Computing supersingular endomorphism rings using inseparable endomorphisms

Jenny Fuselier[1], Annamaria Iezzi[2,3,4], Mark Kozek[5], Travis Morrison[6], and Changningphaabi Namoijam[7]

[1]Department of Mathematical Sciences, High Point University, High Point, NC 27268, USA
[2]Univ. Grenoble Alpes, CNRS, Grenoble INP, LJK, 38000 Grenoble, France
[3]Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli Federico II, I-80126 Napoli, Italy
[4]Laboratoire GAATI, Université de la Polynésie française, 98702 Faaa, French Polynesia
[5]Department of Mathematics & Computer Science, Whittier College, Whittier, CA 90601, USA
[6]Department of Mathematics, Virginia Tech, Blacksburg, VA 24060 USA
[7]Department of Mathematics, Colby College, Waterville, ME 04901, USA

Abstract

We give an algorithm for computing an inseparable endomorphism of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, which, conditional on GRH, runs in expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ bit operations and requires $O((\log p)^2)$ storage. This matches the time and storage complexity of the best conditional algorithms for computing a nontrivial supersingular endomorphism, such as those of Eisenträger–Hallgren–Leonardi–Morrison–Park and Delfs–Galbraith. Unlike these prior algorithms, which require two paths from E to a curve defined over $\mathbb{F}_p$, the algorithm we introduce only requires one; thus when combined with the algorithm of Corte-Real Santos–Costello–Shi, our algorithm will be faster in practice. Moreover, our algorithm produces endomorphisms with predictable discriminants, enabling us to prove properties about the orders they generate. With two calls to our algorithm, we can provably compute a Bass suborder of $\mathrm{End}(E)$. This result is then used in an algorithm for computing a basis for $\mathrm{End}(E)$ with the same time complexity, assuming GRH. We also argue that $\mathrm{End}(E)$ can be computed using $O(1)$ calls to our algorithm along with polynomial overhead, conditional on a heuristic assumption about the distribution of the discriminants of these endomorphisms. Conditional on GRH and this additional heuristic, this yields a $O(p^{1/2}(\log p)^2(\log\log p)^3)$ algorithm for computing $\mathrm{End}(E)$ requiring $O((\log p)^2)$ storage.

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, where q is a power of a prime p. If E is ordinary, in order to compute the (geometric) endomorphism ring $\mathrm{End}(E)$ of E, one must determine the index $[\mathrm{End}(E) : \mathbb{Z}[\pi_E]]$ where $\mathbb{Z}[\pi_E]$ is the order generated by the Frobenius endomorphism π_E of E. This problem has been well-studied, and there exist algorithms for computing the endomorphism ring of an ordinary elliptic curve due to Bisson and Sutherland [BS11] which run in expected subexponential time, conditional on reasonable heuristics including the Generalized Riemann Hypothesis (GRH). Recently, Robert [Rob22] showed that, given access to a factoring oracle, there is a polynomial-time algorithm for computing the endomorphism ring of an ordinary elliptic curve.

When E is supersingular, its endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra, and $\mathrm{End}(E)$ is a maximal order of $\mathrm{End}^0(E)$. In this case, there is no canonical imaginary quadratic order which embeds in $\mathrm{End}(E)$. Even worse, if we have a suborder $\Lambda \subseteq \mathrm{End}(E)$, there can be exponentially (in $\log(\mathrm{disc}(\Lambda))$) many pairwise non-isomorphic maximal orders which contain Λ. This stands in contrast to the ordinary case where we have a canonical embedding of a finite-index suborder and there is a unique maximal order containing both this suborder and $\mathrm{End}(E)$: this maximal order is the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\pi_E) \cong \mathrm{End}^0(E)$.

This suggests that computing the endomorphism ring of a supersingular elliptic curve is a hard problem. More precisely, there are no known efficient algorithms for solving the *endomorphism ring* problem:

Problem 1. *Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute the endomorphism ring* $\mathrm{End}(E)$ *of E, that is, compute a basis of the maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ such that* $\mathrm{End}(E) \cong \mathcal{O}$.

The assumption that Problem 1 is hard is central to the security of isogeny-based cryptography. Indeed, in isogeny-based cryptosystems, a secret key is an isogeny of large, smooth degree between two supersingular elliptic curves – a path in the supersingular isogeny graph – and the problem of path-finding in supersingular isogeny graphs has been proven to be equivalent to the problem of computing supersingular endomorphism rings, assuming GRH (see Eisenträger, Hallgren, Lauter, Morrison, and Petit [EHL+18], Wesolowski [Wes22] and Page and Wesolowski [PW23]).

There are two approaches to computing the endomorphism ring of a supersingular elliptic curve E. One approach uses the reduction of [EHL+18] to path-finding in isogeny graphs, and the second, perhaps more straightforward approach, involves computing endomorphisms of E until computing a generating set for $\mathrm{End}(E)$. In the first approach, one computes a supersingular curve E_0 with known or easily computable endomorphism ring, which can be done efficiently assuming GRH with Bröker's algorithm [Brö09], and then computes an isogeny $E_0 \to E$. With the isogeny $E_0 \to E$ and $\mathrm{End}(E_0)$, one can efficiently compute $\mathrm{End}(E)$ via the reduction in [EHL+18]. However, in isogeny-based cryptosystems such as SQIsign [DFKL+20], there is a curve E_0 with known endomorphism ring as a public parameter for the cryptosystem, a user's public key is another supersingular elliptic curve E, and their corresponding private key is a secret isogeny $E_0 \to E$. Thus the reduction to path-finding gives a roundabout attack: any isogeny $E_0 \to E$ is (at least functionally) the secret key that an attacker wishes to compute, so an attacker would not need $\mathrm{End}(E)$ after having computed any isogeny $E_0 \to E$. This motivates an investigation into the second approach to computing $\mathrm{End}(E)$ and hence into the design of algorithms for computing a single endomorphism of E. This paper focuses on the design of such an algorithm and an investigation into what can be proved about an order generated by the endomorphisms output by a few calls to that algorithm.

The first algorithm for computing nontrivial endomorphisms of a supersingular elliptic curve E is due to Kohel [Koh96] and runs in time $O(p^{1+\epsilon})$ for any $\epsilon > 0$; in Kohel's strategy one first computes a spanning tree of the ℓ-isogeny graph rooted at E and then adds two edges to produce two cycles and thus two endomorphisms of E. These two cycles generate a suborder. Delfs and Galbraith [DG16] compute an endomorphism of E by finding two distinct isogenies $\psi_i \colon E \to E_i$ to two distinct $\mathbb{F}_p$-rational curves E_i, $i = 1, 2$, solve the easier problem of path-finding in the $\mathbb{F}_p$-rational isogeny graph of $\mathbb{F}_p$-rational supersingular elliptic curves to compute an isogeny $\phi \colon E_1 \to E_2$, and return the endomorphism $\widehat{\psi_2} \circ \phi \circ \psi_1$. The complexity of finding an isogeny $\psi_i \colon E \to E_i$ with E_i defined over $\mathbb{F}_p$ is $\widetilde{O}(p^{1/2})$, conditional on GRH, while the complexity of the algorithm of [DG16] for pathfinding in the $\mathbb{F}_p$-subgraph is $\widetilde{O}(p^{1/4})$. Eisenträger, Hallgren, Leonardi, Morrison, and Park [EHL+20] give an algorithm for computing a cycle, based at E, in the ℓ-isogeny graph $G(p, \ell)$ by finding two distinct isogenies $\phi_i \colon E \to E^{(p)}$, $i = 1, 2$, where $E^{(p)}$ is the codomain of the p-power Frobenius isogeny $\pi \colon E \to E^{(p)}$. Then $\widehat{\phi_2} \circ \phi_1$ is an endomorphism of E. An isogeny $E \to E^{(p)}$ is computed by first using random walks in the ℓ-isogeny graph to find an isogeny $\psi_1 \colon E \to E_1$ where E_1 is defined over $\mathbb{F}_p$; then $\widehat{\psi_1^{(p)}} \circ \psi_1$ is an isogeny $E \to E^{(p)}$, where $\psi^{(p)}$ is the isogeny obtained by the action of the Frobenius automorphism on ψ (see Section 3.2.1). The latter two algorithms for computing a nontrivial endomorphism have the same asymptotic complexity, since both require two paths from E to the $\mathbb{F}_p$-subgraph, but the algorithm of [EHL+20] is strictly faster since the overhead is polynomial in $\log p$ compared to the exponential overhead $\widetilde{O}(p^{1/4})$ required to find a path in the $\mathbb{F}_p$-subgraph in the algorithm of [DG16].

In this paper we introduce an algorithm, Algorithm 1, for computing certain inseparable endomorphisms of E which we define as *inseparable reflections* in Section 3. The idea is simple: to compute an inseparable endomorphism of E, compute an isogeny $\psi \colon E \to E^{(p)}$ as described above, and return $\pi \circ \psi$ where π is the p-power Frobenius. Assuming the Generalized Riemann Hypothesis, it terminates in expected $\widetilde{O}(p^{1/2})$ bit operations, it is low storage and easy to parallelize (unlike a generic low-storage collision algorithm such as Pollard's ρ). Algorithm 1 is twice as fast as the algorithms in [DG16, EHL+20] since it requires only one isogeny to a $\mathbb{F}_p$-rational curve, rather than 2. Thus Algorithm 1 reflects the state-of-the-art in conditional algorithms for computing a nontrivial endomorphism of a supersingular elliptic curve (when combined with the algorithm of Santos–Costello–Shi [CSCS22] for fast subfield detection). One might suspect that the fact that the output is always an inseparable endomorphism of the input curve E might be an obstacle if one

was trying to use this algorithm to compute a generating set for $\mathrm{End}(E)$. To the contrary, we show that Algorithm 1 improves on all previous algorithms for computing endomorphisms in a second way: we are able to control the arithmetic properties of orders generated by endomorphisms output by Algorithm 1. More precisely, Algorithm 1 has auxiliary inputs ℓ (a prime) and d (a positive square-free integer) that can be chosen so that the output endomorphism generates an imaginary quadratic order that is maximal at every prime except at ℓ. As a consequence, with an appropriate choice of the auxiliary inputs, two endomorphisms output by the algorithm will generate a Gorenstein order (Proposition 3.13) and, with slightly more care, a Bass order (3.15).

We give two algorithms for computing $\mathrm{End}(E)$ using Algorithm 1: a rigorous (assuming GRH) algorithm and a simple but heuristic algorithm. Let us first outline the rigorous version of the algorithm. First, Algorithm 2 calls Algorithm 1 twice to produce a basis for a Bass suborder of $\mathrm{End}(E)$:

Theorem (Theorem 4.8)**.** *On input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, Algorithm 2 computes a basis of a Bass suborder of $\mathrm{End}(E)$. Assuming the Generalized Riemann Hypothesis, the algorithm terminates in an expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ number of bit operations.*

From a theoretical viewpoint, it suffices to compute a Bass suborder $\mathcal{O}$ of $\mathrm{End}(E)$: by [EHL+20, Proposition 5.2], the number of maximal overorders containing a given Bass order Λ is bounded by a quantity growing subexponentially in the size of Λ[1], and one can efficiently enumerate these maximal overorders. Using algorithms from [KLPT14, EHL+18, Wes22], one can efficiently decide whether a given maximal order $\mathcal{O} \supseteq \Lambda$ is isomorphic to $\mathrm{End}(E)$. Building on ideas in [EHL+20], Algorithm 3 computes $\mathrm{End}(E)$ by computing a Bass suborder Λ of $\mathrm{End}(E)$, and then enumerates maximal orders $\mathcal{O} \supseteq \Lambda$ until finding $\mathcal{O} \cong \mathrm{End}(E)$. In Section 4, we show that one can remove the heuristic assumptions needed in [EHL+20] and we prove the following theorem:

Theorem (Theorem 5.5)**.** *There exists an algorithm (Algorithm 3) which takes as input a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and returns a basis of a maximal order $\mathcal{O}$ contained in the quaternion algebra ramified at $\{p, \infty\}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. Assuming the Generalized Riemann Hypothesis, Algorithm 3 terminates in an expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ number of bit operations.*

Summarizing the above theorems, two endomorphisms produced by Algorithm 1 generate a Bass suborder of $\mathrm{End}(E)$, and with subexponential overhead, we compute a basis for $\mathrm{End}(E)$.

A more straightforward approach to computing $\mathrm{End}(E)$ is to compute several endomorphisms until finding a generating set. Suppose we have an algorithm which generates a random endomorphism of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$. What is the expected number of calls to that algorithm before finding a set of endomorphisms which generate $\mathrm{End}(E)$ as an order? In [GPS17], Galbraith, Petit, and Silva give a heuristic argument that this expectation is $O(\log p)$. Our work in Section 6.1 suggests that this estimate is pessimistic: the expected number of calls is bounded by a constant, assuming a reasonable heuristic on the distribution of the discriminants of random endomorphisms.

In this paper, we focus on computing $\mathrm{End}(E)$ with endomorphisms output by Algorithm 1. We first remark that no collection of inseparable endomorphisms can generate $\mathrm{End}(E)$: the endomorphisms produced by Algorithm 1 are inseparable and hence belong to P, the 2-sided ideal of inseparable endomorphisms of E. We show in Proposition 3.1 that $\mathbb{Z} + P$ is the unique suborder of $\mathrm{End}(E)$ of index p, and the only maximal order containing $\mathbb{Z} + P$ is $\mathrm{End}(E)$. In Section 6.1, we show that the expected number of calls to Algorithm 1 before finding a generating set for $\mathbb{Z} + P$ is bounded by a positive constant that is not dependent on either p or E, assuming Heuristic 6.1 which concerns the distribution of discriminants of endomorphisms produced by Algorithm 1. Finally, with a basis of $\mathbb{Z} + P$, one can efficiently compute a basis of $\mathrm{End}(E)$ using algorithms due to Voight [Voi13]. While this approach is no faster than the enumeration-style approach in Algorithm 3, it is simpler to implement: it requires only an implementation of Algorithm 1, an implementation of a generalization [BCNE+19] of Schoof's algorithm [Sch95], and linear algebra to compute a basis for an order in the quaternion algebra isomorphic to $\mathrm{End}(E)$. Our implementation of this algorithm and all necessary subroutines in SageMath [The22] is available at `https://github.com/travismo/inseparables`.

In conclusion, we prove that two calls to Algorithm 1 produce a Bass order unconditionally, and, assuming Heuristic 6.1, only $O(1)$ calls to Algorithm 1 (along with subexponential overhead) produce $\mathrm{End}(E)$.

[1] Actually, this is proven in [EHL+20] under the additional assumption that Λ is hereditary (i.e. its reduced discriminant is square-free), but this assumption is not necessary; see the proof of Theorem 3.15.

Alternatively, by Theorem 1.1 of [ES24], two calls to Algorithm 1, the factorization of the discriminant of the order generated by the output, and polynomial overhead will produce $\mathrm{End}(E)$.

Note that by Theorem 8.8 of [PW23], there is an algorithm for computing $\mathrm{End}(E)$ in $\widetilde{O}(p^{1/2})$ bit operations unconditionally, but the algorithm also requires $\widetilde{O}(p^{1/2})$ storage. On the other hand, the heuristic algorithm for computing $\mathrm{End}(E)$ we provide in Section 6.1 – compute inseparable endomorphisms with Algorithm 1 until finding a basis for $\mathbb{Z}+P$ and then recover a basis for $\mathrm{End}(E)$ with linear algebra – requires only polylog(p) storage and terminates in expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ bit operations. Our provable variant has the same asymptotic time complexity, and the storage complexity is determined by the storage used to factor a single integer of magnitude $O(p^4)$.

The paper is organized as follows. In Section 2, we review the mathematical background of the paper and fix our notation. In Section 3, we study the properties of the suborder $\mathbb{Z}+P \subseteq \mathrm{End}(E)$, where P is the ideal of inseparable endomorphisms of E. We also define inseparable reflections, building on the definition of (d,ϵ)-structures of Chenu and Smith [CS21], and study the structure of quaternionic orders generated by inseparable reflections. In particular we determine when they generate Gorenstein (Proposition 3.13) and Bass (Theorem 3.15) orders in $\mathrm{End}(E)$. Section 4 makes the ideas in Section 3 effective. First, we analyze Algorithm 1, which computes inseparable endomorphisms of E. Next, we use Algorithm 1 in Algorithm 2 to compute a Bass suborder of $\mathrm{End}(E)$. In Section 5, we introduce Algorithm 3, which provably computes $\mathrm{End}(E)$ and, conditional on GRH but no further heuristics, terminates in $\widetilde{O}(p^{1/2})$ time. Algorithm 3 calls Algorithm 2, along with algorithms of [EHL+18, EHL+20, Wes22], to compute a basis for $\mathrm{End}(E)$. Finally, in Section 6, we propose a heuristic algorithm to compute $\mathrm{End}(E)$ in which we first find enough inseparable reflections to generate $\mathbb{Z}+P$ and then use linear algebra to compute a basis for $\mathrm{End}(E)$ from a basis for $\mathbb{Z}+P$. In Appendix A, we discuss some of the algorithmic aspects of this approach.

Acknowledgements

We thank Heidi Goodson, Christelle Vincent, and Mckenzie West for organizing the first edition of *Rethinking Number Theory* in 2020, where this project began, and the American Institute of Mathematics for their additional support. We also thank John Voight for several helpful discussions. We thank the referee for several useful comments and suggestions that improved the presentation of the results.

The second author was partially supported by the European Union - FSE-REACT-EU, PON Research and Innovation 2014-2020 DM1062/2021 contract number 18-I-15358-2, by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM), by Projet ANR collaboratif Barracuda ANR-21-CE39-0009-BARRACUDA, and by the ANR Grant ANR-20-CE40-0013-MELODIA. The fourth author was partially supported by the National Science Foundation grant CNS-2340564 and the Commonwealth Cyber Initiative. The fifth author was partially supported by MOST Grant 110-2811-M-007-517.

2 Notation and background

In this section we fix our notation and recall some definitions and facts about elliptic curves and quaternion algebras. We refer the reader to Silverman [Sil09, Chapters III and V] and Voight [Voi21] for details.

2.1 Elliptic curves

Let q be a positive power of a prime $p>3$, and let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Since isomorphic elliptic curves have isomorphic endomorphism rings, we may always assume that E is defined by a short Weierstrass affine form $E: y^2 = x^3+ax+b$, with $a,b\in\mathbb{F}_q$, such that $4a^3+27b^2\neq 0$. An *isogeny* $\phi\colon E\to E'$ between two elliptic curves is a non-constant rational map inducing a group homomorphism $E(\overline{\mathbb{F}_q})\to E'(\overline{\mathbb{F}_q})$. An *endomorphism* of E is either an isogeny $E\to E$ or the zero-map on E. We define the elliptic curve $E^{(p)}: y^2 = x^3+a^px+b^p$, and we denote by π the p-power Frobenius isogeny $\pi\colon E\to E^{(p)}$ defined by $\pi(x,y)=(x^p,y^p)$. We use the same notation π for every such Frobenius isogeny, independent of the choice of the starting elliptic curve. We let π_E denote the Frobenius endomorphism which sends

$(x, y) \mapsto (x^q, y^q)$. For an integer n, we denote by $E[n]$ the *n-torsion subgroup* of E, consisting of points of E of order dividing n. The elliptic curve E is *supersingular* if and only if $E[p] = \{0\}$.

For elliptic curves E, E' defined over $\mathbb{F}_q$, we use the notation $\mathrm{Hom}(E, E')$ for the set of isogenies from E to E' defined over $\mathbb{F}_q$ together with the zero map. If $L/\mathbb{F}_q$ is an algebraic extension, we let E_L denote the base change of E from $\mathbb{F}_q$ to L and let $\mathrm{Hom}_L(E, E') \coloneqq \mathrm{Hom}(E_L, E'_L)$. Finally we call $\mathrm{End}(E) \coloneqq \mathrm{Hom}_{\overline{\mathbb{F}_q}}(E, E)$ the (geometric) *endomorphism ring of E* and $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ the (geometric) *endomorphism algebra of E*. When E is a supersingular elliptic curve defined over $\mathbb{F}_q$, E has a model defined over $\mathbb{F}_{p^2}$ since its j-invariant is in $\mathbb{F}_{p^2}$. Moreover, we can choose a model of E so that all of its isogenies are defined over $\mathbb{F}_{p^2}$ as well: indeed we can choose a model so that the trace of π_E of E is $2p$, in which case $\pi_E = [p]$, the multiplication-by-p map. If $\psi\colon E \to E'$ is an isogeny between any two such models of elliptic curves E and E', then $\psi\pi_E = \pi_{E'}\psi$ and so ψ is defined over $\mathbb{F}_{p^2}$ as desired.

In this paper, we focus on supersingular elliptic curves over $\mathbb{F}_{p^2}$, although some of the results are stated for elliptic curves over $\mathbb{F}_q$. If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, then $\mathrm{End}^0(E)$ is isomorphic to the definite quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified exactly at p and ∞, and $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}^0(E)$. Computing $\mathrm{End}(E)$ entails finding a basis of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\mathrm{End}(E) \simeq \mathcal{O}$.

2.1.1 Isogeny graphs

We now define supersingular isogeny graphs; see [Mes86], [Koh96, Chapter 7], and [BCC+23, Section 3] for additional details. Let $p > 3$ and ℓ be distinct primes. The *supersingular ℓ-isogeny graph in characteristic p*, denoted by $G(p, \ell)$, is a directed multigraph, consisting of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and their ℓ-isogenies. More precisely, the vertex set of $G(p, \ell)$ is $V = V(p)$, a complete set of representatives of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. For $E, E' \in V$, the arrows in $G(p, \ell)$ from E to E' are a complete set of representatives of equivalence classes of ℓ-isogenies $E \to E'$, where two ℓ-isogenies $\phi, \psi\colon E \to E'$ are equivalent if $\phi = u\psi$ for some automorphism $u \in \mathrm{Aut}(E)$. This graph is finite, with approximately $(p-1)/12$ many vertices: indeed, by [Sil09, V.4.1(c)], the number of vertices in $G(p, \ell)$ is

$$\#V(p) = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

and the out-degree at each vertex is constant, equal to $\ell + 1$.

Consider the $\mathbb{C}$-vector space H with basis V. Let $a_{E \to E'}$ denote the number of cyclic subgroups $C \leq E[\ell]$ of order ℓ such that $E/C \simeq E'$. Define the adjacency operator $A = A(\ell, p)$ on H by $AE = \sum_{E'} a_{E \to E'} E'$. Define $w_E \coloneqq \#\,\mathrm{Aut}(E)/2$. The vector space H is equipped with an inner product defined by $\langle E, E' \rangle = w_E$ if $E = E'$ and 0 otherwise. Define $\mathcal{E} = \sum_{E \in V} w_E^{-1} E$. Then

$$\langle \mathcal{E}, \mathcal{E} \rangle = \sum_{E \in V} w_E^{-1} = \frac{p-1}{12}$$

and $\mathcal{E}$ is an eigenvector for A with eigenvalue $\ell + 1$. The adjacency operator A is self-adjoint as an operator on H with respect to $\langle \cdot, \cdot \rangle$. Thus A has all real eigenvalues. Moreover, $G(p, \ell)$ is a (directed) *Ramanujan graph*: the magnitude of the second largest eigenvalue of A is bounded by $2\sqrt{\ell}$.

This implies that the random walk in $G(p, \ell)$ mixes rapidly, a fact that we exploit in our algorithms for computing endomorphisms of supersingular elliptic curves. More precisely, a *probability distribution* on $G(p, \ell)$ is a vector $v = \sum_{E \in V} v_E E \in H$ such that $\sum_{E \in V} v_E = 1$ and $v_E \geq 0$ for all $E \in V$. The random walk on $G(p, \ell)$ is the Markov chain defined by the transition matrix $P \coloneqq \frac{1}{\ell+1} A$. Then $s = \mathcal{E}/\langle \mathcal{E}, \mathcal{E} \rangle$ is the stationary distribution for the random walk. Let v be any probability distribution on $G(p, \ell)$ and $v^{(t)} \coloneqq P^t v$, the probability distribution obtained by sampling according to v and then taking t many random steps in $G(p, \ell)$. The Ramanujan property guarantees that as $t \to \infty$, the sequence of distributions $v^{(t)}$ rapidly converges to s: for example, we have that the total variation distance between $v^{(t)}$ and s is $O(p^{-1/2})$ if $t = \Omega(\log p)$, where the implied constants depend on ℓ but not on p or t.

We can compute random walks in $G(p, \ell)$ using the ℓth classical modular polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$, which over a field k with $\mathrm{char}(k) \neq \ell$ parameterizes $\overline{k}$-isomorphism classes of elliptic curves connected by an

ℓ-isogeny with cyclic kernel. Given a supersingular elliptic curve, by selecting a random root j of $\Phi_\ell(j(E), Y)$ (weighted according to its multiplicity as a root), we can effectively take a random step from E to one of its neighbors in $G(p, \ell)$.

2.2 Quaternion algebras

Let F be a field. A quaternion algebra B over F is a central simple F-algebra of dimension 4. Let $a, b \in F^\times$, and let $H(a, b) \coloneqq F \oplus Fi \oplus Fj \oplus Fij$ be the F-algebra with F-basis $\{1, i, j, ij\}$ subject to the multiplication rules $i^2 = a$, $j^2 = b$, and $ij = -ji$. Then, $H(a, b)$ is a quaternion algebra. Moreover, assuming that the characteristic of F is not 2, for any quaternion algebra B over F, there exist $a, b \in F$ such that B is isomorphic to $H(a, b)$.

2.2.1 The canonical involution

Let $B = H(a, b)$ be a quaternion algebra over F with basis $\{1, i, j, ij\}$. The *standard involution* of B is the F-linear map $\bar{\cdot}\colon B \to B$ such that if $\alpha = w + xi + yj + zij \in B$, then $\bar{\alpha} = w - xi - yj - zij$. Note that it satisfies $\bar{1} = 1$, $\bar{\bar{\alpha}} = \alpha$, and $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ for every $\alpha, \beta \in B$. We define the *reduced trace* of $\alpha \in B$ to be $\operatorname{Trd}\alpha \coloneqq \alpha + \bar{\alpha}$ and the *reduced norm of* α to be $\operatorname{Nrd}\alpha \coloneqq \alpha\bar{\alpha}$. Both $\operatorname{Trd}\alpha$ and $\operatorname{Nrd}\alpha$ are in F for any $\alpha \in B$. Note that α and $\bar{\alpha}$ are roots of their characteristic polynomial $x^2 - (\operatorname{Trd}\alpha)x + \operatorname{Nrd}\alpha$.

The reduced trace defines a pairing $\langle \cdot, \cdot \rangle\colon B \times B \to F$ defined by $(\alpha, \beta) \mapsto \operatorname{Trd}(\alpha\bar{\beta})$. The corresponding quadratic form $Q : B \to F$ is defined by $Q(\alpha) = \operatorname{Nrd}(\alpha)$, for $\alpha \in B$. Now, let $\mathcal{B} = \{e_1, e_2, e_3, e_4\}$ be a basis of B. We define the *Gram matrix of* Q with respect to the basis $\mathcal{B}$ as the matrix

$$G = (\langle e_i, e_j \rangle)_{1 \le i,j \le 4} = (\operatorname{Trd}(e_i\bar{e_j}))_{1 \le i,j \le 4}\,.$$

Then, for $\alpha = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$ and $\beta = y_1e_1 + y_2e_2 + y_3e_3 + y_4e_4$, with $x_i, y_i \in F$, we have

$$\langle \alpha, \beta \rangle = \operatorname{Trd}(\alpha\bar{\beta}) = xGy^t,$$

where $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$.

2.2.2 Completions, splitting, and ramification

Let $\mathbb{Q}_v$ denote the completion at a place v of $\mathbb{Q}$. Here, $\mathbb{Q}_v = \mathbb{Q}_p$ for some prime p if v is a finite place, and $\mathbb{Q}_v = \mathbb{R}$ if v is the infinite place. If B is a quaternion algebra over $\mathbb{Q}$, then $B \otimes \mathbb{Q}_v$ is a quaternion algebra over $\mathbb{Q}_v$. A quaternion algebra over $\mathbb{Q}_v$ is either the unique division algebra of dimension 4 over $\mathbb{Q}_v$ or is isomorphic to $M_2(\mathbb{Q}_v)$. If $B \otimes \mathbb{Q}_v \simeq M_2(\mathbb{Q}_v)$, we say that B is *split at* v. If $B \otimes \mathbb{Q}_v$ is a division algebra, we say that B is *ramified at* v. The set of places of $\mathbb{Q}$ where B is ramified is a finite set of even cardinality. If B is not ramified at any place, then $B \simeq M_2(\mathbb{Q})$. The *discriminant* $\operatorname{disc}(B)$ *of* B is the product of all primes p at which B is ramified.

2.2.3 Quaternionic ideals and orders

Let B be a quaternion algebra over $\mathbb{Q}$. A $\mathbb{Z}$*-lattice* I in B is a finitely generated $\mathbb{Z}$-submodule of B such that $\mathbb{Q}I = B$. A $\mathbb{Z}$*-order* $\mathcal{O} \subseteq B$ is a $\mathbb{Z}$-lattice in B which is also a subring. Analogously, one defines a $\mathbb{Z}_p$-order in the quaternion algebra $B \otimes \mathbb{Q}_p$. Given a lattice I in B, the *left order* of I is $\mathcal{O}_L(I) \coloneqq \{\alpha \in B : \alpha I \subseteq I\}$, and we similarly define its right order $\mathcal{O}_R(I) \coloneqq \{\alpha \in B : I\alpha \subseteq I\}$. A lattice $I \subseteq B$ is a *left* (resp. *right*) *fractional* $\mathcal{O}$*-ideal* if $\mathcal{O} \subseteq \mathcal{O}_L(I)$ (resp. $\mathcal{O} \subseteq \mathcal{O}_R(I)$), and a fractional left $\mathcal{O}$-ideal I is an *integral left* $\mathcal{O}$*-ideal* (or simply a left ideal of $\mathcal{O}$) if $I \subseteq \mathcal{O}$. If I is both a left and right $\mathcal{O}$-ideal, we say that I is a *two-sided* ideal of $\mathcal{O}$. For a left (or right) $\mathcal{O}$-ideal I, define the *reduced norm* of I to be $\operatorname{Nrd}(I) \coloneqq \gcd(\{\operatorname{Nrd}(\alpha) : \alpha \in I\})$.

An order $\mathcal{O} \subseteq B$ is *maximal* if it is not properly contained in any other order. There can exist distinct maximal orders in B which can even be non-isomorphic.

The situation is a little simpler for $B \otimes \mathbb{Q}_p$. Indeed, if B is split at p, there are infinitely many maximal orders in $B \otimes \mathbb{Q}_p$, but they are all conjugate to $M_2(\mathbb{Z}_p)$. If $B \otimes \mathbb{Q}_p$ is a division algebra, then one can extend the valuation on $\mathbb{Q}_p$ to $B \otimes \mathbb{Q}_p$, and the unique maximal order is the valuation ring. A $\mathbb{Z}$-order $\mathcal{O} \subseteq B$ is

maximal if and only if $\mathcal{O} \otimes \mathbb{Z}_p$ is a maximal $\mathbb{Z}_p$-order in $B \otimes \mathbb{Q}_p$ for every prime p [Voi21, Lemma 10.4.3]. Thus, maximality of an order in B is a local property.

We can define the notion of discriminant also for an order $\mathcal{O} \subseteq B$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be a $\mathbb{Z}$-basis of $\mathcal{O}$, then the *discriminant* $\mathrm{disc}(\mathcal{O})$ is defined as

$$\mathrm{disc}(\mathcal{O}) := \det(\langle \alpha_i, \alpha_j \rangle)_{1 \le i,j \le 4} = \det(\mathrm{Trd}(\alpha_i \bar{\alpha_j}))_{1 \le i,j \le 4} \in \mathbb{Z}.$$

It is possible to show that $\mathrm{disc}(\mathcal{O})$ is always a square, so we define the *reduced discriminant* $\mathrm{discrd}(\mathcal{O})$ of $\mathcal{O}$ to be the positive integer satisfying $\mathrm{discrd}(\mathcal{O})^2 = \mathrm{disc}(\mathcal{O})$. A $\mathbb{Z}$-order $\mathcal{O}$ is maximal in B if and only if $\mathrm{discrd}(\mathcal{O}) = \mathrm{disc}(B)$ [Voi21, Theorem 15.5.5]. Moreover, if $\mathcal{O} \subseteq \mathcal{O}'$, then $\mathrm{discrd}(\mathcal{O}) = [\mathcal{O}' \colon \mathcal{O}]\,\mathrm{discrd}(\mathcal{O}')$, where $[\mathcal{O}' \colon \mathcal{O}]$ denotes the index of $\mathcal{O}$ in $\mathcal{O}'$ as abelian groups [Voi21, Lemma 15.2.15].

We recall some of the properties of orders in a quaternion algebra B over $\mathbb{Q}$. We say that a $\mathbb{Z}$-order $\mathcal{O} \subseteq B$ is *Gorenstein* if every left ideal I of $\mathcal{O}$ satisfying $\mathcal{O}_L(I) = \mathcal{O}$ is invertible. The order $\mathcal{O}$ is *Bass* if every overorder $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein. An order $\mathcal{O}$ is Bass if and only if it is *basic*, meaning that $\mathcal{O}$ contains a maximal order in a commutative subalgebra of B, and being basic is a local property [Voi21, Proposition 24.5.10]: this fact was originally proved by Eichler [Eic36, Satz 8] for quaternion algebras over $\mathbb{Q}$, and generalized in [CSV21]. This allows us to prove that an order is Bass by producing, for each prime ℓ, an imaginary quadratic order R in $\mathcal{O}$ whose conductor is coprime to ℓ.

2.3 Computing in finite fields and quaternion algebras

2.3.1 Algebraic operations over $\mathbb{F}_{p^2}$

We will state the complexity of our algorithms in terms of bit operations. Let $\mathrm{llog}\, x$ denote $\log \log x$. Because supersingular elliptic curves and their isogenies may all be defined over $\mathbb{F}_{p^2}$, we record here the bit complexity of various algebraic operations over $\mathbb{F}_{p^2}$. Let $\mathsf{M}(n)$ denote the bit-complexity of multiplying two n-bit integers. Then $\mathsf{M}(n) = O(n \log n)$ [HvdH21]. Let $a, b \in \mathbb{F}_{p^2}$. We can compute the sum $a+b$, the product ab, and (when $a \neq 0$) the inverse a^{-1} in $O(\log p)$, $O(\mathsf{M}(\log p)) = O(\log p (\mathrm{llog}\, p))$, and $O(\mathsf{M}(\log p)\, \mathrm{llog}\, p) = O(\log p (\mathrm{llog}\, p)^2)$ bit operations respectively, see [vzGG13, Corollary 9.9, Theorem 8.27, Corollary 11.11]. For a polynomial $f \in \mathbb{F}_{p^2}[x]$ we can compute the irreducible factors of f in $\mathbb{F}_{p^2}[x]$ and their multiplicities in expected $O(d\mathsf{M}(d) \log(pd) \mathsf{M}(\log p)) = O(d^2 (\log d)(\log pd)(\log p)(\mathrm{llog}\, p))$ bit operations [vzGG13, Theorem 14.14].

2.3.2 Computing in quaternion algebras

We will often require algorithms to take an order in a quaternion algebra as an input, or provide one as an output. We represent a quaternion algebra $H(a, b)$ by the rational numbers a, b. The *size* of a rational number m/n with $\gcd(m, n) = 1$ is the number of bits required to specify the integers m and n and therefore $\mathrm{size}(m/n) = O(\max\{\log_2(m), \log_2(n)\})$. We represent elements of $H(a, b)$ as $\mathbb{Q}$-linear combinations of the symbols $1, i, j, ij$ and use the multiplication rules $i^2 = a$, $j^2 = b$, $ij = -ji$. The *size* of $H(a, b)$ is the number of bits required to represent the multiplication table for the basis $1, i, j, ij$, so $\mathrm{size}(H(a, b)) = O(\max\{\mathrm{size}(a), \mathrm{size}(b)\})$. Given a vector $v \in \mathbb{Q}^4$, define $\mathrm{size}(v)$ be to be the sum of the sizes of its coefficients. We represent an order in $\mathcal{O}$ by four vectors $v_1, v_2, v_3, v_4 \in \mathbb{Q}^4$ which are the coefficient vectors of a basis of $\mathcal{O}$ in terms of the basis $1, i, j, ij$. The *size* of a $\mathbb{Z}$-basis $\{v_1, v_2, v_3, v_4\}$ for $\mathcal{O}$ is the size of $H(a, b)$ plus $\sum \mathrm{size}(v_i)$. We will often abuse notation and write $\mathcal{O}$ as the input or output to an algorithm; by this we mean a basis of $\mathcal{O}$ is the input or output. In this context we will also write $\mathrm{size}(\mathcal{O})$ for the size of the input or output basis. Various other integer quantities capturing the size of $\mathcal{O}$, such as its (reduced) discriminant, have size polynomial in the size of a suitable basis of $\mathcal{O}$.

3 Inseparable endomorphisms

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\alpha \in \mathrm{End}(E)$. We say that α is *inseparable* if $\alpha = \pi \circ \phi$, where $\phi \in \mathrm{Hom}(E, E^{(p)})$. The set of inseparable endomorphisms $P := \pi \,\mathrm{Hom}(E, E^{(p)})$ is a 2-sided ideal of $\mathrm{End}(E)$ and we refer to it as the *ideal of inseparable endomorphisms of* E.

In this section, we first study the arithmetic properties of $\mathbb{Z} + P \subseteq \mathrm{End}(E)$. Then in Subsection 3.2, we focus our attention on a particular kind of inseparable endomorphisms that we call *inseparable reflections*.

3.1 Properties of $\mathbb{Z} + P$

For completeness, we present the results of this subsection in the more general setting where B is a quaternion algebra over $\mathbb{Q}$ ramified at a prime p.

Proposition 3.1. *Let B be a quaternion algebra over $\mathbb{Q}$ ramified at a prime p. Let $\mathcal{O}$ be a maximal order in B and let P be the 2-sided ideal in $\mathcal{O}$ of reduced norm p. Then $\mathbb{Z} + P$ is a suborder of $\mathcal{O}$ of index p, and $\mathcal{O}$ is the unique maximal order of B containing $\mathbb{Z} + P$.*

Proof. We begin by showing that $\mathbb{Z} + P$ is an order. First, it is a lattice since it is finitely generated and $B = P\mathbb{Q} \subseteq (\mathbb{Z} + P)\mathbb{Q}$. Second, since P is an ideal, $\mathbb{Z} + P$ is closed under multiplication and contains $1 \in B$ so $\mathbb{Z} + P$ is a subring of B. Therefore $\mathbb{Z} + P$ is a suborder of $\mathcal{O}$.

We now calculate the index of $\mathbb{Z} + P$ in $\mathcal{O}$. Let $D = \mathrm{disc}(B)$. Since P is invertible (as it is an integral ideal of a maximal order, see [Voi21, Proposition 16.1.2]), by [Voi21, Proposition 16.7.7(iv)], we conclude $[\mathcal{O} : P] = \mathrm{Nrd}(P)^2 = p^2$. Since $\mathbb{Z} \cap P \cong p\mathbb{Z}$ by [Voi21, 18.2.7(b)], as $\mathbb{Z}$-modules we have $(\mathbb{Z} + P)/P \cong \mathbb{Z}/(\mathbb{Z} \cap P) \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, $[\mathbb{Z} + P : P] = p$. By multiplicativity of the index, we have $[\mathcal{O} : \mathbb{Z} + P] = p$, so [Voi21, Lemma 15.2.15] implies

$$\mathrm{disc}(\mathbb{Z} + P) = [\mathcal{O} : \mathbb{Z} + P]^2 \,\mathrm{disc}(\mathcal{O}) = p^2 D^2 = (pD)^2.$$

Now we show that $\mathcal{O}$ is the only maximal order containing $\mathbb{Z} + P$. First, an order Λ in B is maximal at a prime $\ell \neq p$ if and only if $v_\ell(\mathrm{discrd}(\Lambda)) = v_\ell(D)$[Voi21, Lemma 15.5.3, Example 15.5.4]. Since the reduced discriminant of $\mathbb{Z} + P$ is pD, we have $v_\ell(\mathrm{discrd}(\mathbb{Z} + P)) = v_\ell(p) + v_\ell(D) = v_\ell(D)$, so the order $\mathbb{Z} + P$ is maximal at any prime $\ell \neq p$. This implies $\mathcal{O} \otimes \mathbb{Z}_\ell = (\mathbb{Z} + P) \otimes \mathbb{Z}_\ell$ for any $\ell \neq p$. Moreover, since B is ramified at p, by [Voi21, Lemmas 10.4.3, 13.3.4], $\mathcal{O} \otimes \mathbb{Z}_p$ is the unique maximal order of $B \otimes \mathbb{Q}_p$ and contains $(\mathbb{Z} + P) \otimes \mathbb{Z}_p$. Therefore, for every prime ℓ, $\mathcal{O} \otimes \mathbb{Z}_\ell$ is the unique maximal $\mathbb{Z}_\ell$-order containing $(\mathbb{Z} + P) \otimes \mathbb{Z}_\ell$. By [Voi21, Corollary 9.4.7, Theorem 9.4.9, Lemma 9.5.3], we conclude that $\mathcal{O}$ is the unique maximal order containing $\mathbb{Z} + P$. □

Remark 3.2. The order $\mathbb{Z} + P$ is not hereditary [Voi21, Definition 21.4.1], since its reduced discriminant is divisible by p^2 and therefore is not square-free [Voi21, Lemma 23.3.18]. It is not Eichler [Voi21, Definition 23.4.1], since it fails to be Eichler at p (it is not maximal at p, and the only Eichler order in a local division quaternion algebra is the unique maximal order). The order $\mathbb{Z} + P$ is Bass, as its reduced discriminant is pD and thus cubefree [Voi21, Exercise 24.6.7(a)]. However, the order $\mathbb{Z} + P$ is residually ramified at p since $(\mathbb{Z} + P)/P \cong \mathbb{Z}/p\mathbb{Z}$ (see [Voi21, 24.3.2] for a definition of *residually ramified*). Finally, the order $\mathbb{Z} + P$ is the *order of level* p^2 in its unique maximal overorder (see [Piz80b, Definition 3.5]).

Remark 3.3. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. To compute a basis of $\mathrm{End}(E)$, one can first compute a basis of $\mathbb{Z} + P \subseteq \mathrm{End}(E)$ and then use Algorithms 7.9 and 3.12 in [Voi13] to recover a basis of the unique maximal order $\mathcal{O}$ containing $\mathbb{Z} + P$. In fact Proposition 3.1 implies $\mathcal{O} = \mathrm{End}(E)$. We refer the reader to section A.5 of the Appendix for algorithmic aspects of recovering $\mathrm{End}(E)$ from $\mathbb{Z} + P$.

3.2 Inseparable reflections

We now define, inside the ideal of inseparable endomorphisms of E, the *inseparable reflections*. These are inseparable endomorphisms whose construction is based on a symmetry of the supersingular ℓ-isogeny graph $G(p, \ell)$ given by the Galois involution (see Subsection 3.2.2 for a formal definition).

3.2.1 The Galois involution of $G(p, \ell)$

Let $\sigma_p \colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ be the p-power Frobenius automorphism such that $\sigma_p(\alpha) = \alpha^p$, for $\alpha \in \mathbb{F}_{p^2}$. The Galois group $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) = \langle \sigma_p \rangle$ acts on the set of elliptic curves defined over $\mathbb{F}_{p^2}$ sending E to $E^{(p)}$. Note that $(E^{(p)})^{(p)} = E$ and that $E^{(p)} = E$ if and only if E is defined over $\mathbb{F}_p$.

Similarly we can define an action of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ on separable isogenies defined over $\mathbb{F}_{p^2}$. Given a rational function $f \in \mathbb{F}_{p^2}(x,y)$, let $f^{(p)}$ denote the rational function obtained by raising the coefficients of f to the p-th power. Given a separable isogeny $\phi\colon E_1 \to E_2$ defined over $\mathbb{F}_{p^2}$, let us choose representative coordinate functions $f, g \in \mathbb{F}_{p^2}(E_1)$, defined on $E_1 - \ker\phi$, so that $\phi(x,y) = (f(x,y), g(x,y))$. Therefore, σ_p maps ϕ to the isogeny $\phi^{(p)}\colon E_1^{(p)} \to E_2^{(p)}$ such that $\phi^{(p)}(x,y) = (f^{(p)}(x,y), g^{(p)}(x,y))$. It is easy to see that the kernel of $\phi^{(p)}$ is $\pi(\ker\phi)$. Moreover, we have $(\phi^{(p)})^{(p)} = \phi$.

Lemma 3.4. *Let E_1, E_2, and E_3 be elliptic curves defined over $\mathbb{F}_{p^2}$, and let $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_3$ be separable isogenies defined over $\mathbb{F}_{p^2}$. The following hold.*

(a) $(\phi_2 \circ \phi_1)^{(p)} = \phi_2^{(p)} \circ \phi_1^{(p)}$.

(b) $\phi_1^{(p)} \circ \pi = \pi \circ \phi_1$.

(c) $(\widehat{\phi_1^{(p)}})^{(p)} = \widehat{\phi_1}$. *Equivalently,* $\widehat{\phi_1}^{(p)} = \widehat{\phi_1^{(p)}}$.

Proof. Part (a) follows from the calculation that for functions $f, g, h \in \mathbb{F}_{p^2}(x,y)$, we have

$$(f(g(x,y), h(x,y)))^{(p)} = f^{(p)}(g^{(p)}(x,y), h^{(p)}(x,y)).$$

Next, we prove (b). Let us choose representative coordinate functions f, g so that $\phi_1(x,y) = (f(x,y), g(x,y))$. Then, $\phi_1^{(p)}(x,y) = (f^{(p)}(x,y), g^{(p)}(x,y))$. This implies

$$\begin{aligned}(\phi_1^{(p)} \circ \pi)(x,y) &= \phi_1^{(p)}(x^p, y^p)\\ &= (f^{(p)}(x^p, y^p), g^{(p)}(x^p, y^p))\\ &= ((f(x,y))^p, (g(x,y))^p)\\ &= (\pi \circ \phi_1)(x,y).\end{aligned}$$

We now prove (c). We compute

$$\begin{aligned}(\widehat{\phi_1^{(p)}})^{(p)} \circ \phi_1 &= (\widehat{\phi_1^{(p)}})^{(p)} \circ (\phi_1^{(p)})^{(p)} = ((\widehat{\phi_1^{(p)}}) \circ \phi_1^{(p)})^{(p)}\\ &= ([\deg \phi_1^{(p)}]_{E_1^{(p)}})^{(p)} = ([\deg \phi_1]_{E_1^{(p)}})^{(p)}\\ &= [\deg \phi_1]_{E_1},\end{aligned}$$

where the first equality follows since ϕ_1 is defined over $\mathbb{F}_{p^2}$, in the second equality we used part (a), and in the fourth one we used $\deg \phi_1 = \deg \phi_1^{(p)}$. The last equality follows from the fact that coordinate functions for the multiplication-by-m map on a curve E are determined by $\psi_{E,m}$, the mth division polynomial of E [Sil09, Exercise 3.7], along with the observation that the recursive definition of $\psi_{E,m}$ implies $\psi_{E,m}^{(p)} = \psi_{E^{(p)},m}$. Therefore $\widehat{\phi_1} = (\widehat{\phi_1^{(p)}})^{(p)}$. □

Because every $\overline{\mathbb{F}_p}$-isomorphism class of supersingular elliptic curves contains a model defined over $\mathbb{F}_{p^2}$ such that all the isogenies are also defined over $\mathbb{F}_{p^2}$, the Frobenius automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ induces an automorphism of order 2, i.e. an involution, of $G(p,\ell)$. In particular, for every ℓ-isogeny $\phi : E_1 \to E_2$ there is the ℓ-isogeny $\phi^{(p)} : E_1^{(p)} \to E_2^{(p)}$. The fixed vertices of this automorphism correspond to supersingular curves defined over $\mathbb{F}_p$, and following the terminology of [ACNL+23], this action can be visualized as a reflection of $G(p,\ell)$ over the *spine* consisting of curves defined over $\mathbb{F}_p$. Going forward, in order to lighten the notation, we write $\psi\phi$, instead of $\psi \circ \phi$, for the composition of two (or more) isogenies.

3.2.2 Arithmetic properties of inseparable reflections

In order to define inseparable reflections we introduce the concept of (d,ϵ)-structures, defined by Chenu and Smith in [CS21] (see also the notion of *d-admissable* curves in [MSS16]).

Definition 3.5. Let d be a positive integer coprime to p. A (d, ϵ)-*structure* is a pair (E, ψ) where E is an elliptic curve defined over $\mathbb{F}_{p^2}$ and $\psi\colon E \to E^{(p)}$ is a degree d-isogeny satisfying $\psi^{(p)} = \epsilon\widehat{\psi}$ with $\epsilon \in \{\pm 1\}$. We say that (E, d) is *supersingular* if E is supersingular.

A (d, ϵ)-structure (E, ψ) yields an endomorphism $\mu = \pi\psi$ of E, which Chenu and Smith call its *associated endomorphism*. When d is square-free, a supersingular (d, ϵ)-structure (E, ψ) yields an associated endomorphism $\mu = \pi\psi$ of E such that $\mathbb{Z}[\mu] \cong \mathbb{Z}[\sqrt{-dp}]$, [CS21, Proposition 2]. In fact, this holds for arbitrary d coprime to p, assuming $p > 3$.

Proposition 3.6. *Let d be an integer coprime to a prime $p > 3$, and let (E, ψ) be a (d, ϵ)-structure. If $\mu = \pi\psi$ is the associated endomorphism of E, then $\mu^2 = [-dp]$ and $\pi_E = -\epsilon p$.*

Proof. The argument is similar to those in Propositions 1 and 2 of [CS21]. First, since (E, ψ) is a (d, ϵ)-structure, we have $\psi^{(p)} = \epsilon\widehat{\psi}$. Therefore,

$$\mu^2 = \pi\psi\pi\psi = \pi\pi\psi^{(p)}\psi = \pi_E\epsilon\widehat{\psi}\psi = \epsilon d\pi_E.$$

Let $x^2 - ax + dp$ be the characteristic polynomial of μ. We now show $a = 0$. Suppose toward a contradiction that a is nonzero. We have $a\mu = \mu^2 + dp = \epsilon d\pi_E + dp$. Taking traces, we have

$$a^2 = \operatorname{Trd}(a\mu) = \operatorname{Trd}(\epsilon d\pi_E + dp) = \epsilon d \operatorname{Trd}\pi_E + 2dp.$$

We first observe that this implies $d|a^2$. Since E is supersingular, we have $p|\operatorname{Trd}\pi_E$, so we conclude $p|a^2$, and since p is prime, $p^2|a^2$ as well. Since p and d are coprime, dp^2 divides a^2. Since we assume a is nonzero, we obtain $dp^2 \leq a^2$. On the other hand, $\mathbb{Z}[\mu]$ must have non-positive discriminant, so $a^2 - 4dp < 0$. Thus

$$dp^2 \leq a^2 \leq 4dp,$$

which implies $p < 4$. This is our desired contradiction, so we conclude $a = 0$ and $\mu^2 = -dp$. Finally, we have $0 = \epsilon d \operatorname{Trd}\pi_E + 2dp$, which implies $\operatorname{Trd}\pi_E = -2\epsilon p$. This implies $\pi_E = -\epsilon p$. □

We now discuss a construction of a (d, ϵ)-structure for d which is not necessarily square-free.

Proposition 3.7. *Let E_1 be a supersingular elliptic curve. If $\phi\colon E_1 \to E_2$ is a d_1-isogeny and (E_2, ψ) is a (d, ϵ)-structure, then $(E_1, \widehat{\phi^{(p)}}\psi\phi)$ is a $(d_1^2 d, \epsilon)$-structure.*

Proof. We must show $(\widehat{\phi^{(p)}}\psi\phi)^{(p)} = \epsilon\widehat{\widehat{\phi^{(p)}}\psi\phi}$:

$$\begin{aligned}
(\widehat{\phi^{(p)}}\psi\phi)^{(p)} &= (\widehat{\phi^{(p)}})^{(p)}\psi^{(p)}\phi^{(p)} && \text{by Lemma 3.4, part (a)} \\
&= \widehat{\phi}\psi^{(p)}\phi^{(p)} && \text{by Lemma 3.4 part (c)} \\
&= \widehat{\phi}\epsilon\widehat{\psi}\phi^{(p)} && (E, \psi) \text{ is a } (d, \epsilon) - \text{structure} \\
&= \epsilon\widehat{\widehat{\phi^{(p)}}\psi\phi}.
\end{aligned}$$

□

Below, we define a special type of associated endomorphism to a (d, ϵ)-structure. We call these endomorphisms *inseparable reflections* since they arise from paths in isogeny graphs whose image under the Galois involution is the same path, traversed in the opposite direction.

Definition 3.8. Let p be a prime, and let d_1, d be coprime integers, with d square-free, which are both coprime to p. An *inseparable reflection* of degree $d_1^2 dp$ of a supersingular elliptic curve E_1 defined over $\mathbb{F}_{p^2}$ is an endomorphism

$$\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$$

such that $\phi\colon E_1 \to E_2$ is a cyclic d_1-isogeny, (E_2, ψ) is a (d, ϵ)-structure, and ϕ does not factor nontrivially through an isogeny $\phi'\colon E_1 \to E_2'$ such that E_2' has a (d, ϵ)-structure (E_2', ψ').

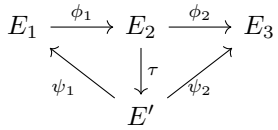
We now study the arithmetic of orders generated by inseparable reflections. First, we determine the imaginary quadratic order generated by a single inseparable reflection, then we study orders generated by two or more inseparable reflections. In particular, we give sufficient conditions for when two inseparable reflections do not commute and hence generate a quaternionic suborder of $\mathrm{End}(E)$. The following proposition follows immediately from Propositions 3.6 and 3.7.

Proposition 3.9. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ be an inseparable reflection of degree $d_1^2 dp$. Then $\alpha^2 = [-d_1^2 dp]$ and in particular α has trace zero.*

We show in Lemma 3.11 that the kernel of an inseparable reflection is cyclic. For this, we need the following lemma. This will be needed in 3.3 when we study orders generated by two or more inseparable reflections.

Lemma 3.10. *Let E_1, E_2, and E_3 be elliptic curves defined over $\mathbb{F}_q$ and let $\phi_1 \colon E_1 \to E_2$ and $\phi_2 \colon E_2 \to E_3$ be separable, cyclic isogenies. Then $\ker(\phi_2\phi_1)$ is cyclic if and only if $\ker\widehat{\phi_1} \cap \ker\phi_2$ is trivial.*

Proof. If $\ker\widehat{\phi_1} \cap \ker\phi_2 = G$ is nontrivial, let $\tau \colon E_2 \to E'$ be a separable isogeny with kernel G, where E' is an elliptic curve defined over $\mathbb{F}_q$. Then, both $\widehat{\phi_1}$ and ϕ_2 factor through τ: there exist isogenies ψ_1, ψ_2 such that $\widehat{\phi_1} = \psi_1\tau$ and $\phi_2 = \psi_2\tau$.



Then,

$$\phi_2\phi_1 = \psi_2\tau\widehat{\tau}\widehat{\psi_1} = \psi_2\widehat{\psi_1}[\#G]$$

does not have cyclic kernel.

Now assume that $\ker(\phi_2\phi_1)$ is not cyclic. Let $S \in E_2(\overline{\mathbb{F}_q})$ such that $\ker\phi_2 = \langle S\rangle$, the cyclic group generated by S, and let $Q \in E_1(\overline{\mathbb{F}_q})$ such that $\phi_1(Q) = S$. Also let $P \in E_1(\overline{\mathbb{F}_q})$ such that $\langle P\rangle = \ker\phi_1$.

First, we claim that $\ker(\phi_2\phi_1) = \langle P\rangle + \langle Q\rangle$. Let $P' \in \ker(\phi_2\phi_1)$. Then, $\phi_1(P') = [a]S$ for some a. Therefore, $P' - [a]Q \in \ker\phi_1$. Thus,

$$P' = (P' - [a]Q) + [a]Q \in \ker\phi_1 + \langle Q\rangle = \langle P\rangle + \langle Q\rangle,$$

i.e. $\ker(\phi_2\phi_1) \subseteq \langle P\rangle + \langle Q\rangle$. Since $\phi_1(\langle P\rangle + \langle Q\rangle) \subseteq \ker\phi_2$, we also have that $\ker(\phi_2\phi_1) \supseteq \langle P\rangle + \langle Q\rangle$. Thus, $\ker(\phi_2\phi_1) = \langle P\rangle + \langle Q\rangle$.

Since we assume that $\ker(\phi_2\phi_1)$ is not cyclic, $\langle P\rangle + \langle Q\rangle$ contains $E_1[d]$ for some $d > 1$. Note that d and $\deg\phi_1$ are not coprime, since otherwise $\phi_1(E_1[d]) = E_2[d]$ and thus $E_2[d] \subseteq \ker\phi_2$, contradicting the assumption that $\ker\phi_2$ is cyclic. Let $g = \gcd(d, \deg\phi_1)$. Then, $E_1[g] \subseteq E_1[d]$ and $E_1[g] \subseteq E_1[\deg\phi_1]$. Now we have that $\phi_1(E_1[g]) \subseteq \ker\phi_2$ and also $\phi_1(E_1[g]) \subseteq \ker\widehat{\phi_1} = \phi_1(E_1[\deg\phi_1])$, therefore $\phi_1(E_1[g]) \subseteq \ker\widehat{\phi_1} \cap \ker\phi_2$. Since ϕ_1 is cyclic and $g > 1$, $\phi_1(E_1[g]) \neq 0$, so $\ker\widehat{\phi_1} \cap \ker\phi_2 \neq 0$. □

Lemma 3.11. *Let E_1 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ be an inseparable reflection of degree $d_1^2 dp$. Then the kernel of α is cyclic.*

Proof. It suffices to show that $\widehat{\phi^{(p)}}\psi\phi \colon E_1 \to E_1^{(p)}$ has cyclic kernel. Assume that $\ker(\widehat{\phi^{(p)}}\psi\phi)$ is not cyclic. Let E_2 be the codomain of ϕ. We show that there is an isogeny $\tau \colon E_2 \to E_3$ such that $\ker\tau \subseteq \ker\widehat{\phi}$ and E_3 has a (d, ϵ)-structure. By Lemma 3.10, we have that $G = \ker\widehat{\phi} \cap \ker\widehat{\phi^{(p)}}\psi \neq 0$. Note that G is defined over $\mathbb{F}_{p^2}$, since it is contained in $\ker\widehat{\phi}$ which is defined over $\mathbb{F}_{p^2}$. Let $\tau \colon E_2 \to E_3$ be an isogeny defined over $\mathbb{F}_{p^2}$ with kernel G.

$$\begin{array}{ccccc} E_1 & \xrightarrow{\phi} & E_2 & \xrightarrow{\tau} & E_3 \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\psi} & & \\ E_1^{(p)} & \xrightarrow{\phi^{(p)}} & E_2^{(p)} & & \end{array}$$

We show that E_3 has an (d,ϵ)-structure. By [CS21, Lemma 1], it suffices to show that $\mathrm{End}(E_3)$ contains a quadratic order isomorphic to $\mathbb{Z}[\sqrt{-dp}]$.

First, we claim that $\pi\psi(G) = G$. Since $G \subseteq \ker(\widehat{\phi^{(p)}}\psi)$, we have that

$$\psi(G) \subseteq \ker \widehat{\phi^{(p)}} = \pi(\ker \widehat{\phi}).$$

Since $\gcd(d_1, d) = 1$, we see that ψ induces an isomorphism $E_2[d_1] \to E_2^{(p)}[d_1]$. Thus, since $G \subseteq E_2[d_1]$, we have $\#\psi(G) = \#G$. Moreover, $\ker\widehat{\phi}$ is cyclic, so $\pi(\ker\widehat{\phi})$ is also cyclic. Therefore, $\psi(G)$ is the unique subgroup of $\pi(\ker\widehat{\phi})$ of order $\#G$. Since the unique subgroup of $\ker\widehat{\phi}$ of order $\#G$ is also G, we have

$$\psi(G) = \pi(G).$$

From this we conclude that

$$\pi\psi(G) = \pi(\pi(G)) = G,$$

where the last equality holds since τ is defined over $\mathbb{F}_{p^2}$. Therefore the proof of the claim is complete.

Now consider the endomorphism

$$\rho = \tau\pi\psi\widehat{\tau} \in \mathrm{End}(E_3).$$

We claim that $\rho(E_3[\deg\tau]) = 0$. Indeed,

$$\rho(E_3[\deg\tau]) = \tau\pi\psi\widehat{\tau}(E_3[\deg\tau]) = \tau\pi\psi(\ker\tau) = \tau\pi\psi(G) = \tau(G) = 0.$$

Thus, $\mu = \frac{1}{\deg\tau}\rho$ is an endomorphism of E_3. Observe that

$$\mu^2 = \frac{1}{(\deg\tau)^2}\tau\pi\psi\widehat{\tau}\tau\pi\psi\widehat{\tau} = \frac{1}{\deg\tau}\tau\pi\psi\pi\psi\widehat{\tau} = \frac{-dp}{\deg\tau}\tau\widehat{\tau} = -dp,$$

so $\mathbb{Z}[\mu] \cong \mathbb{Z}[\sqrt{-dp}]$. As mentioned above, by Lemma 1 of [CS21], it follows that E_3 has a (d,ϵ)-structure (indeed, $\mu = \pi\psi'$ for an isogeny $\psi' \colon E_3 \to E_3^{(p)}$, and (E_3, ψ') is the desired (d,ϵ)-structure).

□

3.3 Quaternionic suborders of $\mathrm{End}(E)$ generated by inseparable reflections

In this section we study orders generated in $\mathrm{End}(E)$ by two inseparable reflections. The main result in this section, Theorem 3.15, shows that assuming some mild restrictions on their degrees, two inseparable reflections generate a Bass suborder of $\mathrm{End}(E)$. First, we use Lemma 3.9, Lemma 3.10 and Lemma 3.11 to give sufficient conditions for two inseparable endormophisms to not commute and therefore to generate a quaternionic suborder of $\mathrm{End}(E)$.

Theorem 3.12. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let $\alpha_1 = \pi\widehat{\phi_1^{(p)}}\psi_1\phi_1$ and $\alpha_2 = \pi\widehat{\phi_2^{(p)}}\psi_2\phi_2$ be inseparable reflections of degree d_1^2dp and d_2^2dp. If $\ker\phi_1 \neq \ker\phi_2$, then α_1 and α_2 do not commute.*

Proof. Assume that α_1 and α_2 commute. Then, $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$, so there exist integers k, m, n such that $[k]\alpha_1 = [m] + [n]\alpha_2$. By Lemma 3.9, we have $\mathrm{Trd}(\alpha_1) = \mathrm{Trd}(\alpha_2) = 0$, so $m = 0$ and $[k]\alpha_1 = [n]\alpha_2$. We claim that $k|n$. Write $n = kq + r$ with $0 \leq r < k$. Note that since $[n](\alpha_2(E[k])) = 0$, we also have $[r](\alpha_2(E[k])) = 0$. This implies $\alpha_2\left(E\left[\frac{k}{\gcd(k,r)}\right]\right) = 0$. The kernel of α_2 is cyclic by Lemma 3.11, so we

must have that $k/\gcd(k,r) = 1$ and hence $\gcd(k,r) = k$ implying $r = 0$. Thus $k|n$. Therefore $\alpha_1 = [n/k]\alpha_2$. Now, since α_1 has cyclic kernel by Lemma 3.11, we conclude $n/k = \pm 1$. Thus $\alpha_1 = \pm\alpha_2$ so $\ker\alpha_1 = \ker\alpha_2$ and $\deg\phi_1 = \deg\phi_2$. Therefore, using the property that $\ker\alpha_i$ is cyclic for $i = 1, 2$, we obtain $\ker\phi_1 = \ker\phi_2$. □

We now show that we can control arithmetic properties of an order generated by two inseparable reflections with mild assumptions on their degrees.

Proposition 3.13. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let d_1, d_2, d be three pairwise coprime integers, with d square-free. For $i = 1, 2$, let $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i \in \mathrm{End}(E)$ be an inseparable reflection of degree $d_i^2 dp$.*

(i) The endomorphisms $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ generate an order

$$\Lambda_{\alpha_1\alpha_2} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2 \subseteq \mathrm{End}(E).$$

(ii) The endomorphism $\alpha_1\alpha_2$ factors through the multiplication-by-p map, so

$$\rho := \frac{-\alpha_1\alpha_2}{p}$$

is an endomorphism of E. The discriminant of $\Lambda_{\alpha_1\alpha_2}$ is

$$\mathrm{disc}(\Lambda_{\alpha_1\alpha_2}) = p^4 \cdot ((\mathrm{Trd}\,\rho)^2 - 4\deg\rho)^2 = p^4 \cdot (\mathrm{disc}\,\rho)^2.$$

(iii) The order $\Lambda_{\alpha_1\alpha_2}$ is Gorenstein.

Proof. Lemma 3.9 implies that α_1 and α_2 are non-scalar endomorphisms. Since $d_1 \neq d_2$, we have that $\ker\phi_1 \neq \ker\phi_2$ so $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$ by Theorem 3.12. The endomorphisms α_1 and α_2 are noncommuting, nonscalar elements of $\mathrm{End}^0(E)$, so $\Lambda_{\alpha_1\alpha_2}$ is a lattice in $\mathrm{End}^0(E)$. Since $\alpha_1, \alpha_2, \alpha_1\alpha_2$ are integral, the lattice $\Lambda_{\alpha_1\alpha_2}$ is a ring containing 1, so it is an order, completing the proof of part (i).

To prove part (ii) we compute $\mathrm{discrd}(\Lambda_{\alpha_1\alpha_2})$. Since $\mathrm{Trd}\,\alpha_i = 0$, we have $\widehat{\alpha_i} = -\alpha_i$, so

$$\rho = \frac{-1}{p}\alpha_1\alpha_2 = \frac{1}{p}\widehat{\phi_1}\widehat{\psi_1}\widehat{\pi}\pi\phi_1^{(p)}\widehat{\phi_2^{(p)}}\psi_2\phi_2 = \widehat{\phi_1}\widehat{\psi_1}\phi_1^{(p)}\widehat{\phi_2^{(p)}}\psi_2\phi_2.$$

The Gram matrix of the basis $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ is

$$G := \begin{pmatrix} 2 & 0 & 0 & -p\,\mathrm{Trd}\,\rho \\ 0 & 2pdd_1^2 & p\,\mathrm{Trd}\,\rho & 0 \\ 0 & p\,\mathrm{Trd}\,\rho & 2pdd_2^2 & 0 \\ -p\,\mathrm{Trd}\,\rho & 0 & 0 & 2(pd_1d_2d)^2 \end{pmatrix}.$$

A calculation shows that its determinant, and therefore the discriminant of $\Lambda\alpha_1\alpha_2$, is

$$\det(G) = p^4 \cdot ((\mathrm{Trd}\,\rho)^2 - 4\deg\rho)^2 = p^4 \cdot (\mathrm{disc}\,\rho)^2.$$

Finally we prove part (iii). We claim that the ternary quadratic form attached to $\Lambda_{\alpha_1\alpha_2}$ is

$$Q(x, y, z) = pdd_2^2x^2 + pdd_1^2y^2 + z^2 - tpxy,$$

where $t = \mathrm{Trd}\,\rho$. A calculation shows the basis $1, i = \alpha_1, j = \alpha_2, k = \alpha_2\alpha_1$ of $\Lambda_{\alpha_1\alpha_2}$ is a *good basis* in the sense of [Voi21, 22.4.7], i.e., there exist integers a, b, c, u, v, w satisfying $i^2 = ui - bc$, $j^2 = vj - ac$, $k^2 = wk - ab$ and $jk = a\widehat{i}$, $ki = b\widehat{j}$, and $ij = c\widehat{k}$. Given a good basis, the corresponding ternary quadratic form is $ax^2 + by^2 + cz^2 + uyz + vxz + wxy$ (see the proof of [Voi21, Proposition 22.4.12]). In the case of the basis $1, \alpha_1, \alpha_2, \alpha_2\alpha_1$ for Λ, we have $a = pdd_2^2$, $b = pd_1^2$, $c = 1$, $u = v = 0$, and $w = -tp$. The quadratic form Q is primitive since its coefficients are coprime, so Λ is Gorenstein by [Voi21, Theorem 24.2.10]. □

Remark 3.14. The lattice $\Lambda_\rho := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\rho$ in $\mathrm{End}(E)$ is also a suborder of $\mathrm{End}(E)$ and clearly $\Lambda_{\alpha_1\alpha_2} \subsetneq \Lambda_\rho$. The order $\Lambda_{\alpha_1\alpha_2}$ is non-maximal precisely at p and the primes dividing the discriminant of ρ. Assuming that $p \nmid \mathrm{disc}(\rho)$, the order Λ_ρ is the unique p-maximal order containing $\Lambda_{\alpha_1\alpha_2}$ whose localizations at all $\ell \neq p$ agree with those of $\Lambda_{\alpha_1\alpha_2}$.

Theorem 3.15. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and let d_1, d_2, d be three pairwise coprime integers, with d square-free. For $i = 1, 2$, let*

$$\alpha_i = \pi_p \widehat{\phi_i^{(p)}} \psi_i \phi_i \in \mathrm{End}(E)$$

be an inseparable reflection of degree $d_i^2 dp$. Finally, assume that $-dp \not\equiv 1 \pmod 4$. Then the order $\Lambda_{\alpha_1\alpha_2}$ is Bass.

Proof. Proposition 3.13 implies that $\Lambda_{\alpha_1\alpha_2}$ is an order. We show that $\Lambda_{\alpha_1\alpha_2}$ is locally basic, and hence locally Bass by [Brz90, Proposition 1.11] at every prime ℓ. This suffices, since being Bass is a local property [Voi21, Proposition 24.5.10].

Consider the quadratic order $R_i = \mathbb{Z}[\alpha_i] \cong \mathbb{Z}[d_i\sqrt{-dp}]$ in $\Lambda_{\alpha_1\alpha_2} \subseteq \mathrm{End}(E)$. Since $-dp$ is square-free and not congruent to 1 modulo 4, the maximal order in the fraction field of R_i is isomorphic to $\mathbb{Z}[\sqrt{-dp}]$, so the conductor of R_i is d_i. Then, for any prime ℓ, at least one of R_1 or R_2 is maximal at ℓ since R_1 is maximal at every prime ℓ which does not divide d_1, and R_2 is maximal at every prime ℓ which does not divide d_2. This shows $\Lambda_{\alpha_1\alpha_2}$ is locally basic at each prime ℓ. □

4 Computing an order in $\mathrm{End}(E)$ with inseparable endomorphisms

By Proposition 3.9, one inseparable reflection α_1 of degree $d_1^2 dp$ of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ generates an imaginary quadratic order of discriminant $-4d_1^2 dp$. If d_2 is another integer coprime to d_1, if we assume d is coprime to both d_1 and d_2, and let α_2 be a $d_2^2 dp$-inseparable reflection, then α_1 and α_2 generate an order $\Lambda_{\alpha_1\alpha_2} \coloneqq \langle \alpha_1, \alpha_2 \rangle$ in $\mathrm{End}(E)$ which is Gorenstein by Proposition 3.13. If we assume $-dp \not\equiv 1 \pmod 4$ then $\Lambda_{\alpha_1\alpha_2}$ is Bass by Theorem 3.15. Therefore, if we can compute inseparable reflections of E for certain values of d_1, d_2, and d, then we can compute orders with certain desirable arithmetic properties in $\mathrm{End}(E)$. We will make the results in Section 3 effective by giving an algorithm for computing one inseparable reflection and then another algorithm which uses inseparable reflections for computing a Bass order Λ in $\mathrm{End}(E)$.

Computing a $d_i^2 dp$-inseparable reflection requires a d_i-isogeny $\phi_i \colon E \to E_i$ where E_i has a d-isogeny $\psi_i \colon E_i \to E_i^{(p)}$. Computing such a d_i-isogeny will be easiest when d_i is smooth: if $d_i = \ell_i^{t_i}$ where ℓ_i is a small prime, then we can take random walks of length t_i in the ℓ_i-isogeny graph until finding a supersingular curve E_i which is d-isogenous to $E_i^{(p)}$. The simplest choice for d is $d = 2$: in this case we have that $-dp \not\equiv 1 \pmod 4$ and it is easy to check whether E_i is 2-isogenous to $E_i^{(p)}$. We follow this strategy in Algorithm 1. We show that it correctly computes an inseparable reflection and analyze its complexity in Proposition 4.5. We conclude with Algorithm 2 which computes a Bass order in $\mathrm{End}(E)$ according to Theorem 4.8.

4.1 Computing inseparable reflections

We compute an inseparable reflection of degree $\ell^{2t} dp$ by taking random non-backtracking walks beginning at E of length t, which correspond to cyclic ℓ^t isogenies $\phi \colon E \to E'$, until finding a (d, ϵ)-structure (E', ψ). The resulting inseparable reflection of E is $\pi\widehat{\phi^{(p)}}\psi\phi$. In order to bound the expected runtime of this approach, we must consider the probability that a random non-backtracking walk of length t terminates at a supersingular curve E' with a (d, ϵ)-structure.

Let $p > 3$ be a prime. We recall some notation for the supersingular ℓ-isogeny graph $G(p, \ell)$ from Section 2 and [BCC+23, Section 3]. Let V denote a complete set of representatives of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. Let H be the $\mathbb{C}$-vector space H with basis V, let $\langle \cdot, \cdot \rangle$ be the inner product such that for $E, E' \in V$, we have $\langle E, E' \rangle = w_E$ if $E = E'$ and 0 otherwise. Let A denote the adjacency operator for $G(p, \ell)$. A *walk* in the graph $G(p, \ell)$ is defined to be a sequence of edges $\phi_1, \phi_2, \ldots, \phi_k$

such that the codomain of ϕ_i is isomorphic to the domain of ϕ_{i+1}. A walk *has no backtracking*, or is non-backtracking, if $\phi_{i+1} \neq u\widehat{\phi_i}$ for any automorphism u. Thus, non-backtracking walks in $G(p,\ell)$ beginning at $E \in V$ are in bijection with cyclic subgroups of $E[\ell^\infty]$. Let $\mathcal{E} = \sum_{E\in V} w_E^{-1} E$, so $s = \frac{1}{\langle \mathcal{E}, \mathcal{E}\rangle}\mathcal{E}$ is the stationary distribution for the random walk in $G(p,\ell)$. For a distribution $v = \sum_{E\in V} v_E E$ and a subset $X \subseteq V$, let $v(X) \coloneqq \sum_{E\in X} v_E$ denote the probability that a vertex sampled according to v is an element of X. For two distributions v, v' on $G(p,\ell)$, let

$$d_{TV}(v,v') = \sup_{X\subseteq V} |v(X) - v'(X)| = \frac{1}{2}|v - v'|_1$$

denote the total variation distance between v and v'. Let $P^{(t)}$ be the transition matrix for the non-backtracking random walk in $G(p,\ell)$ of length t; we remark that $P^{(t)}$ and P^t are not the same matrix for $t > 1$. Holding ℓ constant, the following proposition states that a non-backtracking walk of length $O(\log p)$ will land in a set $X \subseteq V$ with probability proportional to $\#X/\#V$.

Proposition 4.1. *Let $E_0 \in V$ and let $X \subseteq V$ be nonempty. If*

$$t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) \geq \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{E\in X} w_E^{-1}}\right),$$

then a non-backtracking random walk of length t beginning at E_0 lands in X with probability at least

$$\frac{6}{p-1}\sum_{E\in X} w_E^{-1}.$$

Proof. Let $v^{(t)} = P^{(t)}E_0$ be the probability distribution on V resulting from a random non-backtracking walk of length t beginning at E_0. Then, by Theorem 11 of [BCC+23],

$$|v^{(t)}(X) - s(X)| \leq d_{TV}(v^{(t)}, s) \leq \frac{(p-1)^{1/2}}{4}\cdot\left(t + \frac{\ell-1}{\ell+1}\right)\cdot \ell^{-t/2}.$$

We have

$$s(X) = \frac{12}{p-1}\sum_{E\in X} w_E^{-1}.$$

We see that if

$$t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) \geq \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{E\in X} w_E^{-1}}\right),$$

then

$$\frac{(p-1)^{1/2}}{4}\cdot\left(t + \frac{\ell-1}{\ell+1}\right)\cdot \ell^{-t/2} \leq \frac{6}{p-1}\sum_{E\in X} w_E^{-1},$$

so

$$v^{(t)}(X) \geq \frac{6}{p-1}\sum_{E\in X} w_E^{-1},$$

as desired. □

We now bound the expected number of random walks beginning at E which we take before finding a (d,ϵ)-structure. Let $\operatorname{llog} x$ denote $\log\log x$.

Proposition 4.2 (GRH)**.** *Assume GRH. Let $p > 3$ be a prime, and let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ such that $\#E_0(\mathbb{F}_{p^2}) = (p+\epsilon)^2$ for $\epsilon = \pm 1$. Let $\ell \neq p$ be a prime, and let $d = 1$ or 2. Let X be a complete set of representatives for the collection of isomorphism classes of supersingular elliptic curves with a (d,ϵ)-structure. If*

$$t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) \geq \log_\ell\left(\frac{(p-1)^{3/2}}{8}\right),$$

then a non-backtracking walk in $G(p,\ell)$ beginning at E_0 of length t lands in X with probability at least $\Omega\left(\frac{1}{\sqrt{p}\operatorname{llog} p}\right)$.

Proof. The set X is nonempty because [CS21, Corollary 1] implies that the number of isomorphism classes of (d,ϵ)-structures is at least the class number of $\mathbb{Z}[\sqrt{-dp}]$. Since X is nonempty, we may apply the trivial lower bound $\#X \geq 1$ to get

$$\sum_{E \in X} \frac{2}{\#\operatorname{Aut}(E)} \geq 1/3.$$

For t satisfying the hypothesis in the proposition, we conclude

$$\begin{aligned} t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) &\geq \log_\ell\left(\frac{(p-1)^{3/2}}{8}\right) \\ &\geq \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{E\in X}\frac{2}{\#\operatorname{Aut}(E)}}\right). \end{aligned}$$

By Proposition 4.1, a non-backtracking walk beginning at E_0 lands in X with probability at least

$$\frac{6}{p-1} \cdot \sum_{E\in X} \frac{2}{\#\operatorname{Aut}(E)} \geq \frac{6}{p-1}(\#X - 7/6).$$

Let $K = \mathbb{Q}(\sqrt{-pd})$. By [CS21, Corollary 1], there are at least h_K many (d,ϵ)-structures, up to $\mathbb{F}_{p^2}$-isomorphism. Since any given E has at most $d+1$ d-isogenies, and since the number of distinct $\mathbb{F}_{p^2}$-isomorphism classes of curves with the same j-invariant is at most 6, we have that

$$\#X \geq \frac{1}{6(d+1)} h_K.$$

Assuming the Generalized Riemann Hypothesis,

$$h_K = \Omega(\sqrt{pd}/\operatorname{llog}(pd)) = \Omega(\sqrt{p}/\operatorname{llog}(p))$$

by [Lit28, Theorem 1]. We conclude that a non-backtracking walk of length t lands in X with probability $\Omega\left((\sqrt{p}\operatorname{llog}(p))^{-1}\right)$. □

Remark 4.3. We required a lower bound on the class group of an imaginary quadratic order in two places in the proof of Proposition 4.2: once to determine the length t of a walk to guarantee good mixing, and once to extract a lower bound on the probability that a random walk ends in a given set. Since our later algorithms require an *effective* upper bound on t, we need effective lower bounds on the class group for the first part of the argument. One could use non-trivial effective lower bounds, but these would only yield sub-logarithmic improvements to the size of t. For simplicity we just use 1. In the second part of the argument, we do not need an effective lower bound, since the constant is hidden in the big-Ω.

Next, we show that if $d < p/4$, a curve E has a (d,ϵ)-structure if and only if E is d-isogenous to $E^{(p)}$. This holds if and only if $\Phi_d(j(E), j(E)^p) = 0$, giving us an efficient method for testing whether E has a (d,ϵ)-structure. The following lemma is an adaptation of [CGL09, Lemma 6], and we include a proof for convenience.

Lemma 4.4. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$, and let $1 < d < p/4$ be square-free and coprime to p. Then E has a (d,ϵ)-structure (E,ψ) for $\epsilon \in \{\pm 1\}$ if and only if E is d-isogenous to $E^{(p)}$.*

Proof. If (E,ψ) is a (d,ϵ)-structure, then $\psi\colon E \to E^{(p)}$ is a d-isogeny. Assume now that E is d-isogenous to $E^{(p)}$, and let $\psi\colon E \to E^{(p)}$ be a d-isogeny. We show that the characteristic polynomial of $\mu = \pi\psi$ is $x^2 + dp$: if this holds, then we have an embedding $\mathbb{Z}[\sqrt{-dp}] \hookrightarrow \operatorname{End}(E)$ defined by sending $\sqrt{-dp}$ to $\mu = \pi\psi$, and [CS21, Lemma 1] then implies that (E,ψ) is a (d,ϵ)-structure. Since the degree of μ is $(\deg\pi)(\deg\psi) = pd$, we only need to show that $\operatorname{Trd}\mu$ is zero. The ring $\mathbb{Z}[\mu]$ must be an imaginary quadratic order since $\deg\mu$ is not a square, and p does split in $\mathbb{Z}[\mu]$ since E is supersingular. Thus the characteristic polynomial

$$x^2 - (\operatorname{Trd}\mu)x + pd \equiv x(x - \operatorname{Trd}\mu) \pmod{p}$$

of μ cannot have distinct roots modulo p, so we must have $\operatorname{Trd}\mu \equiv 0 \pmod{p}$. Since the discriminant of μ is negative and using our assumption that $d < p/4$, we have

$$|\operatorname{Trd}\mu| < 2\sqrt{pd} < p.$$

Thus $\operatorname{Trd}\mu = 0$. □

We now introduce our algorithm for computing inseparable reflections, Algorithm 1. We only need

Algorithm 1: Compute an inseparable reflection

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ with $p > 3$, a prime ℓ, and an integer d, with $d < p/4$ square-free and coprime to ℓ.

Output: An inseparable reflection $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi \in \operatorname{End}(E)$ where $\phi\colon E \to E'$ is an ℓ^k-isogeny (represented by a sequence of ℓ-isogenies) and $\psi\colon E' \to E'^{(p)}$ is a d-isogeny such that (E', ψ) is a (d, ϵ)-structure.

1 Compute the least integer t such that $t/2 - \log_\ell\left(t + \frac{\ell-1}{\ell+1}\right) \geq \log_\ell\left(\frac{(p-1)^{3/2}}{8}\right)$;

2 **repeat**

3 Compute a random, non-backtracking walk $W = \{\phi_1\colon E \to E_1, \ldots, \phi_t\colon E_{t-1} \to E_t\}$ in $G(p, \ell)$ of length t;

4 **until** E_t *is* d*-isogenous to* $E_t^{(p)}$;

5 Let $k = \min_{1 \leq i \leq t}\{i : E_i \text{ is } d\text{-isogenous to } E_i^{(p)}\}$;

6 Compute a (d, ϵ)-structure (E_k, ψ);

7 **return** $\{\phi_1, \ldots, \phi_k, \psi, \widehat{\phi_k}^{(p)}, \ldots, \widehat{\phi_1}^{(p)}, \pi\}$

to run Algorithm 1 on inputs of the form $(E, \ell, 2)$ (to compute Bass orders) and inputs $(E, \ell, 1)$ (for our heuristic algorithm described in Section 6.1), where ℓ is a fixed small prime, such as $2, 3$, or 5. Thus in our complexity analysis below, we are treating ℓ and d as constants. Similar results hold for square-free $d = O(\log p)$ and prime $\ell = O(\log p)$. Let $\mathsf{M}(n)$ denote the cost of multiplying two n-bit integers (we may take $\mathsf{M}(n) = O(n \log n)$ by [HvdH21]). Below, we analyze the complexity of Algorithm 1.

Proposition 4.5 (GRH)**.** *Algorithm 1 is correct. Assuming GRH, for any prime $\ell \in \{2, 3, 5\}$, integer $d \in \{1, 2\}$, prime $p > 4d$, and supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, Algorithm 1 on input (E, ℓ, d) terminates in expected $O(p^{1/2}(\log p)^2(\operatorname{llog} p)^3)$ bit operations.*

Proof. First, we argue that Algorithm 1 is correct. Let $\alpha = \pi\widehat{\phi^{(p)}}\psi\phi$ with $\deg\phi = \ell^k$ be the output of Algorithm 1 on input (E, ℓ, d). We claim that α satisfies the hypotheses of Theorem 3.12. Because Algorithm 1 uses non-backtracking walks, the ℓ^k-isogeny ϕ is cyclic. Because the walk is truncated so that the final vertex is the first curve in the walk with a (d, ϵ)-structure, ϕ does not factor nontrivially through an isogeny to another curve with a (d, ϵ) structure. We conclude that α is an inseparable reflection.

We now bound the expected number of bit operations performed by the algorithm. We can do Step 1 with Newton's method, for example, and the magnitude of the solution t will be in $O(\log p)$. We compute Φ_ℓ and Φ_2, if $d = 2$, and store these polynomials. Since we treat ℓ and d as constants, we ignore these costs, and in any case this computation can be done in $O(\ell^3 \log^3 \ell \operatorname{llog} \ell)$ expected time assuming GRH [BLS12, Theorem 1]. We can take one step in $G(p, \ell)$ using the modular polynomial Φ_ℓ. Let $E_0 = E$ and $j_0 = j(E_0)$. Suppose we are at vertex j_i. The neighbors of j_i are the roots of $\Phi_\ell(j_i, Y)$. We can evaluate $\Phi_\ell(X, Y)$ at (j_i, Y) in $O(\ell^2) = O(1)$ many multiplications and additions in $\mathbb{F}_{p^2}$, the cost of which is dominated by the $O(\mathsf{M}(\ell \log p)(\operatorname{llog} p))$ bit operations needed to compute a random root of $\Phi_\ell(j_i, Y)$ using the randomized algorithm of [Rab80]. To take a non-backtracking step, we compute a random root of $\Phi_\ell(j_i, Y)/(Y - j_{i-1})$ where j_{i-1} is the previous vertex of the walk. Let X denote the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ which are d-isogenous to their Galois conjugate. By Lemma 4.4, we can test if j_t is in X by testing whether $\Phi_d(j_t, j_t^p) = 0$ when $d > 1$ and simply whether $j_t^p = j_t$ when $d = 1$, both of which we can do with $O(\log p)$ multiplications in $\mathbb{F}_{p^2}$. Since the length of the walk is $O(\log p)$, and since we treat ℓ as a constant, Step 3 takes $O(\mathsf{M}(\log p)(\log p)(\operatorname{llog} p))$ time.

We now calculate the expected number of iterations of Step 3. Assuming GRH, by Proposition 4.2 a non-backtracking walk beginning at E lands in X with probability $\Omega\left(\frac{1}{\sqrt{p}\operatorname{llog} p}\right)$. Thus the expected number of non-backtracking walks we must take is $O(\sqrt{p}\operatorname{llog} p)$. Multiplying the expected number of walks by the expected number of bit operations per walk and using $\mathsf{M}(n) = O(n \log n)$ by [HvdH21] yields the cost

$$O(\mathsf{M}(\log p)(\log p)(\operatorname{llog} p) \cdot \sqrt{p}(\operatorname{llog} p)) = O(p^{1/2}(\log p)^2(\operatorname{llog} p)^3).$$

Let $j_0 = j(E), j_1, \ldots, j_t$ be a sequence of adjacent j-invariants in $G(p, \ell)$ with $j_t \in X$. We next obtain the sequence of isogenies $\phi_i \colon E_i \to E_{i+1}$ for $i = 0, \ldots, t-1$ and the (d, ϵ)-structure (E_t, ψ) with $O((\log p)^{O(1)})$ bit operations: for example, if p is sufficiently large and if j_{i+1} is a simple root of $\Phi_\ell(j_i, Y)$, given an equation for E_i with j-invariant j_i, we can compute a short Weierstrass equation for an elliptic curve E_{i+1} and a normalized ℓ-isogeny $\phi_i \colon E_i \to E_{i+1}$ with $O(\ell^2)$ operations in $\mathbb{F}_{p^2}$ using Elkies algorithm [Elk98] (see [Gal12, Algorithm 28] for an explicit description of the algorithm). The time to compute the sequence of isogenies associated to the path $j_0, \ldots, j_t$ is therefore dominated by the time required to complete the while-loop, since ℓ is a constant. Similarly, the time required to truncate the path and to compute the (d, ϵ)-structure is also dominated by the time required to complete the while-loop. □

Remark 4.6. There are some natural optimizations which we do not explore here, such as testing more vertices along the path for the presence of (d, ϵ)-structures, or, more generally, testing whether a given curve E_k along the path is ℓ'-isogenous to a curve defined over $\mathbb{F}_p$ with the algorithm of [CSCS22].

4.2 Computing a Bass suborder of $\mathrm{End}(E)$

In [EHL+20], the authors give a subexponential algorithm for computing a basis for $\mathrm{End}(E)$ from a Bass suborder of $\mathrm{End}(E)$ but only give a heuristic algorithm for computing the Bass suborder. Theorems 3.12 and 3.15 suggest the following approach to compute a Bass suborder of $\mathrm{End}(E)$: run Algorithm 1 twice, first on the input $(E, 3, 2)$ and then on the input $(E, 5, 2)$, to produce two inseparable reflections $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i$ of E and the Bass order $\Lambda_{\alpha_1\alpha_2}$ generated by α_1 and α_2.

Remark 4.7. The same heuristic the authors make in [EHL+20] to argue that the expectation of the number of calls to their algorithm for computing an endomorphism of a supersingular elliptic curve E before producing a generating for a Bass order will be used in Section 6.1 to argue that the expected number of calls to Algorithm 1 before producing a generating set for $\mathbb{Z} + P$. This approach to computing a basis for $\mathrm{End}(E)$ is taken up in the next section.

Algorithm 2: Compute a Bass order contained in $\mathrm{End}(E)$

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$, two distinct primes $\ell_1, \ell_2 \neq p$, and an integer d, with d square-free, $d < p/4$, and $-dp \not\equiv 1 \pmod 4$.

Output: A compact representation of a Bass order contained in $\mathrm{End}(E)$.

1 Use Algorithm 1 twice, on input respectively (E, ℓ_1, d) and (E, ℓ_2, d), to compute two inseparable reflections α_1, α_2 of E;

2 **return** $\Lambda = \langle 1, \alpha_1, \alpha_2, \alpha_1\alpha_2 \rangle$

Theorem 4.8 (GRH)**.** *Algorithm 2 is correct. Assuming GRH, if $p > 8$ and E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ then on input $(E, 3, 5, 2)$ Algorithm 2 terminates in expected $O(p^{1/2}(\log\log p)^2(\log\log p)^3)$ bit operations.*

Proof. By Proposition 4.5, the two endomorphisms constructed in Step 1 are inseparable reflections. Write $\alpha_i = \pi\widehat{\phi_i^{(p)}}\psi_i\phi_i$ where $\phi_i \colon E \to E_i$ is an isogeny of degree $\ell_i^{k_i}$. Since $\ell_1 \neq \ell_2$, the kernels of ϕ_1 and ϕ_2 are distinct. Therefore Theorem 3.12 implies Λ is an order in $\mathrm{End}(E)$, and Theorem 3.15 implies Λ is Bass. Thus, Algorithm 2 is correct. By Proposition 4.5, Step 1 terminates in expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ time. □

5 Computing $\mathrm{End}(E)$ from a Bass suborder

In this section, we combine Algorithm 2 and the algorithms in [EHL+20, Wes22] to produce an algorithm for computing a basis for the endomorphism ring of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ in expected time $O(p^{1/2}(\log p)^2(\log\log p)^3)$, conditional only on GRH. We begin with a high-level overview of the approach in [EHL+20] for computing a basis for $\mathrm{End}(E)$. First, compute a Bass suborder $\Lambda \subseteq \mathrm{End}(E)$. This can be done with Algorithm 2 in expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ bit operations conditional on GRH by Theorem 4.8. Next, enumerate maximal orders $\mathcal{O} \subseteq \mathrm{End}^0(E)$ containing the Bass order Λ until $\mathcal{O} \cong \mathrm{End}(E)$ using algorithms from [EHL+20]. We can efficiently check whether a given maximal order $\mathcal{O}$ is isomorphic to $\mathrm{End}(E)$ using the algorithms and reductions in [EHL+18, Wes22]. This approach results in Algorithm 3.

In Theorem 5.5, we show that Algorithm 3 correctly computes $\mathrm{End}(E)$, and, conditional only on GRH, terminates in expected $O(p^{1/2}(\log p)^2(\log\log p)^3)$ bit operations.

Remark 5.1. We ask Λ to be Bass because, under this assumption, we can prove that the number of maximal overorders of Λ is subexponential in the size of Λ. In general, there exists an order of size polynomial in $\log p$ contained in $\mathrm{End}(E)$ which is contained in $\Omega(p)$ many distinct, pairwise non-isomorphic maximal orders. For example, choose $e = O(\log p)$ such that every supersingular E' defined over $\mathbb{F}_{p^2}$ is connected by a 2^d isogeny to E for some $d \leq e$, and consider the order $\mathbb{Z} + 2^e\,\mathrm{End}(E)$. We claim that this order has size polynomial in $\log p$ and embeds into the endomorphism ring of each supersingular elliptic curve over $\mathbb{F}_{p^2}$, and therefore into a representative of each conjugacy class of maximal orders in $\mathrm{End}^0(E)$. For any supersingular E' there is an ideal $I \subseteq \mathrm{End}(E)$ such that $\mathcal{O}_R(I) \cong \mathrm{End}(E')$ and $\mathrm{Nrd}(I) = 2^d$ for some $d \leq e$. Then $\mathbb{Z} + 2^e\,\mathrm{End}(E) \subseteq \mathbb{Z} + I \subseteq \mathcal{O}_R(I)$. Since E' was arbitrary, we conclude that $\mathbb{Z} + 2^e\,\mathrm{End}(E)$ is contained in a representative of each conjugacy class of maximal orders, and there are $\Omega(p)$ many conjugacy classes. Despite being contained in an exponentially large number of maximal orders, there is a basis for $\mathbb{Z}+2^e\,\mathrm{End}(E)$ whose size is polynomial in $\log p$ since $e = O(\log p)$ and $\mathrm{End}(E)$ has a basis whose size is polynomial in $\log p$.

Remark 5.2. In [ES24], Eisenträger and Scullard give an algorithm for computing $\mathrm{End}(E)$ in polynomial time given a suborder Λ of $\mathrm{End}(E)$ of polynomial size and a factorization of $\mathrm{disc}\,\Lambda$. Running Algorithm 2 to compute a Bass order $\Lambda = \Lambda_{\alpha_1\alpha_2}$, factoring $|\,\mathrm{disc}(\alpha_1\alpha_2/p)|$, and then using Algorithm 8.1 of [ES24] yields a faster algorithm for computing a basis for $\mathrm{End}(E)$ than the one outlined here, but with the same (conditional GRH) run time of $O(p^{1/2}(\log p)^2(\log\log p)^3)$.

Algorithm 3: Compute End(E)

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$, where $p > 8$.
Output: A maximal order $\mathcal{O} \subseteq B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$.

1 Run Algorithm 2 on input $(E, 3, 5, 2)$ to compute a Bass order Λ contained in $\mathrm{End}(E)$;
2 Compute $a, b \in \mathbb{Q}^\times$ and an isomorphism $f\colon \Lambda \otimes \mathbb{Q} \to H(a, b)$;
3 Enumerate the maximal orders $\mathcal{O} \supseteq f(\Lambda)$ until $\mathcal{O} \cong \mathrm{End}(E)$;
4 **return** $\mathcal{O}$

We require an efficient algorithm for testing whether a maximal order $\mathcal{O}$ is isomorphic to $\mathrm{End}(E)$. To do this, we will make use of an efficient algorithm for computing a supersingular curve E' such that $\mathrm{End}(E') \cong \mathcal{O}$. If $j(E') \in \{j(E), j(E)^p\}$, then $\mathcal{O} \cong \mathrm{End}(E)$. An algorithm for producing a curve with endomorphism ring isomorphic to a given maximal order appears in [EHL+18], which is efficient conditional on heuristics including GRH. The work of Wesolowski [Wes22] allows one to remove the heuristic assumptions (except for GRH). We state that such an efficient algorithm exists here for completeness, noting that this algorithm is due to results and algorithms in [Brö09, GPS17, EHL+18, Wes22, CKMZ22]. See [EPSV23] for a discussion of an efficient implementation of an algorithm addressing this problem.

Lemma 5.3. *There is an algorithm which, on input a basis for a maximal order $\mathcal{O}$ of a quaternion algebra B over $\mathbb{Q}$ ramified at p, ∞, outputs a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. Conditional on GRH, the algorithm runs in time polynomial in the size of $\mathcal{O}$.*

Proof. This follows by combining algorithms and results in [Piz80a, Brö09, KLPT14, GPS17, EHL+18, CKMZ22, Wes22]. First, we compute a quaternion algebra $B_{p,\infty}$ ramified at p and ∞, a supersingular elliptic

curve E_0, and a maximal order $\mathcal{O}_0$ in $B_{p,\infty}$ such that $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ under some explicit isomorphism. This can be done in time polynomial in $\log p$, conditional on GRH [EHL+18, Proposition 3]. Next, we compute an isomorphism $f\colon \mathcal{O} \otimes \mathbb{Q} \to B_{p,\infty}$ of quaternion algebras, which can be done in time polynomial in $\log p$ [CKMZ22, Proposition 4.1].

We now compute a supersingular elliptic curve E such that $\mathrm{End}(E) \cong \mathcal{O}$. First, we compute a connecting ideal J between $\mathcal{O}_0$ and $f(\mathcal{O})$. By Theorem 6.4 of [Wes22], assuming GRH, we can, in expected polynomial time, compute an equivalent ideal I to J such that the norm of I is B-powersmooth for some $B = O((\log p)^c)$ for some constant c, meaning that if p^e exactly divides $\mathrm{Nrd}(I)$ then $p^e \leq B$. Since the norm of I is B-powersmooth, we can efficiently compute the corresponding isogeny $\phi_I\colon E_0 \to E$ [EHL+18, Proposition 4]. The codomain E of ϕ_I is a curve whose endomorphism ring is isomorphic to $\mathcal{O}$, since

$$\mathrm{End}(E) \cong \mathcal{O}_R(I) \cong \mathcal{O}_R(J) = f(\mathcal{O}) \cong \mathcal{O}.$$

Thus the algorithm is correct. □

We require a bound on the number of maximal orders containing a given Bass order Λ. Below we show that that we may bound this quantity in terms of the number of divisors of the reduced discriminant of the order. Assuming Λ has size polynomial in $\log p$, this implies that the number of maximal orders containing Λ grows at most subexponentially in $\log p$.

Lemma 5.4. *Let $\Lambda \subseteq B_{p,\infty}$ be a Bass order. The number of maximal orders in $B_{p,\infty}$ containing Λ is $O((\mathrm{discrd}(\Lambda))^\epsilon)$, for every $\epsilon > 0$.*

Proof. By Proposition 4.2 of [EHL+20] and the local-global dictionary for orders [Voi13, Theorem 9.1.1], the number of maximal overorders of Λ is bounded by

$$\prod_{\substack{q \text{ prime} \\ q \neq p}} v_q(\mathrm{discrd}(\Lambda)) + 1,$$

and this quantity is equal to the number of divisors of $\mathrm{discrd}(\Lambda)/p^{v_p(\mathrm{discrd}(\Lambda))}$. The number of divisors of an integer n is $O(n^\epsilon)$ for every $\epsilon > 0$ [HW08, Theorem 315]. The claim of the lemma follows.

□

We now prove the main theorem of this section, which states that our algorithm computes the endomorphism ring of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ in $O(p^{1/2}(\log p)^2(\log\log p)^3)$ bit operations, conditional on GRH (and assuming no further heuristics).

Theorem 5.5 (GRH)**.** *Algorithm 3 is correct. Assuming GRH, Algorithm 3 terminates in expected*

$$O(p^{1/2}(\log p)^2(\log\log p)^3)$$

bit operations.

Proof. By Theorem 4.8, Step 1 runs in expected time $O(p^{1/2}(\log p)^2(\log\log p)^3)$. Moreover, Λ is Bass. We now discuss Step 2. First, compute the Gram matrix G under the trace pairing of the basis $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ for Λ: by the discussion in Section 4, we need to compute a single trace, namely $\mathrm{Trd}(-\alpha_1\alpha_2/p)$. This trace can be computed in time polynomial in $\log p$ with a generalization of Schoof's algorithm [Koh96, BCNE+19], since $\rho := -\alpha_1\alpha_2/p$ is a cyclic isogeny of degree $2^2 3^{2k_1} 5^{2k_2}$ and $k_1, k_2 = O(\log p)$. With G, compute $a, b \in \mathbb{Q}^\times$ such that $\Lambda \otimes \mathbb{Q}$ is isomorphic to $H(a, b)$ with the Gram-Schmidt process.

We now outline how to do Step 3. We factor $\mathrm{disc}(\rho)$ to obtain a factorization of $\mathrm{discrd}(\Lambda) = p^4 |\mathrm{disc}(\rho)|$. Since ρ is the product of $2 + 2k_1 + 2k_2 = O(\log p)$ isogenies of degree at most 5, the degree of ρ is $O(p^C)$ for some C. This implies $-\mathrm{disc}(\rho) = O(p^C)$ as well. Therefore we can factor $\mathrm{disc}(\rho)$ in time subexponential in $\log p$ [LP92, Theorem 1]. For each $q | \mathrm{discrd}(\Lambda)$ such that $q \neq p$, we can enumerate maximal $\mathbb{Z}_q$-orders containing $f(\Lambda) \otimes \mathbb{Z}_q$ efficiently using Algorithm 4.3 of [EHL+20] and then enumerate the $\mathbb{Z}$-orders containing $f(\Lambda)$; see Steps 1(a) and 3(a) in Algorithm 5.4 of [EHL+20]. For each maximal order $\mathcal{O}$ containing $f(\Lambda)$, compute an elliptic curve E' with $\mathrm{End}(E') \cong \mathcal{O}$. This can be done in polynomial time in $\log p$ by Lemma 5.3. If $j(E') \in \{j(E), j(E)^p\}$, we return $\mathcal{O}$. Thus the algorithm is correct.

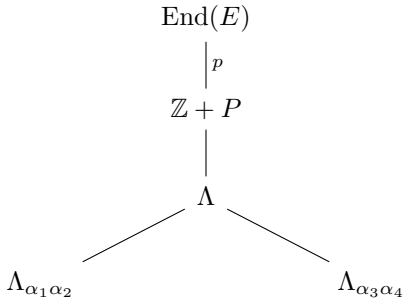
By Lemma 5.4, the number of maximal overorders of $f(\Lambda)$ is $O(p^\epsilon)$ for every $\epsilon > 0$. We conclude that Step 3 takes $O(p^\epsilon)$ time for any $\epsilon > 0$. In particular, the expected time required to complete Step 3 is dominated by the expected time required to complete Step 1. □

6 The number of inseparable reflections needed to generate $\mathrm{End}(E)$

Let E be a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. Let $P \coloneqq \pi \mathrm{Hom}(E, E^{(p)}) \subseteq \mathrm{End}(E)$ be the ideal of inseparable endomorphisms of E. Theorem 4.8 implies that for an appropriate choice of parameters, with two calls to Algorithm 1 we compute a generating set for a Bass order Λ contained in $\mathbb{Z} + P$. If one had a basis for $\mathbb{Z} + P$, rather than just a Bass suborder, then the algorithms of Voight [Voi13] can compute a basis for $\mathrm{End}(E)$ efficiently, since $\mathrm{End}(E)$ is the unique maximal order containing $\mathbb{Z} + P$ by Proposition 3.1. This raises the following question: how many calls to Algorithm 1 does one expect to make before computing a generating set for $\mathbb{Z} + P$? In this section, we give a heuristic argument showing that the number of inseparable endomorphisms required to generate $\mathbb{Z} + P$ is bounded above by a constant, independent of the field; empirically, four inseparable reflections do the trick more often than not. This results in a second algorithm for computing $\mathrm{End}(E)$: compute inseparable reflections with Algorithm 1 until finding a generating set for $\mathbb{Z} + P$, and then compute a basis for the maximal order containing $\mathbb{Z} + P$ using the algorithms of [Voi13]. This algorithm will be slower than Algorithm 3, but is simpler to implement; we discuss further implementation details in the Appendix.

6.1 The expected number of inseparable reflections in a generating set for $\mathbb{Z}+P$

Suppose we run Algorithm 2 twice on input E, a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, producing two orders $\Lambda_{\alpha_1\alpha_2}$ and $\Lambda_{\alpha_3\alpha_4}$ in $\mathbb{Z} + P \subseteq \mathrm{End}(E)$ spanned respectively by $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ and $1, \alpha_3, \alpha_4, \alpha_3\alpha_4$, where α_i is an inseparable reflection for every $i = 1, \ldots, 4$. Let Λ be the order in $\mathrm{End}(E)$ generated by $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.



Then

$$\mathrm{discrd}(\Lambda) = \mathrm{discrd}(\mathbb{Z} + P) \cdot [\mathbb{Z} + P : \Lambda] = p^2 \cdot [\mathbb{Z} + P : \Lambda],$$

and $\mathrm{discrd}(\Lambda)$ divides both $\mathrm{discrd}(\Lambda_{\alpha_1\alpha_2})$ and $\mathrm{discrd}(\Lambda_{\alpha_3\alpha_4})$. Defining $\rho_1 = \frac{\alpha_1\alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3\alpha_4}{p}$, we have

$$\mathrm{discrd}\,\Lambda_{\alpha_1\alpha_2} = p^2|\,\mathrm{disc}(\rho_2)| \text{ and } \mathrm{discrd}\,\Lambda_{\alpha_3\alpha_4} = p^2|\,\mathrm{disc}(\rho_1)|.$$

In particular, $[\mathbb{Z}+P : \Lambda] = \frac{\mathrm{discrd}(\Lambda)}{p^2}$ divides $\gcd(\mathrm{disc}(\rho_1), \mathrm{disc}(\rho_2))$. If $\gcd(\mathrm{disc}\,\rho_1, \mathrm{disc}\,\rho_2) = 1$, then $\Lambda = \mathbb{Z}+P$ and the four inseparable endomorphisms $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathbb{Z} + P$. If the distribution of the integers $\mathrm{disc}(\rho_1)$ and $\mathrm{disc}(\rho_2)$ follow the same distribution as two random integers, then $\mathrm{disc}(\rho_1)$ and $\mathrm{disc}(\rho_2)$ are coprime with probability $6/\pi^2$. Assuming this, four calls to Algorithm 1 produce a generating set for $\mathbb{Z} + P$ with at least $6/\pi^2 \approx 0.6$ probability.

Unfortunately, the integers $D_i = \mathrm{disc}(\rho_i)$ are not distributed like random integers. First of all, the integer D_i is a discriminant, which imposes congruency conditions on D_i. Second, the prime p is not split in $\mathbb{Z}[\rho_i]$, imposing another congruence condition. Finally, the fact that ρ_i is an endomorphism of smooth degree enforces relations in the ideal class group of $\mathbb{Z}[\rho_i]$. In any case, the following heuristic suffices for our purposes:

Heuristic 6.1. Let $p > 3$ be a prime and let $\ell < p/4$ be a prime. Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. There exists a constant $c > 0$, independent of p, such that if $\rho_i = -\alpha_{i1}\alpha_{i2}/p$ where α_{ij}, $1 \le i, j \le 2$ are the outputs of four calls to Algorithm 1 on input $(E/\mathbb{F}_{p^2}, \ell, 1)$, then $\Pr[\gcd(\mathrm{disc}\,\rho_1, \mathrm{disc}\,\rho_2) = 1] \ge c$.

The following theorem follows from the above discussion:

Theorem 6.2. *Assume Heuristic 6.1. Let $p > 3$ and $\ell < p/4$ be primes, and let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Then the expected number of calls to Algorithm 1 on input $(E, \ell, 1)$ in order to produce a generating set for $\mathbb{Z} + P$ is bounded from above by a constant, independent of p.*

Heuristic 6.1 is [EHL+20, Heuristic 5.2] which is assumed in [EHL+18, Theorem 5.3] to prove that [EHL+20, Algorithm 5.1] produces a Bass order in $\mathrm{End}(E)$ and terminates in expected $O(p^{1/2+\epsilon})$ time. We use the heuristic in a new way.

Remark 6.3. This heuristic argument applies to any pair of orders generated by two pairs of of two non-commuting elements of a maximal order in $B_{p,\infty}$, the quaternion algebra ramified at p and ∞. Let α_1, α_2 be two arbitrary non-commuting elements of a quaternion order $\mathcal{O} \subseteq B_{p,\infty}$ and let $\Lambda = \langle \alpha_1, \alpha_2 \rangle := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2$ be the order they generate, and let $T_i := \mathrm{Trd}(\alpha_i)$, $N_i := \mathrm{Nrd}(\alpha_i)$ for $i = 1, 2$, and let $T_{12} = \mathrm{Trd}(\alpha_1\alpha_2)$. Then the discriminant of Λ is

$$\det \begin{pmatrix} 2 & T_1 & T_2 & T_{12} \\ T_1 & 2N_1 & T_1T_2 - T_{12} & N_1T_2 \\ T_2 & T_1T_2 - T_{12} & 2N_2 & N_2T_1 \\ T_{12} & T_2N_1 & T_1N_2 & 2N_1N_2 \end{pmatrix} = \left(\frac{1}{4} \operatorname{disc}(T_2\alpha_1 + T_1\alpha_2 - 2\alpha_1\alpha_2) \right)^2 .$$

Suppose now that we sample $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ uniformly (in some reasonable sense - for example, uniformly from the elements of $\mathcal{O}$ whose norm is bounded by some fixed polynomial in p) and that $\alpha_{i1}\alpha_{i2} \neq \alpha_{i2}\alpha_{i1}$ for $i = 1, 2$. Define Λ_1 and Λ_2 to be the orders generated by α_{11}, α_{12} and α_{21}, α_{22}, respectively, let

$$\rho_i := (\mathrm{Trd}\, \alpha_{i2})\alpha_{i1} + (\mathrm{Trd}\, \alpha_{i1})\alpha_{i2} - 2\alpha_{i1}\alpha_{i2},$$

let $D_i = \operatorname{disc} \rho_i,$, and let Λ denote the order generated by the α_{ij} for $1 \leq i, j \leq 2$. Then

$$[\mathcal{O} : \Lambda] = \frac{\mathrm{discrd}\, \Lambda}{\mathrm{discrd}\, \mathcal{O}}, \quad [\mathcal{O} : \Lambda_i] = \frac{\mathrm{discrd}\, \Lambda_i}{\mathrm{discrd}\, \mathcal{O}} = \frac{|D_i|}{4\, \mathrm{discrd}\, \mathcal{O}}$$

and $[\mathcal{O} : \Lambda]$ divides

$$\gcd([\mathcal{O} : \Lambda_1], [\mathcal{O} : \Lambda_2]) = \gcd\left(\frac{D_1}{4\, \mathrm{discrd}\, \mathcal{O}}, \frac{D_2}{4\, \mathrm{discrd}\, \mathcal{O}} \right).$$

Therefore the α_{ij} will generate $\mathcal{O}$ with probability at least the probability that

$$\gcd(D_1, D_2) = 4\, \mathrm{discrd}\, \mathcal{O}.$$

A reasonable heuristic would then be that this probability is bounded from below by a constant, independent of p. We will explore this experimentally in the next section as well.

6.2 Computational experiments

We implemented Algorithm 1 along with the various algorithms discussed in this section in order to empirically determine the expected value of the number of inseparable reflections of E required before generating $\mathrm{End}(E)$. We believe this expectation is bounded by a constant, independent of p or E. We restricted our attention to elliptic curves E defined over $\mathbb{F}_{p^2}$ but not over $\mathbb{F}_p$, since there are asymptotically faster algorithms for computing the endomorphism ring of such curves.

To experimentally test Heuristic 6.1 and to understand the expected number of inseparable reflections in a generating set for $\mathbb{Z} + P$, we conducted the following experiment. For $n \in \{16, 17, \ldots, 32\}$, we repeated the following procedure 100 times: we chose the first prime p after 2^n and computed a pseudorandom supersingular j-invariant in $\mathbb{F}_{p^2} - \mathbb{F}_p$ by taking a random walk in $G(p, 2)$ of length $\lfloor \log_2 p \rfloor$. We then generated four inseparable reflections α_i, $1 \leq i \leq 4$, of degree $2^{2t}p$ for $i = 1, 3$ and $3^{2s}p$ for $i = 2, 4$. Next, we tested whether $\gcd\left(\operatorname{disc}\left(\frac{\alpha_1\alpha_2}{p}\right), \operatorname{disc}\left(\frac{\alpha_3\alpha_4}{p}\right)\right) = 1$ and whether $1, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathbb{Z} + P$. We report the sample mean for the random variable which is 1 when $\gcd\left(\operatorname{disc}\left(\frac{\alpha_1\alpha_2}{p}\right), \operatorname{disc}\left(\frac{\alpha_3\alpha_4}{p}\right)\right) = 1$ and 0

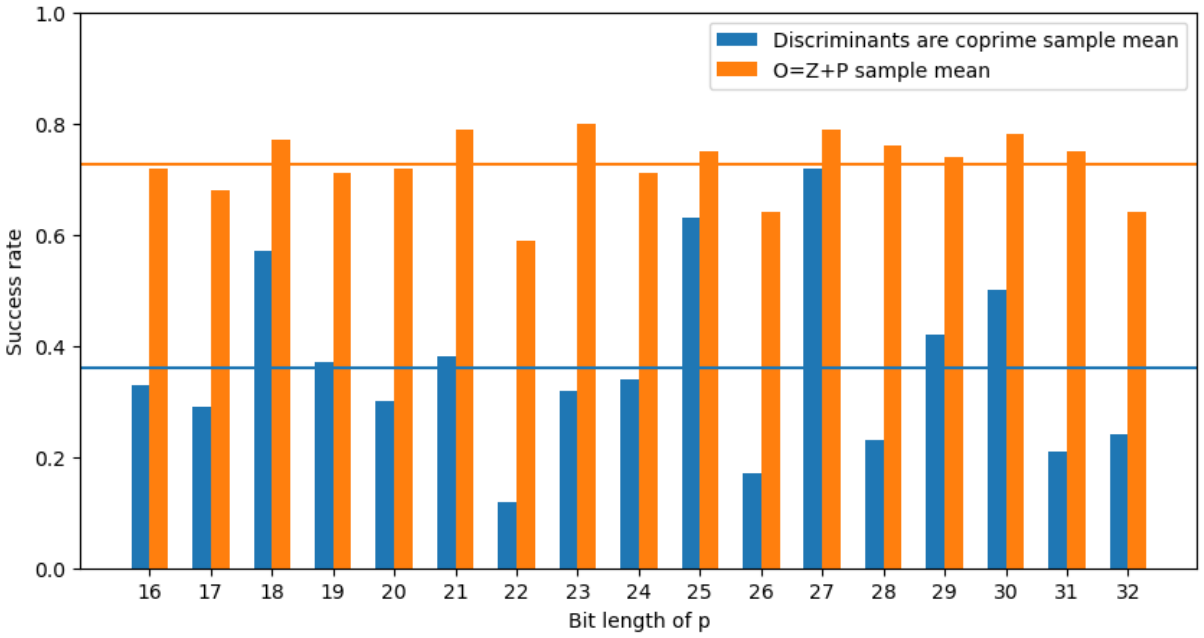


Figure 1: Collected data for testing Heuristic 6.1. Orange bars represent the experimental probability that $\gcd\left(\operatorname{disc}\left(\frac{\alpha_1\alpha_2}{p}\right), \operatorname{disc}\left(\frac{\alpha_3\alpha_4}{p}\right)\right) = 1$, blue bars represent the experimental probability that $1, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathbb{Z} + P$, where α_i are inseparable reflections of a supersingular elliptic curve. Averages of the two frequencies are plotted as well.

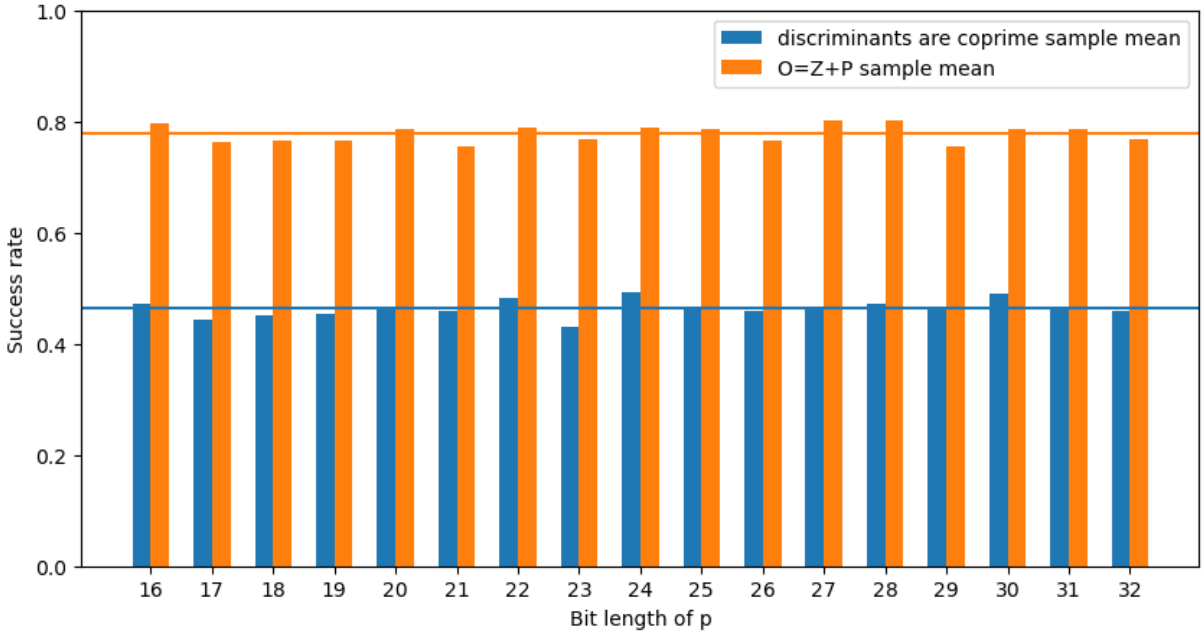


Figure 2: Collected data for testing heuristic in Remark 6.3. Orange bars represent the experimental probability that $\gcd(\operatorname{disc}(D_1, D_2)) = 4p^2$, blue bars represent the experimental probability that $1, \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ generate $\mathbb{Z} + P$ where α_{ij} are random elements of $\mathbb{Z} + P$ in a random maximal order in $B_{p,\infty}$ and D_i is the discriminant of $\rho_i := (\operatorname{Trd}\alpha_{i2})\alpha_{i1} + (\operatorname{Trd}\alpha_{i1})\alpha_{i2} - 2\alpha_{i1}\alpha_{i2}$. Averages of the two frequencies are plotted as well.

otherwise, and the sample mean of the random variable which is 1 when $1, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathbb{Z}+P$ and 0 otherwise in Table 1.

The data does not seem to invalidate Heuristic 6.1, but it also does not illuminate what the actual probability is that two inseparable reflections have coprime discriminants. The data does support our desired conclusion, namely that on average, the number of inseparable reflections needed to generate $\mathbb{Z}+P$ is bounded from above by a constant, independent of p. In particular, that constant appears to be bounded from above by four! In any case, the coprimality of the discriminants is not a necessary condition for the inseparable reflections to generate $\mathbb{Z}+P$.

An idealized version of the algorithm sketched in Section 6 would generate random endomorphisms in $\mathbb{Z}+P$ of bounded norm, rather than "structured" endomorphisms such as the inseparable reflections output by Algorithm 1. One might wonder whether the heuristic suggested in 6.3 holds, and how many random elements of $\mathbb{Z}+P$ are required to generate $\mathbb{Z}+P$. We conducted the following numerical experiment. For $n \in \{16, 17, \ldots, 32\}$, we repeated the following procedure 100 times: we chose the first prime p after 2^n and computed a pseudorandom maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞. We then computed $\mathbb{Z}+P$, where P is the unique 2-sided ideal of $\mathcal{O}$ of reduced norm p and sampled four random elements $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} \in \mathbb{Z}+P$. We compute

$$\rho_i \coloneqq (\operatorname{Trd}\alpha_{i2})\alpha_{i1} + (\operatorname{Trd}\alpha_{i1})\alpha_{i2} - 2\alpha_{i1}\alpha_{i2}$$

and $D_i = \operatorname{disc}\rho_i$ and then tested whether $\gcd(D_1, D_2) = 4\operatorname{discrd}(\mathbb{Z}+P) = 4p^2$ and whether $1, \alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathbb{Z}+P$. The sample means are reported in Table 2. The probabilities that $\gcd(D_1, D_2) = 4p^2$ and that $\{1, \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}\}$ generate $\mathbb{Z}+P$ do not appear to decay as p increases in the range $[2^{16}, 2^{32}]$.

A Appendix

In this appendix, we discuss an algorithm following the idea suggested in Section 6, that is, to compute a basis for the endomorphism ring of a supersingular elliptic curve E by making repeated calls to Algorithm 1 to produce inseparable endomorphisms. The extra ingredients include a generalization of Schoof's algorithm for computing the trace of an endomorphism, some algorithms of Voight [Voi13] for local and global quaternion orders, and linear algebra. Below, we provide the details regarding the linear algebra necessary to complete the algorithm. Our implementation in SageMath is available at `https://github.com/travismo/inseparables`.

The algorithm goes as follows: we first compute three inseparable reflections $\gamma_1, \gamma_2, \gamma_3$ of E. Let $P \coloneqq \operatorname{Hom}(E^{(p)}, E)\pi$ be the ideal of inseparble endomorhisms of E; then P is the unique 2-sided ideal of reduced norm p in $\operatorname{End}(E)$. Defining $\gamma_0 = 1$, we next compute the Gram matrix $G = (\operatorname{Trd}(\gamma_i\widehat{\gamma_j}))$ for the sequence $\Gamma = (\gamma_0, \gamma_1, \gamma_2, \gamma_3)$; this is where we require a generalization of Schoof's algorithm [BCNE+19]. Then Γ is a basis for $\operatorname{End}^0(E)$ as a $\mathbb{Q}$-vector space if and only if $\det(G) \neq 0$, which we now assume. At this point, we have computed $\operatorname{End}^0(E)$ as a quadratic module: if we let $Q(x) = x^T G x$ denote the quadratic form induced by G on $\mathbb{Q}^4$, then $(\operatorname{End}^0(E), \deg) \cong (\mathbb{Q}^4, Q)$. Having computed $\operatorname{End}^0(E)$ as a quadratic module, we determine its structure as a quaternion algebra: we compute a multiplication table for the basis Γ. We then compute the order $\mathcal{O} \subseteq \operatorname{End}(E)$ generated by $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. Finally, we enlarge the order $\mathcal{O}$ by computing additional inseperable reflections until $\mathcal{O} = \mathbb{Z}+P$. As mentioned above, a basis for $\operatorname{End}(E)$ is efficiently recovered from a basis for $\mathbb{Z}+P$ using algorithms of Voight [Voi21].

A.1 Computing a quadratic submodule of $\mathbb{Z}+P$

Recall that the output of Algorithm 1 on input E is a trace-zero endomorphism of E belonging to P. We assume that, by running Algorithm 1 three times (with $d = 1$ for simplicity) we have computed three inseparable reflections $\gamma_1, \gamma_2, \gamma_3$ of E and we define $\gamma_0 = 1 \in \operatorname{End}(E)$. Since $d = 1$, for $i = 1, 2, 3$ we have

$$\gamma_i = \pi_p \widehat{\phi_i^{(p)}} \phi_i,$$

where $\phi_i \colon E \to E_i$ is a separable isogeny.

Let $\Lambda \coloneqq \mathbb{Z}\gamma_0 + \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2 + \mathbb{Z}\gamma_3$ be the $\mathbb{Z}$-span of $\gamma_0, \gamma_1, \gamma_2$ and γ_3. Let $G \coloneqq (\mathrm{Trd}(\gamma_i\widehat{\gamma_j}))$ be the Gram matrix for $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. First, by Proposition 3.9, we have $\mathrm{Trd}(\gamma_i) = 0$ for $i = 1, 2, 3$. For $1 \leq i < j \leq 3$ define

$$\rho_{ij} \coloneqq \widehat{\phi_i}\phi_i^{(p)}\widehat{\phi_j^{(p)}}\phi_j.$$

Then $\mathrm{Trd}(\gamma_i\widehat{\gamma_j}) = p\,\mathrm{Trd}(\rho_{ij})$ and the Gram matrix of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ is

$$G \coloneqq (\mathrm{Trd}(\gamma_i\widehat{\gamma_j}))_{0\leq i,j\leq 3} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2p\deg(\phi_1)^2 & p\,\mathrm{Trd}(\rho_{12}) & p\,\mathrm{Trd}(\rho_{13}) \\ 0 & p\,\mathrm{Trd}(\rho_{13}) & 2p\deg(\phi_2)^2 & p\,\mathrm{Trd}(\rho_{23}) \\ 0 & p\,\mathrm{Trd}(\rho_{13}) & p\,\mathrm{Trd}(\rho_{23}) & 2p\deg(\phi_3)^2 \end{pmatrix}.$$

We can compute the entries of G with an algorithm for computing the trace of an endomorphism represented as a sequence of low degree isogenies with a generalization of Schoof's algorithm [BCNE+19]. If $\det(G) \neq 0$, then Λ is a lattice in $\mathbb{Z} + P \subseteq \mathrm{End}(E)$, which we now assume. Therefore, as quadratic $\mathbb{Z}$-modules, we have $(\Lambda, \deg) \cong (\mathbb{Z}^4, G)$ under the isomorphism which sends γ_i to the ith standard basis vector in $\mathbb{Z}^4$.

A.2 From a quadratic module to an order in a quaternion algebra

With the Gram matrix G of the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ in hand, we move on to determining the structure of $\Lambda \otimes \mathbb{Q}$ as a quaternion algebra. We discuss two approaches: the first involves computing an embedding of $\Lambda = \mathbb{Z}\gamma_0 + \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2 + \mathbb{Z}\gamma_3$ into a quaternion algebra $H(a, b)$ such that $(\mathbb{Z}^4, G) \cong (H(a, b), \mathrm{Nrd})$ are isomorphic as quadratic spaces. A second approach is to directly compute a multiplication table for $\gamma_1, \gamma_2, \gamma_3$, i.e. computing rational numbers m_{rst} such that $\gamma_r\gamma_s = \sum_t m_{rst}\gamma_t$. We discuss both in detail. In the first, we compute the LDL^T-decomposition of G and read off a and b from the second and third entries of D. In the other, we solve for m_{rst} by setting up a system of equations using G.

A.2.1 Computing an isomorphism of quaternion algebras using the Gram–Schmidt process

Let $G \coloneqq (G_{rs})_{0\leq r,s\leq 3} \coloneqq (\mathrm{Trd}(\gamma_r\widehat{\gamma_s}))_{0\leq r,s\leq 3}$ be the Gram matrix for the basis $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ of a lattice Λ in $\mathrm{End}(E)$. One approach to giving $\Lambda \otimes \mathbb{Q}$ the structure of a quaternion algebra is as follows. First, we diagonalize the quadratic form induced by G (to be precise, we compute the LDL^T-decomposition of G). We obtain a lower-triangular matrix L with 1's on the diagonal and a diagonal matrix D such that $G = LDL^T$. Denote the diagonal entries of D by $d_0 = 2, d_1, d_2, d_3$ and define $a, b \in \mathbb{Q}$ by $d_1 = -2a$, $d_2 = -2b$. Define $H(a, b)$ to be the quaternion algebra with basis $1, i, j, ij$ such that $i^2 = a$, $j^2 = b$, and $ij = -ji$. Define $R = L^T$ and $\tilde{\gamma_i} = \sum_j (R^{-1})_{ij}\gamma_j$ for $i = 0, 1, 2, 3$. Then $\{\tilde{\gamma_0}, \tilde{\gamma_1}, \tilde{\gamma_2}, \tilde{\gamma_3}\}$ is the result of the application of the Gram–Schmidt process to the basis $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ of $\Lambda \otimes \mathbb{Q}$. Since $\mathrm{Trd}(\tilde{\gamma_1}) = 0$, we have

$$\tilde{\gamma_1}^2 = -\tilde{\gamma_1}\widehat{\tilde{\gamma_1}} = \frac{-1}{2}\,\mathrm{Trd}(\tilde{\gamma_1}\widehat{\tilde{\gamma_1}})) = \frac{-d_1}{2} = a.$$

Similarly, $(\tilde{\gamma_2})^2 = b$. Since $\tilde{\gamma_3}$ and $\tilde{\gamma_1}\tilde{\gamma_2}$ are both orthogonal to each of $1, \tilde{\gamma_1}, \tilde{\gamma_2}$, there exists $c \in \mathbb{Q}$ such that $\tilde{\gamma_3} = c\tilde{\gamma_1}\tilde{\gamma_2}$. Taking reduced norms, we obtain

$$\frac{d_3}{2} = \mathrm{Nrd}(\tilde{\gamma_3}) = \mathrm{Nrd}(c\tilde{\gamma_1}\tilde{\gamma_2}) = \frac{c^2 d_1 d_2}{4}.$$

Define $c' \coloneqq \sqrt{\frac{2d_3}{d_1 d_2}}$. We therefore obtain an isomorphism of quadratic spaces

$$\begin{aligned} (\mathrm{End}^0(E), \deg) &\to (H(a, b), \mathrm{Nrd}) \\ x_0 + x_1\tilde{\gamma_1} + x_2\tilde{\gamma_2} + x_3\tilde{\gamma_3} &\mapsto x_0 + x_1 i + x_2 j + x_3 c' ij. \end{aligned}$$

This map factors through the map of quadratic modules $f\colon \mathrm{End}^0(E) \to (\mathbb{Q}^4, G)$ which sends γ_r to e_r, the r-th standard basis vector of $\mathbb{Q}^4$, via the map $g\colon (\mathbb{Q}^4, G) \to (H(a, b), \mathrm{Nrd})$ obtained from sending the rows of $(L^T)^{-1}$ to the basis $1, i, j, ij$. The isomorphism $(\mathrm{End}^0(E), \deg) \cong (H(a, b), \mathrm{Nrd})$ induces an isomorphism of quaternion algebras between $\mathrm{End}^0(E)$ with either $H(a, b)$ (in the case that $c = c'$) or $H(a, b)^{\mathrm{op}}$ (in the case that $c = -c'$).

A.2.2 Computing a multiplication table using linear algebra

An alternative method for representing $\mathrm{End}^0(E)$ using the basis $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ is to compute a multiplication table, i.e. rational numbers m_{rst}, for $0 \le r, s, t \le 3$, such that

$$\gamma_r \gamma_s = \sum_{t=0}^{3} m_{rst} \gamma_t.$$

We sketch this approach, although we do not use it in our implementation.

To compute the multiplication table $\{m_{rst}\}$, we use $G = (G_{rs})_{0 \le r,s \le 3}$ and linear algebra. In particular, we use G to set up a system of linear equations whose solutions are the $\{m_{rst}\}$ we seek.

Proposition A.1. *Let $\gamma_0 = 1, \gamma_1, \gamma_2, \gamma_3$ be as above. Define*

$$m_{000} = 1, \quad m_{rrt} = \begin{cases} -\frac{G_{rr}}{2} & : t = 0 \text{ and } 1 \le r \le 3 \\ 0 & : 0 \le r \le 3 \text{ and } 1 \le t \le 3. \end{cases}$$

Let $\{m_{120}, \dots, m_{123}\}$, $\{m_{130}, \dots, m_{133}\}$, and $\{m_{230}, \dots, m_{233}\}$ respectively solve the following three systems of linear equations:

$$G \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -G_{12} \\ \frac{1}{2}G_{11}G_{21} \\ \frac{1}{2}G_{22}G_{11} \\ 2\,\mathrm{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}) \end{pmatrix}, \quad G \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -G_{13} \\ \frac{1}{2}G_{11}G_{31} \\ 2\,\mathrm{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}) \\ \frac{1}{2}G_{33}G_{11} \end{pmatrix}, \quad G \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \begin{pmatrix} -G_{23} \\ 2\,\mathrm{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}) \\ \frac{1}{2}G_{22}G_{31} \\ \frac{1}{2}G_{33}G_{21} \end{pmatrix}.$$

Finally, for $0 \le s < r \le 3$, let

$$m_{srt} = \begin{cases} \mathrm{Trd}(\gamma_r\gamma_s) - m_{rs0} & : t = 0 \\ -m_{rst} & : 1 \le t \le 3. \end{cases}$$

Then $(2\,\mathrm{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}))^2 = \det G$, and for $0 \le r \le s \le 3$, we have

$$\gamma_r \gamma_s = \sum_{t=0}^{3} m_{rst} \gamma_t.$$

In particular, the matrix G determines an isomorphism between the quaternion algebra over $\mathbb{Q}$ with multiplication table given by $\{m_{rst}\}$ with either $\mathrm{End}^0(E)$ or its opposite algebra depending on a choice for a square root of $\det G$.

Proof. We have $\gamma_0^2 = 1$, and for $r \ne 0$, we have $\mathrm{Trd}(\gamma_r) = 0$ so $\gamma_r^2 = \mathrm{Trd}(\gamma_r)\gamma_r - \mathrm{Nrd}(\gamma_r) = -\deg(\gamma_r)$. Therefore

$$m_{000} = 1, \quad m_{rrt} = \begin{cases} -\frac{G_{rr}}{2} & : t = 0 \text{ and } 1 \le r \le 3 \\ 0 & : 0 \le r \le 3 \text{ and } 1 \le t \le 3. \end{cases}$$

Also, note that

$$\gamma_r\gamma_s = \widehat{\widehat{\gamma_s}\widehat{\gamma_r}} = \widehat{\gamma_s\gamma_r} = \mathrm{Trd}(\gamma_s\gamma_r) - \gamma_s\gamma_r,$$

so if $\gamma_r\gamma_s = \sum_t m_{rst}\gamma_t$ then

$$\gamma_s\gamma_r = \mathrm{Trd}(\gamma_r\gamma_s) - m_{rs0} - \sum_{t=1}^{3} m_{rst}\gamma_t.$$

Therefore

$$m_{srt} = \begin{cases} \mathrm{Trd}(\gamma_r\gamma_s) - m_{rs0} & : t = 0 \\ -m_{rst} & : 1 \le t \le 3. \end{cases}$$

We conclude that it suffices to calculate m_{rst} for $1 \le r < s \le 3$.

By pairing both sides of $\gamma_r\gamma_s = \sum_{t=0}^{3} m_{rst}\gamma_t$ against γ_k for $k = 0, 1, 2, 3$, we obtain for each pair (r, s) satisfying $1 \le r < s \le 3$ a system of four equations in the indeterminates $m_{rs0}, m_{rs1}, m_{rs2}, m_{rs3}$:

$$\operatorname{Trd}(\gamma_r\gamma_s\widehat{\gamma_k}) = \sum_{t=0}^{3} m_{rst} \operatorname{Trd}(\gamma_t\widehat{\gamma_k}). \tag{A.1}$$

We will show that the entries of G determine the left-hand side of Equation (A.1) uniquely (up to a choice of a square root of $\det(G)$). We compute the left hand side of Equation (A.1) for each $0 \le r < s \le 3$, $0 \le k \le 3$. We have that

$$\operatorname{Trd}(\gamma_r\gamma_s\widehat{\gamma_r}) = \deg(\gamma_r)\operatorname{Trd}(\gamma_s) = \frac{1}{2}\operatorname{Trd}(\gamma_r\widehat{\gamma_r})\operatorname{Trd}(\gamma_s\widehat{1}) = \frac{1}{2}G_{rr}G_{s1},$$

and similarly $\operatorname{Trd}(\gamma_r\gamma_s\widehat{\gamma_s}) = \operatorname{Trd}(\gamma_r)\deg(\gamma_s) = \frac{1}{2}G_{ss}G_{r1}$, for $1 \le r < s \le 3$. Finally, since $\gamma_0 = 1$,

$$\operatorname{Trd}(\gamma_r\gamma_s\widehat{\gamma_0}) = \operatorname{Trd}(\gamma_r\gamma_s) = -\operatorname{Trd}(\gamma_r\widehat{\gamma_s}) = -G_{rs}.$$

We are left with the case that $\{r, s, k\}$ is a permutation of $\{1, 2, 3\}$. First, we calculate $\operatorname{Trd}(\gamma_1\gamma_2\widehat{\gamma_3})$. For that, we recall the following trilinear form on the quaternion algebra $\operatorname{End}^0(E)$: for elements $\alpha_1, \alpha_2, \alpha_3 \in \operatorname{End}^0(E)$, define

$$m(\alpha_1, \alpha_2, \alpha_3) = \operatorname{Trd}((\alpha_1\alpha_2 - \alpha_2\alpha_1)\widehat{\alpha_3}).$$

Using the fact that $\widehat{\gamma_i} = -\gamma_i$ and that for elements $\alpha, \beta \in B$ we have $\operatorname{Trd}(\alpha\beta) = \operatorname{Trd}(\beta\alpha)$ and $\operatorname{Trd}(\widehat{\alpha}) = \operatorname{Trd}(\alpha)$, a calculation shows

$$m(\gamma_1, \gamma_2, \gamma_3) = \operatorname{Trd}((\gamma_1\gamma_2 - \gamma_2\gamma_1)\widehat{\gamma_3}) = 2\operatorname{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}).$$

The proof of Lemma 15.4.7 in [Voi21] shows that, for any elements $\alpha_0 = 1, \alpha_1, \alpha_2, \alpha_3$ in a quaternion algebra B, we have

$$m(\alpha_1, \alpha_2, \alpha_3)^2 = \det((\operatorname{Trd}(\alpha_i\widehat{\alpha_j}))_{0 \le i,j \le 3}).$$

We conclude that $m(\gamma_1, \gamma_2, \gamma_3)^2 = \det(G)$. We have that $m(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \gamma_{\sigma(3)}) = \operatorname{sgn}(\sigma)m(\gamma_1, \gamma_2, \gamma_3)$ for any $\sigma \in S_3$, e.g. by checking this for the three transpositions of S_3. The upshot is that we can make a consistent choice of values for $\operatorname{Trd}(\gamma_{\sigma(1)}\gamma_{\sigma(2)}\widehat{\gamma_{\sigma(3)}})$ by choosing, for example, $\operatorname{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}) = \frac{1}{2}\sqrt{\det(G)}$ and then setting

$$\operatorname{Trd}(\gamma_{\sigma(1)}\gamma_{\sigma(2)}\widehat{\gamma_{\sigma(3)}}) = \frac{\operatorname{sgn}(\sigma)}{2}\sqrt{\det(G)}.$$

With linear algebra over $\mathbb{Q}$, we solve the above three systems of four equations to compute all coefficients m_{rst} with $1 \le r < s \le 3$. With our earlier calculations, this determines a complete multiplication table which gives $\Lambda \otimes \mathbb{Q}$ the structure of a quaternion algebra whose underlying quadratic space is isomorphic to $(\mathbb{Q}^4, G) \cong (\operatorname{End}^0(E), \operatorname{Nrd})$. □

Remark A.2. We encounter the same phenomenon we observed in Section A.2.1: we must choose a sign for a square root to determine the multiplication table. The choice of sign of a square root of $\det(G)$ corresponds to the choice of an isomorphism of the quaternion algebra $\Lambda \otimes \mathbb{Q}$ equipped with the multiplication table $\{m_{rst}\}$ with either $\operatorname{End}^0(E)$ or $(\operatorname{End}^0(E))^{\mathrm{op}}$.

Remark A.3. We could eliminate this ambiguity by computing $\operatorname{Trd}(\gamma_1\gamma_2\widehat{\gamma_3})$ directly via Schoof's algorithm.

A.2.3 Gram–Schmidt versus multiplication tables

One may ask if the approaches in Sections A.2.1 and A.2.2 for obtaining a quaternion algebra from the basis $\{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$ with Gram matrix G are compatible. This is the case: first of all, G determines the structure of $\operatorname{End}^0(E)$ as a quadratic space, and by [Voi21, Proposition 5.2.4], there are only two (up to isomorphism) quaternion algebras with underlying quadratic spaces isomorphic to $(\operatorname{End}^0(E), \operatorname{Nrd}) \cong (\mathbb{Q}^4, G)$. We can make this explicit, and in fact the choices of square root in each approach are consistent with one another.

Let $LDL^T = G$ with D diagonal and L lower-triangular with 1's on its diagonal. Let $\{\tilde{\gamma_0}, \tilde{\gamma_1}, \tilde{\gamma_2}, \tilde{\gamma_3}\}$ and $a, b, c, d_1, d_2, d_3 \in \mathbb{Q}$ be defined as in Section A.2.1. Then by [Voi21, 15.4.5],

$$m(\tilde{\gamma_1}, \tilde{\gamma_2}, \tilde{\gamma_3}) = \det(L) m(\gamma_1, \gamma_2, \gamma_3) = m(\gamma_1, \gamma_2, \gamma_3).$$

On the other hand, we have $\tilde{\gamma_3} = c\tilde{\gamma_1}\tilde{\gamma_2}$, so

$$m(\tilde{\gamma_1}, \tilde{\gamma_2}, \tilde{\gamma_3}) = 4abc,$$

and $4ab > 0$, so the sign of $m(\gamma_1, \gamma_2, \gamma_3)$ and the sign of c are equal. The choice of sign for a square root of $\det(G) = m(\gamma_1, \gamma_2, \gamma_3)^2$ is therefore consistent with a choice of sign of the square root of

$$\frac{2d_3}{d_1 d_2} = \frac{\det(G)}{16a^2b^2} = \frac{1}{(4ab)^2} \left(m(\tilde{\gamma_1}, \tilde{\gamma_2}, \tilde{\gamma_3})\right)^2.$$

A.3 Computing an order $\mathcal{O}$ in $\mathbb{Z} + P$

We assume that we have computed three inseparable endomorphisms $\gamma_1, \gamma_2, \gamma_3$ such that $\gamma_0 \coloneqq 1$ and $\gamma_1, \gamma_2, \gamma_3$ generate a lattice Λ inside $\mathrm{End}(E)$, along with the Gram matrix $G = (\mathrm{Trd}(\gamma_i \widehat{\gamma_j}))_{0 \le i,j \le 3}$ and isomorphisms of quadratic spaces $f\colon (\mathbb{Q}^4, G) \to H(a, b)$ and $g\colon (\mathrm{End}^0(E), \mathrm{Nrd}) \to (\mathbb{Q}^4, G)$, where $g(\gamma_r) = e_r$, the rth standard basis vector of $\mathbb{Q}^4$. For $0 \le r, s, t \le 3$, let $m_{rst} \in \mathbb{Q}$ be the elements of the multiplication table for the basis $\mathcal{B} = \{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$: for $0 \le r, s \le 3$, we have

$$\gamma_r \gamma_s = \sum_{t=0}^{3} m_{rst} \gamma_t.$$

Let M_r be the matrix $M_r = (m_{rst})_{0 \le s,t \le 3}$. From this data, we can compute a basis for $\mathcal{O}$, the minimal order in $\mathrm{End}(E)$ containing Λ. The order $\mathcal{O}$ is generated as a $\mathbb{Z}$-module by $\gamma_0, \gamma_1, \gamma_2$, and γ_3 and their products.

We compute a basis for $\mathcal{O}$ in which basis elements are represented as linear combinations of the γ_i as follows. Let M_{rs} denote the sth row of M_r. Define the 12×4 matrix A to have rows given by the rows of M_0, i.e. the 4×4 identity matrix, followed by M_{rs} for $0 < r < s \le 3$. Let H be the Hermite normal form of A. Let $B = (b_{ij})_{0 \le i,j \le 3} \in M_4(\mathbb{Z})$ be the matrix whose rows are the top four rows of H. The rows of B form a lattice L in $\mathbb{Q}^4$ such that $g^{-1}(L) = \mathcal{O}$. In particular, if we define $\beta_i = \sum_{j=0}^{3} b_{ij} \gamma_i$ for $0 \le i \le 3$, then $\{\beta_0 = 1, \beta_1, \beta_2, \beta_3\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$.

A.4 Computing $\mathbb{Z} + P$

We now assume that we have computed a suborder $\mathcal{O}$ of $\mathbb{Z} + P$ generated by $\gamma_0 = 1$ and three inseparable endomorphisms $\gamma_1, \gamma_2, \gamma_3$, where $\mathcal{O}$ is represented by four vectors $\{(b_{ij})_{0 \le j \le 3}\}_{0 \le i \le 3}$ in $\mathbb{Q}^4$ such that $\beta_i \coloneqq \sum_{j=0}^{3} b_{ij} \gamma_j$ form a $\mathbb{Z}$-basis for $\mathcal{O}$. We proceed to compute $\mathbb{Z} + P$ by iteratively computing an additional inseparable endomorphism γ and the order $\mathcal{O}[\gamma]$, defined to be the smallest order containing both $\mathcal{O}$ and γ. It suffices to compute a basis for the $\mathbb{Z}$ lattice spanned by $\beta_0, \ldots, \beta_3, \beta_0\gamma, \ldots, \beta_3\gamma$. The approach is similar to how we computed an order generated by a lattice basis in the previous subsection. We first compute $(c_0, \ldots, c_3) \in \mathbb{Q}^4$ such that

$$\gamma = \sum_{s=0}^{3} c_s \gamma_s$$

by computing the traces $t_r \coloneqq \mathrm{Trd}(\gamma_r \widehat{\gamma})$ for $0 \le r \le 3$ and then solving the system of equations

$$t_r = \sum_{s=0}^{3} c_s G_{rs}.$$

Define $M_\gamma \coloneqq \sum_{r=0}^{3} c_r M_r$. Then the matrix

$$M'_\gamma \coloneqq H^{-1} M H$$

gives the action of left multiplication of γ on the basis elements $b_r = \sum_{s=0} H_{rs}\gamma_s$ for $\mathcal{O}$. Let A be the matrix whose rows are the rows of H and the rows of $M_{\gamma'}$. The top four rows of the Hermite normal form of A yield a basis for a lattice $L_{\mathcal{O}[\gamma]}$ in $\mathbb{Q}^4$ such that $g^{-1}(L_{\mathcal{O}[\gamma]}) = \mathcal{O}$. We then define B to be the top four rows of H.

We remark that we can check whether the order $\mathcal{O}$ given by the matrix B is equal to $\mathbb{Z} + P$ by simply computing its discriminant and checking if the discriminant is p^4. The discriminant of $\mathcal{O}$ is the determinant of the Gram matrix $B^T G B$.

A.5 From $\mathbb{Z} + P$ to $\mathrm{End}(E)$

Assume that we have computed three inseparable endomorphisms γ_i for $1 \leq i \leq 3$, the Gram matrix $G = (\mathrm{Trd}(\gamma_i\widehat{\gamma}_j))$, and a matrix $B = (b_{ij}) \in M_4(\mathbb{Q})$ so that $\beta_i \coloneqq \sum_{j=0}^{3} b_{ij}\gamma_i$ form the $\mathbb{Z}$-basis for $\mathbb{Z}+P$. Then we have so far computed a basis for the unique order of index p in $\mathrm{End}(E)$, according to Proposition 3.1. Using results and algorithms in [Voi21], we only need a little linear algebra to efficiently compute a basis for $\mathrm{End}(E)$. We recall the notion of a p-saturated order from [Voi21] below, and show that in our case, a p-saturated order containing $\mathbb{Z} + P$ is $\mathrm{End}(E)$.

Definition A.4. Let p be an odd prime. An order $\mathcal{O} \subseteq B$ is said to be *p-saturated* if $\mathcal{O}_p \coloneqq \mathcal{O} \otimes \mathbb{Z}_p$ has a basis x_1, x_2, x_3, x_4 such that the quadratic form $\mathrm{Nrd}\colon \mathcal{O}_p \to \mathbb{Q}_p$ is diagonal with respect to that basis and such that $v_p(\mathrm{Nrd}(x_i)) \leq 1$ for all $1 \leq i \leq 4$. An order $\mathcal{O} \subseteq B$ is said to be *p-maximal* for a prime p if $\mathcal{O}_p \coloneqq \mathcal{O} \otimes \mathbb{Z}_p$ is maximal in $B \otimes \mathbb{Q}_p$.

The following proposition shows that for quaternion algebras over $\mathbb{Q}$ ramified at p, orders that are p-saturated must also be p-maximal.

Proposition A.5. *Let B be a quaternion algebra over $\mathbb{Q}$ ramified at p. If $\mathcal{O} \subseteq B$ is a $\mathbb{Z}$-order which is p-saturated, then $\mathcal{O}$ is p-maximal.*

Proof. Let $x_0 = 1, x_1, x_2, x_3$ be a normalized basis of $\mathcal{O}_p \coloneqq \mathcal{O} \otimes \mathbb{Z}_p$ with respect to the quadratic form Nrd such that $e_i \coloneqq v_p(\mathrm{Nrd}(x_i)) \leq 1$ for $i = 1, 2, 3$ and $e_1 \leq e_2 \leq e_3$.

Then

$$\begin{aligned}
\mathrm{disc}(\mathcal{O}_p) &= \det(\mathrm{Trd}(x_i\overline{x_j}))\mathbb{Z}_p \\
&= \det \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & u_1 p^{e_1} & 0 & 0 \\ 0 & 0 & u_2 p^{e_2} & 0 \\ 0 & 0 & 0 & u_3 p^{e_3} \end{pmatrix} \mathbb{Z}_p \\
&= p^{e_1+e_2+e_3}\mathbb{Z}_p \supseteq p^3\mathbb{Z}_p,
\end{aligned}$$

where $u_1, u_2, u_3 \in \mathbb{Z}_p^\times$. The discriminant of $\mathcal{O}_p$ is the square of an ideal in $\mathbb{Z}_p$, so $e_1 + e_2 + e_3$ has to be even and therefore is either 0 or 2. The first case is not possible since B is ramified at p. This implies that $v_p(\mathrm{discrd}(\mathcal{O}_p)) = 1 = v_p(\mathrm{disc}(B))$, so we conclude $\mathcal{O} \subseteq B$ is p-maximal. □

Corollary A.6. *Let $\mathcal{O} \subseteq \mathrm{End}^0(E)$ be a p-saturated order such that $\mathbb{Z} + P \subseteq \mathcal{O}$. Then $\mathcal{O} = \mathrm{End}(E)$.*

Proof. By Proposition 3.1, the order $\mathbb{Z} + P$ is locally maximal at all primes $\ell \neq p$. Since $\mathbb{Z} + P \subseteq \mathcal{O} \subseteq \mathrm{End}(E)$, the order $\mathcal{O}$ is also ℓ-maximal for all $\ell \neq p$. Moreover $\mathcal{O}$ is p-saturated, so $\mathcal{O}$ is p-maximal by Proposition A.5. This implies that $\mathcal{O}$ is maximal in $\mathrm{End}^0(E)$ and, since $\mathbb{Z} + P \subseteq \mathcal{O}$, by Proposition 3.1 we have $\mathcal{O} = \mathrm{End}(E)$. □

Therefore given the order $\mathbb{Z} + P$, we can recover the maximal order containing $\mathbb{Z} + P$ by computing the p-saturated order that contains $\mathbb{Z} + P$. This is done efficiently with Algorithm 3.12 and Algorithm 7.9 in [Voi21].

References

[ACNL+23] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. *Experimental Mathematics*, 32(2):241–268, 2023.

[BCC+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *Advances in Cryptology – EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part II*, page 405–437, Berlin, Heidelberg, 2023. Springer-Verlag.

[BCNE+19] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. In Jennifer S. Balakrishnan, Amanda Folsom, Matilde Lalín, and Michelle Manes, editors, *Research Directions in Number Theory*, pages 41–66, Cham, 2019. Springer International Publishing.

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comp.*, 81(278):1201–1231, 2012.

[Brö09] Reinier Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.

[Brz90] J. Brzezinski. On automorphisms of quaternion orders. *J. Reine Angew. Math.*, 403:166–186, 1990.

[BS11] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *J. Number Theory*, 131(5):815–831, 2011.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[CKMZ22] Tímea Csahók, Péter Kutas, Mickaël Montessinos, and Gergely Zábrádi. Explicit isomorphisms of quaternion algebras over quadratic global fields. *Res. Number Theory*, 8(4):Paper No. 77, 24, 2022.

[CS21] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 2021.

[CSCS22] Maria Corte-Real Santos, Craig Costello, and Jia Shi. Accelerating the delfs-galbraith algorithm with fast subfield root detection. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III*, volume 13509 of *Lecture Notes in Computer Science*, pages 285–314. Springer, 2022.

[CSV21] Sara Chari, Daniel Smertnig, and John Voight. On basic and Bass quaternion orders. *Proc. Amer. Math. Soc. Ser. B*, 8:11–26, 2021.

[DFKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. In *Advances in cryptology – ASIACRYPT 2020. 26th international conference on the theory and application of cryptology and information security, Daejeon, South Korea, December 7–11, 2020. Proceedings. Part I*, pages 64–93. Cham: Springer, 2020.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptography*, 78(2):425–440, February 2016.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

[EHL+20] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 215–232. Math. Sci. Publ., Berkeley, CA, 2020.

[Eic36] Martin Eichler. Untersuchungen in der Zahlentheorie der rationalen Quaternionenalgebren. *J. Reine Angew. Math.*, 174:129–159, 1936.

[Elk98] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[EPSV23] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the people: Supersingular elliptic curves with prescribed endomorphism ring in general characteristic. Cryptology ePrint Archive, Paper 2023/106, 2023. `https://eprint.iacr.org/2023/106`.

[ES24] Kirsten Eisenträger and Gabrielle Scullard. Connecting Kani's lemma and path-finding in the bruhat-tits tree to compute supersingular endomorphism rings, 2024. `https://arxiv.org/abs/2402.05059`.

[Gal12] Steven D. Galbraith. *Mathematics of public key cryptography.* Cambridge University Press, Cambridge, 2012.

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology—ASIACRYPT 2017. Part I*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Springer, 2017.

[HvdH21] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Ann. of Math. (2)*, 193(2):563–617, 2021.

[HW08] Godfrey H. Hardy and Edward M. Wright. *An introduction to the theory of numbers.* Oxford University Press, Oxford, sixth edition, 2008.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.

[Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.

[Lit28] John E. Littlewood. On the class-number of the corpus $P(\sqrt{-k})$. *Proc. London Math. Soc. (2)*, 27(5):358–372, 1928.

[LP92] H. W. Lenstra, Jr. and Carl Pomerance. A rigorous time bound for factoring integers. *J. Amer. Math. Soc.*, 5(3):483–516, 1992.

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242. Nagoya Univ., Nagoya, 1986.

[MSS16] François Morain, Charlotte Scribot, and Benjamin Smith. Computing cardinalities of Q-curve reductions over finite fields. *LMS Journal of Computation and Mathematics*, 19(A):15, August 2016.

[Piz80a] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[Piz80b] Arnold Pizer. Theta series and modular forms of level p^2M. *Compositio Math.*, 40(2):177–241, 1980.

[PW23] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. Cryptology ePrint Archive, Paper 2023/1399, 2023. `https://eprint.iacr.org/2023/1399`.

[Rab80] Michael O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, 9(2):273–280, 1980.

[Rob22] Damien Robert. Some applications of higher dimensional isogenies to elliptic curves (overview of results). Cryptology ePrint Archive, Paper 2022/1704, 2022. `https://eprint.iacr.org/2022/1704`.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, New York, 2009.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.7)*, 2022. `https://www.sagemath.org`.

[Voi13] John Voight. Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms. *Developments in Mathematics*, 31:255–298, 2013.

[Voi21] John Voight. *Quaternion algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, third edition, 2013.

[Wes22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2021 - 62nd Annual IEEE Symposium on Foundations of Computer Science*, Denver, Colorado, United States, February 2022.