \rightarrow (E')^{(p)}$ of the same degree. Unless otherwise specified (such as Frobenius), **isogenies will be assumed to be separable** throughout the paper (many of the algorithms herein would not apply to inseparable endomorphisms or isogenies).

There is only one fixed supersingular ℓ -isogeny graph under consideration at any time, which we denote simply by \mathcal{G} . Namely, this is the graph whose vertices are $\overline{\mathbb{F}}_p$ -isomorphism classes of supersingular elliptic curves (which we will often refer to simply by their j -invariants), and whose directed edges are ℓ -isogenies (when there are no extra automorphisms, we can identify dual pairs to create an undirected graph).

We consider imaginary quadratic fields $K = \mathbb{Q}(\sqrt{\Delta})$, where $\Delta < 0$ is a fundamental discriminant. Then the ring of integers has the form $\mathcal{O}_K = \mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \frac{1+\sqrt{\Delta}}{2} & \text{if } \Delta \equiv 1 \pmod{4}, \\ \frac{\sqrt{\Delta}}{2} & \text{if } \Delta \equiv 0 \pmod{4}. \end{cases}$$

Since we sometimes have multiple quadratic orders under consideration, we use the notation $(\alpha, \beta)_{\mathcal{O}}$ for the ideal generated by α and β in \mathcal{O} . The (possibly non-maximal) orders \mathcal{O} of K are parameterized by a positive integer called the *conductor*. If \mathcal{O} has conductor f and ω is as above, then $\mathcal{O} = \mathbb{Z}[f\omega]$ and the discriminant of \mathcal{O} is $f^2\Delta$. If $\ell \nmid f$, then we say that both \mathcal{O} and its discriminant are ℓ -*fundamental*. Given a discriminant Δ , its ℓ -*fundamental part* is the maximal ℓ -fundamental discriminant dividing Δ .

Write $B_{p,\infty}$ for the rational quaternion algebra ramified at p and ∞ . **Every quadratic field K is assumed to embed in the quaternion algebra $B_{p,\infty}$** , i.e. to be an imaginary quadratic field in which p does not split [56, Proposition 14.6.7(v)]; the only exception is in the discussion of Heuristic 6.4. Every quadratic order \mathcal{O} is assumed to generate such a field K , and to **have discriminant not divisible by p** . Every quadratic discriminant is assumed to be the discriminant of such a quadratic order \mathcal{O} , and we write $\Delta_{\mathcal{O}}$. We denote by \mathcal{O}_K the maximal order of the quadratic field K and reserve Δ_K for the discriminant of \mathcal{O}_K .

Complex conjugation (which is also the action of $\text{Gal}(K/\mathbb{Q})$) is denoted by an overline: $\alpha \mapsto \bar{\alpha}$. We use the notation $\text{Cl}(\mathcal{O})$ and $h_{\mathcal{O}}$ for the class group and class number, respectively, of a quadratic order \mathcal{O} .

The reduced norm and trace of $B_{p,\infty}$ coincide with the norm and trace of an element when it is considered as a quadratic algebraic number; when we discuss norm and trace it is always this we refer to.

For runtime analyses we use big O notation, including soft \tilde{O} for absorbing log factors. The notation $\mathbf{M}(n)$ will indicate the runtime of field operations (addition, multiplication, inversion) in a finite field of cardinality n ; here, we note that $\mathbf{M}(n^k) = O(\mathbf{M}(n))$ when k is constant. In the later portions of the paper we are mainly concerned with the distinction between polynomial, subexponential and exponential algorithms. We write runtime as $\text{poly}(x)$ if there exists a polynomial f so the runtime is $O(f(x))$. When we are concerned only with whether runtime is polynomial, we will suppress the notation \mathbf{M} , by assuming that $\mathbf{M}(n) = \text{poly}(\log n)$. For subexponential runtimes, we use notation $L_x(y) = \exp(O((\log x)^y (\log \log x)^{1-y}))$.

For general background on isogeny-based cryptography and supersingular isogeny graphs, we will assume the reader is familiar with a resource such as [25, Section 2] or [21].

2.2 Runtime Lemmata

In this section, we recall some basic runtimes for isogenies and torsion points, etc. The first lemma is standard.

Lemma 2.1 *Given $P, Q \in E[N]$, and $0 \leq a, b < N$, computing $[a]P + [b]Q$ takes time $O((\log N)\mathbf{M}(p^{N^2}))$.*

Lemma 2.2 ([4, Corollary 2.5]). *Let $\varphi : E \rightarrow E'$ be an isogeny between two supersingular elliptic curves, both defined over \mathbb{F}_{p^2} . Then φ is defined over $\mathbb{F}_{p^{12}}$. If neither of $j(E)$ or $j(E')$ are 0 or 1728, then φ is defined over \mathbb{F}_{p^4} .*

Lemma 2.3 *Let t denote the smallest integer such that $E[N] \subseteq E(\mathbb{F}_{p^t})$. Then $t \leq N^2 - 1$. Finding a basis of $E[N]$ has runtime $\tilde{O}(N^4(\log p)\mathbf{M}(p^{N^2}))$.*

Proof This can be proved by adapting the second paragraph of the proof of Lemma 5 in [29]. In particular, the limiting runtime is the call to the equal-degree factorization algorithm of [58], which takes time $\tilde{O}(N^4(\log p)\mathbf{M}(p^{N^2}))$. See also [4, Lemma 6.9]. \square

In practice, this can be done much faster in some cases, e.g. when N is large and t is small.

Lemma 2.4 *Let $\varphi : E \rightarrow E'$ be an isogeny of degree d , given as a rational map. Let $P \in E(\mathbb{F}_{p^t})$, where $12 \mid t$. Then computing $\varphi(P)$ takes time $O(d\mathbf{M}(p^t))$. In particular, if $P \in E[N]$, then the time taken is $O(d\mathbf{M}(p^{\text{lcm}(12, N^2)}))$.*

Proof Write φ as $\varphi(x, y) = (\varphi_1(x), \varphi_2(x)y)$. Then the denominators and numerators of $\varphi_1(x)$ and $\varphi_2(x)$ are polynomials in x of degree at most $3d$. By Lemma 2.2, we can assume that their coefficients are in $\mathbb{F}_{p^{12}} \subseteq \mathbb{F}_{p^t}$. To compute $\varphi(P)$, we apply Horner's algorithm [34, p. 467], which requires $O(d)$ operations in the field. Assume that P is an N -torsion point on E . Then t can be chosen such that $t \leq \text{lcm}(12, N^2)$ by Lemma 2.3. \square

In the case that $\varphi = [n]$ for some integer n , it is more efficient to use a standard double-and-add approach, which will take logarithmic time in the degree [51, XI.1.1].

Lemma 2.5 ([55], [50, Theorem 3.5], [31, Section 5.1]). *Vélu’s formulas for an isogeny of degree d compute the rational maps for the isogeny in time $\tilde{O}(d\mathbf{M}(p^{d^2}))$.*

By Lemma 2.2, the isogeny created via Vélu’s formulas has coefficients in the field $\mathbb{F}_{p^{12}}$.

Lemma 2.6 *Let $\varphi : E \rightarrow E'$ and $\psi : E' \rightarrow E''$ be isogenies represented as rational maps, of respective degrees d and d' , where E, E', E'', φ and ψ are defined over some finite field \mathbb{F} . Then computing the composition $\psi \circ \varphi : E \rightarrow E''$ as a rational map takes time $\tilde{O}(dd'\mathbf{M}(\#\mathbb{F}))$.*

Proof As usual, write $\varphi = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ where $u(x), v(x), s(x), t(x) \in \mathbb{F}[x]$ are polynomials of degree $O(d)$ with $\gcd(u, v) = \gcd(s, t) = 1$. Similarly, write $\psi = \left(\frac{u'(x)}{v'(x)}, \frac{s'(x)}{t'(x)}y\right)$ with analogous conditions on $u'(x), v'(x), s'(x), t'(x) \in \mathbb{F}[x]$. Then

$$\psi \circ \varphi = \left(\frac{u'(\frac{u(x)}{v(x)})}{v'(\frac{u(x)}{v(x)})}, \frac{s'(\frac{u(x)}{v(x)})s(x)}{t'(\frac{u(x)}{v(x)})t(x)}y\right).$$

Obtaining $\psi \circ \varphi$ requires computing four compositions of the form $f(\frac{u(x)}{v(x)})$ where $f \in \{u', v', s', t'\}$ has degree $O(d')$. Writing $f(x) = \sum_{i=0}^n f_i x^i$ with $n = O(d')$, we have

$$f\left(\frac{u(x)}{v(x)}\right) = \frac{F(u(x), v(x))}{v(x)^n} \quad \text{where} \quad F(x, y) = \sum_{i=0}^n f_i x^i y^{n-i}.$$

The computation of $F(u(x), v(x))$ is dominated by computing the powers of $u(x)$ and $v(x)$ which can be accomplished in time $\tilde{O}(dd'\mathbf{M}(\#\mathbb{F}))$ using fast polynomial multiplication [30]. An alternative way to compute $F(u(x), v(x))$ that is slightly faster but has asymptotically the same runtime is via the Horner-like recursion

$$F_n(x) = f_n, \quad F_{i-1}(x) = f_{i-1}v(x)^{n-i+1} + F_i(x)u(x) \quad (n \geq i \geq 1),$$

where it is easy to see that $F_0(x) = F(u(x), v(x))$. □

Lemma 2.7 *Let E be an elliptic curve defined over some finite field \mathbb{F} , $\theta \in \text{End}(E)$ an endomorphism represented as a rational map, and N an integer. Then computing the endomorphism $\theta + [N] \in \text{End}(E)$ as a rational map takes time $\tilde{O}(\max\{\deg \theta, N^2\}\mathbf{M}(\#\mathbb{F}))$.*

Proof By [51, Exercise 3.7, pp. 105f.], we have

$$[N](x, y) = \left(\frac{\phi_N(x)}{\psi_N(x)^2}, \frac{\omega_N(x, y)}{\psi_N(x, y)^3}\right),$$

where $\phi_N = x\psi_N^2 - \psi_{N+1}\psi_{N-1}$, $\omega_n = (\psi_{N+2}\psi_{N-1}^2 - \psi_{N-2}\psi_{N+1}^2)/4y$ and ψ_n is the n -th division polynomial on E . The required division polynomials have degree $O(N^2)$ and can be computed in $O(\log(N))$ steps using the recursive formulas

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \quad \psi_{2n} = \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).$$

Using the point addition formulas on E and fast polynomial multiplication techniques [30], the rational map $\theta + [N]$ can be computed using $\tilde{O}(\max\{\deg \theta, N^2\})$ operations in \mathbb{F} . \square

Throughout the paper, we will assume that **all endomorphisms are provided with a trace and norm** (which is the same as the degree) that carries through computations; see Sect. 5.1.

3 Oriented Isogeny Graphs

In this section, we recall and strengthen basic results about oriented isogeny graphs, mainly based on work of Colò-Kohel [15] and Onuki [43], and provide some minor new extensions of the general theory.

3.1 Orientations

Fixing a curve E , we have $\text{End}^0(E) \cong B_{p,\infty}$. The field K embeds into $B_{p,\infty}$ if and only if p does not split in K . There may be many distinct such embeddings. We define a K -orientation of E to be an embedding $\iota : K \rightarrow \text{End}^0(E)$. If \mathcal{O} is an order of K , then an \mathcal{O} -orientation is a K -orientation such that $\iota(\mathcal{O}) \subseteq \text{End}(E)$. We say that a K -orientation ι is a *primitive* \mathcal{O} -orientation if $\iota(\mathcal{O}) = \text{End}(E) \cap \iota(K)$. It will often be expedient to have a local notion of primitivity: for a prime ℓ , we say that a K -orientation ι is an ℓ -primitive \mathcal{O} -orientation if it is an \mathcal{O} -orientation and the index $[\text{End}(E) \cap \iota(K) : \iota(\mathcal{O})]$ is coprime to ℓ . In particular, a primitive \mathcal{O} -orientation is exactly one which is ℓ -primitive for all primes ℓ .

If $\varphi : E \rightarrow E'$ is an isogeny of degree ℓ , where ι is a K -orientation of E , then there is an induced K -orientation $\iota' = \varphi_*(\iota)$ on E' defined to be $\varphi_*(\iota)(\omega) := \frac{1}{\ell}\varphi \circ \iota(\omega) \circ \widehat{\varphi} \in \text{End}^0(E')$.

A K -oriented elliptic curve is a pair (E, ι) where $\iota : K \rightarrow \text{End}^0(E)$ is a K -orientation. An isogeny of K -oriented elliptic curves $\varphi : (E, \iota) \rightarrow (E', \iota')$ is an isogeny $\varphi : E \rightarrow E'$ such that $\iota' = \varphi_*(\iota)$; we call this a K -oriented isogeny and write $\varphi \cdot (E, \iota) = (\varphi(E), \varphi_*(\iota))$. One verifies directly that $\varphi_2 \cdot \varphi_1 \cdot (E, \iota) = (\varphi_2 \circ \varphi_1) \cdot (E, \iota)$. A K -oriented isogeny is a K -isomorphism if it is an isomorphism of the underlying curves.

3.2 Oriented Isogeny Graphs

Fixing a quadratic field K , we define the graph \mathcal{G}_K of K -oriented supersingular curves over $\overline{\mathbb{F}}_p$. This is the graph whose vertices are K -isomorphism classes of pairs (E, ι)

and for which an edge joins (E, ι) and (E', ι') for each K -oriented isogeny (defined over $\overline{\mathbb{F}}_p$) of degree ℓ between these oriented curves. If $\varphi : (E, \iota) \rightarrow (E', \iota')$ is a K -oriented isogeny, then $\widehat{\varphi} : (E', \iota') \rightarrow (E, \iota)$ is also one (since $\widehat{\varphi}_*(\iota') = \widehat{\varphi}_*(\varphi_*(\iota)) = [\ell]_*(\iota) = \iota$). Therefore the edges may be taken to be undirected by pairing isogenies with their duals, when the vertices involved are not $j = 0$ or 1728 . Also, isogenies are taken up to equivalence, meaning we quotient by the same isomorphisms as for the vertices; see [43, Definition 4.1]. The graph \mathcal{G}_K has (out-)degree $\ell + 1$ at every vertex. (Note that our graph differs slightly from the definition in [43, Section 4], where only the images of curves over a number field with complex multiplication are included; we discuss this distinction in the next section.) This graph was first studied in [15].

Every K -orientation is a primitive \mathcal{O} -orientation for a unique order $\mathcal{O} := \iota(K) \cap \text{End}(E)$. Therefore, the set of vertices of \mathcal{G}_K is stratified by the order \mathcal{O} by which a vertex is primitively oriented.

Definition 3.1 Let $\text{SS}_{\mathcal{O}}^{pr}$ denote the set of isomorphism classes of K -oriented supersingular elliptic curves for which the orientation is a primitive \mathcal{O} -orientation.

This set is non-empty if and only if p is not split in K and does not divide the conductor of \mathcal{O} [43, Proposition 3.2]. As mentioned in Sect. 2.1, we make those assumptions throughout the paper.

Let $\varphi : (E, \iota) \rightarrow (E', \iota')$ be a K -oriented ℓ -isogeny. Suppose that ι is a primitive \mathcal{O} -orientation and ι' is a primitive \mathcal{O}' -orientation. There are exactly three possible cases:

- (1) $\mathcal{O} = \mathcal{O}'$, in which case we say φ is *horizontal*,
- (2) $\mathcal{O} \supsetneq \mathcal{O}'$, in which case $[\mathcal{O} : \mathcal{O}'] = \ell$ and we say φ is *descending*,
- (3) $\mathcal{O} \subsetneq \mathcal{O}'$, in which case $[\mathcal{O}' : \mathcal{O}] = \ell$ and we say φ is *ascending*.

Example 3.2 (Introducing our running example). To illustrate the algorithms in this paper, we consider supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$ for $p = 179$. As $p \equiv 3 \pmod{4}$, the curve $E : y^2 = x^3 - x$ with $j(E) = 1728$ is supersingular. This curve is well-known to have extra automorphisms, and its endomorphism ring is generated by the endomorphisms $[1], [i], \frac{[1] + \pi_p}{2}, \frac{[i] + [i] \circ \pi_p}{2}$, where $[i](x, y) := (-x, iy)$ and π_p is as defined in Sect. 2.1. We define $K := \mathbb{Q}(\sqrt{\Delta})$ with $\Delta = -47$ and $\omega = \frac{1 + \sqrt{-47}}{2}$. We consider the oriented 2-isogeny graph of supersingular elliptic curves with respect to this imaginary quadratic field K .

3.3 Frobenius and Class Group Actions

Let \mathcal{O} be a quadratic order of K . Next we define an action of $\text{Cl}(\mathcal{O})$ on $\text{SS}_{\mathcal{O}}^{pr}$. For an invertible ideal \mathfrak{a} of \mathcal{O} embedded into $\text{End}(E)$ via a K -orientation ι , there exists a horizontal isogeny $\varphi_{\mathfrak{a}}$ defined by the kernel $E[\iota(\mathfrak{a})] := \cap_{\theta \in \iota(\mathfrak{a})} \ker(\theta)$ [15, Section 3] [43, Proposition 3.5], and we write

$$\mathfrak{a} \cdot (E, \iota) := \varphi_{\mathfrak{a}} \cdot (E, \iota).$$

A different choice of $\varphi_{\mathfrak{a}}$ with the same kernel gives an isomorphic oriented curve [43, Section 3.3], so this is well-defined on the oriented ℓ -isogeny graph \mathcal{G}_K . The action

of $\text{Cl}(\mathcal{O})$ is free, but not necessarily transitive; it may have as many as two orbits [43, Proposition 3.3]. In particular,

$$\# \text{SS}_{\mathcal{O}}^{pr} \in \{h_{\mathcal{O}}, 2h_{\mathcal{O}}\}. \tag{1}$$

Consider the effect of the Frobenius isogeny on an oriented curve, namely $\pi_p \cdot (E, \iota) = (E^{(p)}, \iota^{(p)})$ where $\iota^{(p)} := (\pi_p)_*(\iota)$. For any isogeny φ , we have $\pi_p \circ \varphi(x, y) = \varphi^{(p)}(x^p, y^p) = \varphi^{(p)} \circ \pi_p(x, y)$. Hence, one has $(\pi_p)_*(\iota)(\alpha) = \frac{1}{p}\pi_p \circ \iota(\alpha) \circ \widehat{\pi}_p = \frac{1}{p}\iota(\alpha)^{(p)} \circ \pi_p \circ \widehat{\pi}_p = \iota(\alpha)^{(p)}$. Since $\varphi \mapsto \varphi^{(p)}$ gives an isomorphism $\text{End}(E) \cong \text{End}(E^{(p)})$, we see that π_p is horizontal, so this gives an action on $\text{SS}_{\mathcal{O}}^{pr}$ for any \mathcal{O} by the two-element group $\{1, \pi_p\} = \langle \pi_p \rangle$. In fact, it is an action on the graph \mathcal{G}_K , not just the vertices, i.e. it preserves adjacency. Onuki shows that when there are two orbits of the action of $\text{Cl}(\mathcal{O})$ on $\text{SS}_{\mathcal{O}}^{pr}$, then the second orbit can be reached from the first by the action of Frobenius [43, Proposition 3.3]. In [2], a complete classification of when there are two (instead of one) orbit is given.

For our algorithms, we will sometimes need to compute the action of \mathcal{O} on $\text{SS}_{\mathcal{O}}^{pr}$ without actually knowing \mathcal{O} . We can define and use an action of a suborder $\mathcal{O}' \subseteq \mathcal{O}$ as a proxy. To accomplish this, define, for $[\alpha'] \in \text{Cl}(\mathcal{O}')$, that $\alpha' \cdot (E, \iota) := \cap_{\theta \in \iota(\alpha')} \ker(\theta)$. Observe that there is a homomorphism $\rho : \text{Cl}(\mathcal{O}') \rightarrow \text{Cl}(\mathcal{O})$. Using the previous proposition, this gives a group action of $\text{Cl}(\mathcal{O}')$ on $\text{SS}_{\mathcal{O}}^{pr}$. The following proposition states that these two definitions agree. Although it implements the action of \mathcal{O} , using the kernel intersection formula does not require knowledge of \mathcal{O} .

Proposition 3.3 *Let $\mathcal{O}' \subseteq \mathcal{O}$ with relative index f . Let α' be an ideal of \mathcal{O}' which has norm coprime to f . Suppose that E has a K -orientation ι which is \mathcal{O} -primitive. Let $\varphi_{\alpha'}$ be defined as the isogeny with kernel $\cap_{\theta \in \iota(\alpha')} \ker(\theta)$. Let $\alpha := \alpha' \mathcal{O}$ be the extension of α' to \mathcal{O} . Then $\alpha \cdot (E, \iota) = \varphi_{\alpha'}(E, \iota)$.*

Proof We have $\iota(\alpha') \subseteq \iota(\alpha) \subseteq \text{End}(E)$. We will show $\cap_{\theta \in \iota(\alpha')} \ker(\theta) = \cap_{\theta \in \iota(\alpha)} \ker(\theta)$. From that, we can complete the proof, since

$$\alpha \cdot (E, \iota) = \varphi_{\alpha}(E, \iota) = \varphi_{\alpha'}(E, \iota).$$

We immediately have $\cap_{\theta \in \iota(\alpha')} \ker(\theta) \supseteq \cap_{\theta \in \iota(\alpha)} \ker(\theta)$. We will show the index between these two groups must divide a power of f . But the larger of the groups has cardinality coprime to f by hypothesis. So this would imply they are equal.

Write $\alpha' = \alpha_1 \mathcal{O}' + \alpha_2 \mathcal{O}'$ and $\mathcal{O} = \mathbb{Z} + g\omega\mathbb{Z}$ using the notation of Sect. 2.1. Then

$$\begin{aligned} \cap_{\theta \in \iota(\alpha')} \ker(\theta) &= \ker(\iota(\alpha_1)) \cap \ker(\iota(\alpha_2)) \cap \ker(\iota(\alpha_1 fg\omega)) \cap \ker(\iota(\alpha_2 fg\omega)), \\ \cap_{\theta \in \iota(\alpha)} \ker(\theta) &= \ker(\iota(\alpha_1)) \cap \ker(\iota(\alpha_2)) \cap \ker(\iota(\alpha_1 g\omega)) \cap \ker(\iota(\alpha_2 g\omega)). \end{aligned}$$

We have $\ker(\iota(\alpha_i g\omega)) \subseteq \ker(\iota(\alpha_i fg\omega))$ with index f^2 . Thus the index of $\cap_{\theta \in \iota(\alpha)} \ker(\theta)$ inside $\cap_{\theta \in \iota(\alpha')} \ker(\theta)$ must divide a power of f . \square

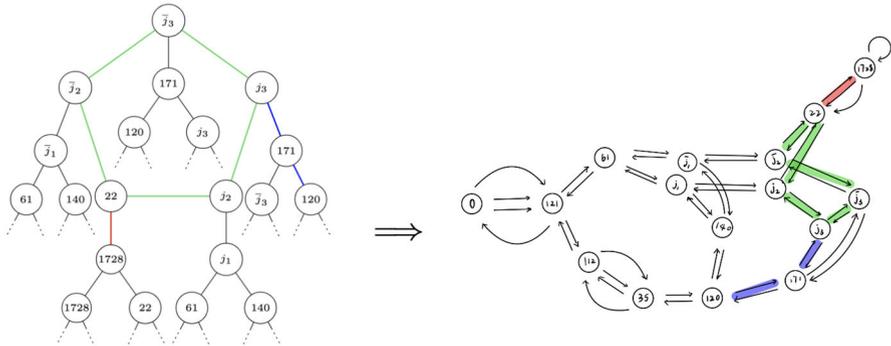


Fig. 1 On the left hand side is a component of \mathcal{G}_K for $p = 179$, $\ell = 2$ and $K = \mathbb{Q}(\sqrt{-47})$. On the right hand side is the supersingular 2-isogeny graph over \mathbb{F}_{p^2} . Here $j_1 = 64i + 5$, $j_2 = 99i + 107$, $j_3 = 5i + 109$, where i denotes a root of -1 in \mathbb{F}_{p^2} . Since the oriented graph is undirected while the supersingular isogeny graph is directed, we have undirected edges in the left graph and directed edges in the right graph. Note that the green 5-cycle represents the rim of the volcano

3.4 Volcano Structure

Any component of the oriented ℓ -isogeny graph \mathcal{G}_K has a *volcano structure* (see Fig. 1), which is made precise by the following statement. (This behaviour is similar to the ordinary ℓ -isogeny graph, except here volcanoes have no floor; they descend forever.) Here we remind the reader that $p \neq \ell$ throughout the paper.

Proposition 3.4 ([43, Proposition 4.1]). *Consider a vertex (E, ι) of the oriented ℓ -isogeny graph associated to K , a quadratic field of discriminant Δ . Suppose that ι is a primitive \mathcal{O} -orientation for E . If ℓ does not divide the conductor of \mathcal{O} , then the following hold.*

- (1) *There are no ascending edges from (E, ι) .*
- (2) *There are $\left(\frac{\Delta}{\ell}\right) + 1$ horizontal edges from (E, ι) .*
- (3) *The remaining edges from (E, ι) are descending.*

If ℓ divides the conductor of \mathcal{O} , then the following hold.

- (1) *There is exactly one ascending edge from (E, ι) .*
- (2) *The remaining edges from (E, ι) are descending.*

When \mathcal{O} has unit group $\{\pm 1\}$, i.e. except for the Gaussian and Eisenstein integers, the out-degree of (E, ι) is $\ell + 1$. For the out-degree in these special cases, see [2, Proposition 2.11].

Proposition 3.4 implies that each connected component of the oriented ℓ -isogeny graph \mathcal{G}_K is a *volcano*, containing a *rim* comprised of the vertices with no ascending edges. Each vertex on a rim is the root of a tree that radiates infinitely downward and in which each node other than the root generically has one parent and ℓ children. The vertices at altitude r are precisely those pairs (E, ι) for which ι is a primitive \mathcal{O} -orientation such that the conductor of \mathcal{O} has ℓ -adic valuation r . Specifically, the vertices at the rims are exactly those for which \mathcal{O} is ℓ -fundamental. For any fixed

ℓ -fundamental order \mathcal{O} , we define the \mathcal{O} -cordillera to be subgraph of \mathcal{G}_K comprised of only those volcanoes whose rims are pairs (E, ι) with ι a primitive \mathcal{O} -orientation. The vertices at the rims of the \mathcal{O} -cordillera are exactly $\text{SS}_{\mathcal{O}}^{pr}$.

The action of an ideal class $[\mathfrak{a}] \in \text{Cl}(\mathcal{O})$ gives a permutation on $\text{SS}_{\mathcal{O}}^{pr}$, which we can visualize as a directed graph. This consists of cycles, all of which are the same size, given by the order of $[\mathfrak{a}]$ in $\text{Cl}(\mathcal{O})$. Applying this to a prime ideal \mathfrak{l} of \mathcal{O} lying above ℓ , the rims of the \mathcal{O} -cordillera are exactly these cycles. All these rims have the same size dividing $h_{\mathcal{O}}$, and each of them is either a single vertex, a single or double edge or a cycle. If ℓ is inert, they are each singletons. If ℓ is ramified, they are each of size 2 with one connecting edge (the isogeny and its dual are identified). If ℓ splits into two classes of order 2, we obtain a rim of size two with two connecting edges. Otherwise, the rims are non-trivial cycles in the oriented ℓ -isogeny graph, of size equal to the order of $[\mathfrak{l}] \in \text{Cl}(\mathcal{O})$. We summarize the discussion as follows.

Proposition 3.5 *Let \mathcal{O} be ℓ -fundamental. Let $R_{\mathfrak{l}}$ be the order of $[\mathfrak{l}] \in \text{Cl}(\mathcal{O})$, for \mathfrak{l} a prime ideal of \mathcal{O} lying above ℓ . The \mathcal{O} -cordillera consists of $\#\text{SS}_{\mathcal{O}}^{pr} / R_{\ell}$ volcanoes of rim size R_{ℓ} .*

3.5 From Oriented Isogeny Graph to Isogeny Graph

There is a graph quotient $\mathcal{G}_K \rightarrow \mathcal{G}$ induced by forgetting the orientation.

Proposition 3.6 *Under this quotient, every component of \mathcal{G}_K (i.e. every volcano) covers \mathcal{G} .*

Proof Fix a volcano $\mathcal{V} \subset \mathcal{G}_K$. Choose a vertex $(E, \iota) \in \mathcal{V}$. The image E under the quotient map lies on \mathcal{G} . Since both \mathcal{V} and \mathcal{G} are regular of degree $\ell + 1$ at every vertex, the image of \mathcal{V} must be all of \mathcal{G} . \square

As a corollary, every j -invariant occurs on every volcano infinitely many times. Given p , a result of Kaneko [32, Theorem 2'] implies that the multiple occurrences of a given j -invariant cannot occur too quickly as one descends the oriented ℓ -isogeny volcano. In fact, there is at most one occurrence in the range $|\Delta| < p$ (here Δ is the discriminant at a certain altitude in the volcano).

3.6 Graph Statistics and Heuristics

In the ℓ -isogeny graph \mathcal{G} , two vertices are at distance d if the shortest path between them in the graph consists of d edges. The distance between two arbitrary vertices is known to be at most $2 \log p$ [44, Theorem 1]. In fact, for most pairs of vertices, the distance between them is at most $(1 + \epsilon) \log p$ (see [48, Theorem 1.5] for a precise statement).

We will use the following heuristic to justify the runtimes in the paper. One expects the number of occurrences of a j -invariant in a volcano to be governed by the number of trees emanating from the rim of the volcano. The heuristic in essence asserts a uniform behaviour within any cordillera. Specifically, the proportion of occurrences

of any j -invariant in any individual volcano of a cordillera approaches the overall proportion of trees (or equivalently, of edges descending from a rim). A more precise statement is given in Heuristic 3.7. In a follow-up paper [2], we discuss this and some related heuristics in more detail.

Heuristic 3.7 *Let \mathcal{O} be an ℓ -fundamental quadratic order. Consider the finite union $SS_{\mathcal{O}}$ of \mathcal{O}' -cordilleras in the oriented supersingular ℓ -isogeny graph for all $\mathcal{O}' \supseteq \mathcal{O}$. Let $d(v)$ denote the distance of a vertex v to the rim of its volcano. Let $j(v)$ denote its j -invariant. Define:*

- $R_{\mathcal{V}}$, the number of edges descending from the rim of the volcano $\mathcal{V} \in SS_{\mathcal{O}}$;
- $R_{SS_{\mathcal{O}}}$, the sum of the number of edges descending from all rims in $SS_{\mathcal{O}}$.

Then for any j -invariant j_0 and any volcano $\mathcal{V} \in SS_{\mathcal{O}}$, the ratio

$$\frac{\#\{v \in \mathcal{V} : j(v) = j_0, d(v) \leq t\}}{\#\{v \in SS_{\mathcal{O}} : j(v) = j_0, d(v) \leq t\}}$$

approaches $R_{\mathcal{V}}/R_{SS_{\mathcal{O}}}$ as $t \rightarrow \infty$.

Briefly, one expects this because sufficiently long random walks from any rim vertex will visit all vertices with an asymptotically uniform distribution [29, Theorem 1]. This observation suffices to prove the case the rims are singletons; other cases should behave similarly.

The following lemma is useful for runtime analyses of our main algorithms (Propositions 8.1 and 10.1). It states that sum of the class numbers of all the orders containing \mathcal{O} (approximately the cardinality of the union of the sets $SS_{\mathcal{O}}^{pr}$ involved in $SS_{\mathcal{O}}$ in Heuristic 3.7) is only marginally bigger than just the class number $h_{\mathcal{O}}$ (approximately the size of the largest $SS_{\mathcal{O}}^{pr}$ in the union).

Lemma 3.8 *Let \mathcal{O} be an imaginary quadratic order of conductor f in some quadratic field K with class number $h_{\mathcal{O}}$, and put*

$$H_{\mathcal{O}} = \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} h_{\mathcal{O}'}, \tag{2}$$

where the sum ranges over all the quadratic orders \mathcal{O}' containing \mathcal{O} and $h_{\mathcal{O}'}$ denotes the class number of \mathcal{O}' . Then $H_{\mathcal{O}} \leq h_{\mathcal{O}} O((\log \log f)^2)$ as $f \rightarrow \infty$.

Proof Let \mathcal{O}' be a quadratic order of discriminant D' containing \mathcal{O} and $f' = [\mathcal{O}' : \mathcal{O}]$ the index of \mathcal{O} in \mathcal{O}' . Then f' divides f . By [18, Corollary 7.28], we have

$$h_{\mathcal{O}} = \frac{f' h_{\mathcal{O}'}}{w'/w} \prod_{\substack{q|f' \\ q \text{ prime}}} \left(1 - \left(\frac{D'}{q}\right) \frac{1}{q}\right),$$

where $w, w' \in \{2, 4, 6\}$ are the sizes of the unit groups of \mathcal{O} and \mathcal{O}' , respectively. Thus,

$$h_{\mathcal{O}'} \leq \frac{w'}{w f'} h_{\mathcal{O}} \prod_{\substack{q|f' \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right)^{-1} = \frac{w'}{w \varphi(f')} h_{\mathcal{O}},$$

where $\varphi(\cdot)$ denotes Euler’s phi function. It follows that

$$H_{\mathcal{O}} \leq \sum_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} \frac{w'}{w \varphi(f')} h_{\mathcal{O}} = \frac{w'}{w} \left(\sum_{f'|f} \frac{1}{\varphi(f')} \right) h_{\mathcal{O}}.$$

By [1, Exercise 3.9 (a)], we have

$$\frac{n}{\varphi(n)} < \frac{\pi^2}{6} \frac{\sigma(n)}{n}$$

for all integers $n \geq 3$, where $\sigma(\cdot)$ is the sum of divisors function. From Robin’s Theorem [46], we obtain $\sigma(n)/n < c \log \log n$ for all $n \geq 3$ and some constant c . Therefore,

$$\begin{aligned} \sum_{3 \leq f'|f} \frac{1}{\varphi(f')} &< \frac{c\pi^2}{6} \sum_{3 \leq f'|f} \frac{\log \log f'}{f'} < \frac{c\pi^2}{6} (\log \log f) \sum_{f'|f} \frac{1}{f'} \\ &= \frac{c\pi^2}{6} (\log \log f) \frac{\sigma(f)}{f} < \frac{(c\pi)^2}{6} (\log \log f)^2, \end{aligned}$$

and hence $H_{\mathcal{O}} = h_{\mathcal{O}} O((\log \log f)^2)$. □

4 Navigating the K -Oriented ℓ -Isogeny Graph

In this section, we will show how to transform a given endomorphism of a supersingular elliptic curve into a suitable orientation, and then use it to navigate the oriented ℓ -isogeny graph.

4.1 Conjugate Orientations and Orientations from Endomorphisms

Motivated by our computational goals, we replace the abstract data of an orientation with the more computational data of an endomorphism. Given an element $\theta \in \text{End}(E)$ along with its minimal polynomial $m_{\theta}(x)$, we can infer a unique $\mathbb{Z}[\theta]$ -orientation only up to conjugation. Namely, if α is a quadratic irrational root of $m_{\theta}(x)$, then we define $\iota_{\theta}(\alpha) = \theta$ and extend to a ring homomorphism. The conjugate orientation is defined by $\widehat{\iota}_{\theta}(\alpha) = \widehat{\theta}$, or equivalently, by $\widehat{\iota}_{\theta}(\overline{\alpha}) = \theta$. An example in [43, Section

3.1] demonstrates a pair of $\text{Gal}(K/\mathbb{Q})$ -conjugate K -oriented curves which are not isomorphic. In other words, given $\varphi \in \text{End}(E)$, one may be in either of two locations in the oriented ℓ -isogeny graph: (E, ι) or $(E, \widehat{\iota})$. However, locally at least, navigating from either location looks the same, in the sense of ascending/descending/horizontal edges and j -invariants.

Lemma 4.1 *The map $(E, \iota) \mapsto (E, \widehat{\iota})$ is a graph isomorphism and an involution, taking $\text{SS}_{\mathcal{O}}^{pr}$ back to itself for each \mathcal{O} . If $\varphi : (E, \iota) \rightarrow (E', \iota')$ is a K -oriented ℓ -isogeny, then $\varphi : (E, \widehat{\iota}) \rightarrow (E', \widehat{\iota}')$ is a K -oriented ℓ -isogeny, and the type (ascending, descending, or horizontal) is the same.*

Proof The map is clearly a bijection on vertices. Observe that the dual of $\widehat{\varphi} \circ \iota \circ \varphi$ is $\widehat{\varphi} \circ \widehat{\iota} \circ \varphi$. From this, it follows that the map is a graph isomorphism. The observation about type follows from the fact that $\text{SS}_{\mathcal{O}}^{pr}$ is taken back to itself. \square

As consequences of this lemma, for two vertices (E, ι) and $(E, \widehat{\iota})$, we have the following:

- (1) the j -invariant is the same at both vertices;
- (2) both vertices are at the same altitude in the volcano;
- (3) if the vertices are not at a rim, the ascending isogeny from either vertex is the same;
- (4) if the vertices are at the rim, the pair of horizontal isogenies from either vertex is the same;
- (5) given an ℓ -power isogeny originating at E , the resulting path of j -invariants does not depend on the orientation ι or $\widehat{\iota}$.

For these reasons, it will not, in practice, be necessary for us to know which of two conjugate orientations we are dealing with. Therefore, we do not make any choice between the two. In the remainder of the paper, we will not dwell on this distinction and will work with endomorphisms instead of orientations.

Remark 4.2 It is a natural question to ask when a subset of the four oriented curves (E, ι) , $(E^{(p)}, \iota^{(p)})$, $(E, \widehat{\iota})$ and $(E^{(p)}, \widehat{\iota}^{(p)})$ coincide. This question may have importance to a more detailed runtime analysis than we present in this paper, for example. It is considered in [2].

4.2 ℓ -Primitivity, ℓ -Suitability, and Direction Finding

Having associated an endomorphism to an orientation, we can now define the following.

Definition 4.3 Let $\theta \in \text{End}(E)$ be an endomorphism and α the corresponding quadratic element (up to conjugation). Then θ (as well as α) is called ℓ -primitive if the associated orientations $\iota_{\theta} : \alpha \mapsto \theta$ and $\widehat{\iota}_{\theta} : \bar{\alpha} \mapsto \theta$ are ℓ -primitive $\mathbb{Z}[\alpha]$ -orientations. Moreover, θ (as well as α) is called N -suitable, for an integer N , if α is of the form $f\omega + kN$ where k is some integer, f is the conductor of $\mathbb{Z}[\alpha]$, and $f\omega$ is the generator of $\mathbb{Z}[\alpha]$ as described in the conventions of Sect. 2.1.

The purpose of this definition is made clear by the following lemma.

Lemma 4.4 *If $\theta \in \text{End}(E)$ is ℓ -suitable, then θ is not ℓ -primitive if and only if $\theta/\ell \in \text{End}(E)$.*

Proof The endomorphism θ is not ℓ -primitive if and only if there exists a (unique) order $\mathcal{O}' \subseteq \text{End}(E)$ of index $\ell = [\mathcal{O}' : \mathbb{Z}[\theta]]$. But this happens if and only if $\theta/\ell \in \text{End}(E)$, since under the ℓ -suitability hypothesis, $\mathbb{Z}[\theta/\ell]$ is precisely this order \mathcal{O}' . \square

Lemma 4.5 *Let $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ with trace t . Let f be the conductor and Δ_K the fundamental discriminant of $\mathbb{Z}[\alpha]$. Then*

$$\{T \in \mathbb{Z} : \alpha + T \text{ is } N\text{-suitable}\} = \begin{cases} \frac{f-t}{2} + N\mathbb{Z} & \text{if } \Delta_K \equiv 1 \pmod{4} \\ \frac{f-t}{2} + N\mathbb{Z} & \text{if } \Delta_K \equiv 0 \pmod{4} \end{cases}.$$

In our algorithms, we sometimes choose an optimal T in the sense of the following definition.

Definition 4.6 *If $\alpha + T$ has the smallest possible non-negative trace amongst all N -suitable translates of α , we say that $\alpha + T$ is a minimal N -suitable translate.*

Knowing just one suitable endomorphism θ on an elliptic curve E , we can determine the type (ascending, descending or horizontal) of isogenies originating at (E, ι_θ) .

Proposition 4.7 *Suppose $\psi : E \rightarrow E'$ is an ℓ -isogeny and $\theta \in \text{End}(E)$ is an ℓ -suitable ℓ -primitive endomorphism. Then, with regards to the orientation ι_θ induced by θ ,*

- (1) ψ is ascending if and only if $[\ell]^2 \mid \psi \circ \theta \circ \widehat{\psi}$ in $\text{End}(E')$.
- (2) ψ is horizontal if and only if $[\ell] \mid \psi \circ \theta \circ \widehat{\psi}$ but $[\ell]^2 \nmid \psi \circ \theta \circ \widehat{\psi}$ in $\text{End}(E')$.
- (3) ψ is descending if and only if $[\ell] \nmid \psi \circ \theta \circ \widehat{\psi}$ in $\text{End}(E')$.

Proof Let ι_θ be the orientation on E associated to θ . Let ι' be the induced orientation on E' by ι_θ via ψ . Let $\mathcal{O}, \mathcal{O}' \subseteq K$ be two orders such that ι_θ is \mathcal{O} -primitive and ι' is \mathcal{O}' -primitive. The three cases in the proposition correspond to the cases when $\mathcal{O} \subsetneq \mathcal{O}'$, $\mathcal{O} = \mathcal{O}'$ and $\mathcal{O} \supsetneq \mathcal{O}'$, respectively. Therefore, ψ is ascending, horizontal and descending correspondingly. \square

The previous proposition demonstrates that it is enough to check the action of $\psi \circ \theta \circ \widehat{\psi}$ on $E[\ell]$ to determine whether ψ is ascending, horizontal or descending. However, we can also write down the ascending or horizontal endomorphisms directly by analysing the eigenspaces of θ on $E[\ell]$, as follows. Note that a version of this for Frobenius is used in CSIDH [8] to walk horizontally, earlier used in [33, Section 3.2] and [23, Section 2.3].

Proposition 4.8 *Suppose $\theta \in \text{End}(E)$ is ℓ -suitable and ℓ -primitive. For each $P \in E[\ell]$ of order ℓ let ψ_P denote the degree ℓ quotient isogeny induced by $\langle P \rangle$. Let $\lambda_1, \lambda_2 \in \mathbb{F}_{\ell^2}$ be the eigenvalues of θ acting on $E[\ell]$. Consider the oriented curve (E, ι_θ) .*

- (1) *If $\lambda_1, \lambda_2 \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, then all ψ_P 's are descending.*

(2) If $\lambda_1, \lambda_2 \in \mathbb{F}_\ell$, and

- (2a) $\lambda_1 = \lambda_2 = 0$, then there is a unique eigenspace $\langle Q \rangle$ and that gives rise to an ascending isogeny ψ_Q ; the other ψ_P 's are descending.
- (2b) $\lambda_1 = \lambda_2 \neq 0$, then there is a unique eigenspace $\langle Q \rangle$ and that gives rise to a horizontal isogeny ψ_Q ; the other ψ_P 's are descending.
- (2c) $\lambda_1 \neq \lambda_2$, then there are two eigenspaces $\langle Q_1 \rangle, \langle Q_2 \rangle$ that correspond to λ_1, λ_2 respectively. The two isogenies ψ_{Q_1}, ψ_{Q_2} are horizontal, and the other ψ_P 's are descending.

Proof Suppose $\alpha \mapsto \theta$ gives a K -orientation of E , for $K = \mathbb{Q}(\alpha)$. Define \mathcal{O} to be $\mathbb{Z}[\alpha]$. Let $f(x) \in \mathbb{Z}[x]$ denote the minimal polynomial of α over \mathbb{Q} , then $f(x) \pmod{\ell}$ is the characteristic polynomial of the action of θ on $E[\ell]$. From this one can show that Case (2a) appears if and only if α is divisible by ℓ as an algebraic integer. Since α is ℓ -suitable, this is equivalent to \mathcal{O} being non-maximal at ℓ . Therefore we divide the proof into two cases. In both cases, the statements on the number of descending isogenies follow from the volcano structure as described in Proposition 3.4.

Case I: \mathcal{O} is not maximal at ℓ . The eigenspace corresponds to 0 is one-dimensional as otherwise it violates the fact that α is ℓ -primitive, denote the eigenspace by $\langle Q \rangle$. Then $\langle Q \rangle = E[\mathfrak{l}]$ where $\mathfrak{l} := (\alpha, \ell)_{\mathcal{O}}$ is a non-invertible ideal in \mathcal{O} . According to [43, Proposition 3.5], the corresponding isogeny ψ_Q is ascending.

Case II: \mathcal{O} is maximal at ℓ .

- Case (1) is equivalent to ℓ being inert in K , there are only descending isogenies.
- Case (2b) is equivalent to ℓ ramifying in K . In this case, the eigenspace is again one-dimensional, we denote it by $\langle Q \rangle$. Let $\lambda := \lambda_1 = \lambda_2$, then $\langle Q \rangle = E[\mathfrak{l}]$ where $\mathfrak{l} := (\alpha - \lambda, \ell)_{\mathcal{O}}$ is an invertible ideal in \mathcal{O} . According to [43, Proposition 3.5], the corresponding isogeny ψ_Q is horizontal.
- Case (2c) is equivalent to ℓ splitting in K . In this case, there are two distinct \mathbb{F}_ℓ -eigenvalues and two eigenspaces $\langle Q_1 \rangle, \langle Q_2 \rangle$. For $i = 1$ or 2 , $\langle Q_i \rangle = E[\mathfrak{l}_i]$ where $\mathfrak{l}_i := (\alpha - \lambda_i, \ell)_{\mathcal{O}}$ are invertible ideals in \mathcal{O} . They give rise to two horizontal isogenies. □

Remark 4.9 Observe from the proposition that in order to detect which outgoing ℓ -isogeny at an oriented curve (E, θ) is ascending or horizontal, we only need to know how θ acts on $E[\ell]$. Indeed, we can formalize as follows. Let $T_\ell(E)$ have basis $P = (P_n), Q = (Q_n)$, where $P_n, Q_n \in E[\ell^n]$. Let $\theta \in \text{End}(E)$ have matrix $M_\theta = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z}_\ell)$ with respect to that basis. Let ϕ_a have kernel $\langle P_1 - [a]Q_1 \rangle$ for $0 \leq a < \ell$ and kernel $\langle Q_1 \rangle$ for $a = \infty$. We determine a basis P', Q' for the codomain $T_\ell(\phi_a(E))$ as follows: take any P' satisfying $[\ell]P' = \phi_a(P - [a]Q)$ and take $Q' = \phi_a(Q)$, in the case $a \neq \infty$. In the case $a = \infty$, we take $P' = \phi_\infty(P)$ and take Q' to be any point satisfying $[\ell]Q' = \phi_\infty(Q)$. With the setup as described above, for any ℓ -isogeny $\phi : E \rightarrow E'$, we have that $\phi = \phi_a$ for some $a \in \{0, 1, \dots, \ell - 1, \infty\}$. Furthermore, for any endomorphism $\theta \in \text{End}(E)$, with respect to bases P, Q and P' ,

Q' as described above, $\phi_a \theta \widehat{\phi}_a \in \text{End}(E')$ has ℓ -adic matrix representation

$$\begin{pmatrix} \ell & 0 \\ a & 1 \end{pmatrix} M_\theta \begin{pmatrix} 1 & 0 \\ -a & \ell \end{pmatrix} \in M_2(\mathbb{Z}_\ell) \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} M_\theta \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{Z}_\ell),$$

depending upon whether $a \neq \infty$ or $a = \infty$ respectively. Furthermore, as a consequence of Proposition 4.8,

- (1) Suppose (E, θ) is not at the rim in the oriented isogeny graph. Then, the ascending isogeny is given by ϕ_a for $a \equiv \alpha/\beta \pmod{\ell}$ (where $a = \infty$ if $\beta \equiv 0 \pmod{\ell}$).
- (2) Suppose instead that (E, θ) is at the rim. Then, the two horizontal isogenies are given by the two values of a satisfying $\beta a^2 - (\alpha - \delta)a - \gamma \equiv 0 \pmod{\ell}$, if such exist (if $\beta \equiv 0 \pmod{\ell}$, the solutions are $a = \infty$ and $a \equiv \gamma/(\delta - \alpha) \pmod{\ell}$).

These observations show that one can navigate in the oriented graph, one can perform a Waterhouse transfer (see the next section), divide by ℓ , and translate by integers, using the matrix representation. In fact, the algorithms presented in this paper for finding a path to $j = 1728$ can be adapted (using the observations just mentioned) to work for an endomorphism given as an approximate element of $T_\ell(E)$. Note that one loses precision every time one divides by ℓ , so that one’s precision limits the number of steps one can take. A situation where one may be provided with such an endomorphism is the situation of the cryptographic SIDH problem (the subject of recent attacks [7, 40]), where an unknown isogeny $\varphi : E \rightarrow E_{\text{init}}$ to a starting curve gives rise to various endomorphisms $\widehat{\varphi}\theta\varphi$ for $\theta \in \text{End}(E_{\text{init}})$ whose action on certain torsion groups is known.

5 Representing Orientations and Endomorphisms

In this section, we will introduce several ways to represent isogenies and endomorphisms and then provide functionality for each type of representation.

5.1 Representations and Functionality

We remind the reader that throughout the paper, isogenies and endomorphisms will be assumed separable unless otherwise stated (see Sect. 2.1). In this section, we discuss two types of representations of an endomorphism. The first is the most basic.

Definition 5.1 A *rationally represented isogeny* is an isogeny given by a rational map. A *rationally represented endomorphism* is an endomorphism which is rationally represented as an isogeny.

We may also represent endomorphisms of large degree (e.g. not polynomial in $\log p$) by writing them as a chain of isogenies of manageable degree.

Definition 5.2 An *isogeny chain* isogeny $\varphi : E_0 \rightarrow E_k$ is an isogeny which is given in the form of a sequence of rationally represented isogenies $(\varphi_i : E_{i-1} \rightarrow E_i)_{i=1}^k$ which compose to φ , i.e. $\varphi_k \circ \varphi_{k-1} \circ \dots \circ \varphi_2 \circ \varphi_1 = \varphi$.

Let $B > 0$. Recall that an integer is called B -smooth (or B -friable) if its largest prime factor is at most B . It is called B -powersmooth (or B -ultrafriable) if its largest prime power factor is at most B . In order to handle isogeny chain endomorphisms, we will generally *refactor* them, meaning we will replace the chain with another chain representing the same endomorphism, but whose component isogenies have coprime prime power degrees. Moreover, we also fix a powersmooth bound B for the prime power degrees. In Sect. 5.3.4, we explain our choice of B for the best algorithm runtime.

Definition 5.3 An isogeny chain whose component isogenies have coprime prime power degrees is called a *prime-power* isogeny chain. Moreover, it is called a B -powersmooth prime-power isogeny chain if its component isogenies have coprime prime power degrees at most B .

For isogenies represented in any manner, we will need the following functionality:

- (1) **Evaluation at ℓ -torsion:** Given $\theta \in \text{End}(E)$, and $P \in E[\ell]$, compute $\theta(P) \in E[\ell]$. (See Lemma 2.4.)
- (2) **ℓ -suitable translation:** Given $\theta \in \text{End}(E)$, compute $\theta + [t] \in \text{End}(E)$, for some $t \in \mathbb{Z}$, so that $\theta + [t]$ is ℓ -suitable (Definition 4.3) and again separable. (See Lemma 2.7 for rational representations and Algorithm 5.3 for isogeny chains.) Note that for powersmooth prime power isogeny chains, by computing an ℓ -suitable translation, we always mean that we compute a translate that is a B -powersmooth prime power isogeny chain unless otherwise specified. This is exactly what Algorithm 5.3 does.
- (3) **Division by ℓ :** Given $\theta \in \text{End}(E)$ such that $\theta = [\ell] \circ \theta'$, compute $\theta' \in \text{End}(E)$. (See Algorithm 12.2 for rational representations and Algorithm 5.2 for isogeny chains.)
- (4) **Waterhouse transfer:** Given $\theta \in \text{End}(E)$ and $\varphi : E \rightarrow E'$ an ℓ -isogeny, compute $\varphi \circ \theta \circ \widehat{\varphi} \in \text{End}(E')$. (See Lemma 2.6 for rational representations and Algorithm 5.1 for isogeny chains.) The terminology is based on [59].

We have endeavoured to write the paper in a modular fashion, so that these two types of representations—or another unforeseen type of representation, as long as it provides these functionalities—can be used at will. In particular, we write our algorithms (Sects. 7.1 onwards) in terms of these functionalities (writing for example $\theta \leftarrow \theta/[\ell]$ for division by ℓ , to be implemented according to the endomorphism representation chosen).

Although isogeny chain endomorphisms may have large degree, we assume that for any type of endomorphism representation, **the overall degree, trace and discriminant are polynomially bounded in p** .

It can be rather involved to compute the trace of an endomorphism ([60, Lemma 1], [25, Lemma 4], [4, Theorem 3.6]); however, the manipulations we perform in our algorithms transform the trace predictably. Therefore, it is to our advantage to attach the trace data to all endomorphisms under consideration and update it as needed. For either rationally represented or isogeny chain endomorphisms, our data type will be the following.

Definition 5.4 A *traced endomorphism* is a tuple of data (E, θ, t, n) where $\theta \in \text{End}(E)$ is either rationally represented or an isogeny chain, and t and n are the reduced trace and norm (degree) of θ , respectively.

5.2 Functionality for Rationally Represented Endomorphisms

In the case of a rationally represented endomorphism, we can evaluate at ℓ -torsion directly (Lemma 2.4). We can translate by an integer by adding the rational maps under the group law (Lemma 2.7). We can Waterhouse transfer by composing the maps (Lemma 2.6). However, division by ℓ requires a dedicated algorithm. In Sect. 12, we describe the algorithm of McMurdy [42] for exactly this purpose, and analyse its runtime in greater detail. For the completeness of this section, we record here that the runtime of dividing an isogeny $\varphi : E \rightarrow E'$ of supersingular elliptic curves defined over \mathbb{F}_{p^2} (Algorithm 12.2) is $O(\deg^2(\varphi)\mathbf{M}(p))$.

5.3 Functionality for Isogeny Chain Endomorphisms

An isogeny chain representation of an endomorphism can be more space efficient than its rational representation, and more efficient to compute with. Computing the Waterhouse transfer of an isogeny chain endomorphism is essentially trivial: include the transfer isogenies in the chain. To evaluate at ℓ -torsion, we evaluate the sequence of maps one-by-one (Lemma 2.4); the runtime depends polynomially on the largest degree of their component isogenies.

In this section, we give algorithms for the more onerous tasks of division-by- ℓ and translation by integers. Their runtimes will depend polynomially on the largest prime power appearing in the degree of the endomorphism, which must therefore be kept small for efficiency. To address this problem, which arises when translating to something ℓ -suitable, we use a search step to find a translate of powersmooth degree.

In order to keep the largest prime power in the degree below a certain bound, we will be interested in B -powersmooth prime power isogeny chains. In the last subsection of this section, we balance the runtime considerations by choosing a subexponential powersmoothness bound B for the degree of an isogeny chain endomorphism. Thus, working with a general such endomorphism is a subexponential endeavour.

Although our concern is with endomorphisms, both Algorithm 5.1 and Algorithm 5.2 work for isogenies in general.

5.3.1 Refactoring into an Isogeny Chain

If an endomorphism is not in the prime power isogeny chain form, we can refactor it. To achieve this, one factors the degree, then builds the new chain from scratch kernel-by-kernel, as described in Algorithm 5.1. In fact, any endomorphism that can be evaluated at arbitrary points on the curve can be converted to an isogeny chain representation using this algorithm.

Remark 5.5 In principle, it is possible to refactor into degrees that are primes as opposed to prime powers. However, this doesn't circumvent the need for powersmooth-

ness (in practice, it would provide some savings, e.g. in Vélu’s formulas, but it wouldn’t avoid the overall polynomial dependence on the powersmoothness bound). During refactoring, for any prime power factor q^k of the degree, the endomorphism needs to be evaluated on the q^k -torsion, which should therefore be defined over a field of manageable size. See [10, Section 5.2.1] for a nice discussion of this issue in another context.

Algorithm 5.1: Refactoring into an isogeny chain

Input: A traced endomorphism (E, θ, t, n) in any form in which it can be evaluated (such as rationally represented or a translation of an isogeny chain), of degree coprime to p .

Output: The same traced endomorphism $(E, \theta, t, n) \in \text{End}(E)$ in prime-power isogeny chain form.

- 1 $H \leftarrow []$
 - 2 $E_0 \leftarrow E$
 - 3 Write $n = \prod_{j=0}^u q_j^{k_j}$ by factoring.
 - 4 **For** $j = 0, \dots, u$ **do**
 - 5 Compute a basis for $E[q_j^{k_j}]$.
 - 6 Compute $G_j = \ker(\theta) \cap E[q_j^{k_j}]$ by evaluating θ on $E[q_j^{k_j}]$.
 - 7 Compute a rationally represented isogeny $\varphi_j : E_j \rightarrow E_{j+1}$ given by the kernel $\varphi_{j-1} \circ \dots \circ \varphi_0(G_j)$, using Velu’s formulas.
 - 8 Append $(\varphi_j : E_j \rightarrow E_{j+1})$ to H .
 - 9 **Return** (E, θ, t, n) where θ is given by the isogeny chain H .
-

Proposition 5.6 *Let B be the largest prime power dividing $\deg \theta$. Then Algorithm 5.1 is correct and has runtime $O(\log \deg \theta)$ times the maximum of the following three runtimes: $O(B^4(\log p)\mathbf{M}(p^{B^2}))$, $O(B^2(\log B)\mathbf{M}(p^{B^2}))$ and the runtime of evaluation of θ on $O(B)$ -torsion. The space requirement of Algorithm 5.1 is $O(B^2 \log p)$. In particular, if θ is an integer translate of an isogeny chain with B -powersmooth degree, then the runtime is $O((\log \deg \theta)B^4(\log p)\mathbf{M}(p^{B^2}))$.*

Proof The **For** loop builds an isogeny chain for θ . One can see this by induction: assuming $\theta = v' \circ v$ where $v := \varphi_{j-1} \circ \dots \circ \varphi_0$, we have by construction that $v(G_j)$ vanishes under v' . Hence θ factors through $\varphi_j \circ v$.

To write the factorization of n is at worst $O(B \log^2 B)$ in time (by trial division), but $O(\log n)$ in space. For each prime power factor (so at most $\log n$ times), we must do each of the following: (i) Compute a basis for the torsion subgroup in time $O(B^4 \log p \mathbf{M}(p^{B^2}))$ and space $O(B^2 \log p)$ by Lemma 2.3. (ii) Evaluate θ on the basis (iii) List the elements of the kernel G_j ; this involves computing all linear combinations of the basis images and recording those combinations which vanish; and then computing the corresponding linear combinations of the original torsion points, a total of $B^2 + B$ linear combinations; by Lemma 2.1, this takes time $O(B^2(\log B)\mathbf{M}(p^{B^2}))$. (iv) Apply Vélu’s formulas in time $O(B\mathbf{M}(p^{B^2}))$ by Lemma 2.5. Writing down the resulting isogeny takes $O(B)$ coefficients in a subfield of $\mathbb{F}_{p^{12}}$ (Lemma 2.2), hence we use $O(B \log p)$ space for each isogeny of the chain.

If θ is a translate of an isogeny chain whose component degrees are bounded by B , we can further estimate the time taken to evaluate θ on the torsion basis. This involves one evaluation for each component isogeny (at most $\log n$ such). Each evaluation of a component φ_i takes time $O((\deg \varphi_i)\mathbf{M}(p^{B^2}))$ by Lemma 2.4. (Evaluation of the integer translation is of smaller runtime by Lemma 2.1; since the integer is taken modulo the torsion, its size is irrelevant.) \square

Remark 5.7 The exponent of the dependence on B can surely be improved here; for example, if $\deg \theta$ is prime, then our bound on the number of linear combinations on which to evaluate θ is a substantial overestimate.

5.3.2 Division by ℓ

In this section, we demonstrate in Algorithm 5.2 how to divide an isogeny chain endomorphism by $[\ell]$.

Algorithm 5.2: Dividing-by- $[\ell]$ for an endomorphism given as a prime-power isogeny chain.

Input: A traced endomorphism (E, θ, t, n) in prime-power isogeny chain form, such that $\theta(E[\ell]) = \{O_E\}$.

Output: A traced endomorphism $(E, \theta', t', n') \in \text{End}(E)$ such that $\theta = [\ell] \circ \theta'$, in prime-power isogeny chain form.

- 1 $i \leftarrow$ the index at which the chain has ℓ -power degree.
 - 2 Modify the chain for θ by replacing φ_i with $\varphi_i/[\ell]$ using Algorithm 12.2.
 - 3 $t \leftarrow t/\ell$
 - 4 $n \leftarrow n/\ell^2$.
 - 5 **Return** (E, θ, t, n) .
-

Proposition 5.8 *Let B be an upper bound on the degrees of the prime powers in θ . Then Algorithm 5.2 is correct and runs in time $O(B^2 \text{poly}(\log p))$.*

Proof The runtime is negligible except for the call to Algorithm 12.2. By Proposition 12.6, that algorithm runs in time $O(\deg^2(\varphi_i)\mathbf{M}(p))$ (and we bound $\mathbf{M}(p)$ by $\text{poly}(\log p)$ as discussed in Sect. 2.1). \square

5.3.3 Finding a B -Powersmooth ℓ -Suitable Translate

As discussed earlier, we wish to keep the powersmoothness bound B on the degree of an isogeny chain endomorphism low when translating by an integer. Since our goal is to find ℓ -suitable endomorphisms, and translation by ℓ preserves ℓ -suitability, we may search amongst nearby translates for one which is B -powersmooth for our desired bound B . This is done in Algorithm 5.3.

Proposition 5.9 *Algorithm 5.3 is correct, and the runtime is that of Algorithm 5.1 plus the time taken for Step 2.*

Proof The ℓ -suitability of the output is guaranteed by Lemma 4.5. \square

Algorithm 5.3: Computing a B -powersmooth ℓ -suitable translate in prime-power isogeny-chain form.

Input: A traced endomorphism (E, θ, t, n) in prime-power isogeny chain form, and a powersmoothness bound B (where $B = \infty$ is acceptable).

Output: A traced endomorphism (E, θ', t', n') which satisfies $\mathbb{Z}[\theta'] = \mathbb{Z}[\theta]$ but where θ' is ℓ -suitable, and is given as a separable prime-power isogeny chain, with prime powers $\leq B$.

- 1 Compute the minimal ℓ -suitable translate T for θ (Lemma 4.5).
 - 2 Try values $n(b) = n + (T + b\ell)t + (T + b\ell)^2$ for small integers b , to find b such that $n(b)$ is B -powersmooth and coprime to p .
 - 3 $\theta' \leftarrow$ a refactored prime-power isogeny chain for $\theta + T + b\ell$, using Algorithm 5.1.
 - 4 $t' \leftarrow t + 2T + 2b\ell$
 - 5 $n' \leftarrow n + (T + b\ell)t + (T + b\ell)^2$.
 - 6 **Return** (E, θ', t', n')
-

5.3.4 Choosing a Powersmoothness Bound B

In practice, we need to balance the runtimes of the various functionalities of an isogeny chain endomorphism by choosing an appropriate powersmoothness bound B .

The number of B -smooth and B -powersmooth numbers below a bound X is asymptotically the same, provided that $B/\log^2 X \rightarrow \infty$ [53] (another reference shows they are asymptotically proportional, provided $\log B/(\log \log X) \rightarrow \infty$ [16, Section 3.1]). In our situation, we expect to handle endomorphisms which may have degree as much as exponential in $\log p$. Fortunately, we can, at least heuristically, find subexponentially smooth translates in subexponential time [16, Section 3.1].

Heuristic 5.10 *Given integers n, t , and T , values of the function $n(b) = n + (T + b\ell)t + (T + b\ell)^2$, as $b \rightarrow \infty$, are powersmooth with the same probability as randomly chosen integers of the same size.*

This is the powersmooth analogue of the heuristic assumption underlying the quadratic sieve; see [19].

Proposition 5.11 *Assume Heuristic 5.10. Let $\theta \in \text{End}(E)$ have degree d such that $L_d(1/2) > \text{poly}(\log p)$, and assume that its trace t is polynomial in d . Then Algorithm 5.3 produces an $L_d(1/2)$ -powersmooth prime power isogeny chain of total degree $O(d)$. Furthermore, on $L_d(1/2)$ -powersmooth prime power isogeny chains of total degree $O(d)$, the maximum runtime of Algorithm 5.1, Algorithm 5.2 and Algorithm 5.3 is $L_d(1/2)$, and the output of these algorithms is again an $L_d(1/2)$ -powersmooth prime power isogeny chain of total degree $O(d)$.*

Proof We have seen that all the runtimes in Algorithms 5.1 through 5.3 are polynomial in $B, \log d$, and $\log p$, with the exception of Step 2 in Algorithm 5.3. Hence, taking $B = L_d(1/2)$, the runtime (except for this step) will be $L_d(1/2)$.

As far as Step 2, under Heuristic 5.10, we can call on [16, Section 3.1] (note that the L -notation in the reference differs from ours here). According to [16, Section 3.1], the probability that a random integer between 1 and d is B -powersmooth is $1/L_d(1/2)$. Testing values of b between 1 and $L_d(1/2)$, we do indeed have $n(b) < d$. Thus,

we expect to find a B -powersmooth integer, by Heuristic 5.10. For each b -value, to see whether $n(b)$ is B -powersmooth, we use naïve division in time $O(B \log^2 B)$. Therefore, in total, one will find $L_d(1/2)$ -powersmooth integers in time $L_d(1/2)$. In Step 5, $n' = n + O(b^2 \ell^2)$ (since $|t + 2T| \leq 1$), so the total degree of the output is $O(d)$. \square

A few important notes for the remainder of the paper: **we will assume $B = L_{\deg \theta}(1/2)$, where θ is the initial input endomorphism, when dealing with isogeny chains, and that whenever we perform an ℓ -suitable translation on an isogeny chain, we choose a B -powersmooth prime power ℓ -suitable translate.**

Example 5.12 (Computing an ℓ -suitable translation via Algorithm 5.3). We continue with our running example, computing an ℓ -suitable translate of a degree 47 endomorphism θ on the curve $E_{1728} : y^2 = x^3 - x$ for $\ell = 2$. Here θ is given as a rational map:

$$\theta(x, y) = \left(\frac{99x^{47} + 22x^{46} + \dots + 77}{x^{46} + 40x^{45} + \dots + 77}, \frac{113ix^{69} + 157ix^{68} + \dots + 63i}{x^{69} + 60x^{68} \dots + 158} y \right).$$

The traced endomorphism is $(E_{1728}, \theta, 0, 47)$. In Step 1, we compute the minimal 2-suitable translate T using Lemma 4.5. From the traced endomorphism, we compute $\Delta_\theta = t^2 - 4n = 0^2 - 4 \cdot 47 = -188$. This implies that the fundamental discriminant is -47 and the conductor is 2. Therefore, the 2-suitable translates are of the form $\theta + T$ for T in $1 + 2\mathbb{Z}$, and the minimal 2-suitable translate is obtained for $T = 1$. In Step 2, we find $b = 0$ produces $n(b) = 2^4 \cdot 3$, which is B -powersmooth for $B = 50$. In Step 3, we factor $\theta + 1$ into an isogeny chain $\theta' = \varphi_{171} \circ \varphi_{1728}$ where $\deg(\varphi_{1728}) = 16$ and $\deg(\varphi_{171}) = 3$, which requires a call to Algorithm 5.1. Here,

$$\begin{aligned} \varphi_{1728}(x, y) &= \left(\frac{x^{16} + (156i + 63)x^{15} + \dots + 56i + 36}{x^{15} + (156i + 63)x^{14} + \dots + 10i + 71}, \right. \\ &\quad \left. \frac{x^{23} + (55i + 95)x^{22} + \dots + 105i + 82}{x^{23} + (55i + 95)x^{22} + \dots + 26i + 87} y \right) \end{aligned}$$

and

$$\begin{aligned} \varphi_{171}(x, y) &= \left(\frac{x^3 + (102i + 30)x^2 + (31i + 74)x + 10i + 158}{x^2 + (102i + 30)x + 98i + 130}, \right. \\ &\quad \left. \frac{x^3 + (153i + 45)x^2 + (3i + 88)x + 102i + 108}{x^3 + (153i + 45)x^2 + (115i + 32)x + 45i + 174} y \right). \end{aligned}$$

The quantities in Steps 4 and 5 can be computed immediately from the values of t, n, T, b , and ℓ , yielding $t' = 2$ and $n' = 48$. The algorithm returns $(E_{1728}, \theta', t', n')$.

5.4 Poly-Rep Runtime

In the last two sections, we computed the runtimes of the basic operations for rationally represented and isogeny chain endomorphisms. We summarize here.

Proposition 5.13 *Suppose θ is an endomorphism whose trace t , norm n and discriminant Δ are polynomially bounded in p . If θ is rationally represented, then:*

- (1) *Evaluating at ℓ -torsion takes time $O(n \text{ poly}(\log p))$ (Lemma 2.4).*
- (2) *Waterhouse transfer by an ℓ -isogeny takes time $O(n \text{ poly}(\log p))$ (Lemma 2.6).*
- (3) *Dividing by ℓ takes time $O(n^2 \text{ poly}(\log p))$ (Proposition 12.6).*
- (4) *Computing an ℓ -suitable translate takes time $\tilde{O}(\max\{n, t^2\} \text{ poly}(\log p))$ (Lemma 2.7).*

If θ of degree d is represented as a B -powersmooth prime power isogeny chain with $B = L_d(1/2)$ as described in Sect. 5.3.4, then, assuming Heuristic 5.10 (see Proposition 5.11):

- (1) *Evaluating at ℓ -torsion takes time $L_d(1/2)$ (Lemma 2.4).*
- (2) *Waterhouse transfer takes time $L_d(1/2)$ (Proposition 5.6).*
- (3) *Dividing by ℓ takes time $L_d(1/2)$ (Proposition 5.8).*
- (4) *Computing a B -powersmooth ℓ -suitable translate takes time $L_d(1/2)$ (Proposition 5.9).*

Of course, in individual situations, these runtimes may be much lower (for example, dividing an isogeny chain by $[\ell]$ may depend only on the power of ℓ if no refactoring is necessary).

In the following algorithms, we will need to call all of these operations many times. It will be convenient to set the following definition.

Definition 5.14 We define the *representation runtime* of a given representation (rationally represented or isogeny chain) to be the maximum runtime of implementing the following operations: evaluating at ℓ -torsion, ℓ -suitable translation, division-by- ℓ , and Waterhouse transfer by an ℓ -isogeny. We say that an algorithm has *poly-rep runtime* if its runtime is bounded above by a constant power of $\log p$ times the relevant representation runtime.

Note that our definition above means that, **throughout the paper** $\text{poly}(\log p) \leq \text{poly-rep}$.

6 Orientation-Finding for $j = 1728$

For many cryptographic applications, a supersingular elliptic curve with known endomorphism ring is assumed. Most commonly used is the curve with $j = 1728$, which is supersingular when $p \equiv 3 \pmod{4}$. For simplicity, this is the curve we will consider here, but our algorithm can be modified to suit other situations (see Sect. 6.3). We will use the model given by $E_{\text{init}} : y^2 = x^3 - x$, which has endomorphism ring with a \mathbb{Z} -basis

$$\left\langle 1, \mathbf{i}, \frac{\mathbf{i} + \mathbf{k}}{2}, \frac{1 + \mathbf{j}}{2} \right\rangle, \quad \mathbf{i}^2 = -1, \quad \mathbf{j}^2 = -p, \quad \mathbf{k} = \mathbf{ij}.$$

In particular, \mathbf{i} is given by $(x, y) \mapsto (-x, \sqrt{-1}y)$ and \mathbf{j} is the Frobenius endomorphism² $(x, y) \mapsto (x^p, y^p)$.

Let \mathcal{O} be an imaginary quadratic order of conductor coprime to ℓ such that \mathcal{O} embeds into $B_{p,\infty}$. In this section we give an algorithm for finding an endomorphism $\theta \in \text{End}(E_{\text{init}})$, generating a suborder $\mathcal{O}' \subseteq \mathcal{O}$ of discriminant $\ell^{2r} \Delta_{\mathcal{O}}$ for the minimal possible r . In other words, we wish to find an ℓ -primitive orientation by a suborder \mathcal{O}' of \mathcal{O} . Or, rephrased again, we want to find an orientation for E_{init} placing it as near to the rim as possible in the oriented supersingular isogeny graph cordillera with rims at \mathcal{O} . Alternatively, the algorithm can be run continuously, to return all ℓ -primitive orientations by suborders of \mathcal{O} in order of increasing r .

The algorithm we provide (Algorithm 6.1) has similarities to [35, Integer Representation, Section 3.2], where the difference arises because we seek a given discriminant instead of a given norm. In fact, this algorithm applies more generally to curves over \mathbb{F}_p satisfying the hypotheses of [35, Section 3.2]; in Sect. 6.3 we make some comments on adapting this algorithm for other initial curves of known endomorphism ring.

An algorithm for a similar problem appears in [60, Section 4.3]. However, that algorithm finds the ‘smallest’ quadratic order only: it requires the discriminant be bounded above by $2\sqrt{p} - 1$. We wish to find orientations by more general orders.

6.1 In Terms of $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$

The goal of Algorithm 6.1 is to find such an endomorphism as a linear combination of $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$.

The idea is to solve a norm equation for E_{init} under extra conditions that guarantee that the result is an element of the desired quadratic order. The algorithm depends on Cornacchia’s algorithm, which is discussed in [14, Section 1.5.2] and [28, Section 3.1]. It solves the equation $x^2 + y^2 = n$ when a square root of -1 modulo n is known (e.g., such a square root can be found if n is factored).

Remark 6.1 Algorithm 6.1 can be adapted to run continuously, finding many K -orientations of 1728. Simply continue the loops instead of breaking out of them, returning an endomorphism θ every time one is found.

Remark 6.2 If one wishes to find *all* possible solutions, remove the requirements that D be a prime congruent to 1 (mod 4), although this will adversely affect runtime (Cornacchia’s algorithm will require factoring D). Furthermore, we must make sure Cornacchia’s algorithm returns *all* solutions, and we must include solutions obtained by changing the sign of x on each solution already obtained. We must also be aware that some of the solutions obtained by continuously running Cornacchia’s algorithm may

² Note that some papers use the model $y^2 = x^3 + x$, such as [25, Section 5.1]; this model is a quartic twist of ours and under the induced isomorphism of the endomorphism rings, the element which is realized as Frobenius is not preserved. The model we choose for this paper has 2-torsion conveniently defined over \mathbb{F}_p . See [52].

Algorithm 6.1: Computing an orientation for the initial curve.

```

Input: A discriminant  $\Delta_{\mathcal{O}}$  coprime to  $p$ , which is the discriminant of an  $\ell$ -fundamental quadratic order  $\mathcal{O}$  that embeds into  $B_{p,\infty}$ .
Output:  $(\theta, r)$  where  $\theta \in \text{End}(E_{\text{init}})$  is represented as a linear combination of  $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ , with  $\mathbb{Z}[\theta] = \mathcal{O}' \subseteq \mathcal{O}$  where  $[\mathcal{O} : \mathcal{O}'] = \ell^r$ . Furthermore,  $\theta$  is  $\ell$ -primitive. (Here  $E_{\text{init}}$  and  $\mathbf{i}, \mathbf{j}$  and  $\mathbf{k}$  are as in the introduction to this section, namely the specified model of  $j = 1728$ .)

1  $r \leftarrow -1$ .
2 repeat
3    $r \leftarrow r + 1$ .
4   Find the smallest positive  $x$  such that  $x^2 \equiv -\Delta_{\mathcal{O}}\ell^{2r} \pmod{p}$ .
5   While  $x < \sqrt{-\Delta_{\mathcal{O}}\ell^{2r}}$  do
6      $D \leftarrow (-\Delta_{\mathcal{O}}\ell^{2r} - x^2)/p$ .
7     If  $D \equiv 1 \pmod{4}$  then
8       If  $D$  is prime then
9         Find a square root of  $-1$  modulo  $D$ .
10        Use the output of Step 9 and Cornacchia’s algorithm to find  $y$  and  $z$  such that  $y^2 + z^2 = D$ .
11        If  $y$  is odd then
12           $\lfloor$  Swap  $y$  and  $z$ .
13        If  $x$  is even then
14           $\lfloor \theta \leftarrow \frac{1}{2} + \frac{x}{2}\mathbf{i} + \frac{z}{2}\mathbf{j} + \frac{y}{2}\mathbf{k}$ .
15        else
16           $\lfloor \theta \leftarrow \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$ .
17        break out of the While loop
18       $x \leftarrow x + p$ 
19 until  $\theta$  is defined
20  $c \leftarrow 0$ 
21 While  $c < r$  do
22   Translate  $\theta$  to be minimally  $\ell$ -suitable (Lemma 4.5).
23   If  $\theta/\ell \in \text{End}(E_{\text{init}})$  then
24      $\lfloor \theta \leftarrow \theta/\ell$ .
25      $\lfloor c \leftarrow c + 1$ 
26   else
27     break out of the While loop
28  $r \leftarrow r - c$ 
29 Return  $(\theta$  as a linear combination,  $r)$ 

```

fail to be ℓ -primitive; these can be discarded. With these adjustments, every orientation of the form specified will eventually be found by the algorithm (not every θ , but every embedding of \mathcal{O}' into $\text{End}(E_{\text{init}})$ for all \mathcal{O}') – see the proof of Proposition 6.3 for relevant details.

Because of the primality testing step, the algorithm terminates only heuristically. We separately prove its correctness (if it returns) and then give a heuristic runtime.

In what follows, write $\Delta := \Delta_{\mathcal{O}}$ for convenience.

Proposition 6.3 Any output returned by Algorithm 6.1 is correct.

Proof We attempt to find an endomorphism θ for each fixed r increasing from $r = 0$.

If the order \mathcal{O}' of index ℓ^r in \mathcal{O} has even discriminant (namely $\Delta\ell^{2r}$), then we seek an element of reduced trace zero and reduced norm $-\Delta\ell^{2r}/4$. Such an element must generate \mathcal{O}' , and \mathcal{O}' must contain a generator of this form. Write the element as $\theta = \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$. Then, simplifying the equation, the norm condition is

$$x^2 + py^2 + pz^2 = -\Delta\ell^{2r}.$$

Any solutions must have $x^2 < \sqrt{-\Delta\ell^{2r}}$, and for a valid x , solutions y and z are found by Cornacchia’s algorithm applied to

$$y^2 + z^2 = (-\Delta\ell^{2r} - x^2)/p.$$

In order to be contained in $\text{End}(E_{\text{init}})$, we require $x \equiv z \pmod{2}$ and y is even. The variable r is incremented if no solution exists, or if Cornacchia’s algorithm is not applied because D is not a prime congruent to $1 \pmod{4}$ (in which case we may miss solutions).

If $\Delta\ell^{2r}$ is odd, we instead seek an element of reduced trace 1 and reduced norm $(-\Delta\ell^{2r} + 1)/4$. Such an element will again necessarily generate \mathcal{O}' , and \mathcal{O}' must contain a generator of this form. Writing the element as $\theta = \frac{1}{2} + \frac{x}{2}\mathbf{i} + \frac{y}{2}\mathbf{j} + \frac{z}{2}\mathbf{k}$, after slightly simplifying the norm equation, we must solve the same equation as before:

$$x^2 + py^2 + pz^2 = -\Delta\ell^{2r}.$$

However, in order to lie in $\text{End}(E_{\text{init}})$, such an element must satisfy the conditions that $x \equiv z \pmod{2}$ and y is *odd* (note the parity difference). The rest of this case is as above.

If θ is not ℓ -primitive, the algorithm will translate and divide by ℓ until it is. □

For the runtime analysis, and the assertion that the algorithm returns an output at all, we need a heuristic similar to that used for torsion-point attacks [24, Heuristic 1] and the KLPT algorithm [35, Section 3.2].

Heuristic 6.4 Fix integers $D > 0$, $b > 0$, and a prime p coprime to Db that splits in the real quadratic field $\mathbb{Q}(\sqrt{D})$. Ranging through pairs

$$\left\{ (r, x) : 0 < x, x^2 < Db^{2r}, 0 \leq r, Db^{2r} - x^2 \equiv 0 \pmod{p} \right\},$$

consider the value

$$N(r, x) = \frac{Db^{2r} - x^2}{p}.$$

The probability that $N(r, x)$ is a prime congruent to 1 modulo 4 is at least $O(1/(\log D \log N(r, x)))$, where the implied constant is independent of p , D , and b .

We now give a brief justification for this heuristic by passing to the real quadratic field $\mathbb{Q}(\sqrt{D})$. Write $D = f^2d$ where $d > 0$ is squarefree. We have $N(r, x) = q$ if and only if $\pm pq = N(x + fb^r\sqrt{d})$. Hence we need to estimate the probability, given that $N(x + fb^r\sqrt{d})$ is divisible by p , that it is of the form $\pm pq$ for some other prime q . We analyse instead the probability, for $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ (having no assumptions on the form of α), given that $N(\alpha)$ is divisible by p , that it is of the form $\pm pq$ for some prime q . Heuristically, we assume that this will be the same probability.

Given that p splits, there is a prime ideal \mathfrak{p} above p in the maximal order of $\mathbb{Q}(\sqrt{d})$. Hence $N(\alpha)$ has the form $\pm pq$ if and only if there is a prime ideal \mathfrak{q} of norm q satisfying $\mathfrak{p}\mathfrak{q} = (\alpha)$ (or $\bar{\mathfrak{p}}\mathfrak{q} = (\alpha)$). If $p \mid N(\alpha)$, then replacing \mathfrak{p} with $\bar{\mathfrak{p}}$ if necessary, this occurs if and only if the integral ideal $(\alpha)\mathfrak{p}^{-1} \in [\mathfrak{p}]^{-1}$ has norm q .

Therefore, we estimate the probability that integral elements in $[\mathfrak{p}]^{-1}$ of size X have prime norm. This is bounded below by the probability that integers of size X have a norm which is a prime represented by the class $[\mathfrak{p}]^{-1}$. This in turn is bounded below by $\frac{1}{h \log X}$ where h is the class number of $\mathbb{Q}(\sqrt{d})$. We apply this estimate with $X = N(r, x)$.

Finally, following the Cohen-Lenstra heuristics for real quadratic fields, it may be reasonable to expect the class number $h_{\mathbb{Q}(\sqrt{d})}$ to have an expected value bounded by $O(\log d)$, since the number of prime factors of d is around $\log \log d$ (see [62] for a result for prime discriminants and recall that the 2-part of the class group is controlled by the number of prime factors of d).

Heuristic 6.4 has been confirmed numerically in some small cases; we will consider this heuristic in more detail in [2]. The corresponding heuristic, in the case of the KLPT norm equation, has been verified by Wesolowski [61]; it would be nice to know if similar methods apply here.

Proposition 6.5 *Suppose Heuristic 6.4 holds and Δ is coprime to p . If $|\Delta| \leq p^{2+\epsilon}$, then Algorithm 6.1 returns a pair (θ, r) , where θ has norm bounded by $p^2 \log^{2+\epsilon}(p)$ and $r = O(\log p)$, in time $O(\log^{6+\epsilon}(p))$. Otherwise, the algorithm returns a pair (θ, r) , where θ has norm bounded by $O(|\Delta|)$ and $r = O(1)$, in time $O(\sqrt{|\Delta|} \log^{4+\epsilon}(\Delta)(\log p)p^{-1})$.*

Running the algorithm continuously, subsequent pairs (θ, r) should be found in the same runtime, with r expected to increase by 1, and their norms expected to increase by a constant factor of ℓ^2 at each subsequent pair.

Proof Suppose $r \leq u \log_\ell p$, where u is positive (otherwise r is not positive). Then $\sqrt{-\Delta \ell^{2r}} \leq |\Delta|^{1/2} p^u$. Thus, we expect to iterate the **While** loop at Step 5 at most $X(\Delta, u) := \lceil |\Delta|^{1/2} p^{u-1} \rceil + 1$ times. Each time we enter the loop, we obtain a value $D = (-\Delta \ell^{2r} - x^2)/p$ of size $\leq pX(\Delta, u)^2$. The probability that D is prime and $1 \pmod{4}$ is heuristically at least $1/(\log |\Delta| \log(p^{1/2} X(\Delta, u)))$ (Heuristic 6.4). Hence we expect to reach Cornacchia’s algorithm once u is large enough such that

$$X(\Delta, u) \geq O(\log(p^{1/2} X(\Delta, u))) \geq O(1).$$

Reaching it will terminate the algorithm. This is a mild condition, satisfied asymptotically when $X(\Delta, u) \geq (\log p)^{1+\epsilon}$. In fact, it suffices to take $\sqrt{|\Delta|} p^u \geq p \log^{1+\epsilon}(p)$, or equivalently,

$$u \log p \geq \log p - \frac{1}{2} \log |\Delta| + (1 + \epsilon) \log \log p. \quad (3)$$

In particular, $u > 1$ is always enough, and if $|\Delta| > p^{2+\epsilon}$, then any positive value for u will suffice. (An informal explanation of this behaviour: even for a volcano with a trivial rim, distance $(1 + \epsilon) \log p$ down its sides is enough to capture all j -invariants. At the same time, if Δ is large enough that the rim likely captures all j -invariants, then we needn't descend the volcano at all.) This shows that the algorithm needs to increase r at most $O(\log p)$ times before it reaches Cornacchia's algorithm.

For $|\Delta| \leq p^{2+\epsilon}$, the optimal value of u is given by (3). However, since u cannot be negative, when $|\Delta| > p^{2+\epsilon}$, the optimal value of u is 0. (Again, informally: the class group will be of size $\approx \sqrt{|\Delta|} > p$, and we will find all $\approx \frac{p}{12}$ supersingular j -invariants already on the rim of an isogeny volcano.)

We first determine the overall runtime in terms of $X(\Delta, u)$ and p . The primality test can be run in time $O(\log^{4+\epsilon} D)$ for example, using the Miller-Rabin algorithm [49, Section 2]. This algorithm is probabilistic, so there is a negligible possibility that Cornacchia's algorithm may fail on false positives.

Once D is a prime congruent to 1 (mod 4), we must find a square root of -1 with which to run Cornacchia's algorithm. There is a nice analysis of this exact situation in [28, Section 3.1], which concludes that it takes probabilistic time $\tilde{O}(\log^2 D)$, which is negligible compared to the primality testing.

Thus, for the final runtime, we increment r at most $O(\log p)$ times, running a primality test of cost $O(\log^{4+\epsilon} D)$ at most $O(X(\Delta, u))$ times for each r , before reaching a point where Cornacchia's algorithm is invoked. Using $D \leq pX(\Delta, u)^2$, this gives runtime $O(X(\Delta, u)(\log p)(\log p + 2 \log X(\Delta, u))^{4+\epsilon})$.

In the case of large $|\Delta| > p^{2+\epsilon}$, we put $u = 0$ and obtain $X(\Delta, u) = O(\sqrt{|\Delta|}/p)$ and asymptotically $X(\Delta, u) > p^\epsilon > O(\log(p^{1/2} X(\Delta, u)))$. This yields a runtime of $O(\sqrt{|\Delta|} \log^{4+\epsilon}(\Delta)(\log p)p^{-1})$. In this case $r = O(1)$ and the norm of the solution found by Cornacchia's algorithm is bounded by $O(|\Delta|)$.

In the case of small $|\Delta| \leq p^{2+\epsilon}$, we optimize u according to (3) and obtain $X(\Delta, u) = \log^{1+\epsilon}(p)$, and asymptotically $X(\Delta, u) > \log p + O(\log \log p) \geq O(\log(p^{1/2} X(\Delta, u)))$, giving runtime $O(\log^{6+\epsilon}(p))$. At the same time, the norm of the solution found is bounded by $|\Delta| \ell^{2r} \leq p^2 X(\Delta, u)^2 \leq p^2 \log^{2+2\epsilon}(p)$.

Once r has reached $O(\log p)$, we expect solutions for each r with high probability. Therefore, running the algorithm continuously, subsequent solutions should be found in the same runtime as the first, and their sizes should be increasing by an expected constant factor of ℓ^2 at each subsequent solution. \square

Example 6.6 (Computing an orientation for the initial curve via Algorithm 6.1). We return to our working example $p = 179$, $\Delta = -47$, $\ell = 2$, and $E_{1728} : y^2 = x^3 - x$. Note that $\log_\ell(p) \approx 7.48$, so we expect the algorithm to succeed reliably once $r = 7$ or 8, if not earlier. Beginning with $r = 0$, in Step 4 we compute the smallest positive x such that $x^2 \equiv 47 \pmod{179}$, namely $x = 88$. As $x = 88$ exceeds $\sqrt{47} \approx 6.9$, we return to Step 3 and increment r to $r = 1$. This reflects the fact that the curve E_{1728} does not admit a $\mathbb{Q}(\sqrt{-47})$ -orientation on the rim. Continuing, we find the smallest positive integer x such that $x^2 \equiv 188 \pmod{179}$, namely $x = 3$. As $x = 3 < \sqrt{47 \cdot 4} \approx 13.7$, we define $D = (47 \cdot 4 - 3^2)/179 = 1$ in Step 6. Cornacchia's algorithm returns

$1^2 + 0^2 = 1$. We obtain the element $\frac{3\mathbf{i}+\mathbf{k}}{2} \in \text{End}(E_{1728})$. This indicates (correctly) that E_{1728} admits an orientation at $r = 1$ of the $\mathbb{Q}(\sqrt{-47})$ -oriented 2-isogeny volcano, see the node with j -invariant 1728 in Fig. 1. If we continue to run the algorithm, looking for pairs (r, θ) for r up to 8, it returns three more pairs:

$$\begin{aligned} & \left(r = 7, \theta = \frac{371}{2}\mathbf{i} + 29\mathbf{j} + \frac{13}{2}\mathbf{k} \right), \\ & \left(r = 8, \theta = \frac{153}{2}\mathbf{i} + 27\mathbf{j} + \frac{119}{2}\mathbf{k} \right), \\ & \left(r = 8, \theta = \frac{511}{2}\mathbf{i} + 41\mathbf{j} + \frac{95}{2}\mathbf{k} \right). \end{aligned}$$

We now formalize a heuristic about the behaviour of Algorithm 6.1 needed for what follows. This is a version of Heuristic 3.7 specific to the algorithm we use.

Heuristic 6.7 *Let \mathcal{O} be a quadratic order. Let $\text{SS}_{\mathcal{O}}$ be the finite union of \mathcal{O}' -cordilleras where $\mathcal{O}' \supseteq \mathcal{O}$. Write $R_{\text{SS}_{\mathcal{O}}}$ for the sum of the number of descending edges from all rims of $\text{SS}_{\mathcal{O}}$. Fix a volcano \mathcal{V} having $R_{\mathcal{V}}$ edges descending from its rim. Then Algorithm 6.1 running continuously will (i) eventually produce solutions on every volcano of $\text{SS}_{\mathcal{O}}$, and (ii) produce solutions on the fixed volcano \mathcal{V} with probability approaching $R_{\mathcal{V}}/R_{\text{SS}_{\mathcal{O}}}$.*

If $\text{SS}_{\mathcal{O}}$ has only one volcano, this heuristic is immediate as long as the algorithm produces infinitely many solutions (which happens by Proposition 6.5, under heuristic assumptions from Sect. 3.6). If Algorithm 6.1 returned *all* orientations of 1728, then this heuristic would follow directly from Heuristic 3.7. The difficulty is that it finds only those solutions where the primality testing step succeeds. In other words, we cannot rule out the unlikely possibility that the primality condition causes all the orientations of 1728 to be missed on some individual volcano. Thus, we seem to require a version of Heuristic 6.4 which asserts that the primality is independent of whether the eventual solution is on any fixed volcano of the cordillera. We consider Heuristic 6.7 more closely in the companion paper [2].

6.2 As an Isogeny Chain Endomorphism

Since \mathbf{i} and \mathbf{j} are known endomorphisms which can be evaluated at points, any combination of these can also be evaluated at points. Therefore the output of Algorithm 6.1 can be input into Algorithm 5.3, and an ℓ -suitable isogeny chain endomorphism will result. Thus, in poly-rep time (that is, depending on B , the powersmoothness bound), we can obtain the output of Algorithm 6.1 as an isogeny chain endomorphism.

6.3 Curves Other Than $j = 1728$

Algorithm 6.1 can be adapted to work for certain curves E_{init} other than the curve with $j = 1728$. In particular, if the endomorphism ring $\text{End}(E)$ of a curve E defined over \mathbb{F}_p

is of the form $\mathcal{O} + \mathbf{j}\mathcal{O}$, where \mathbf{j} is the Frobenius endomorphism and \mathcal{O} is a quadratic order, then the adaptation of Algorithm 6.1 is clear, where we use the principal norm form of \mathcal{O} in place of $x^2 + y^2$. As before, this will reduce to Cornacchia's algorithm. Instead of primes that are $1 \pmod{4}$, we seek primes that split in the field and are coprime to the conductor of \mathcal{O} ; this requires a Legendre symbol computation. The runtime is essentially unchanged provided that $\Delta_{\mathcal{O}} < p$ (so Cornacchia's algorithm applies; see [28, Section 3.1]). This adaptation follows the discussion in [35, Section 3.2], which also discusses good choices for E_{init} and \mathcal{O} .

7 Supporting Algorithms for Walking on Oriented Curves

Given a suitable endomorphism, we will present algorithms for walking on an oriented ℓ -isogeny graph.

7.1 Computing an ℓ -Primitive Endomorphism

Recall from Definition 4.3 that an endomorphism θ is ℓ -primitive if the associated orientation is ℓ -primitive. If θ is chosen to be ℓ -suitable, then equivalently, θ is ℓ -primitive if and only if it is not divisible by $[\ell]$ in $\text{End}(E)$ (Lemma 4.4). Therefore, given θ , we can translate it to become ℓ -suitable and then divide by $[\ell]$ as often as possible to obtain an ℓ -primitive endomorphism.

Algorithm 7.1: Computing an ℓ -primitive endomorphism given an endomorphism.

Input: A traced endomorphism (E, θ, t, n) providing the functionality of Section 5.1.

Output: A traced endomorphism (E, θ', t', n') which is ℓ -primitive, and the ℓ -valuation of the index $[\mathbb{Z}[\theta'] : \mathbb{Z}[\theta]]$.

```

1 If  $t^2 - 4n$  is  $\ell$ -fundamental then
2   | Return  $(E, \theta, t, n)$  and 0.
3  $(E, \theta, t, n) \leftarrow$  an  $\ell$ -suitable translate of  $(E, \theta, t, n)$ 
4  $c \leftarrow 0$ 
5 While  $[\ell] \mid \theta$  do
6   |  $(E, \theta, t, n) \leftarrow (E, \theta/[\ell], t/\ell, n/\ell^2)$ 
7   |  $c \leftarrow c + 1$ 
8   | If  $t^2 - 4n$  is  $\ell$ -fundamental then
9     | | Return  $(E, \theta, t, n)$  and  $c$ .
10  |  $(E, \theta, t, n) \leftarrow$  an  $\ell$ -suitable translate of  $(E, \theta, t, n)$ 
11 Return  $(E, \theta, t, n)$  and  $c$ .
```

Proposition 7.1 *Algorithm 7.1 is correct, and runs in poly-rep time (see Definition 5.14).*

Proof If $t^2 - 4n$ is ℓ -fundamental, then the conductor of the quadratic order generated by θ is not divisible by ℓ ; in this case θ is already ℓ -primitive. In order to check if any order of superindex ℓ contains $\mathbb{Z}[\theta]$ within $\text{End}(E)$, we first translate θ to be ℓ -suitable,

and then check whether it is divisible by $[\ell]$ within $\text{End}(E)$. If it is, we divide it by ℓ and repeat.

For runtime, the algorithm translates to an ℓ -suitable translate, tests for divisibility by ℓ , and divides by ℓ , at most a polynomial number of times (since we assume that the discriminant of $\mathbb{Z}[\theta]$ is bounded by a power of p ; see Sect. 5.1). \square

Example 7.2 (Computing an ℓ -primitive endomorphism via Algorithm 7.1). We apply Algorithm 7.1 to the output of Example 5.12, namely $(E_{1728}, \theta', t', n')$ where $\theta' = \varphi_{171} \circ \varphi_{1728}$, $t' = 2$, $n' = 48$. This is not at the rim, but is already ℓ -suitable. We find $[2] \nmid \theta'$ by evaluating on $E_{1728}[2]$; hence we return the input unchanged.

7.2 Rim Walking via the Class Group Action

In the case that an orientation is available, one can walk the rim of the oriented ℓ -isogeny volcano using the class group action. Using the class group action to walk an isogeny graph of elliptic curves was first introduced by [17] and [47], followed by work of Bröker-Charles-Lauter [6]. These papers consider the case of ordinary elliptic curves, which carry an orientation by Frobenius. This was later used in CSIDH [8], and it was remarked that it extends to orientations by $\mathbb{Q}(\sqrt{-np})$ in Chenu-Smith [11]. In this section we provide a generalization of the same algorithm to arbitrary orientations. The algorithm walks the rim from a specified start curve in an arbitrary direction until it encounters a specified end curve. This path is computed using the action of the class group on the oriented curves in the rim of the oriented volcano. As such, it requires knowledge of the orientation, so the steps of the algorithm must pull the orientation (i.e. the endomorphism) along with them.

More precisely, the ideal we wish to apply to (E, θ) is given in terms of θ , so that one can use the methods of Bröker-Charles-Lauter [6, Section 3] with θ in place of Frobenius. One can apply the Waterhouse transfer of θ , and divide by ℓ to carry along θ in the computation.

The algorithm works by applying the action of $\text{Cl}(\mathcal{O})$ to a rim of elements primitively oriented by a quadratic order \mathcal{O} . In fact, using $\text{Cl}(\mathcal{O})$ works just as well if the rim is primitively oriented by $\mathcal{O}' \supseteq \mathcal{O}$, where $\ell \nmid [\mathcal{O}' : \mathcal{O}]$. This allows us to walk on any rim associated to an ℓ -fundamental discriminant Δ , without knowing for sure that the orientation is primitive with respect to Δ . See Proposition 3.3.

Calling Algorithm 7.2 without lines 4 and 5 on identical input curves (i.e. $(E_1, t_1) = (E_2, t_2)$) yields the entire rim of the ℓ -oriented isogeny graph.

Proposition 7.3 *Algorithm 7.2 is correct. Each step of the rim walk has poly- rep runtime. The number of steps is bounded $O(h_{\mathcal{O}})$. Furthermore, if θ is in prime power isogeny chain form with any powersmoothness bound B , then each step of the rim walk has runtime polynomial in B .*

Proof If $\ell \mid t^2 - 4n$, then either we are not at the rim, or the field discriminant is not coprime to ℓ . If $j(E_1) = j(E_2)$, we have already completed our task. Assuming neither of those cases, we compute the quadratic order \mathcal{O} generated by θ using its minimal polynomial, and associate an element α_{θ} to θ . The volcano rim in question is contained in $\text{SS}_{\mathcal{O}'}$ for some $\mathcal{O}' \supseteq \mathcal{O}$, where the relative index $f = [\mathcal{O}' : \mathcal{O}]$ is coprime

Algorithm 7.2: Walking along the rim of the oriented supersingular ℓ -isogeny graph

Input: An ℓ -primitive traced endomorphism $(E_1, \theta_1, t_1, n_1)$ providing the functionality of Section 5.1, and a target curve E_2 .

Output: If E_1 and E_2 are on the same volcano rim in the oriented isogeny graph for the field $\mathbb{Q}(\theta)$, with discriminant coprime to ℓ , the algorithm returns a path of oriented horizontal ℓ -isogenies from $(E_1, \theta_1, t_1, n_1)$ to a vertex with curve E_2 . Otherwise returns FAILURE.

```

1 If  $\ell \mid t^2 - 4n$  then
2   | Return FAILURE.
3  $H \leftarrow []$ .
4 If  $j(E_1) = j(E_2)$  then
5   | Return  $H$ .
6 Compute  $\mathcal{O} \cong \mathbb{Z}[\theta_1]$ , the quadratic order generated by  $\theta_1$  (using trace and norm), together with an
   explicit isomorphism given in the form of  $\alpha_{\theta_1} \in \mathcal{O}$  corresponding to  $\theta_1$ .
7 If  $\ell$  is inert in  $\mathcal{O}$  then
8   | Return FAILURE.
9 Compute  $\tau \in \mathcal{O}$  such that  $\mathfrak{l} = (\ell, \tau)_{\mathcal{O}}$  is a prime ideal of  $\mathcal{O}$  above  $\ell$ .
10 Compute  $a, b \in \mathbb{Z}$  so that  $\tau = a + b\alpha_{\theta_1}$ .
11  $(E, \theta, t, n) \leftarrow (E_1, \theta_1, t_1, n_1)$ .
12 repeat
13   | Compute  $E[\ell]$ .
14   | Compute  $E[\mathfrak{l}] \leftarrow E[\ell] \cap \ker(a + b\theta)$  by evaluating  $a + b\theta$  on  $E[\ell]$ .
15   | Use Vélu's algorithm to compute the  $\ell$ -isogeny  $v : E \rightarrow E'$  with kernel  $E[\mathfrak{l}]$ .
16   |  $(E, \theta, t, n) \leftarrow (E', v \circ \theta \circ \widehat{v}, t\ell, n\ell^2)$ .
17   |  $(E, \theta, t, n) \leftarrow (E, \theta/\ell, t/\ell, n/\ell^2)$ .
18   | Append  $(v, (E, \theta, t, n))$  to  $H$ .
19 until  $(j(E), \theta, t, n) = (j(E_1), \theta_1, t_1, n_1)$  or  $j(E) = j(E_2)$ 
20 If  $j(E) = j(E_2)$  then
21   | Return  $H$ 
22 else
23   | Return FAILURE

```

to ℓ (by ℓ -primitivity). If ℓ is inert in \mathcal{O} , then it is also inert in \mathcal{O}' . Hence the rim of the associated volcano is trivial; since $j(E_1) \neq j(E_2)$, this indicates there is no valid path to be found. Otherwise, ℓ is split or ramified in \mathcal{O} , so we factor it and compute a and b and τ as in the algorithm. Namely, we have the factorization $\ell\mathcal{O} = (\ell, \tau)_{\mathcal{O}}(\ell, \bar{\tau})_{\mathcal{O}}$ in \mathcal{O} . Then $\ell\mathcal{O}' = (\ell, \tau)_{\mathcal{O}'}(\ell, \bar{\tau})_{\mathcal{O}'}$ in \mathcal{O}' . Therefore, the isogeny computed is the action of the ideal \mathfrak{l} lying above ℓ in \mathcal{O}' on $\text{SS}_{\mathcal{O}}$ as desired, which is thus a horizontal isogeny. The **repeat** clause walks the rim step by step.

We stop if we meet E_2 or return to our (oriented) starting point. The latter occurs only if we have walked the entire rim, which means E_2 was not on that rim.

For runtime, all individual steps are polynomial, except for calls to evaluate at ℓ -torsion points, Waterhouse transfer and divide by ℓ . The number of repeats is equal to the path length from E_1 to E_2 along the rim. The size of the rim is $O(h_{\mathcal{O}})$ (Sect. 3.4).

For the final statement of the proposition, note that no ℓ -suitable translation is needed in the algorithm. In fact, the norm of the endomorphism remains constant as one walks the rim. \square

Example 7.4 (Walking along the rim of the oriented supersingular ℓ -isogeny graph via Algorithm 7.2). As before, we have $K = \mathbb{Q}(\sqrt{-47})$. We use Algorithm 7.2 on input $\ell = 2, (E_{22}, \theta_{22}, t_{22}, n_{22})$ and target curve E_{22} to compute the entire rim of the oriented 2-isogeny volcano for purposes of demonstration. The endomorphism θ_{22} is a primitive \mathcal{O}_K -orientation, so the curve E_{22} lies on the rim of an \mathcal{O}_K -oriented isogeny volcano. Step 9 computes the prime ideal $\mathfrak{l} = (2, \omega)_{\mathcal{O}_K}$. In Step 13, we compute $E_{22}[2] = \{\mathcal{O}_{E_{22}}, (2, 0), (156i + 178, 0), (23i + 178, 0)\}$. We obtain $E_{22}[\mathfrak{l}] = \langle (156i + 178, 0) \rangle$ in Step 14. Velu’s formulas in Step 15 compute the isogeny $\varphi_{22} : E_{22} \rightarrow E_{99i+107}$. The codomain of φ_{22} is $E_{99i+107} : y^2 = x^3 + (26i + 88)x + (141i + 104)$. In Step 16, we compute the traced endomorphism $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$ with $\theta_{99i+107} := \frac{1}{2} \varphi_{22} \circ \theta_{22} \circ \hat{\varphi}_{22}$, an endomorphism of degree 12. Step 18 appends the isogeny φ_{22} and the traced endomorphism $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$ to H .

In the next rim step, starting with $(E_{99i+107}, \theta_{99i+107}, t_{99i+107}, n_{99i+107})$, we compute the isogeny $\varphi_{99i+107} : E_{99i+107} \rightarrow E_{5i+109}$. The isogeny $\varphi_{99i+107}$ and traced endomorphism $(E_{5i+109}, \theta_{5i+109}, t_{5i+109}, n_{5i+109})$ are appended to H in Step 18.

In the next rim step, we find the isogeny $\varphi_{5i+109} : E_{5i+109} \rightarrow E_{174i+109}$ and corresponding traced endomorphism $(E_{174i+109}, \theta_{174i+109}, t_{174i+109}, n_{174i+109})$ with $\theta_{174i+109} = \frac{1}{2}(\varphi_{5i+109}) \circ \theta_{5i+109} \circ \hat{\varphi}_{5i+109}$.

A fourth step along the rim produces the isogeny $\varphi_{174i+109} : E_{174i+109} \rightarrow E_{80i+107}$ and traced endomorphism $(E_{80i+107}, \theta_{80i+107}, t_{80i+107}, n_{80i+107})$.

The final step along the rim produces the isogeny $\varphi_{80i+107} : E_{80i+107} \rightarrow E'_{22}$ with codomain $E'_{22} : y^2 = (125i + 98)x + (84i + 152)$ and induced traced endomorphism $(E'_{22}, \theta'_{22}, t'_{22}, n'_{22})$. The codomain E'_{22} is isomorphic to E_{22} via an isomorphism ρ , and we use the same isomorphism ρ to confirm that E'_{22} and E_{22} are in fact isomorphic as oriented curves by computing $\theta'_{22} = \rho \circ \theta_{22} \circ \rho^{-1}$.

Algorithm 7.2 terminates and returns the rim cycle

$$\begin{array}{ccccccccc}
 E_{22} & \xrightarrow{\varphi_{22}} & E_{99i+107} & \xrightarrow{\varphi_{99i+107}} & E_{5i+109} & \xrightarrow{\varphi_{5i+109}} & E_{174i+109} & \xrightarrow{\varphi_{174i+109}} & E_{80i+107} \\
 & & \xrightarrow{\varphi_{80i+107}} & & E'_{22} \cong E_{22} & & & &
 \end{array}$$

of length 5 (see the green rim cycle in Fig. 1). Indeed, K has class number 5, and the ideal class of \mathfrak{l} generates the class group of K .

7.3 Ascending to the Rim Using an Orientation

The other major component of navigating the supersingular ℓ -isogeny graph using an orientation is to walk to the rim. We can use Proposition 4.8 to determine the ascending direction and walk up. This is described in Algorithm 7.3. The number of steps to the rim is expected to be $\log(p)$ in general; see Sect. 3.6.

Proposition 7.5 *Algorithm 7.3 is correct and has poly-rep runtime times the distance to the rim.*

Proof The number of steps to the rim is given by the number of times ℓ^2 divides the discriminant of θ (we assume θ is ℓ -primitive); this is k in Step 2. We translate θ to be

Algorithm 7.3: Walking to the rim of the oriented ℓ -isogeny graph.

Input: An ℓ -primitive traced endomorphism (E, θ, t, n) providing the functionality of Section 5.1.

Output: The shortest path from (E, θ, t, n) to the rim of the oriented ℓ -isogeny volcano upon which (E, θ, t, n) lies.

```

1  $H \leftarrow []$ .
2  $k \leftarrow \left\lfloor \frac{v_\ell(t^2-4n)}{2} \right\rfloor$ .
3 If  $\ell = 2$  and  $(t^2 - 4n)/2^{2k} \not\equiv 1 \pmod{4}$  then
4    $k \leftarrow k - 1$ 
5 For  $j = 1, \dots, k$  do
6   Compute  $E[\ell]$ .
7    $(E, \theta, t, n) \leftarrow$  an  $\ell$ -suitable translate of  $(E, \theta, t, n)$ .
8   Compute a generator  $P$  for  $E[\ell] \cap \ker(\theta)$ .
9   Use Vélú's algorithm to compute the  $\ell$ -isogeny  $v : E \rightarrow E'$  with kernel  $\langle P \rangle$ .
10   $(E, \theta, t, n) \leftarrow (E', v \circ \theta \circ \hat{v}, t\ell, n\ell^2)$ 
11   $(E, \theta, t, n) \leftarrow (E, \theta/[\ell^2], t/\ell^2, n/\ell^4)$ 
12  Append  $(v, (E, \theta, t, n))$  to  $H$ .
13 Return  $H$ 

```

ℓ -suitable, which implies that $v \circ \theta \circ \hat{v}$ can be divided by $[\ell]$ twice when v is ascending. Since there is no horizontal direction (by the choice of k in Step 2), there exists a non-trivial $P \in E[\ell] \cap \ker(\theta)$. This gives the ascending isogeny by Proposition 4.8. Once we have found the ascending isogeny, we divide the Waterhouse transfer of θ by $[\ell]^2$ (Step 11), and the result is ℓ -primitive, in preparation for the next loop iteration. For each iteration of the **For** loop, the work is clearly poly-rep. □

Example 7.6 (Walking to the rim of the oriented ℓ -isogeny graph for rationally represented endomorphisms via Algorithm 7.3). We apply Algorithm 7.3 to the output of Step 4 of Example 8.3, namely E_{120} and θ_{120} having $t_{120} = 0, n_{120} = 188$. We find that we expect to take two steps to the rim. Since θ_{120} is already 2-suitable, we evaluate it on $E_{120}[2]$ and obtain the kernel $\langle (121i + 4, 0) \rangle$ for the ascending isogeny. The codomain is E_{171} . Computing the Waterhouse transfer and dividing by $[2]$ twice, we obtain an endomorphism θ' which is not 2-suitable, but Lemma 4.5 shows that $\theta_{171} := \theta' + [1]$ is 2-suitable. The second ascending step is similar; this has kernel $\langle (121i + 131, 0) \rangle$ and codomain E_{5i+109} . The two ascending steps are in blue in Fig. 1.

Example 7.7 (Walking to the rim of the oriented ℓ -isogeny graph for isogeny chain endomorphisms via Algorithm 7.3). We begin with input $(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48)$, from Step 8 of Example 8.3. This will require one step to the rim and is already $[2]$ -suitable. Evaluating on $E_{1728}[2]$, we obtain a kernel of $\langle (178, 0) \rangle$ for the ascending isogeny; the codomain is E_{22} . Waterhouse transfer yields an isogeny-chain which is not prime-power refactored, namely $\varphi'_{1728} \circ \varphi_{171} \circ \varphi_{1728} \circ \hat{\varphi}'_{1728}$ having component degrees 2, 3, 16, 2, respectively. We could apply Algorithm 5.1, but we proceed in a slightly more expedient manner. We rewrite $\varphi'_{1728} \circ \varphi_{171}$, having degrees 2 and 3, respectively, in a form having degrees 3 and 2, respectively. Thus, we evaluate $\varphi'_{1728} \circ \varphi_{171}$ on the 2-torsion to obtain the kernel $\langle (29i + 50, 0) \rangle$ determining $\varphi'_{171} : E_{171} \rightarrow E_{174i+109}$. Then we apply φ'_{171} to the generator of $\ker(\varphi'_{1728} \circ \varphi_{171}) \cap E_{171}[3] = \langle (128i + 164, 28i + 90) \rangle$

to obtain a kernel for which Vélu gives $\varphi_{174i+109} : E_{174i+109} \rightarrow E_{22}$. We obtain the refactored isogeny chain $\varphi_{174i+109} \circ \varphi'_{171} \circ \widehat{\varphi}_{1728} \circ \varphi'_{1728}$. We can then divide the 2-power degree component $\varphi'_{171} \circ \widehat{\varphi}_{1728} \circ \varphi'_{1728}$ by [2] twice and let $\varphi'_{22} := \varphi'_{171} \circ \widehat{\varphi}_{1728} \circ \varphi'_{1728}/[4]$. Replacing this in our isogeny chain above, we now have an isogeny that gives the one step up to the rim (see the red step in Fig. 1):

$$(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48) \xrightarrow{\varphi'_{1728}} (E_{22}, \varphi_{174i+109} \circ \varphi'_{22}, 1, 12).$$

7.4 Ascending and Walking the Rim Using the Endomorphism Ring

When we find an orientation of $j = 1728$, we have more information than just the specified orientation: we also know the endomorphism ring. This extra information allows us to navigate the oriented graph in polynomial time using known algorithms.

Specifically, with Algorithm 7.4 given here, we can walk up the volcano and traverse the rim (being careful not to back-track by comparing to our previous steps), where each step is polynomial in $\log p$ and the length of the representation of θ . To get started, we use E_{init} as the curve defining $B_{p,\infty}$ as in [61], and take the path P to be the trivial path.

Algorithm 7.4: Extending a path from E_{init} by an ascending or horizontal step.

Input: A fixed endomorphism $\theta \in \text{End}(E_{\text{init}})$. An elliptic curve E and path P from E_{init} to E , with no descending steps, and s equal to the number of ascending steps in the path P .

Output: For each of the available horizontal or ascending steps $E \rightarrow E'$ (with regards to the orientation induced by θ), returns the data (E', P', s') , where P' is the path obtained from P by extending it by the extra step, and s' is the number of ascending steps in the path P' .

```

1  $H \leftarrow []$ 
2 For each  $\ell$ -isogeny  $v : E \rightarrow E'$  departing  $E$  do
3    $P' \leftarrow$  the path formed by appending  $v$  to  $P$ .
4    $(\varphi : E_{\text{init}} \rightarrow E') \leftarrow$  the isogeny associated to the path  $P'$ .
5   Compute a  $\mathbb{Z}$ -basis of the maximal quaternion order  $\mathfrak{D}$  of  $E'$  and connecting ideal  $I$  between  $E_{\text{init}}$  and  $E'$  using [61, Algorithm 3] from the path  $P'$ .
6   Compute  $\text{End}(E')$  together with an isomorphism  $\Psi : \text{End}(E') \rightarrow \mathfrak{D}$ , using [61, Algorithm 6].
7    $\beta \leftarrow \Psi(\varphi \circ \theta \circ \widehat{\varphi})$  (The ability to evaluate  $\Psi(\varphi \circ \theta \circ \widehat{\varphi})$  for  $\theta \in \text{End}(E_{\text{init}})$  is also obtained when [61, Algorithm 6] is performed in the last step.)
8    $\beta \leftarrow \beta + T$  where  $T \in \mathbb{Z}$  is chosen so that  $\beta + T$  is the minimal  $\ell^s$ -suitable translate of  $\varphi \circ \theta \circ \widehat{\varphi}$  using Lemma 4.5.
9   If  $\beta/\ell^{s+1} \in \mathfrak{D}$  then
10      $s' \leftarrow s$ 
11     If  $\beta/\ell^{s+2} \in \mathfrak{D}$  then
12        $s' \leftarrow s' + 1$ 
13     Append  $(E', P', s')$  to  $H$ .
14 Return  $H$ .
```

Proposition 7.8 *Under GRH, Algorithm 7.4 is correct and runs in expected polynomial time in the following quantities: $\log p$, the size of the representation of θ , and the length of the path P .*

Proof Each of the cited algorithms runs in the time specified under GRH. We determine which steps are ascending or horizontal by testing whether $\beta/\ell^{s+1}, \beta/\ell^{s+2} \in \mathfrak{O}$, by Proposition 4.7. Since β is represented as a linear combination of a basis of $\text{End}(E')$, this involves dividing the coefficients, which is polynomial time. \square

8 Classical Path-Finding to $j = 1728$

We now present an algorithm which, given a suitable endomorphism on a curve E in the supersingular ℓ -isogeny graph, will find a path to the initial curve E_{1728} , under heuristic assumptions. An illustration of the method is given in Fig. 1: using the endomorphism on E , we first walk from the oriented curve E to the rim of its associated volcano, then find an orientation of E_{1728} and use it to walk from E_{1728} to the rim of its associated volcano, and finally hope to collide on the same rim.

If one wishes to adapt this algorithm to find a path to a more general initial curve, one would need a replacement to Algorithm 6.1 that works for that initial curve (see Sect. 6.3 for a discussion of how this may be done). For this reason, we restrict ourselves to considering the $j = 1728$ curve.

Proposition 8.1 *Assume GRH, Heuristic 6.4, and the assumptions of Sect. 5.1. Consider an endomorphism $\theta \in \text{End}(E)$ in rationally-represented or prime-power isogeny-chain form as described in Sect. 5.4, whose discriminant is coprime to p and has ℓ -fundamental part Δ satisfying $|\Delta| \leq p^{2+\epsilon}$. Write \mathcal{O}_Δ for the order of discriminant Δ . Algorithm 8.1 produces a path of length $O(\log p + h_{\mathcal{O}_\Delta})$ to E_{1728} in the supersingular ℓ -isogeny graph, under Heuristic 6.7 part (i). The runtime is expected poly-rep times $O(h_{\mathcal{O}_\Delta})$, under Heuristic 6.7 part (ii). Furthermore, the following hold:*

- (1) *If ℓ is inert in K , then the runtime improves to $h_{\mathcal{O}_\Delta} \text{poly}(\log p) + \text{poly-rep}$, and the path length improves to $O(\log p)$.*
- (2) *If ℓ is inert in K and the discriminant of θ is already ℓ -fundamental, then the runtime improves to $h_{\mathcal{O}_\Delta} \text{poly}(\log p)$ and the path length improves to $O(\log p)$.*
- (3) *If Δ is a fundamental discriminant, ℓ is split in K and a prime above ℓ generates the class group $\text{Cl}(\mathcal{O}_\Delta)$, then the dependence on Heuristic 6.7 is removed.*

Proof Let θ be the input to the algorithm. The pair (E, ι_θ) , where $\iota_\theta : K \rightarrow \text{End}(E)$ is the orientation given by θ , lies somewhere on the oriented ℓ -isogeny graph associated to K . More specifically, it lies on a volcano of the \mathcal{O} -cordillera for some order \mathcal{O} whose discriminant divides the ℓ -fundamental discriminant Δ computed in Step 3. In other words, if we write \mathcal{O}_Δ for the order of discriminant Δ , then $\mathcal{O} \supseteq \mathcal{O}_\Delta$. Since all endomorphisms throughout the paper are taken to have norm and discriminant at worst polynomial in p , the distance of (E, ι_θ) to the rim is at worst polynomial in $\log p$, and so walking to the rim (Step 4) is poly-rep by Proposition 7.5. Next, we walk around the rim; the runtime depends on the size of the rim and we defer that question to later in the proof.

Algorithm 8.1: Finding a path to E_{1728} .

- Input:** A traced endomorphism (E, θ, t, n) providing the functionality of Section 5.1, where the discriminant of θ is coprime to p .
- Output:** A path in the ℓ -isogeny graph between E and E_{1728} .
- 1 **If** $(E, \theta, t, n) \leftarrow (E, \theta / [\ell^k], t / \ell^k, n / \ell^{2k})$ which is ℓ -primitive, using Algorithm 7.1.
 - 2 $\Delta_\theta \leftarrow t^2 - 4n$.
 - 3 $\Delta \leftarrow$ the ℓ -fundamental part of Δ_θ .
 - 4 Call Algorithm 7.3 on input (E, θ, t, n) to produce an ascending path H_2 from (E, θ, t, n) to $(E_1, \theta_1, t_1, n_1)$ on the rim, i.e. where $\mathbb{Z}[\theta_1] \subseteq \text{End}(E_1)$ is ℓ -fundamental.
 - 5 Call Algorithm 7.2 on input $(E_1, \theta_1, t_1, n_1)$ to walk the rim until we encounter E_1 again, storing the j -invariants encountered as a list L .
 - 6 **repeat**
 - 7 Call Algorithm 6.1 on input Δ , to obtain a new solution $\theta_{1728} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. (Algorithm 6.1 can be suspended and then resumed to find subsequent solutions; see Remark 6.1)
 - 8 Using the methods of Section 7.4, produce an ascending path H_1 from E_{1728} with endomorphism θ_{1728} up to the rim, i.e. to a traced endomorphism $(E_0, \theta_0, t_0, n_0)$ having ℓ -fundamental order $\mathbb{Z}[\theta_0]$ contained in $\text{End}(E_0)$.
 - 9 **until** $E_0 \in L$ or $E_0^{(p)} \in L$
 - 10 Compute H_{rim} , the path from E_1 to E_0 or $E_0^{(p)}$, using L .
 - 11 **If** H_{rim} joins E_1 to E_0 **then**
 - 12 $H \leftarrow H_2 H_{rim}^{-1} H_1^{-1}$, a path from E_{1728} to E .
 - 13 **else**
 - 14 From H_1 , compute the conjugate path $H_1^{(p)}$ from E_{1728} to $E_0^{(p)}$.
 - 15 $H \leftarrow H_2 H_{rim}^{-1} (H_1^{(p)})^{-1}$, a path from E_{1728} to E .

When Δ is passed on to Algorithm 6.1 in Step 7, the result (which is returned in polynomial time by Proposition 6.5 under Heuristic 6.4) is an endomorphism of $\text{End}(E_{1728})$ which gives an oriented elliptic curve lying somewhere on a volcano in an \mathcal{O}' -cordillera, where again $\mathcal{O}' \supseteq \mathcal{O}_\Delta$. (We do not necessarily have $\mathcal{O} = \mathcal{O}'$.) This has norm polynomial in p by Proposition 6.5. By Proposition 6.5 again, the distance to the rim is $O(\log p)$, so walking to the rim is expected polynomial time by Proposition 7.8. Hence each **repeat** iteration has expected polynomial time.

Walking to the rim in Step 8, E_0 lies on the rim of a volcano. This volcano is somewhere in the set of volcanoes $\text{SS}_\mathcal{O}$ defined as the finite union of the \mathcal{O} -cordilleras for all $\mathcal{O} \supseteq \mathcal{O}_\Delta$ in Heuristic 3.7. Note that its conjugate $E_0^{(p)}$ also lies on a rim in $\text{SS}_\mathcal{O}$. Now E_1 also lies on a rim of $\text{SS}_\mathcal{O}$. If E_0 (or $E_0^{(p)}$) and E_1 lie on the same rim, the algorithm will discover this. If not, then one continues the calls to Algorithm 6.1, and another endomorphism will be found. Under Heuristic 6.7 part (i), eventually one of these will produce E_0 or $E_0^{(p)}$ on the same rim as E_1 . The algorithm will then succeed.

Let R denote the number of descending edges from the rim containing E_0 , referred to in this paragraph as the *adjusted rim size* (which is bounded above and below by a constant multiple of the rim size). The sum of the adjusted rim sizes of all rims of $\text{SS}_{\mathcal{O}_\Delta}$ is $O(h_{\mathcal{O}_\Delta})$, with $h_{\mathcal{O}_\Delta}$ given by (2) (Equation (1) and Proposition 3.5). By Lemma 3.8, this is $O(h_{\mathcal{O}_\Delta}(\log \log |\Delta|)^2) = O(h_{\mathcal{O}_\Delta})(\log \log p)^2$ (using $|\Delta| \leq p^{2+\epsilon}$). By Heuristic 6.7 part (ii), the number of times we must **repeat** is therefore $O(h_{\mathcal{O}_\Delta}/R)(\log \log p)^2$. Each iteration performs Steps 7 and 8 and then checks

membership in L . By Proposition 6.5, under GRH, Step 7 runs in polynomial time in $\log p$ and provides a solution θ_{init} of norm at most $p^2 \log^{2+\epsilon} p$. Then θ_{init} can be written as a linear combination of the \mathbb{Z} -basis of $\text{End}(E_{1728})$ with integer coefficients of size $O(\log p)$. Hence Step 8 requires a runtime polynomial in $\log p$ by Proposition 7.8; we store the j -invariant of the output for comparison to L . Thus, each iteration takes expected polynomial time times $O(R)$ (to check membership in L). The walk to produce L in Step 5 takes at most $O(R)$ steps, each of which is poly-rep. Hence the runtime is poly-rep (for Step 4) plus $O(h_{\mathcal{O}_\Delta}) \cdot \text{poly}(\log p) + O(R) \cdot (\text{poly-rep})$.

This runtime is overall bounded by $O(h_{\mathcal{O}_\Delta})$ times poly-rep. But if ℓ is inert, then E_0 lies on a rim of size 1, so we don't need Step 5, and we have poly-rep plus $h_{\mathcal{O}_\Delta} \text{poly}(\log p)$. If θ is already at the rim, then we don't need Step 4. Combined with inertness, this gives runtime $h_{\mathcal{O}_\Delta} \text{poly}(\log p)$.

Finally, if Δ is a fundamental discriminant, ℓ is split and a prime above ℓ generates $\text{Cl}(\mathcal{O}_\Delta)$, then there is only one volcano, obviating the need for Heuristic 6.7. \square

The restriction that $|\Delta| \leq p^{2+\epsilon}$ is required to ensure that Algorithm 6.1 is heuristically polynomial time. If $|\Delta|$ is larger, and ℓ is inert, this failure of polynomial time could become the bottleneck. On the other hand, suppose ℓ is split in K . Under the Cohen-Lenstra heuristics, class groups are usually cyclic, and most elements of a cyclic group are generators, so with high probability, Heuristic 6.7 will not be necessary.

In the case that ℓ is coprime to the conductor of \mathcal{O}_Δ , then we will not need to ascend in Step 4. This improves our runtime by eliminating the call to Algorithm 7.3. If we do need Algorithm 7.3 in Step 4, then we can remove the dependence on GRH by replacing Algorithm 7.4 by another call to Algorithm 7.3 without impact on runtime.

Remark 8.2 One might hope to modify Algorithm 8.1 to produce a shorter path along with a square-root runtime improvement, by removing Step 5, and in each **repeat**, attempting to solve a vectorization problem (see Sect. 9.1) between E_0 and E_{1728} . Unfortunately, we cannot: the problem is that we do not know the correct quadratic order \mathcal{O} with respect to which these oriented curves are primitively oriented. To overcome this, one might try to factor Δ and ascend with respect to any square factors, to guarantee that Δ is fundamental. Ascending would be polynomial in the largest square prime factor of Δ , which could be very costly. An alternative that would usually work may be to try guessing Δ , working backward from the largest (and hence most likely) divisors. Just assuming Δ is fundamental would work much of the time.

Example 8.3 (Finding a path to E_{1728} via Algorithm 8.1). We again let $p = 179$, $\Delta = -47$, $\ell = 2$, and $E_{\text{init}} = E_{1728} : y^2 = x^3 - x$. As input, we consider the curve $E_{120} : y^2 = x^3 + (7i + 86)x + (45i + 174)$ with $j(E_{120}) = 120$, and a trace endomorphism given as $(E_{120}, \theta_{120}, t_{120}, n_{120})$ with $t_{120} = 20$, $n_{120} = 2^5 \cdot 3^2$ and

$$\theta_{120}(x, y) = \left(\frac{(122i + 167)x^{288} + (17i + 68)x^{287} + \dots + 174i + 157}{x^{287} + (78i + 156)x^{286} + \dots + 16i + 54}, \frac{(69i + 109)x^{431} + (60i + 178)x^{430} + \dots + 98i + 124}{x^{431} + (146i + 53)x^{430} + \dots + 44i + 89} y \right).$$

We apply Algorithm 8.1 to find a path from E_{120} to E_{1728} (see Fig. 1). Step 1 on input $(E_{120}, \theta_{120}, t_{120}, n_{120})$ produces the ℓ -suitable and ℓ -primitive traced endomorphism $\theta_{120} \leftarrow \theta_{120} + [-10]$ with $t_{120} \leftarrow 0$ and $n_{120} \leftarrow 188$. Here $\Delta' = t_{120}^2 - 4n_{120} = -752$ and its ℓ -fundamental part is $\Delta = -47$. Step 4 calls Algorithm 7.3 on input $(E_{120}, \theta_{120}, t_{120}, n_{120})$ to produce the following ascending path H_2 to the rim, see Example 7.6:

$$H_2 : (E_{120}, \theta_{120}, 0, 188) \xrightarrow{\varphi_{120}} (E_{171}, \theta_{171}, 0, 47) \xrightarrow{\varphi_{171}} (E_{5i+109}, \theta_{5i+109}, 1, 12).$$

Now we apply Algorithm 7.2 on input $(E_{5i+109}, \theta_{5i+109}, t_{5i+109}, n_{5i+109})$ to walk the rim in Step 5 as in Example 7.4. The list of all the j -invariants is $L = \{5i + 109, 174i + 109, 80i + 107, 22, 99i + 107\}$. In Step 7, calling Algorithm 6.1 on input Δ , we obtain $\theta_{1728} = (3i + k)/2$ as in Example 6.6. For simplicity in this example, we use Algorithm 7.3 in Step 8, instead of the methods of Sect. 7.4. We apply Algorithms 5.3 and 7.1 (see Sect. 6.2) to $(E_{1728}, \theta_{1728}, 0, 47)$ to obtain an ℓ -primitive isogeny chain endomorphism $\theta'_{1728} = \varphi_{171} \circ \varphi_{1728}$ where $\deg(\varphi_{1728}) = 16$, $\deg(\varphi_{171}) = 3$ and with $t_{1728} = 2$, $n_{1728} = 48$ as in Example 5.12. We call Algorithm 7.3 on input $(E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48)$ to produce the following ascending path (see Example 7.7):

$$H_1 : (E_{1728}, \varphi_{171} \circ \varphi_{1728}, 2, 48) \xrightarrow{\varphi'_{1728}} (E_{22}, \varphi_{174i+109} \circ \varphi'_{22}, 1, 12).$$

Finally, since $j(E_{22}) = 22 \in L$, joining the previous paths, we obtain a path from E_{1728} to E_{120} (see the whole path in Fig. 1) as

$$H : E_{1728} \xrightarrow{\varphi'_{1728}} E_{22} \xrightarrow{\varphi_{22}} E_{99i+107} \xrightarrow{\varphi_{99i+107}} E_{5i+109} \xrightarrow{\hat{\varphi}_{171}} E_{171} \xrightarrow{\hat{\varphi}_{120}} E_{120}.$$

9 Quantum Algorithms for VECTORIZATION and PRIMITIVEORIENTATION Problems

We will introduce two hard problems: the oriented vectorization and the primitive orientation problems and then provide quantum algorithms to solve them.

9.1 Vectorization

Since the class group acts on the rim, a problem closely related to walking along the rim is the following, where we use the terminology *vectorization* in analogy with [17] and [11, Section 6.1]. This problem was also recently introduced in [60, Section 3.1].

Problem 9.1 (ORIENTEDVECTORIZATION(Δ)). Let \mathcal{O} be the quadratic order of discriminant Δ . Suppose $(E_1, \iota_1), (E_2, \iota_2) \in \text{SS}_{\mathcal{O}}^{pr}$. Find an ideal class $[b] \in \text{Cl}(\mathcal{O})$ such that $[b] \cdot (E_1, \iota_1) = (E_2, \iota_2)$.

Remark 9.2 This problem is somewhat related to the uber isogeny assumption, which asks for $[b]$ without knowledge of ι_2 ; the difficulty of this problem is shown to be crucial for a variety of supersingular isogeny-based schemes [22].

The following result was implied without details in a more restricted case in [11, Section 6.1]. A variation also appears in [60, Proposition 4].

Heuristic 9.3 *The values of a definite binary quadratic form $f(x, y)$, as $x, y \rightarrow \infty$, are powersmooth and coprime to the first N primes with the same probability as randomly chosen integers of the same size.*

Proposition 9.4 *Assume Heuristic 9.3. Suppose (E_1, ι_1) and (E_2, ι_2) are given by $\iota_i := \iota_{\theta_i}$ for some endomorphisms $\theta_i \in \text{End}(E_i)$ which can be evaluated on $E_i(\mathbb{F}_{p^k})$ in time $T_{\theta_i}(k, p) \geq \text{poly}(k \log p)$. Define $T_{\theta_1, \theta_2}(k, p) := \max\{T_{\theta_1}(k, p), T_{\theta_2}(k, p)\}$ and $d := \max\{\deg \theta_1, \deg \theta_2\}$. Then $\text{ORIENTEDVECTORIZATION}(|\Delta|)$ can be reduced to a hidden shift problem and solved in quantum time $T_{\theta_1, \theta_2}(O(\log^2 d), p)L_{|\Delta|}(1/2)$ under GRH, where, furthermore, the ideal class is $L_{|\Delta|}(1/2)$ -smooth and of size $O(\sqrt{|\Delta|})$.*

Proof The approach is based on that in Childs-Jao-Soukharev [13], who developed a subexponential means of evaluating the action of the class group (by finding a smooth representative of the needed ideal class), and then applying Kuperberg's algorithm, which requires subexponentially many evaluations. The difference is that we need to apply the class group action, in the form of isogenies, to *oriented* curves, i.e. carry along the orientation.

The reduction to the hidden shift problem is formalized in [37, Theorem 3.3]; the *malleability oracle* in the sense of [37, Definition 3.2], with respect to their notation, is given in terms of $I = G = \text{Cl}(\mathcal{O})$, $O = \text{SS}_O^{\text{pr}}$, and $f : I \rightarrow O$ defined by $f([\alpha]) = [\alpha] \cdot (E_1, \iota_1)$. Then to find $[b] \in \text{Cl}(\mathcal{O})$ such that $[b] \cdot (E_1, \iota_1) = (E_2, \iota_2)$, we observe that f is malleable, because we can compute $[\alpha] \mapsto f([\alpha b]) = [\alpha b] \cdot (E_1, \iota_1) = [\alpha] \cdot (E_2, \iota_2)$ (this is the malleability oracle at (E_2, ι_2)).

To evaluate the action of $[\alpha]$ on E_i takes time $\text{poly}(\log p)L_{|\Delta|}(1/2)$ using the methods of [13] or [5] and involves finding an $L_{|\Delta|}(1/2)$ -smooth integral representative \mathfrak{a} which can be evaluated as a composition chain of isogenies. Unfortunately, to evaluate the action of $[\alpha]$ on θ_i , we require a powersmooth representative instead. Calling on Heuristic 9.3 and [16, Section 3.1] (similarly to the proof of Proposition 5.11), we can find a representative with norm $L_{|\Delta|}(1/2)$ -powersmooth and coprime to the first $\log \deg \theta_i$ primes, by random search. The time taken is $L_{|\Delta|}(1/2)$, because by Mertens' Theorem, the probability of satisfying the coprimality hypothesis is $\prod_{p < O(\log \deg \theta)} (1 - 1/p) \sim O(1/\log \log \deg \theta_i)$. Having done this, write the result as $\mathfrak{a} := \prod_{p \text{ prime}} \alpha_k$, where the $N(\alpha_k)$ are coprime prime powers.

We also need to evaluate the action of \mathfrak{a} on θ_i in some way that is distinguishable (since isogeny chains are not unique for a given endomorphism). For each j -invariant we choose a fixed model. We replace the data of θ with the data of its linear action on the $O(\log \deg \theta_i)$ smallest prime-torsion subgroups $E[q]$, as well as all the prime-power $N(\alpha_k)$ -torsion subgroups. By Chinese Remainder Theorem, this is enough to distinguish different results, since if $\theta - \theta'$ vanishes on all of the prime-power subgroups, then it vanishes on a subgroup (generated by all of the subgroups together),

whose size exceeds a fixed multiple of d , which implies that $\theta = \theta'$ (this method is inspired by the Schoof algorithm, as adapted for example in [36, Theorem 81], [25, Lemma 4]).

To compute the action on θ_i , we first need to compute φ_{α_k} . This is done as in Algorithm 7.2, where we consider the linear action of $a + b\theta_i$ on the $N(\alpha_k)$ -torsion to find the kernel of φ_{α_k} . In order to compute the linear action of $\varphi_{\alpha_k} \circ \theta_i \circ \widehat{\varphi_{\alpha_k}}/[N(\alpha_k)]$ on the prime or prime-power torsion subgroups $E[q]$ described in the last paragraph, we proceed as follows. If q is coprime to $N(\alpha_k)$, then to find this action, we evaluate $\varphi_{\alpha_k} \circ \theta_i \circ \widehat{\varphi_{\alpha_k}}$ on $E[q]$ and then apply the action of $[n']$ where $n' \equiv N(\alpha_k)^{-1} \pmod{q}$. Otherwise we store **null** for that value of q (by assumption, this occurs only for q larger than $\log \deg \theta_i$).

This gives a way to evaluate the function f suitable for quantum computation. Taken together, the time taken for evaluating $[\alpha_k]$ is $\text{poly}(\log \deg \theta_i)$ times the time taken to evaluate θ_i and φ_{α_k} , namely $T_{\theta_1, \theta_2}(O(\log^2 d), p) + \text{poly}(\log p)L_{|\Delta|}(1/2)$.

There is a small caveat that the action of Frobenius may take us out of the orbit of $\text{Cl}(\mathcal{O})$, so this will only work when the oriented curves E_1 and E_2 are in the same $\text{Cl}(\mathcal{O})$ -orbit. Of course, there are at most two orbits, so in the case of failure, we can apply Frobenius to one of the curves and try again.

The evaluation algorithm of [13] runs in time $L_{|\Delta|}(1/2)$ under GRH and results in an $L_{|\Delta|}(1/2)$ -smooth isogeny of size $O(\sqrt{|\Delta|})$ [13, Proposition 3.2]. Our modification above results in the stated runtime. \square

Remark 9.5 If we wish to avoid the coprimality aspect of Heuristic 9.3, then we can take subexponentially many prime power torsion subgroups, at an increased cost in runtime and memory (thanks to Benjamin Wesolowski for this and other helpful observations and corrections to this proof).

Remark 9.6 If we wish to avoid Heuristic 9.3 in Proposition 9.4, we could first transform θ_i into a powersmooth isogeny chain (using Algorithm 5.3 at a runtime cost of $T_{\theta_1, \theta_2}(L_{\deg \theta_i}(1/2), p)$) and then use the method for horizontal stepping of Algorithm 7.2 to evaluate $[\alpha]$ prime-by-prime. This depends on Heuristic 5.10 instead. This allows for the representative α to be chosen as smooth, not necessarily powersmooth, but incurs an additional runtime cost to the algorithm as a whole.

9.2 Primitive Orientation Computation

The vectorization problem 9.1 requires knowledge of the order with respect to which (E, ι) is a primitive orientation. This requirement naturally leads to the following problem:

Problem 9.7 (PRIMITIVEORIENTATION). Given an supersingular elliptic curve E , and an endomorphism $\theta \in \text{End}(E)$, determine the quadratic order \mathcal{O} such that ι_θ is \mathcal{O} -primitive.

We briefly describe two classical algorithms here for solving Problem 9.7. Let f be the conductor of $\mathbb{Z}[\theta]$, we compute a B -powersmooth f -suitable translation and factorize $f = \prod f_i^{r_i}$. For any prime power factor $f_i^{r_i}$ of f , one needs to check

whether the translated endomorphism is divisible by $f_i^{r_i}$, which amounts to checking whether θ vanishes on the $f_i^{r_i}$ -torsion of E . We take B to be $L_d(1/2)$ with $d = \deg \theta$, as discussed in the proof of Theorem 11.1, using Algorithm 5.3, computing the translation takes time $T_\theta(L_d(1/2), p)$ assuming Heuristic 5.10 with ℓ replaced by f in Heuristic 5.10. Furthermore, evaluating the translated endomorphism on $\tilde{f}^{\tilde{r}}$ -torsion takes time $\text{poly}(\log p)L_d(1/2)\mathbf{M}(p^{\text{lcm}(12, \tilde{f}^{2\tilde{r}})})$ where $\tilde{f}^{\tilde{r}} = \max\{f_i^{r_i}\}$. Alternatively, one can compute an integer T with smallest absolute value such that $\theta + T$ is f -suitable translation instead of a B powersmooth translation. Checking whether θ vanishes on the $f_i^{r_i}$ -torsion of E takes time $\text{poly}(\log p)T_\theta(\tilde{f}^{2\tilde{r}}, p)$ where $\tilde{f}^{\tilde{r}} = \max\{f_i^{r_i}\}$. Both methods have runtimes polynomial in $\tilde{f}^{\tilde{r}}$.

Quantumly we give the following algorithm that runs in subexponential time. Our method for solving Problem 9.7 has similarities to that of Proposition 9.4, with a hidden subgroup problem in place of the hidden shift problem. The subexponential runtime in Δ still arises from the need to evaluate the action of the class group.

Proposition 9.8 *Assume Heuristic 9.3. Suppose θ can be evaluated on $E(\mathbb{F}_{p^k})$ in time $T_\theta(k, p)$. Then there is a quantum algorithm to solve PRIMITIVEORIENTATION in time $T_\theta(O(\log^2 \deg \theta), p) + \text{poly}(\log p)L_{|\Delta|}(1/2)$.*

Proof Let $\mathcal{O}_\theta := \mathbb{Z}[\theta]$. Compute $\text{Cl}(\mathcal{O}_\theta)$ as a product of cyclic groups with given generators, using the quantum algorithm [12, Algorithm 10], as described in [13, Proof of Theorem 4.5]. It is possible to solve the PRIMITIVEORIENTATION problem by computing the kernel of the map $\text{Cl}(\mathcal{O}_\theta) \rightarrow \text{Cl}(\mathcal{O})$ (where we do not a priori know \mathcal{O}). This can be done by solving a hidden subgroup problem. Namely, we consider the action of $\text{Cl}(\mathcal{O}_\theta)$ on $\text{SS}_\mathcal{O}^{\text{pr}}$, defining $f([\mathfrak{b}]) = [\mathfrak{b}] \cdot (E, \iota_\theta)$. We evaluate the action of \mathfrak{b} on θ as described in the proof of Proposition 9.4.

Once the kernel G has been computed in the form of generators $\mathfrak{g}_1, \dots, \mathfrak{g}_n$, one writes each \mathfrak{g}_i as principal in the maximal order via a generator $\mathfrak{g}_i = (g_i)$. Then \mathcal{O} is by definition the order generated from \mathcal{O}_θ by adjoining the g_i 's. One computes the conductor of this order by taking the gcd of the conductors of the $\mathbb{Z}[g_i]$ and $\mathbb{Z}[\theta]$, and hence computing the discriminant $\Delta_\mathcal{O}$. These last computations are polynomial in $\log |\Delta_\theta|$. \square

An improvement is available: to evaluate the action of $[\mathfrak{b}]$ on E takes time $\text{poly}(\log p) \exp(\tilde{O}(\log^{1/3} |\Delta_\theta|))$ using the methods of Biasse-Iezzi-Jacobson [5]; they also improve on the computation of $\text{Cl}(\mathcal{O})$.

10 Quantum Algorithm for Finding a Smooth Isogeny to $j = 1728$

The problems of computing the endomorphism ring of an elliptic curve E , computing an ℓ -power isogeny to an initial curve (such as $j = 1728$), and computing a smooth isogeny to an initial curve, are all equivalent [61]. In this section, we modify Algorithm 8.1 to find a smooth isogeny, using the quantum algorithms of the previous section (Propositions 9.4 and 9.8). The resulting quantum algorithm is Algorithm 10.1.

Proposition 10.1 *Assume GRH, Heuristic 6.4, 6.7, and 9.3, and the assumptions of Sect. 5.1. Suppose θ can be evaluated on $E(\mathbb{F}_{p^k})$ in time $T_\theta(k, p) \geq \text{poly}(k \log p)$.*

Algorithm 10.1: Finding a smooth isogeny to E_{init} (quantum)

Input: A traced endomorphism (E, θ, t, n) which can be evaluated on arbitrary points, where the discriminant of θ is coprime to p .

Output: A smooth isogeny $E \rightarrow E_{\text{init}}$.

- 1 $\Delta \leftarrow t^2 - 4n$
- 2 Choose the smallest prime ℓ so that ℓ^2 does not divide Δ or n .
- 3 $\Delta^* \leftarrow$ the discriminant of the solution to PRIMITIVEORIENTATION for (E, θ) via Proposition 9.8.
- 4 **repeat**
- 5 Call Algorithm 6.1 on input Δ^* , to obtain a new traced endomorphism $(E_{\text{init}}, \theta_{\text{init}}, t_{\text{init}}, n_{\text{init}})$. (Algorithm 6.1 can be suspended and then resumed to find subsequent solutions; see Remark 6.1.)
- 6 Walk from $(E_{\text{init}}, \theta_{\text{init}}, t_{\text{init}}, n_{\text{init}})$ to produce an ascending path H_1 from $(E_{\text{init}}, \theta_{\text{init}}, t_{\text{init}}, n_{\text{init}})$ to $(E_0, \theta_0, t_0, n_0)$ on the rim, i.e. where $\mathbb{Z}[\theta_0] \subseteq \text{End}(E_0)$ is ℓ -fundamental (methods of Section 7.4).
- 7 $\Delta^{**} \leftarrow$ the discriminant of the solution to PRIMITIVEORIENTATION for (E_0, θ_0) via Proposition 9.8.
- 8 **until** $\Delta^* = \Delta^{**}$
- 9 Use a quantum computer to solve ORIENTEDVECTORIZATION(Δ') as described in Proposition 9.4, to find an ideal class $[\mathfrak{a}] \in \text{Cl}(\mathcal{O}_{\Delta'})$ such that $[\mathfrak{a}](E_1, \iota_{\theta_1})$ is (E_0, ι_{θ_0}) or $(E_0^{(p)}, \iota_{\theta_0}^{(p)})$ (try both).

Let $d = \max\{\deg \theta, |\Delta|\}$. Suppose $|\Delta| \leq p^{2+\epsilon}$ and Δ is coprime to p . Algorithm 10.1 is correct and succeeds in heuristic expected time $T_\theta(O(\log^2 d), p)L_{|\Delta|}(1/2)$. The resulting $L_{|\Delta|}(1/2)$ -smooth isogeny has norm $O(\sqrt{|\Delta|})$.

Proof The algorithm determines Δ^* so that ι_θ is \mathcal{O}_{Δ^*} -primitive. In the **repeat** loop, it finds an orientation of $j = 1728$ and a path from that oriented curve to an oriented curve (E_0, ι_{θ_0}) which is primitive with respect to the same order. Thus vectorization applies, and finds a smooth isogeny between (E, ι_θ) and (E_0, ι_{θ_0}) . Combining the path and isogeny, we find a smooth isogeny between E and the initial curve.

The first two steps take time $O(\log |\Delta|)$. The third step takes time $T_\theta(\log \deg \theta, p) + \text{poly}(\log p)L_{|\Delta|}(1/2)$ by Proposition 9.8. Steps 5 and 6 take polynomial time in $\log p$ and $\log |\Delta|$ by Proposition 6.3 and Proposition 7.8. Step 7 again takes time $T_\theta(\log \deg \theta, p) + \text{poly}(\log p)L_{|\Delta|}(1/2)$. To determine how often we must **repeat**, we compute that the probability that $\Delta^* = \Delta$ is equal to $h_{\mathcal{O}}/H_{\mathcal{O}}$, with $H_{\mathcal{O}}$ given by (2) (by consideration of the sizes of $\text{SS}_{\mathcal{O}}^{pr}$ (Equation (1) and Proposition 3.5) and using Heuristic 6.7). Thus, by Lemma 3.8, the expected number of iterations is $\text{poly}(\log p)$.

Note that the endomorphism found by Algorithm 6.1 is of norm $O(|\Delta|)$. Therefore the rim endomorphism θ_0 is also of norm $O(|\Delta|)$. Thus, ORIENTEDVECTORIZATION in Step 9 takes time $T_\theta(O(\log^2 d), p)L_{|\Delta|}(1/2)$ (Proposition 9.4). Note that the evaluation time for θ_0 on small torsion is $O(\log p)$ since we have expressed θ_0 as a linear combination of basis elements, each of which can be evaluated via the chain down to $j = 1728$. □

11 Proofs of Main Theorems and Special Cases

11.1 Proof of Main Theorems

Theorem 11.1 Choose a small prime ℓ and assume the heuristic assumptions of Proposition 8.1. Let $\theta \in \text{End}(E)$ be an endomorphism of degree d , such that

$L_d(1/2) \geq \text{poly}(\log p)$. Suppose θ can be evaluated on points $P \in E(\mathbb{F}_{p^k})$ in time $T_\theta(k, p)$. Let Δ' be the ℓ -fundamental part of the discriminant Δ of θ , and assume that $|\Delta'| \leq p^{2+\epsilon}$. There is a classical algorithm that, given any such θ , finds an ℓ -isogeny path of length $O(\log p + h_{\Delta'})$ from E to the curve E_{init} of j -invariant $j = 1728$ in runtime $T_\theta(L_d(1/2), p) + h_{\Delta'} L_d(1/2) \text{poly}(\log p)$.

The runtime comes as a sum of two terms because the algorithm has two steps: first, evaluate the endomorphism on points in order to create a presentation of the endomorphism that meets the needs of the main algorithm; and then use the result to walk in the oriented graph.

Proof of Theorem 11.1 Suppose θ is such an endomorphism. Then set $B = L_d(1/2)$. We can apply Algorithm 5.3 (having Algorithm 5.1 as a subroutine) to θ , whose runtime depends on the evaluation of θ on inputs in a field $\mathbb{F}_{p^{O(B^2)}}$. The runtime for this conversion is therefore $T_\theta(L_d(1/2), p)$. The result is a prime-power isogeny-chain representation of θ . We can then use Algorithm 8.1, with the representation runtime being $L_d(1/2)$, by Proposition 5.13. The classical runtime follows from Proposition 8.1. \square

Theorem 11.2 Assume GRH, Heuristic 6.4, 6.7, and 9.3, and the assumptions of Sect. 5.1. Let $\theta \in \text{End}(E)$ be an endomorphism which can be evaluated on points $P \in E(\mathbb{F}_{p^k})$ in time $T_\theta(k, p)$, where $T_\theta(k, p) \geq \text{poly}(k \log p)$. Suppose θ has discriminant Δ coprime to p with $|\Delta| \leq p^{2+\epsilon}$. Let $d = \max\{\deg \theta, |\Delta|\}$. There is a quantum algorithm that, given any such θ , finds an $L_{|\Delta|}(1/2)$ -smooth isogeny of norm $O(\sqrt{|\Delta|})$ from E to $j = 1728$ in runtime $T_\theta(O(\log^2 d), p) L_{|\Delta|}(1/2)$.

Proof of Theorem 11.2 We use Algorithm 10.1, with no need to pre-process θ . Runtime follows from Proposition 10.1. \square

11.2 Special Cases

In this section, we refer to an endomorphism as *insecure* if access to such an endomorphism allows for a polynomial time path-finding algorithm. Endomorphisms of small size are known to be insecure [39]. We obtain a version of this from our methods also.

Theorem 11.3 Assume the situation of Theorem 11.1. In the following special cases, the runtime and path length of Algorithm 8.1 are polynomial in $\log p$:

- (1) The input endomorphism is rationally represented in polynomial space.
- (2) $h_{\mathcal{O}_\Delta} = \text{poly}(\log p)$ and ℓ is coprime to Δ and inert in K . In this case, the endomorphism is not even needed as input; only its existence, trace and norm are needed.

Proof The second case is a consequence of Algorithm 8.1 and Proposition 8.1, in which the hypotheses imply Steps 4 and 5 are unnecessary. The first is a consequence of the observation that such endomorphisms have polynomially sized discriminants and class numbers. \square

The following result demonstrates for all curves the existence of non-small degree endomorphisms which are insecure under our algorithm. (Recall that most curves do not have small degree endomorphisms. It is known that there are curves having no endomorphisms of norm smaller than $p^{2/3-\epsilon}$ (see [38, Proposition B.5], [26, Section 4], [63, Proposition 1.4]).)

Theorem 11.4 *Suppose $\Delta = f^2 \Delta^*$ where Δ^* is a discriminant of $\text{poly}(\log p)$ size, f is $\text{poly}(\log p)$ -smooth, and θ is f -suitable with $\text{poly}(\log p)$ -powersmooth norm, and represented in some fashion so that it can be evaluated in $\text{poly}(\log p)$ time on points of $\text{poly}(\log p)$ size. Then there is a classical algorithm to find an $O(\log p)$ -powersmooth isogeny to E_{init} in time $\text{poly}(\log p)$.*

Proof The dependence on ℓ throughout the paper has been suppressed by assuming $\ell = O(1)$, but it is at worst polynomial throughout. We refactor θ in $\text{poly}(\log p)$ time (this is possible by Proposition 5.6 and the evaluation runtime assumption), to obtain an isogeny chain. Taking each prime ℓ dividing f in turn, we ascend as far as possible on the oriented ℓ -isogeny volcano. By f -suitability, we can ascend without any further translation or refactoring. Having ascended, we obtain an endomorphism of discriminant Δ^* of $\text{poly}(\log p)$ size and trace zero, and hence call on Theorem 11.3 with respect to some suitable ℓ . □

In fact, every elliptic curve has insecure endomorphisms: one can provide an endomorphism in the form of a closed walk in the ℓ -isogeny graph that passes through 1728. Such a path is guaranteed to exist by the diameter of the graph. In that case, one hardly needs the algorithms of this paper, as the path to 1728 is already explicit. A variation on this theme is to provide a $\text{poly}(\log p)$ -powersmooth isogeny chain whose endomorphism has minimal polynomial $x^2 + L^2$ (i.e., L is powersmooth). Such a chain will be insecure because it explicitly passes through 1728 and also under the algorithms provided in this paper (by Theorem 11.4).

More interestingly, examples of such endomorphisms exist whose minimal polynomial places them in any field $\mathbb{Q}(\omega)$ with $\text{poly}(\log p)$ discriminant (not just the Gaussian field as above); indeed one can take any element of the form $L(\omega + k)$ for $k \in \mathbb{Z}$ and a $\text{poly}(\log p)$ -powersmooth L such that the norm $N(\omega + k)$ is $\text{poly}(\log p)$ -powersmooth.

Finally, we remark on one more special case. When the norm of θ is well-behaved, and we are already at the rim with respect to ℓ (perhaps by choosing ℓ judiciously), then we have improved dependence on p . Note that in the following theorem, there is no requirement on the factorization of Δ .

Theorem 11.5 *Suppose the norm of θ has powersmoothness bound $B(p)$, and suppose that Δ is coprime to ℓ . Then there is a classical algorithm to find an ℓ -isogeny path of length $O(\log p + h_{\mathcal{O}})$ to E_{init} in time $h_{\mathcal{O}} \text{poly}(B(p) \log p)$.*

Proof Use Algorithm 8.1. By the assumption on Δ , we need not ascend with θ (that is, we skip Step 4). We only walk horizontally, and those steps are polynomial in $B(p)$ by Proposition 7.3. □

12 Division by $[\ell]$

We conclude with a detailed description and analysis of McMurdy’s algorithm (Algorithm 12.2) which can be used to divide any *isogeny* (not just an endomorphism) by $[\ell]$ if it is a multiple of $[\ell]$. Given a rationally represented traced endomorphism, we apply Algorithm 12.2 and then adjust the trace and norm accordingly.

We follow the notation of McMurdy [42]. Let E_1 and E_2 be two supersingular elliptic curves given by respective short Weierstrass equations

$$E_1 : y^2 = W_1(x), \quad E_2 : y^2 = W_2(x).$$

with $W_1(x), W_2(x) \in \mathbb{F}_{p^2}[x]$. Denote by $\psi_{E_1, \ell}$ the ℓ -division polynomial of E_1 , made monic, and let $X_i(x)$ and $Y_i(x)$ be the rational functions representing the multiplication-by- ℓ map on E_i , i.e. $[\ell]_{E_i}(x, y) = (X_i(x), Y_i(x)y)$ for $i = 1, 2$. For a polynomial $P(x) = (x - r_1) \cdots (x - r_n)$ with coefficients in some field \mathbb{F} whose roots r_i lie in some field extension \mathbb{F}' of \mathbb{F} , and a rational function $T(x)$ over \mathbb{F}' , define

$$P(x)|_T := (x - T(r_1)) \cdots (x - T(r_n)).$$

Given $[\ell]\varphi : E_1 \rightarrow E_2$ as a pair of rational maps, where $\varphi : E_1 \rightarrow E_2$ is an isogeny, the rational maps of φ are obtained as follows.

Proposition 12.1 ([42, Proposition 2.6]). *Suppose that $\varphi : E_1 \rightarrow E_2$ is a separable isogeny such that $([\ell]\varphi)(x, y) = (F(x), G(x)y)$ for rational functions $F(x), G(x)$. Write $F(x)$ in lowest terms, i.e. as either $\frac{c_F \cdot P(x)}{W_1(x)Q(x)}$ when $\ell = 2$ or $\frac{c_F \cdot P(x)}{(\psi_{E_1, \ell}(x))^2 Q(x)}$ when $\ell \neq 2$, with monic polynomials $P(x), Q(x)$. Set*

$$p(x) = P(x)|_{X_1}, \quad q(x) = Q(x)|_{X_1}.$$

Then $p(x) = p_0(x)^{\ell^2}$ and $q(x) = q_0(x)^{\ell^2}$ for monic polynomials $p_0(x), q_0(x)$. Moreover, we have $\varphi(x, y) = (f(x), g(x)y)$, where $f(x) = c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)}$ and $g(x) = \frac{G(x)}{Y_2(f(x))}$.

Algorithm 12.1 computes the polynomials $p(x)$ and $q(x)$ as given in Proposition 12.1. The main division-by- $[\ell]$ process (Algorithm 12.2) then calls Algorithm 12.1 twice.

Division by $\ell = 2$ has been implemented by McMurdy [42] (code available at [41]). Division by odd primes $\ell > 2$ is complicated by the non-vanishing of the y -coordinates of the ℓ -torsion points. Fix an odd prime $\ell > 2$. In order to compute $p(x) = P(x)|_{X_1}$ and $q(x) = Q(x)|_{X_1}$ in Steps 3 and 4 of Algorithm 12.2, we compute the rational map $N_P = \prod_i P(\mathbf{x}_i)$ as a function of the variable x only. In contrast to the case of 2-torsion points, the ℓ -torsion points on E_1 have non-zero y -coordinates, so some \mathbf{x}_i depend not only on x (as in the case $\ell = 2$) but also on y and y_i for $i \leq (\ell^2 - 1)/2$. As a consequence, N_P also depends on these variables. To overcome this obstruction, we employ a new technique presented in Steps 5–11 of Algorithm 12.1. In these steps, we compute the products $\mathbf{x}_i \cdot \bar{\mathbf{x}}_i$, and hence the products $P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i)$. Each product

Algorithm 12.1: Computing the polynomial $P(x)|_{X_1}$

- Input:** An elliptic curve E_1 , a monic polynomial $P(x)$ defined over \mathbb{F}_{p^m} , and the rational map $X_1(x)$ associated to E_1 .
- Output:** $P(x)|_{X_1}$.
- 1 Compute a root ζ (in some field extension of F_{p^2}) of X_1 .
 - 2 Compute the x -coordinates x_i (in some field extension of F_{p^2}) of the points $S_i = (x_i, y_i) \in E_1[\ell]$, indexed by $i = 1, \dots, \ell^2 - 1$ so that $x_{i+\frac{\ell^2-1}{2}} = x_i$, using the ℓ -th division polynomial (note that we do not compute the y_i here). Let $S_0 = O_{E_1}$.
 - 3 Compute the x -coordinates $\mathbf{x}_i(x, y, y_i)$ for $1 \leq i \leq \frac{\ell^2-1}{2}$ of the maps representing point addition $(x, y) + S_i$ on E_1 , using the values of x_i computed in step 2 but leaving y_i 's as indeterminates. Set $\bar{\mathbf{x}}_i(x, y, y_i) = \mathbf{x}_i(x, y, -y_i)$ which is the x -coordinate of the point addition $(x, y) + (-S_i)$.
 - 4 $N(x) \leftarrow P(x)$ and $D(x) \leftarrow 1$.
 - 5 **For** $i = 1, \dots, \frac{\ell^2-1}{2}$ **do**
 - 6 Compute $P(\mathbf{x}_i(x, y, y_i))$ and $P(\bar{\mathbf{x}}_i(x, y, y_i))$ (as rational functions in x, y and y_i) using Horner's algorithm.
 - 7 Compute the numerator N_i and denominator D_i of $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ as polynomials in x, y and y_i .
 - 8 Replace y^2 with $W_1(x)$ and y_i^2 with $W_1(x_i)$ in N_i . Denote the result by $N_i(x)$, as no y 's or y_i 's should remain.
 - 9 Replace y_i^2 with $W_1(x_i)$ in D_i . Denote the result by $D_i(x)$, as no y 's or y_i 's should remain.
 - 10 $N(x) \leftarrow N(x) \cdot N_i(x)$, and $D(x) \leftarrow D(x) \cdot D_i(x)$.
 - 11 $N_P(x) \leftarrow \frac{N(x)}{D(x)}$, $i \leftarrow 0$, $p(x) \leftarrow 0$.
 - 12 **For** $i = 0, \dots, \deg(P(x))$ **do**
 - 13 $a_i \leftarrow N_P(\zeta)$.
 - 14 $p(x) \leftarrow p(x) + a_i x^i$.
 - 15 $N_P(x) \leftarrow N_P(x) - a_i x^i$.
 - 16 $N_P(x) \leftarrow N_P(x)/X_1(x)$.
 - 17 **Return** $p(x)$.

Algorithm 12.2: Division by $[\ell]$.

- Input:** Elliptic curves E_1, E_2 , rational maps $F(x)$ and $G(x)$ where $([\ell]\varphi)(x, y) = (F(x), G(x)y)$ for some isogeny $\varphi : E_1 \rightarrow E_2$.
- Output:** Rational maps $f(x)$ and $g(x)$ such that $\varphi(x, y) = (f(x), g(x)y)$.
- 1 Determine c_F , and the monic polynomials $P(x)$ and $Q(x)$ such that $F(x) = \frac{c_F \cdot P(x)}{W_1(x) \cdot Q(x)}$ ($\ell = 2$) or $F(x) = \frac{c_F \cdot P(x)}{(\psi_{E_1, \ell}(x))^2 \cdot Q(x)}$ ($\ell \neq 2$).
 - 2 Compute $X_1(x)$ and $Y_2(x)$.
 - 3 Compute $p(x) \leftarrow P(x)|_{X_1}$ using Algorithm 12.1 on input $E_1, P(x), X_1(x)$.
 - 4 Compute $q(x) \leftarrow Q(x)|_{X_1}$ using Algorithm 12.1 on input $E_1, Q(x), X_1(x)$. In this step we can skip Steps 1–4 in Algorithm 12.1 since they were already performed in Step 3 of this algorithm.
 - 5 Compute $p_0(x) \leftarrow p(x)^{1/\ell^2}$ and $q_0(x) \leftarrow q(x)^{1/\ell^2}$ using a truncated variant of Newton's method.
 - 6 $f(x) \leftarrow c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)}$, $g(x) \leftarrow \frac{G(x)}{Y_2(f(x))}$.
 - 7 **Return** $f(x), g(x)$.

$P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i)$ is a rational map in x, y^2 , and y_i^2 ($i \leq (\ell^2 - 1)/2$) by Lemma 12.4. We replace y^2 (respectively y_i^2) with $W_1(x)$ (respectively $W_1(x_i)$) to obtain rational maps in the variable x only.

Example 12.2 (Computing the polynomial $P(x)|_{X_1}$ via Algorithm 12.1). Let $\ell = 3$, $p = 179$, and $E_{1728} : y^2 = x^3 - x$ the supersingular elliptic curve over \mathbb{F}_p with $j = 1728$. Let $X_1(x), Y_1(x)$ be associated to multiplication-by-3, i.e.

$$[3]_{E_{1728}}(x, y) = (X_1(x), Y_1(x)y) \quad \text{where}$$

$$X_1(x) = \frac{20x^9 + 61x^7 + 63x^5 + 175x^3 + x}{x^8 + 175x^6 + 63x^4 + 61x^2 + 20}.$$

Let $P(x) = x^{18} + 122x^{16} + 136x^{14} + 65x^{12} + 29x^{10} + 150x^8 + 114x^6 + 43x^4 + 57x^2 + 178$. We compute $p(x) = P(x)|_{X_1}$ using Algorithm 12.1 as follows.

In Steps 1 and 2, we may choose $\zeta = 0$. Let \mathbb{F}_{p^4} be generated by \mathbf{a} having minimal polynomial $x^4 + x^2 + 109x + 2$. We obtain $S_0 = O_{E_{1728}}, S_1 = (103, y_1), S_2 = (76, y_2), S_3 = (24\mathbf{a}^3 + 39\mathbf{a}^2 + 119\mathbf{a} + 102, y_3), S_4 = (155\mathbf{a}^3 + 140\mathbf{a}^2 + 60\mathbf{a} + 77, y_4), S_5 = -S_1, S_6 = -S_2, S_7 = -S_3, S_8 = -S_4$. In Steps 3, we compute $\mathbf{x}_i(x, y, y_i)$ and $\bar{\mathbf{x}}_i(x, y, y_i)$ as $\mathbf{x}_0 = x, \bar{\mathbf{x}}_i(x, y, y_i) = \mathbf{x}_i(x, y, -y_i), \forall i, 1 \leq i \leq 4$ where

$$\mathbf{x}_1(x, y, y_1) = \frac{-x^3 + y^2 - 2yy_1 + y_1^2 - 76x^2 + 48x + 68}{x^2 - 27x + 48},$$

$$\mathbf{x}_2(x, y, y_2) = (-x^3 + y^2 - 2yy_2 + y_2^2 + 76x^2 + 48x - 68)/(x^2 + 27x + 48),$$

$$\mathbf{x}_3(x, y, y_3) = \frac{-x^3 + y^2 - 2yy_3 + y_3^2 + (24\mathbf{a}^3 + 39\mathbf{a}^2 - 60\mathbf{a} - 77)x^2 - 46x + (30\mathbf{a}^3 + 4\mathbf{a}^2 - 75\mathbf{a} + 38)}{(x^2 + (-48\mathbf{a}^3 - 78\mathbf{a}^2 - 59\mathbf{a} - 25)x - 46)},$$

$$\mathbf{x}_4(x, y, y_4) = \frac{-x^3 + y^2 - 2yy_4 + y_4^2 + (-24\mathbf{a}^3 - 39\mathbf{a}^2 + 60\mathbf{a} + 77)x^2 - 46x + (-30\mathbf{a}^3 - 4\mathbf{a}^2 + 75\mathbf{a} - 38)}{x^2 + (48\mathbf{a}^3 + 78\mathbf{a}^2 + 59\mathbf{a} + 25)x - 46}.$$

In Steps 4–11: We compute the norm $N_P(x)$ of $P(x)$ by first computing $P(\mathbf{x}_i) \cdot P(\bar{\mathbf{x}}_i) = \frac{N_i}{D_i}, 1 \leq i \leq 4$. We then have $N(x) = P(x) \prod_i N_i = 14x^{162} + 157x^{160} + \dots + 22x^2 + 165$ and $D(x) = \prod_i D_i = x^{144} + 107x^{142} + \dots + 90x^2 + 75$. Hence $N_P(x) = \frac{N(x)}{D(x)}$. Finally, we compute all the coefficients of $p(x)$ by repeating Steps 13–16. The result is

$$p(x) = x^{18} + 170x^{16} + 36x^{14} + 95x^{12} + 126x^{10} + 53x^8 + 84x^6 + 143x^4 + 9x^2 + 178.$$

Example 12.3 (Division by $\ell = 3$ via Algorithm 12.2). As before, let $p = 179$ and $E_{1728} : y^2 = x^3 - x$ the supersingular elliptic curve over \mathbb{F}_p of j -invariant $j(E_{1728}) = 1728$ as in Example 12.2. Then the endomorphism ring of E_{1728} contains the endomorphism $[i]$ defined as $[i](x, y) := (-x, iy)$ with $i \in \mathbb{F}_{p^2}$ and $i^2 = -1$.

The map $\theta = 1 + [i]$ is a separable endomorphism and we have $([3]\theta)(x, y) = \left(\frac{F_1(x)}{F_2(x)}, \frac{G_1(x)}{G_2(x)}y\right)$, defined over \mathbb{F}_{p^2} , with

$$\begin{aligned} F_1(x) &= 169ix^{18} + 33ix^{16} + 72ix^{14} + 66ix^{12} + 68ix^{10} + 111ix^8 + 113ix^6 \\ &\quad + 107ix^4 + 146ix^2 + 10i, \\ F_2(x) &= x^{17} + 8x^{15} + 45x^{13} + 124x^{11} + 110x^9 + 124x^7 + 45x^5 + 8x^3 + x, \\ G_1(x) &= (58i + 58)x^{26} + (170i + 170)x^{24} + \dots + (170i + 170)x^2 + 58i + 58, \\ G_2(x) &= x^{26} + 12x^{24} + 2x^{22} + 66x^{20} + 128x^{18} + 44x^{16} + 171x^{14} + 44x^{12} \\ &\quad + 128x^{10} + 66x^8 + 2x^6 + 12x^4 + x^2. \end{aligned}$$

We apply Algorithm 12.2 to divide $[3]\theta$ by 3 to obtain $\theta = [f(x), g(x)y]$ as follows.

In Step 1, we write $F(x) = \frac{c_F \cdot P(x)}{(\psi_{E_{1728,3}}(x))^2 \cdot Q(x)}$ where $c_F = 169i$, $\psi_{E_{1728,3}}(x) = x^4 + 177x^2 + 119$ and

$$\begin{aligned} P(x) &= x^{18} + 122x^{16} + \dots + 57x^2 + 178, \\ Q(x) &= x^9 + 12x^7 + 30x^5 + 143x^3 + 9x. \end{aligned}$$

In Step 2, we compute X_1 and Y_2 using the formula for multiplication by 3 map on E_{1728} . Here, X_1 is as given in Example 12.2 and

$$Y_2 = \frac{126x^{12} + 92x^{10} + 153x^8 + 136x^6 + 139x^4 + 63x^2 + 159}{x^{12} + 173x^{10} + 11x^8 + 175x^6 + 56x^4 + 59x^2 + 53}.$$

Then we compute $p(x) = P(x)|_{X_1}$ and $q(x) = Q(x)|_{X_1}$ in Steps 3 and 4 using Algorithm 12.1 to obtain $p(x) = x^{18} + 170x^{16} + \dots + 9x^2 + 178$, and $q(x) = x^9$. In Step 5, computing 9-th roots of $p(x)$ and $q(x)$ yields $p_0(x) = x^2 + 178$ and $q_0(x) = x$. The final output is

$$\begin{aligned} f(x) &= c_F \ell^2 \cdot \frac{p_0(x)}{q_0(x)} = \frac{89ix^2 + 90i}{x}, \\ g(x) &= \frac{G(x)}{Y_2(f(x))} = \frac{(134i + 134)x^2 + 134i + 134}{x^2}. \end{aligned}$$

To determine the complexity of Algorithm 12.1, we first prove the following lemma which is needed in the proof of Proposition 12.5.

Lemma 12.4 Fix $0 \leq i \leq \frac{\ell^2-1}{2}$, the products $\mathbf{x}_i \bar{\mathbf{x}}_i$ and $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ are rational functions in x, y^2 , and y_i^2 .

Proof By direct computation, both $\mathbf{x}_i + \bar{\mathbf{x}}_i$ and $\mathbf{x}_i \bar{\mathbf{x}}_i$ are rational functions in x, y^2 , and y_i^2 . As a symmetric polynomial in \mathbf{x}_i and $\bar{\mathbf{x}}_i$, the quantity $P(\mathbf{x}_i)P(\bar{\mathbf{x}}_i)$ is a polynomial in $\mathbf{x}_i + \bar{\mathbf{x}}_i$ and $\mathbf{x}_i \bar{\mathbf{x}}_i$, hence also a rational function in x, y^2 and y_i^2 . □

Proposition 12.5 *Algorithm 12.1 is correct and has runtime $O(\deg^2(P)\mathbf{M}(p^m))$.*

Proof Algorithm 12.1 is correct by [42, Pages 8–9] and Lemma 12.4. Steps 1–3 are negligible because they require a fixed number of operations in an extension of \mathbb{F}_{p^2} of degree $O(\ell^2)$. Since $P(x) \in \mathbb{F}_{p^m}[x]$ and $E_1[\ell]$ is defined over an extension of \mathbb{F}_{p^2} of degree at most ℓ^2 by Lemma 2.3, all the arithmetic in the remaining steps takes place in a field extension of \mathbb{F}_{p^2} of degree $\text{lcm}(\ell^2, m) = O(m)$.

In the first loop (Steps 5–10), the most costly steps are 7 and 10 which both require $O(\deg^2(P))$ operations; the remaining steps are linear in $\deg P$ when Horner’s algorithm is used. In the second loop (Steps 12–11), $p(x)$ is computed as described in [42, Page 9]. Step 13 requires $O(\deg P)$ field operations using Horner’s algorithm again. Since X_1 has degree $O(\ell^2)$, Step 11 also takes $O(\deg P)$ operations. Hence the second loop takes $O(\deg^2(P))$ field operations. \square

Proposition 12.6 *Algorithm 12.2 is correct and has runtime $O(\deg^2(\varphi)\mathbf{M}(p))$.*

Proof The correctness of Algorithm 12.2 follows from [42, Proposition 2.6]. By Lemma 2.2, φ is defined over $\mathbb{F}_{p^{12}}$, so all the rational functions appearing in the algorithm belong to $\mathbb{F}_{p^{12}}(x)$. We also note that $P(x)$ and $Q(x)$ have degree $O(\deg \varphi)$, hence so do $p(x)$, $q(x)$, $p_0(x)$ and $q_0(x)$.

Since $\psi_{E_1, \ell}(x)$ and $W_1(x)$ have fixed degree, Step 1 requires $O(\deg \varphi)$ field operations. Steps 5 and 6 take $\tilde{O}(\deg \varphi)$ operations using fast polynomial arithmetic; see [30, Theorem 1.2]. Here, to extract an ℓ^2 -th root of $p(x)$, we apply a truncated variant of Newton’s method (see [57, Sections 9.4 and 9.6]) to the polynomial $H(y) = y^{\ell^2} - p(x)$ and compute the sequence of polynomials

$$f_0(x) = x^{\deg p}, \quad f_{i+1}(x) = f_i(x) - \left\lfloor \frac{H(f_i(x))}{H'(f_i(x))} \right\rfloor \quad (i \geq 0)$$

to obtain $p_0(x)$ after at most $\lceil \log_2(\deg p) \rceil$ iterations; similarly for $q_0(x)$.

The runtime of Algorithm 12.2 is thus dominated by Steps 3 and 4, which have runtime $O(\deg^2(\varphi)\mathbf{M}(p^{12})) = O(\deg^2(\varphi)\mathbf{M}(p))$. \square

Acknowledgements We would like to thank Catalina Camacho-Navarro, Elena Fuchs, Steven Galbraith, David Kohel, Péter Kutas, and Christophe Petit for helpful discussion. We are especially grateful to Benjamin Wesolowski, who took the time to share highly valuable suggestions on an earlier draft, particularly some important corrections concerning Proposition 9.4. We thank the conference *Women in Numbers 5* for the opportunity to form this research group. Last but not least, we thank our anonymous referees for their careful reading and helpful suggestions which led to clarifications and improvements to this paper.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included

in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Apostol, T.M.: Introduction to Analytic Number Theory. Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg (1976)
2. Arpin, S., Chen, M., Lauter, K.E., Scheidler, R., Stange, K.E., Tran, H.T.N.: Orientations and cycles in supersingular isogeny graphs. [arXiv:2205.03976](https://arxiv.org/abs/2205.03976) (2022)
3. Arpin, S., Chen, M., Lauter, K.E., Scheidler, R., Stange, K.E., Tran, H.T.N.: WIN5 github repository. <https://github.com/SarahArpin/WIN5> (2022)
4. Bank, E., Camacho-Navarro, C., Eisenträger, K., Morrison, T., Park, J.: Cycles in the supersingular 1-isogeny graph and corresponding endomorphisms. In: Research Directions in Number Theory, pp. 41–66. Springer, Berlin (2019)
5. Biasse, J.-F., Iezzi, A., Jacobson, M.J.: A note on the security of csidh. In: Chakraborty, D., Iwata, T. (eds.) Progress in Cryptology - INDOCRYPT 2018, pp. 153–168. Springer International Publishing, Cham (2018)
6. Bröker, R., Charles, D., Lauter, K.: Evaluating large degree isogenies and applications to pairing based cryptography. In: Pairing-Based Cryptography-Pairing 2008. Lecture Notes in Computer Science, vol. 5209, pp. 100–112. Springer, Berlin (2008)
7. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH (preliminary version). (2022)
8. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Advances in Cryptology—ASIACRYPT 2018, Part III Lecture Notes in Computer Science, vol. 11274, pp. 395–427. Springer, Cham (2018)
9. Castryck, W., Panny, L., Vercauteren, F.: Rational isogenies from irrational endomorphisms. In: Advances in Cryptology—EUROCRYPT 2020. Part II Lecture Notes in Computer Science, vol. 12106, pp. 523–548. Springer, Cham (2020)
10. Charles, D.X., Goren, E.Z., Lauter, K.E.: Cryptographic hash functions from expander graphs. *J. Cryptol.* **22**(1), 93–113 (2009)
11. Chenu, M., Smith, B.: Higher-degree supersingular group actions. *Math. Cryptol.* **1**(1), 1–15 (2021)
12. Cheung, K.K.H., Mosca, M.: Decomposing finite abelian groups. *Quantum Inf. Comput.* **1**(3), 26–32 (2001)
13. Childs, A., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.* **8**(1), 1–29 (2014)
14. Cohen, H.: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics, vol. 138. Springer-Verlag, Berlin (1993)
15. Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. *J. Math. Cryptol.* **14**(1), 414–437 (2020)
16. Coron, J.S., Naccache, D.: Security analysis of the Gennaro–Halevi–Rabin signature scheme. In: Preeel, B. (ed.) Advances in Cryptology—EUROCRYPT 2000, pp. 91–101. Springer, Berlin, Heidelberg (2000)
17. Couveignes, J.-M.: Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291. <https://ia.cr/2006/291> (2006)
18. Cox, D.A.: Primes of the Form $x^2 + ny^2$. Pure and Applied Mathematics, 2nd edn. Wiley, Hoboken, NJ (2013)
19. Croot, E., Granville, A., Pemanle, R., Tetali, P.: On sharp transitions in making squares. *Ann. Math.* **175**(3), 1507–1550 (2012)
20. Dartois, P., De Feo, L.: On the security of osidh. In: Public-Key Cryptography—PKC 2022: 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part I, volume 13177 of Lecture Notes in Computer Science, pp 52–81. Springer, Cham, (2022)
21. De Feo, L.: Mathematics of isogeny based cryptography. [arXiv:1711.04062](https://arxiv.org/abs/1711.04062) (2017)

22. De Feo, L., Delpech de Saint Guilhem, C., Fouotsa, T.B., Kutas, P., Leroux, A., Petit, C., Silva, J., Wesolowski, B.: SÉTA: Supersingular Encryption from Torsion Attacks, volume 13090 of Lecture Notes in Computer Science, pp. 249–278. Springer International Publishing, Cham (2021)
23. De Feo, L., Kieffer, J., Smith, B.: Towards practical key exchange from ordinary isogeny graphs. In: Advances in Cryptology—ASIACRYPT 2018. Part III, volume 11274 of Lecture Notes in Computer Science
24. de Quehen, V., Kutas, P., Leonardi, C., Martindale, C., Panny, L., Petit, C., Stange, K.E.: Improved Torsion-Point Attacks on SIDH Variants, volume 12827 of Lecture Notes in Computer Science, pp. 432–470. Springer International Publishing, Cham (2021)
25. Eisenträger, K., Hallgren, S., Lauter, K., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In: Advances in Cryptology—EUROCRYPT 2018. Part III, volume 10822 of Lecture Notes in Computer Science, pp. 329–368. Springer, Cham (2018)
26. Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over \mathbb{Q} . *Invent. Math.* **89**(3), 561–567 (1987)
27. Feo, L.D., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S.-P., Panny, L., Wesolowski, B.: Scallop: scaling the csi-fish. *Cryptology ePrint Archive*, Paper 2023/058. <https://eprint.iacr.org/2023/058> (2023)
28. Fité, F., Sutherland, A. V.: Sato-Tate groups of $y^2 = x^8 + c$ and $y^2 = x^7 - cx$. In: Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, volume 663 of Contemporary Mathematics, pp. 103–126. American Mathematical Society, Providence, RI (2016)
29. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. *J. Cryptol.* **33**(1), 130–175 (2020)
30. Harvey, D., van Der Hoeven, J.: Polynomial multiplication over finite fields in time $O(n \log n)$. <https://hal.archives-ouvertes.fr/hal-02070816/document> (2019)
31. Ionica, S., Joux, A.: Pairing the volcano. In: Algorithmic Number Theory. Lecture Notes in Computer Science, pp. 201–208. Springer, Berlin (2010)
32. Kaneko, M.: Supersingular j -invariants as singular moduli mod p . *Osaka J. Math.* **26**(4), 849–855 (1989)
33. Kieffer, J.: Accelerating the couveignes rostovtsev stolbunov key exchange protocol. Master’s thesis, l’Université Paris IV. <https://arxiv.org/pdf/1804.10128.pdf> (2018)
34. Knuth, D.E.: The Art of Computer Programming. Addison-Wesley Series in Computer Science and Information Processing. Seminumerical algorithms. Addison-Wesley Publishing Co., Reading, MA (1981)
35. Kohel, D., Lauter, K., Petit, C., Tignol, J.-P.: On the quaternion ℓ -isogeny path problem. *LMS J. Comput. Math.* **17**, 151 (2014)
36. Kohel, D. R.: Endomorphism rings of elliptic curves over finite fields. ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.)—University of California, Berkeley (1996)
37. Kutas, P., Merz, S.-P., Petit, C., Weitkaemper, C.: One-way functions and malleability oracles: hidden shift attacks on isogeny-based protocols. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology—EUROCRYPT 2021. Lecture Notes in Computer Science, pp. 242–271. Springer, Berlin (1996)
38. Love, J., Boneh, D.: Supersingular curves with small non-integer endomorphisms. [arXiv:1910.03180](https://arxiv.org/abs/1910.03180) (2020)
39. Love, J., Boneh, D.: Supersingular curves with small noninteger endomorphisms. In: ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium, volume 4 of Open Book Ser., pp. 7–22. Math. Sci. Publ., Berkeley, CA (2020)
40. Maino, L., Martindale, C.: An attack on sidh with arbitrary starting curve. (2022)
41. McMurdy, K.: https://phobos.ramapo.edu/~kcmurdy/research/SAGE_ssEndos/. Accessed Jan 10 (2022)
42. McMurdy, K.: Explicit representation of the endomorphism rings of supersingular elliptic curves. <https://phobos.ramapo.edu/~kcmurdy/research/McMurdy-ssEndoRings.pdf> (2014)
43. Onuki, H.: On oriented supersingular elliptic curves. *Finite Fields App.* **69**, 101777 (2021)
44. Pizer, A.K.: Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)* **23**(1), 127–137 (1990)
45. Robert, D.: Evaluating isogenies in polylogarithmic time. *Cryptology ePrint Archive*, Paper 2022/1068. <https://eprint.iacr.org/2022/1068> (2022)
46. Robin, G.: Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann. *J. Math. Pures Appl.* **63**(2), 187–213 (1984)

47. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145. <https://eprint.iacr.org/2006/145> (2006)
48. Sardari, N.T.: Diameter of Ramanujan graphs and random Cayley graphs. *Combinatorica* **39**(2), 427–446 (2019)
49. Schoof, R.: Four primality testing algorithms. In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, Volume 44 of Math. Sci. Res. Inst. Publ., pp. 101–126. Cambridge Univ. Press, Cambridge (2008)
50. Shumow, D.: Isogenies of elliptic curves: a computational approach. Master's thesis, University of Washington. [arXiv:0910.5370](https://arxiv.org/abs/0910.5370) (2009)
51. Silverman, J.H.: *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009)
52. Stange, K. E.: Frobenius and the endomorphism ring of $j = 1728$. <http://math.colorado.edu/~kstange/papers/1728.pdf> (2021)
53. Tenenbaum, G.: On ultrafriable integers. *Q. J. Math.* **66**(1), 333–351 (2015)
54. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*. <https://www.sagemath.org> (2022)
55. Vélou, J.: Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B* **273**, 238–241 (1971)
56. Voight, J.: *Quaternion Algebras*. Graduate Texts in Mathematics, vol. 288. Springer, Cham (2021)
57. von zur Gathen, J., Gerhard, J.: *Modern Computer Algebra*, 2nd edn. Cambridge University Press, Cambridge (2013)
58. von zur Gathen, J., Shoup, V.: Computing Frobenius maps and factoring polynomials. *Comput. Complex.* **2**(3), 187–224 (1992)
59. Waterhouse, W.C.: Abelian varieties over finite fields. *Ann. Sci. l'École Normale Supérieure* **2**, 521–560 (1969)
60. Wesolowski, B.: Orientations and the supersingular endomorphism ring problem. In: *Advances in Cryptology—EUROCRYPT 2022*. Lecture Notes in Computer Science, vol. 13277, pp. 345–371. Springer, Cham (2022)
61. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science—FOCS 2021*, pp. 1100–1111. IEEE Computer Soc., Los Alamitos, CA (2022)
62. Williams, H.C., te Riele, H.: New computations concerning the Cohen–Lenstra Heuristics. *Exp. Math.* **12**(1), 99–113 (2003)
63. Yang, T.: Minimal CM liftings of supersingular elliptic curves. *Pure Appl. Math. Q.* **4**(4), 1317–1326 (2008)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Sarah Arpin¹  · Mingjie Chen²  · Kristin E. Lauter³  · Renate Scheidler⁴  ·
Katherine E. Stange⁵  · Ha T. N. Tran⁶ 

Mingjie Chen
m.chen.1@bham.ac.uk

Kristin E. Lauter
klauter@fb.com

Renate Scheidler
rscheidl@ucalgary.ca

Katherine E. Stange
kstange@math.colorado.edu

Ha T. N. Tran
hatran1104@gmail.com

- ¹ Mathematics Institute, Universiteit Leiden, Leiden, The Netherlands
- ² School of Computer Science, University of Birmingham, University Road West, Birmingham B15 2TT, UK
- ³ Facebook AI Research, Meta, Seattle, WA, USA
- ⁴ Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada
- ⁵ Department of Mathematics, University of Colorado, Campus Box 395, Boulder, CO 80309-0395, USA
- ⁶ Department of Mathematical and Physical Sciences, Concordia University of Edmonton, 7128 Ada Blvd NW, Edmonton AB T5B 4E4, Canada