Computing supersingular endomorphism rings using inseparable endomorphisms

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

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

March 1, 2023

Abstract

We give an algorithm for computing inseparable endomorphisms of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, which, conditional on GRH runs in expected $O(p^{1/2+\epsilon})$ time. With two calls to this algorithm, we compute a Bass suborder of $\mathrm{End}(E)$, improving on the results of [EHL$^+$] which only gave a heuristic algorithm for computing a Bass suborder. We further improve on the results of [EHL$^+$] by removing the heuristics involved in an algorithm for recovering $\mathrm{End}(E)$ from a Bass suborder. In another direction, we argue that under a heuristic assumption about the distribution of the discriminants of endomorphisms generated by our algorithm, with $O(1)$ of such endomorphisms we compute a generating set for $\mathrm{End}(E)$, where the implied constant is independent of p or E. We discuss a heuristic algorithm for computing $\mathrm{End}(E)$ based on this approach.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{F}_q$, where q is a prime power. If E is ordinary, to compute $\mathrm{End}(E) \coloneqq \mathrm{End}_{\overline{\mathbb{F}_q}}(E)$, the geometric endomorphism ring 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 is well-studied, and there exist algorithms for computing the endomorphism ring of an ordinary elliptic curve [BS11] which run in expected subexponential time, conditional on reasonable heuristics including the Generalized Riemann Hypothesis (GRH).

When E is supersingular, however, its endomorphism algebra $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes \mathbb{Q}$ 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 finite-index suborder 'for free' and there is a unique maximal order containing both this suborder and $\mathrm{End}(E)$: the maximal order is the ring of integers of the imaginary quadratic number field $\mathrm{End}^0(E) = \mathbb{Q}(\pi_E)$.

This suggests that computing the endomorphism ring of a supersingular elliptic curve is a hard problem, and this assumption is central to the security of isogeny-based cryptography: indeed, the problems of path-finding in supersingular isogeny graphs and of computing supersingular endomorphism rings are equivalent, assuming the GRH [EHL+18, Wes22]. The first algorithm for computing a suborder of $\mathrm{End}(E)$ is due to Kohel [Koh96], and runs in time $O(p^{1+\epsilon})$ for any $\epsilon > 0$. Eisenträger et. al. [EHL+] give a $O(p^{1/2+\epsilon})$ algorithm for computing a Bass suborder of $\mathrm{End}(E)$, conditional on heuristics including GRH. They also discuss how to find $\mathrm{End}(E)$ among the maximal overorders of a Bass suborder $\Lambda \subseteq \mathrm{End}(E)$.

One approach to computing the endomorphism ring of a supersingular elliptic curve is to compute several endomorphisms until finding a generating set. Suppose we have an algorithm which generates a random endomorphism of E, a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. A simple question arises: what is the expectation of the number of calls to that algorithm before finding a set of endomorphisms which generate $\mathrm{End}(E)$ as an order? In [GPS17], the authors give a heuristic argument that this expectation is $O(\log p)$.

In this paper, we give an algorithm, Algorithm 1, for computing inseparable endomorphisms of E and show that with two calls to our algorithm, we provably compute a Bass suborder of $\mathrm{End}(E)$. Under GRH, Algorithm 1 runs in expected time $O(p^{1/2+\epsilon})$. From a theoretical viewpoint, it suffices to compute a Bass suborder of $\mathrm{End}(E)$: building on ideas in [EHL+], in Section 5 we show that $\mathrm{End}(E)$ can be recovered from a Bass suborder Λ, and the time required to find $\mathrm{End}(E)$ among the maximal overorders of Λ is dominated by the time required to compute Λ.

Thus two calls to Algorithm 1 produce a Bass order – how many calls should we make if we want a *maximal* order? First, observe that no collection of such endomorphisms could generate $\mathrm{End}(E)$: let P be the 2-sided ideal of inseparable endomorphisms of E, so the endomorphisms produced by Algorithm 1 belong to P. We show in Proposition 3.1 that $\mathbb{Z} + P \subsetneq \mathrm{End}(E)$ is the unique suborder of index p, and the only maximal order containing $\mathbb{Z} + P$ is $\mathrm{End}(E)$. At the end of Section 5 we argue that the expectation of the number of calls to Algorithm 1 before finding a generating set for $\mathbb{Z} + P$ is bounded by a constant, independent of p or E, assuming the heuristic that the probability that the discriminants of two endomorphisms produced by Algorithm 1 are coprime is bounded from below by a constant. With a basis for $\mathbb{Z} + P$, one can efficiently compute a basis of $\mathrm{End}(E)$. In conclusion, we prove that $O(1)$ calls to Algorithm 1 produce a

Bass order unconditionally, and $O(1)$ calls to Algorithm 1 along with negligible overhead produce the endomorphism ring, assuming the heuristic mentioned above.

This is the heuristic assumed in [EHL+18] in order to prove that their algorithm for producing a Bass order in $\mathrm{End}(E)$ terminates in expected $O(p^{1/2+\epsilon})$ time, but we use it in a new way.

Acknowledgement

The authors thank the organizers of Rethinking Number Theory 2020 where this project began. We also thank John Voight for several helpful discussions.

2 Background and notation

In this section, we recall some basic definitions and facts about elliptic curves over finite fields and quaternion algebras. We refer the reader to [Sil09, Chapter III and V] and [Voi21] for details.

Let q be a positive power of a prime $p > 3$, and let E 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 $a, b \in \mathbb{F}_q$ and, if E is supersingular, we will assume that E is defined over $\mathbb{F}_{p^2}$ (i.e. $a, b \in \mathbb{F}_{p^2}$). We let π_p denote the p-power Frobenius isogeny $\pi_p \colon E \to E^{(p)}$ defined by $\pi_p(x, y) = (x^p, y^p)$. We will use the same notation π_p for every such Frobenius isogeny, independent of the choice of the starting elliptic curve. Clearly, if $E : y^2 = x^3 + ax + b$ then $E^{(p)} : y^2 = x^3 + a^p x + b^p$, and E is supersingular if and only if $E^{(p)}$ is supersingular. 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 endomorphism ring of E and $\mathrm{End}^0(E) \coloneqq \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ the endomorphism algebra of E. When E is a supersingular elliptic curve defined over $\mathbb{F}_q$, it has a model defined over $\mathbb{F}_{p^2}$ since its j-invariant is in $\mathbb{F}_{p^2}$, and moreover we can choose a model for E so that all of its isogenies are defined over $\mathbb{F}_{p^2}$ as well: this is because we can choose a model so that $\#E(\mathbb{F}_{p^2}) = (p-1)^2$, so the p^2-Frobenius endomorphism π_E of E is simply $\pi_E = [p]$.

In this paper, we focus on supersingular elliptic curves over $\mathbb{F}_{p^2}$, although some of the results are stated for general elliptic curves over $\mathbb{F}_q$. If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, $\mathrm{End}^0(E)$ 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 $\mathrm{End}^0(E)$. Therefore, computing $\mathrm{End}(E)$ for us means to find a basis of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.

2.1 Quaternion algebras

Let F be a field. A quaternion algebra B over F is a central simple F-algebra of dimension 4. Let $a, b \in F^*$ 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, and for every quaternion algebra B over F, there exist $a, b \in F$ such that B is isomorphic to $H(a,b)$ (assuming the characteristic of F is not 2).

2.1.1 The canonical involution, the reduced trace and the reduced norm

From now on we will be working with $F = \mathbb{Q}$, though the following definitions can be given for any field F whose characteristic is not 2.

Let B be a quaternion algebra over $\mathbb{Q}$. Then B has a *standard involution*, that is a $\mathbb{Q}$-linear map $\bar{}\colon B \to B$ satisfying:

1. $\bar{1} = 1$;
2. $\bar{\bar{\alpha}} = \alpha$;
3. $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$.

If we write $B = H(a,b)$ with $\mathbb{Q}$-basis $1, i, j, ij$, and if $\alpha = w + xi + yj + zij \in B$, then $\bar{\alpha} = w - xi - yj - zij$. We define the *reduced trace* of $\alpha \in B$ to be $\mathrm{Trd}(\alpha) \coloneqq \alpha + \bar{\alpha}$. We define the *reduced norm* of α to be $\mathrm{Nrd}(\alpha) \coloneqq \alpha\bar{\alpha}$. Both $\mathrm{Trd}(\alpha)$ and $\mathrm{Nrd}(\alpha)$ are in $\mathbb{Q}$ for any $\alpha \in B$. Note that α is a root of its characteristic polynomial $x^2 - \mathrm{Trd}(\alpha)x + \mathrm{Nrd}(\alpha)$.

The reduced trace defines a pairing on B, i.e. a $\mathbb{Q}$-bilinear map $\langle \cdot, \cdot \rangle \colon B \times B \to \mathbb{Q}$. For $\alpha, \beta \in B$, the pairing is defined by

$$\langle \alpha, \beta \rangle \coloneqq \mathrm{Trd}(\alpha\bar{\beta}).$$

The corresponding quadratic form $Q : B \to \mathbb{Q}$ is defined by $Q(\alpha) = \mathrm{Nrd}(\alpha)$, for all $\alpha \in B$. 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 $\mathcal{B}$ to be the matrix

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

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 $x_i, y_i \in \mathbb{Q}$ we have

$$\langle \alpha, \beta \rangle = \mathrm{Trd}(\alpha\bar{\beta}) = x^t G y,$$

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

2.1.2 Completions of a quaternion algebra; splitting and ramification

Let v be a place of $\mathbb{Q}$ and let $\mathbb{Q}_v$ denote the completion of $\mathbb{Q}$ at v. Here, $\mathbb{Q}_v = \mathbb{Q}_p$ for some prime p if v is a finite place, or $\mathbb{Q}_v = \mathbb{R}$ if v is the infinite place. If B

is a quaternion algebra over $\mathbb{Q}$, then $B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a quaternion algebra over $\mathbb{Q}_v$. There is a unique division algebra of dimension 4 over $\mathbb{Q}_v$, and a quaternion algebra over $\mathbb{Q}_v$ is either a division algebra or is isomorphic to $M_2(\mathbb{Q}_v)$. If $B \otimes_{\mathbb{Q}} \mathbb{Q}_v \simeq M_2(\mathbb{Q}_v)$, we say that B is *split* at v. If $B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a division algebra, we say that B is *ramified* at v. The set of places 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 of* B, $\mathrm{disc}(B)$, is the product of all primes p at which B is ramified.

A $\mathbb{Z}$*-order* $\Lambda \subseteq B$ is a $\mathbb{Z}$-lattice of B which is also a subring such that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q} = B$. Similarly, we define a $\mathbb{Z}_p$-order in the quaternion algebra $B \otimes \mathbb{Q}_p$. 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 $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Indeed, if p is split, i.e. if $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$, then there are infinitely many maximal orders in $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, but they are all conjugate to $M_2(\mathbb{Z}_p)$. If $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra, then there is a unique maximal order (one can extend the valuation on $\mathbb{Q}_p$ to $B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and the unique maximal order is the valuation ring).

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

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 $\mathcal{O}$. The the discriminant $\mathrm{disc}(\mathcal{O})$ is defined as

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

It is possible to show that the discriminant of an order is always a square, so we define the *reduced discriminant* $\mathrm{discrd}(\mathcal{O})$ of $\mathcal{O}$ to be the positive integer satisfying $\mathrm{discrd}(\mathcal{O})^2 = \mathrm{disc}(\mathcal{O})$. An 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].

2.1.3 Quaternionic orders

We recall here some of the properties of orders in a quaternion algebra. Let B be a quaternion algebra over $\mathbb{Q}$. We say that an order $\mathcal{O} \subset B$ is *Gorenstein* if

$$\mathrm{codiff}(\mathcal{O}) := \{\alpha \in B | \, \mathrm{Trd}(\alpha \mathcal{O}) \subseteq \mathbb{Z}\}$$

is an invertible $\mathcal{O}$-ideal. The order $\mathcal{O}$ is Bass if every super-order $\mathcal{O}' \supseteq \mathcal{O}$ is Gorenstein. We are interested in Bass orders because we can bound the number of maximal superorders containing a given Bass order $\mathcal{O}$ with a quanitity which grows subexponentially in the reduced discriminant (and therefore the size) 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 $\alpha = \pi_p \circ \phi$, where $\phi \in \mathrm{Hom}(E, E^{(p)})$. The set of

inseparable endomorphisms $P := \pi_p \operatorname{Hom}(E, E^{(p)})$ is a 2-sided ideal of $\operatorname{End}(E)$ and we refer to it as the *ideal of inseparable endomorphisms* of E.

In this section, we first study the arithmetic properties of $\mathbb{Z} + P \subseteq \operatorname{End}(E)$ and we later focus our attention on a particular kind of inseparable endomorphisms in P 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, $\mathcal{O}$ is a maximal order in B, and P is the unique 2-sided ideal in $\mathcal{O}$ of reduced norm 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 because it is finitely generated and $B = P\mathbb{Q} \subseteq (\mathbb{Z} + P)\mathbb{Q}$. Secondly, it is a subring of B since it contains $1 \in B$ and is closed under multiplication since P is an ideal. Therefore $\mathbb{Z} + P$ is a suborder of $\mathcal{O}$.

We now calculate the index of $\mathbb{Z} + P$ in $\mathcal{O}$. Let D be the discriminant of B. Because 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 $[\mathcal{O} : P] = \operatorname{Nrd}(P)^2 = p^2$. Since $\mathbb{Z} \cap P \simeq p\mathbb{Z}$ by [Voi21, 18.2.7(b)], as $\mathbb{Z}$-modules we have $(\mathbb{Z} + P)/P \simeq \mathbb{Z}/(\mathbb{Z} \cap P) \simeq \mathbb{Z}/p\mathbb{Z}$. Therefore $[\mathbb{Z} + P : P] = p$. By multiplicativity of the index, we have $[\mathcal{O} : \mathbb{Z} + P] = p$, and so [Voi21, Lemma 15.2.15] implies

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

Now we show $\mathcal{O}$ is the only maximal order containing $\mathbb{Z}+P$. First, we recall that an order Λ in B is maximal at a prime $\ell \neq p$ if and only if $v_\ell(\operatorname{discrd}(\Lambda)) = v_\ell(\operatorname{disc}(B))$: this is because a maximal order in $M_2(\mathbb{Q}_\ell)$ has reduced discriminant equal to $\mathbb{Z}_\ell$ [Voi21, Lemma 15.5.3], and a maximal order in the division quaternion algebra over $\mathbb{Q}_\ell$ has reduced discriminant equal to $\ell\mathbb{Z}_\ell$ [Voi21, Example 15.5.4]. Since the reduced discriminant of $\mathbb{Z} + P$ is pD, we have $v_\ell(\operatorname{discrd}(\mathbb{Z} + P)) = v_\ell(p) + v_\ell(D)$, and so the order $\mathbb{Z} + P$ is maximal at any prime $\ell \neq p$. 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 $(\mathbb{Z}+P)\otimes\mathbb{Z}_p$. We see that, for every prime ℓ, $\mathcal{O} \otimes \mathbb{Z}_\ell$ is the unique maximal $\mathbb{Z}_\ell$-order containing $(\mathbb{Z} + P) \otimes \mathbb{Z}_\ell$, so by [Voi21, Corollary 9.4.7, Theorem 9.4.9, Lemma 9.5.3], $\mathcal{O}$ is the unique maximal order containing $\mathbb{Z} + P$. □

Remark 3.2. The order $\mathbb{Z} + P$ is Bass, as its reduced discriminant is p^2 and thus cubefree [Voi21, Exercise 24.7(a)]. It is not Eichler, 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). It is not hereditary: its reduced discriminant is divisible by p^2 and is therefore not squarefree ([Voi21, lemma 23.3.18]. It is residually ramified at p since $(\mathbb{Z}+P)/P \simeq \mathbb{Z}/p\mathbb{Z}$ (see [Voi21, 24.3.2] for a definition of *residually ramified*).

From a computational point of view, given a basis of $\mathbb{Z} + P$, one can use algorithms 7.9 and 3.12 in [Voi13] to recover a basis of the unique maximal order $\mathcal{O}$ containing $\mathbb{Z} + P$. We will recall the relevant results of [Voi13] for computing $\mathrm{End}(E)$ in Section 6.

3.2 Inseparable reflections

Inside P we consider the inseparable endomorphisms whose construction is based on a simmetry of the supersingular isogeny graph $G(p, l)$ given by the Galois involution.

3.2.1 The Galois involution

Let $\sigma_p \colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ be the p-power Frobenius automorphism: $\sigma_p(\alpha) = \alpha^p$. 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 $(E^{(p)})^{(p)} = E$, so π defines an involution. Moreover $E^{(p)} = E$ 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 pth 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 $\pi_p(\ker \phi)$. Moreover we have $(\phi^{(p)})^{(p)} = \phi$.

Lemma 3.3. *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 $\mathbb{F}_{p^2}$. Then*

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

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

(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 $f, g, h \in \mathbb{F}_{p^2}(x, y)$, one has

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

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

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

We now prove part (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 in the first equality we used that ϕ_1 is defined over $\mathbb{F}_{p^2}$, in the second equality we used part (a), in the fourth one we used the fact that $\deg \phi_1 = \deg \phi_1^{(p)}$, and the last equality follows from the fact that coordinate functions for the multiplication-by-m map on a curve E is 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 $\widehat{\phi_1} = (\widehat{\phi_1^{(p)}})^{(p)}$. □

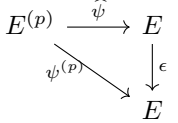
Geometrically we can imagine the action of π as a "mirror reflection" of $G(p,l)$ whose "axis of symmetry" is given by the "line" of vertices defined over $\mathbb{F}_p$. Such line is called the *spine* of $G(p,l)$ in [ACNL+19].

Going forward, in order to lighten the notation, we will be writing $\psi\phi$ instead of $\psi \circ \phi$ for the composition of two (or more) isogenies.

3.2.2 Arithmetic properties of inseparable reflections

We consider inseparable endomorphisms which exploit the mirror symmetry of $G(p,l)$ and which are based on the concept of (d,ϵ)-structures, defined by Chenu and Smith in [CS21]:

Definition 3.4. 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 $\epsilon \in \{\pm 1\}$.



A trivial example of (d, ϵ)-structure, with $d = 1$, is given by a supersingular elliptic curve defined over $\mathbb{F}_p$ together with the identity map.

We're interested in (d, ϵ)-structures (E, ψ) because they give rise to endomorphisms $\mu = \pi_p \circ \psi$ such that $\mathbb{Z}[\mu] \simeq \mathbb{Z}[\sqrt{-dp}]$ [CS21].

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let (E', ψ) be a (d_2, ϵ)-structure. Let $\phi\colon E \to E'$ be a d_1-isogeny.

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle \pi_p}\uparrow & & \downarrow{\scriptstyle \psi} \\ E^{(p)} & \xleftarrow{\widehat{\phi^{(p)}}} & E'^{(p)} \end{array}$$

Consider the isogeny $\varphi := \widehat{\phi^{(p)}}\psi\phi$ in $\mathrm{Hom}(E, E^{(p)})$. Then $\alpha := \pi_p\varphi \in P$ is an inseparable endormorphism of E. We call such endomorphisms the name of *inseparable reflections* of E. Under possibly some additional assumptions, inseparable reflections have interesting arithmetic properties, which we study in the rest of this section.

Lemma 3.5. *Let E_1 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, let (E_2, ψ) be a (d_2, ϵ)-structure with d_2 squarefree, and let $\phi\colon E_1 \to E_2$ be a d_1-isogeny. Let $\alpha = \pi_p\widehat{\phi^{(p)}}\psi\phi$. Then $\alpha^2 = [-d_1^2 d_2 p]$ and in particular $\mathrm{Tr}(\alpha) = 0$.*

Proof. Let $\mu = \pi_p\psi$. Then $\mu^2 = [-d_2 p]$ by Proposition 2 of [CS21]. We calculate

$$\begin{aligned}
\alpha^2 &= \pi_p\widehat{\phi^{(p)}}\psi\phi\pi_p\widehat{\phi^{(p)}}\psi\phi && \text{definition of } \alpha \\
&= \pi_p\widehat{\phi^{(p)}}\psi\pi_p\phi^{(p)}\widehat{\phi^{(p)}}\psi\phi && \text{Lemma 3.3 part (b)} \\
&= [d_1]\pi_p\widehat{\phi^{(p)}}\psi\pi_p\psi\phi && \text{properties of dual} \\
&= [d_1]\widehat{\phi}\pi_p\psi\pi_p\psi\phi && \text{Lemma 3.3 parts (b),(c)} \\
&= [d_1]\widehat{\phi}\mu^2\phi && \text{definition of } \mu \\
&= [-d_1 d_2 p]\widehat{\phi}\phi && \text{by [CS21] Proposition 2} \\
&= [-d_1^2 d_2 p] && \text{by properties of dual isogenies.}
\end{aligned}$$

□

Lemma 3.6. *Let E_1, E_2, E_3 be elliptic curves defined over $\mathbb{F}_q$ and let $\phi\colon E_1 \to E_2$ and $\psi\colon E_2 \to E_3$ be separable, cyclic isogenies. Then $\ker(\psi \circ \phi)$ is cyclic if and only if $\ker\widehat{\phi} \cap \ker\psi$ is trivial.*

Proof. If $\ker\widehat{\phi} \cap \ker\psi = G$ is nontrivial, let $f\colon E_2 \to E'$ be a separable isogeny with kernel G. Then both $\widehat{\phi}$ and ψ factor through f: there exist isogenies g, h such that $\widehat{\phi} = g \circ f$ and $\psi = h \circ f$.

$$\begin{array}{ccccc} E_1 & \xrightarrow{\phi} & E_2 & \xrightarrow{\psi} & E_3 \\ & \nwarrow^{h} & \downarrow{\scriptstyle f} & \nearrow_{g} & \\ & & E' & & \end{array}$$

But then

$$\psi \circ \phi = h \circ f \circ \widehat{f} \circ \widehat{g} = h \circ \widehat{g} \circ [\#G]$$

does not have cyclic kernel.

Now assume that $\ker(\psi \circ \phi)$ is not cyclic. Let $S \in E_2(\overline{\mathbb{F}}_q)$ such that $\langle S \rangle = \ker \psi$ and let $Q \in E_1(\overline{\mathbb{F}}_q)$ such that $\phi(Q) = S$. Also let $P \in E_1(\overline{\mathbb{F}}_q)$ such that $\langle P \rangle = \ker \phi$.

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

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

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

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

Lemma 3.7. *Let E_1 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\phi\colon E_1 \to E_2$ be a cyclic, separable d_1-isogeny defined over $\mathbb{F}_{p^2}$. Assume that E_2 has a (d_2, ϵ)-structure (E_2, ψ) with $\gcd(d_1, d_2) = 1$ and d_2 square-free. Finally, assume that $\widehat{\phi}$ does not factor through any isogeny $g\colon E_2 \to E_3$ with $1 < \deg g < d_1$ to a curve E_3 with a (d_2, ϵ)-structure. Then $\widehat{\phi^{(p)}}\psi\phi$ has cyclic kernel.*

Proof. Assume that $\ker \widehat{(\phi^{(p)}}\psi\phi)$ is not cyclic. We will show that there is an isogeny $g\colon E_2 \to E_3$ such that $\ker g \subseteq \ker \widehat{\phi}$ and E_3 has a (d_2, ϵ)-structure. By Lemma 3.6, 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 $g\colon E_2 \to E_3$ be an isogeny defined over $\mathbb{F}_{p^2}$ with kernel G.

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

We will show that E_3 has an (d_2, ϵ)-structure. By Lemma 1 of [CS21], it suffices to show that $\mathrm{End}(E_3)$ contains a quadratic order isomorphic to $\mathbb{Z}[\sqrt{-d_2 p}]$.

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

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

Because $\gcd(d_1, d_2) = 1$, ψ induces an isomorphism $E_2[d_1] \to E_2^{(p)}[d_1]$, so, since $G \subset E_2[d_1]$, we have $\#\psi(G) = \#G$. Moreover $\ker \widehat{\phi}$ is cyclic, so $\pi_p(\ker \widehat{\phi})$ is also cyclic. Therefore $\psi(G)$ is the unique subgroup of $\pi_p(\ker \widehat{\phi})$ of order $\#G$. The unique subgroup of $\ker \widehat{\phi}$ of order $\#G$ is G. Therefore

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

From this we conclude that

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

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

Now consider the endomorphism

$$\rho = g\pi_p\psi\widehat{g} \in \mathrm{End}(E_3).$$

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

$$\rho(E_3[d]) = g\pi_p\psi\widehat{g}(E_3[d]) = g\pi_p\psi(\ker g) = g\pi_p\psi(G) = g(G) = 0.$$

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

$$\mu^2 = \frac{1}{d^2} g\pi_p\psi\widehat{g}g\pi_p\psi\widehat{g} = \frac{1}{d} g\pi_p\psi\pi_p\psi\widehat{g} = \frac{-d_2 p}{d} g\widehat{g} = -d_2 p,$$

so $\mathbb{Z}[\mu] \simeq \mathbb{Z}[\sqrt{-d_2 p}]$. As mentioned above, by Lemma 1 of [CS21], it follows that E_3 has a (d_2, ϵ)-structure (indeed, $\mu = \pi_p\psi'$ for an isogeny $\psi' \colon E_3 \to E_3^{(p)}$, and (E_3, ψ') is the desired (d_2, ϵ)-structure. □

We now use Lemma 3.5, Lemma 3.6 and Lemma 3.7 to prove that we can choose two inseparable endormophisms in a way that they do not commute.

Theorem 3.8. *Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let $\phi_1 \colon E \to E_1$ and $\phi_2 \colon E \to E_2$ be two cyclic, separable isogenies such that (E_i, ψ_i) are both (d, ϵ)-structures for some squarefree d coprime to $\deg \phi_i$ for $i = 1, 2$. Also assume that neither $\widehat{\phi_1}$ nor $\widehat{\phi_2}$ factor nontrivially through an isogeny to a curve with a (d, ϵ)-structure. Assume that $\ker \phi_1 \neq \ker \phi_2$. Then $\alpha_1 = \pi_p\widehat{\phi_1^{(p)}}\psi_1\phi_1$ and $\alpha_2 = \pi_p\widehat{\phi_2^{(p)}}\psi_2\phi_2$ are endomorphisms of E which 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 3.5, 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 $[n](\alpha_2(E[k])) = 0$, so $[r](\alpha_2(E[k])) = 0$ too. This implies $\alpha_2\left(E\left[\frac{k}{\gcd(k,r)}\right]\right) = 0$. The kernel of α_2 is cyclic by Lemma 3.7, 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, α_1 has cyclic kernel again by Lemma 3.7, 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 that $\ker\alpha_i$ is cyclic for $i = 1, 2$, we obtain $\ker\phi_1 = \ker\phi_2$. □

4 Bass suborders of $\mathrm{End}(E)$

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and for each $i = 1, 2$ let (E_i, ψ_i) be a (d_3, ϵ)-structure where d_3 is square-free. Let $\phi_1 \colon E \to E_1$ be an isogeny of degree d_1 and $\phi_2 \colon E \to E_2$ an isogeny of degree d_2, where the integers d_1, d_2, d_3 are pairwise coprime, and neither of $\widehat{\phi_1}, \widehat{\phi_2}$ factor through an isogeny to a curve with a (d_3, ϵ)-structure. For $i = 1, 2$ set $\alpha_i := \pi_p\widehat{\phi_i^{(p)}}\psi_i\phi_i$. Then $\mathrm{Tr}(\alpha_i) = 0$ by Lemma 3.5, or equivalently $\widehat{\alpha_i} = -\alpha_i$. Since $d_1 \neq d_2$, we have that $\ker\phi_1 \neq \ker\phi_2$, and hence $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$ by Theorem 3.8. Thus $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ generate an order in $\mathrm{End}(E)$, which we denote by

$$\Lambda_{\alpha_1\alpha_2} := \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2.$$

Furthermore $\alpha_1\alpha_2$ factors through the multiplication-by-p map, so

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

is an endomorphism of E as well. 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 $\Lambda_{\alpha_1\alpha_2} \subsetneq \Lambda_\rho$.

We focus our attention on $\Lambda_{\alpha_1\alpha_2}$. We compute $\mathrm{discrd}(\Lambda_{\alpha_1\alpha_2})$. The Gram matrix of the basis $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ is

$$G := \begin{pmatrix} 2 & 0 & 0 & -p\,\mathrm{Tr}(\rho) \\ 0 & 2pd_3d_1^2 & p\,\mathrm{Tr}(\rho) & 0 \\ 0 & p\,\mathrm{Tr}(\rho) & 2pd_3d_2^2 & 0 \\ -p\,\mathrm{Tr}(\rho) & 0 & 0 & 2p^2d_1^2d_2^2d_3^2 \end{pmatrix}.$$

We get

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

We see that $\Lambda_{\alpha_1\alpha_2}$ is non-maximal precisely at p and the primes dividing the discriminant of the endomorphism 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 $q \neq p$ agree with those of $\Lambda_{\alpha_1\alpha_2}$.

Proposition 4.1. *Let $\Lambda_{\alpha_1\alpha_2}$ be as above. Then the ternary quadratic form attached to $\Lambda_{\alpha_1\alpha_2}$ is*

$$Q(x,y,z) = pd_3d_2^2x^2 + pd_3d_1^2y^2 + z^2 - tpxy,$$

where $t = \mathrm{Tr}(\rho)$. Consequently, $\Lambda_{\alpha_1\alpha_2}$ is Gorenstein.

Proof. Consider the basis $1, i = \alpha_1, j = \alpha_2, k = \alpha_2\alpha_1$ of $\Lambda_{\alpha_1\alpha_2}$. We claim that this 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]). To see that we have a good basis, we compute

$$\begin{aligned}
i^2 &= \alpha_1^2 = -pd_3d_1^2,\\
j^2 &= \alpha_2^2 = -pd_3d_2^2,\\
k^2 &= (\alpha_2\alpha_1)^2 = \mathrm{Tr}(\alpha_2\alpha_1)(\alpha_2\alpha_1) - \deg(\alpha_2\alpha_1) = tpk - p^2d_1^2d_2^2d_3^2,\\
jk &= \alpha_2^2\alpha_1 = -pd_3d_2^2\alpha_1 = pd_3d_2^2\widehat{\alpha_1},\\
ki &= \alpha_2\alpha_1^2 = pd_3d_1^2\widehat{\alpha_2},\\
ij &= \alpha_1\alpha_2 = \widehat{\alpha_2\alpha_1} = \widehat{k}.
\end{aligned}$$

So we have $a = pd_3d_2^2, b = pd_3d_1^2, c = 1, u = v = 0, w = tp$. Therefore the ternary quadratic form for Λ is

$$Q(x,y,z) = pd_3d_2^2x^2 + pd_3d_1^2y^2 + z^2 - tpxy,$$

as claimed. Finally, because d_1, d_2, d_3 and p are pairwise coprime we see that Q is primitive and thus Λ is Gorenstein [Voi21, Theorem 24.2.10]. □

Proposition 4.2. *Let $\Lambda_{\alpha_1\alpha_2}$ be as above, under the further assumption that d_3 is even (so d_1, d_2 are odd). Then $\Lambda_{\alpha_1\alpha_2}$ is Bass.*

Proof. We will show that $\Lambda_{\alpha_1\alpha_2}$ is locally basic, and hence Bass by [Brz90, Proposition 1.11] at every prime ℓ. This suffices, since being Bass is a local property (for a reference, see [Voi21, Proposition 24.5.10], originally proved in Satz 8 by Eichler in [Eic36]). Consider the quadratic order $R_i = \mathbb{Z}[\alpha_i] \simeq \mathbb{Z}[d_i\sqrt{-d_3p}]$ in $\Lambda_{\alpha_1\alpha_2} \subseteq \mathrm{End}(E)$. Because $-d_3p$ is square-free and congruent to 2 modulo 4, the maximal order in the fraction field of R_i is isomorphic to $\mathbb{Z}[\sqrt{-d_3p}]$, so the conductor of R_i is d_i. Thus 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. Thus for any prime ℓ, we have that at least one of R_1 or R_2 is maximal at ℓ. Thus $\Lambda_{\alpha_1\alpha_2}$ is locally basic at each prime ℓ hence locally Bass at each prime ℓ, so $\Lambda_{\alpha_1\alpha_2}$ is Bass. □

5 Computing $\mathrm{End}(E)$ with inseparable endomorphisms and enumeration

We consider the following computational problem:

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

In the previous section we saw that inseparable reflections of E can be used to build a Bass suborder Λ of $\mathrm{End}(E)$. Then we can enumerate the maximal orders of $B_{p,\infty}$ containing Λ and return the one which is isomorphic to $\mathrm{End}(E)$.

Our algorithm to compute the endomorphism ring of a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ involves three algorithms:

1. Algorithm 1: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and two coprime integers ℓ and d, with d square-free, the algorithm returns an ℓ^n-isogeny $\phi\colon E \to E'$ and a d-isogeny $\psi\colon E' \to E'^{(p)}$ such that (E', ψ) is a (d, ϵ)-structure.

2. Algorithm 2: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2 and d, with d square-free, the algorithm runs twice Algorithm 1 to get two $\ell_i^{n_i}$-isogenies $\phi_i\colon E \to E_i$ and two d-isogenies $\psi_i\colon E_i \to E_i^{(p)}$. Then it returns the Bass order

   $$\Lambda((\phi_1,\psi_1),(\phi_2,\psi_2)) \coloneqq \mathbb{Z}+\mathbb{Z}\alpha(\phi_1,\psi_1)+\mathbb{Z}\alpha(\phi_2,\psi_2)+\mathbb{Z}\rho((\phi_1,\psi_1),(\phi_2,\psi_2)),$$

   where

   $$\alpha(\phi_i,\psi_i) \coloneqq \pi_p\widehat{\phi_i^{(p)}}\psi_i\phi_i, \quad \rho((\phi_1,\psi_1),(\phi_2,\psi_2)) = \widehat{\phi_1}\widehat{\psi_1}\phi_1\widehat{\phi_2^{(p)}}\psi_2\phi_2.$$

3. Algorithm 3: Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2 and d, with d square-free, the algorithm runs Algorithm 2 to get a Bass order Λ contained in $\mathrm{End}(E)$. The algorithm enumerates the maximal orders $\mathcal{O}$ of $B_{p,\infty}$ containing Λ, until $\mathcal{O} \cong \mathrm{End}(E)$.

In this section we denote by $\Phi_N(X,Y)$ the modular polynomial for level N and, for ℓ a prime number, we denote by $G(p,\ell)$ the supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$. We will use Φ_ℓ to navigate $G(p,\ell)$.

5.1 Algorithm 1

Algorithm 1: Compute an inseparable reflection

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and two coprime integers ℓ and d, with d square-free and $d < p/4$.

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

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

repeat

  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;

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

Compute a (d, ϵ)-structure (E_t, ψ);

return $\{\phi_1, \ldots, \phi_t, \psi, \widehat{\phi_t}^{(p)}, \ldots, \widehat{\phi_1}^{(p)}, \pi_p\}$

Below, we analyze the complexity of Algorithm 1. First, we bound the expectation of the number of random walks beginning at E which we take before finding a (d, ϵ)-structure. For simplicity, we assume $d = 1$ or 2, since these are the only cases we will need. Similar results hold for square-free $d = O(\log p)$. 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]). Let $\operatorname{llog} x$ denote $\log \log x$.

Proposition 5.1 (GRH)**.** *Assume GRH. Let $p > 12$ be a prime and let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ where $\#E(\mathbb{F}_{p^2}) = (p+\epsilon)^2$ for $\epsilon = 1$ or -1. Let ℓ be a another prime, and let $d = 1$ or 2. Let X be the collection of isomorphism classes of supersingular elliptic curves with a (d, ϵ)-structure. Then 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 of length t in $G(p, \ell)$ beginning at E lands in X with probability at least $\Omega\left(\frac{1}{\sqrt{p}\operatorname{llog} p}\right)$.

Proof. First, we show that X is nonempty. Indeed, if an elliptic curve E' has an endomorphism μ satisfying $\mu^2 = -[dp]$ and $\#E'(\mathbb{F}_{p^2}) = (p+\epsilon)^2$, then E' has a (d, ϵ)-structure (E, ψ). Since $\mu^2 = [-dp]$, we may factor μ as $\mu = \pi_p \psi$ for an isogeny $\psi\colon E \to E^{(p)}$ of degree d. By [CS21, Lemma 1], (E, ψ) is a (d, ϵ)-structure. We conclude that X is nonempty, since the reduction at a prime above p of a curve over $\overline{\mathbb{Q}_p}$ with CM by the ring of integers of $\mathbb{Q}(\sqrt{-dp})$ will have an embedding of $\mathbb{Z}[\sqrt{-dp}]$ into its endomorphism ring.

Since X is nonempty, we have

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

so for t satisfying the hypothesis in the proposition, we have

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

Thus, for t satisfying the inequality in the statement of the proposition, by Proposition A.1 we have that a non-backtracking walk beginning at E 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,

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

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

While we allow ℓ and d to vary to give the previous algorithm some flexibility, we will only need to run it on inputs of the form $(E, \ell, 2)$ (to compute Bass orders) and inputs $(E, \ell, 1)$ (for our later heuristic algorithm). Thus in our complexity analysis below, we are treating ℓ and d as constants.

Proposition 5.2 (GRH)**.** *Assume GRH. Let $p > 3$ be a prime and let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\ell \in \{2, 3, 5, 7\}$ be prime, and let $d \in \{1, 2\}$. On input (E_0, ℓ, d), Algorithm 1 terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time.*

Proof. We can do Step 1 with Newton's method, for example, and the resulting t will be in $O(\log p)$. Since we assume that ℓ and d are constant, we may precompute $\Phi_\ell(X, Y)$ and store this polynomial to take random walks in $G(p, \ell)$. We may also precompute $\Phi_d(X, Y)$ if $d = 2$ to test whether a given vertex has a

$(2,\epsilon)$-structure; thus we ignore this cost in our complexity analysis as it will be dominated by 3. We can take one step in $G(p,\ell)$ using modular polynomials. 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 $O(\ell^2)$ many operations in $\mathbb{F}_{p^2}$, which is dominated by the time to compute a random root of $\Phi_\ell(j_i,Y)$ which requires $O(\mathsf{M}(\ell\log p)(\operatorname{llog} p))$ bit operations 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. We can test if j_t is in S 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 5.1 the probability that a non-backtracking walk beginning at E_0 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 $\mathsf{M}(n) = O(n\log n)$ yields the cost

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

If j_t is in X, we may obtain the associated sequence of isogenies $\phi_i\colon E_i \to E_{i+1}$ for $i = 0,\ldots,t-1$ and the (d,ϵ)-structure using Elkies's algorithm, for example, which will take $O((\log p)^{O(1)})$ many operations in $\mathbb{F}_{p^2}$. This cost is dominated by the time required to just find the path. □

5.2 Algorithm 2

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

Input: A supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and three pairwise coprime integers ℓ_1, ℓ_2 and d, with d square-free

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

1 Use Algorithm 1 twice to compute an $\ell_i^{n_i}$-isogeny $\phi_i\colon E \to E_i$ and two (d,ϵ)-structures (E_i,ψ_i), for $i = 1,2$;

2 Let $\alpha_i = \pi_p\widehat{\phi_i^{(p)}}\pi_p\widehat{\phi_i^{(p)}}\psi_i\phi_i$ **return** $\Lambda = \langle 1,\alpha_1,\alpha_2,\alpha_1\alpha_2\rangle$

Theorem 5.3 (GRH)**.** *Assume GRH. On input a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and the primes $\ell_1 = 3$, $\ell_2 = 5$, and $d = 2$, Algorithm 2 is correct and terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time.*

Proof. By Proposition 5.2, Step 1 terminates in expected $O(\sqrt{p}(\log p)^2(\operatorname{llog} p)^3)$ time. Given an isogeny $\phi_1\colon E \to E_1$ represented by a sequence of 3-isogenies

from E to E_1, we can find the $(2,\epsilon)$-structure of E_1 by simply enumerating its three 2-isogenies and, for each such ψ, checking if $\psi^{(p)} = \epsilon\widehat{\psi}$. Let ψ_1 be such a 2-isogeny. We similarly find the desired 2-isogeny ψ_2 of E_2, where E_2 is the final curve in the path in the 5-isogeny graph constructed in Step 1. The two endomorphisms constructed in this algorithm satisfy the hypotheses of Theorem 3.8, so the order returned by this algorithm is Bass and thus the algorithm is correct. □

5.3 Algorithm 3

Algorithm 3: Compute End(E)

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

1 Let $\ell_1 = 3$, $\ell_2 = 5$ and $d = 2$;
2 Given E, ℓ_1, ℓ_2 and d, use Algorithm 2 to compute a Bass order Λ contained in $\mathrm{End}(E)$;
3 Enumerate the maximal orders $\Lambda \subseteq \mathcal{O}' \subseteq B_{p,\infty}$ until $\mathcal{O}' \simeq \mathrm{End}(E)$;
4 **return** $\mathcal{O}'$

With an algorithm for computing a Bass order Λ in $\mathrm{End}(E)$, we obtain an algorithm for computing the endomorphism ring of E using the algorithms of [EHL$^+$]. We factor $\mathrm{discrd}(\Lambda)$ and, for each prime $q|\,\mathrm{discrd}(\Lambda)$ with $q \neq p$, we enumerate the maximal orders containing $\Lambda \otimes \mathbb{Q}_q$ using Algorithm 4.3 of [EHL$^+$].

Proposition 5.4. *Algorithm 3 terminates in expected $O(\sqrt{p}(\log p)^2(\mathrm{llog}\, p)^3)$ time.*

Proof. Step 2 runs in expected time $O(\sqrt{p}(\log p)^2(\mathrm{llog}\, p)^3)$, by Theorem 5.3. We sketch how to do step 3. First, compute an isomorphism $f\colon \Lambda \otimes \mathbb{Q} \to B_{p,\infty}$ of quaternion algebras, which can be done in time polynomial in $\log p$ [CKMZ22, Proposition 4.1]. Also, compute a supersingular elliptic curve E_0 and an order $\mathcal{O}_0 \subseteq B_{p,\infty}$ isomorphic to $\mathrm{End}(E_0)$, which can be done efficiently, assuming GRH [EHL$^+$18, Proposition 3]. Let $\rho = \alpha_1\alpha_2$. We factor $\mathrm{disc}(\rho)$ to obtain a factorization of $\mathrm{discrd}(\Lambda) = p\,\mathrm{disc}(\rho)$. Since ρ is the product of $O(\log p)$ many 3- and 5-isogenies and two 2-isogenies, the degree of ρ is $O(p^C)$ for some C and thus $\mathrm{disc}(\rho)$ is also $O(p^C)$. We may 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$^+$] and then enumerate the $\mathbb{Z}$-orders containing $f(\Lambda)$; see Steps 1(a) and 3(a) in Algorithm 5.4 of [EHL$^+$]. For each maximal order $\mathcal{O}'$ containing $f(\Lambda)$, compute an elliptic curve E' with $\mathrm{End}(E') \simeq \mathcal{O}'$. This can be done in polynomial time in $\log p$: compute a connecting ideal J between $\mathcal{O}_0$ and $\mathcal{O}'$, then, by Theorem 6.4 of [Wes22], one can compute an equivalent ideal I to J. From I, one can compute the corresponding isogeny $\phi_I\colon E_0 \to E'$, thus constructing E' with $\mathrm{End}(E') \simeq \mathcal{O}'$. If $j(E') \in \{j(E), j(E)^p\}$, we return $\mathcal{O}'$.

By Proposition 4.2 of [EHL$^+$], the number of maximal overorders of $f(\Lambda)$ is bounded by

$$\prod_{\substack{q|\operatorname{disc}(\rho)\\ q\neq p}} v_q(\operatorname{disc}(\rho)) + 1,$$

the number of divisors of $\operatorname{disc}(\rho)/p^{v_p(\operatorname{disc}(\rho))}$. The number of divisors of an integer n is $O(n^\epsilon)$ for every $\epsilon > 0$ [HW08, Theorem 315]. We conclude that step 3 takes $O(p^\epsilon)$ time for any $\epsilon > 0$, so in particular, the expected time required to complete step 3 is dominated by the expected time required to complete step 2. □

5.4 Computing a q-maximal suborder of $\mathrm{End}(E)$

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, Algorithm 2 returns a necessarily non-maximal suborder Λ of $\mathrm{End}(E)$. We sketch a preprocessing step one could perform before computing $\mathrm{End}(E)$ by enumerating maximal overorders of Λ. Let $1, \alpha_1, \alpha_2, \alpha_1\alpha_2$ be the basis returned by Algorithm 2 and let $\rho = \alpha_1\alpha_2/p$. Suppose $q \neq p$ is a prime, that $q|\operatorname{disc}(\rho)$, and let $e = v_q(\operatorname{disc}(\rho))$. Then Λ is non-maximal at q. We sketch how to compute an order $\Lambda \subseteq \Lambda' \subseteq \mathrm{End}(E)$ which is q-maximal. Working over an extension of degree at most $(q-1)$ over $\mathbb{F}_{p^2}$, we find generators P_1, P_2 of $E[q]$ and then find x_1, x_2, x_3, x_4, $0 \leq x_j \leq q-1$, such that

$$x_1P_i + x_2\alpha_1(P_i) + x_3\alpha_2(P_i) + x_4\rho(P_i) = 0$$

for $i = 1, 2$. Then the endomorphism

$$\gamma = x_1 + x_2\alpha_1 + x_3\alpha_2 + x_4\rho$$

factors through $[q]$, so $\gamma' = \gamma/q$ is an endomorphism of E. The smallest overorder Λ' of Λ containing γ' properly contains Λ. We repeat this procedure until Λ' is q-maximal. Repeating this procedure for all primes $q|\operatorname{disc}(\rho)$ such that $q^{v_q(\operatorname{disc}(\rho))} < B$ for a suitable bound B will significantly speed up the enumeration step. After the process described above there will be very few primes dividing $\operatorname{disc}(\rho)$, and thus substantially fewer maximal orders $\mathcal{O}'$ such that we must check if $\mathcal{O}' \simeq \mathrm{End}(E)$.

6 Computing $\mathrm{End}(E)$ by generating inseparable endomorphisms

Let E be a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. In this section, we discuss an algorithm for computing $\mathrm{End}(E)$ using only Algorithm 1 and we describe all the technical steps that we need in order to:

- Find $a, b \in \mathbb{Q}$ such that $\mathrm{End}^0(E) \cong H(a,b) = \mathbb{Q}x_1 + \mathbb{Q}x_2 + \mathbb{Q}x_3 + \mathbb{Q}x_4$, with $x_1 = 1$, $x_2^2 = a$, $x_3^2 = b$ and $x_4 = x_2x_3 = -x_3x_2$.

- Determine a basis $\{b_1, b_2, b_3, b_4\}$, where $b_i = \sum_{j=1}^{4} c_{ij} x_j, \quad c_{ij} \in \mathbb{Q}$ of a maximal order $\mathcal{O} \subseteq \left(\frac{a,b}{\mathbb{Q}}\right)$ so that $\mathrm{End}(E) \cong \mathcal{O}$.

The fundamental idea is to use Algorithm 1 to compute the suborder $\mathbb{Z}+P$ and then the algorithms in [Voi21] to recover $\mathrm{End}(E)$ from $\mathbb{Z}+P$.

Compared to what described in Section 5, this algorithm has the advantage that once enough endomorphisms of E have been found, one just needs linear algebra in order to recover the endomorphism ring. We will finally provide an heuristic that in our case we expect to compute $O(1)$ endomorphisms before finding a generating set for $\mathbb{Z}+P$.

6.1 Computing a quadratic submodule of $\mathbb{Z}+P$

Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ and let P be the ideal of inseparable endomorphisms of E. We now discuss an algorithm for computing $\mathbb{Z}+P \subseteq \mathrm{End}(E)$, using Algorithm 1. 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 elements $\gamma_1, \gamma_2, \gamma_3$ of P such that $\gamma_0 \coloneqq 1, \gamma_1, \gamma_2, \gamma_3$ generate a lattice contained in $\mathbb{Z}+P$. 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 separable a isogeny such that E_i is defined over $\mathbb{F}_p$ and $\widehat{\phi_i}$ does not factor through any nontrivial $\mathbb{F}_p$-isogenies.

Let $\Lambda \coloneqq \mathbb{Z}\gamma_0 + \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2 + \mathbb{Z}\gamma_3$ be the lattice with basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. By computing the Gram matrix of this lattice with respect to the trace pairing, we upgrade the lattice to a quadratic module. So let $G \coloneqq (\mathrm{Trd}(\gamma_i \widehat{\gamma_j}))$ be the Gram Matrix for the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. First, by Proposition 3.5, we have $\mathrm{Trd}(\gamma_i) = 0$ for $i = 1, 2, 3$. For $1 \le i < j \le 3$ define

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

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

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

Therefore, as quadratic $\mathbb{Z}$-modules, we have $(\Lambda, \deg) \simeq (\mathbb{Z}^4, G)$ under the isomorphism which sends γ_i to the ith standard basis vector in $\mathbb{Z}^4$.

6.2 From a quadratic module to an order in a quaternion algebra

With the Gram matrix G of the basis $\gamma_0, ldots, \gamma_3$ in hand, we move on to 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

$H(a,b)$, or alternatively, to computing 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 present two equivalent approaches. In one, 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. We will see that each approach requires a single choice of a square root for a square integer, and that these choices are consistent with one another.

6.2.1 Computing an isomorphism of quaternion algebras using the Gram-Schmidt process

Let $G = (\mathrm{Trd}(\gamma_r\widehat{\gamma_s}))_{0\le r,s\le 3}$ be the Gram matrix for the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$ 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 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 let a, b be such that $d_1 = -2a$, $d_2 = -2b$. Define $R = L^T$ and $\tilde{\gamma_i} = \sum_j (R^{-1})_{ij}\gamma_j$ for $i = 0, 1, 2, 3$; these are the elements of $\Lambda \otimes \mathbb{Q}$ resulting from the application of the Gram-Schmidt process to the basis $\gamma_0, \gamma_1, \gamma_2, \gamma_3$. 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 the reduced norm of each side, we get that $d_3/2 = c^2 d_1 d_2/4$. Define $c' \coloneqq \sqrt{\frac{2d_3}{d_1 d_2}}$. We therefore obtain an the isomorphism of quadratic spaces

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

where $i^2 = a$, $j^2 = b$, and $ij = -ji$. This map induces an isomorphism of $\mathrm{End}^0(E)$ with either $H(a,b)$ (in the case that $c = c'$) or $H(a,b)^{\mathrm{op}}$ (in the case that $c = -c'$).

6.2.2 Computing a multiplication table using linear algebra

Alternatively, we can compute a multiplication table for $\mathrm{End}^0(E) \simeq \Lambda \otimes \mathbb{Q}$, 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 have $\gamma_0^2 = 1$ and for $r \neq 0$, we have $\gamma_r^2 = \mathrm{Trd}(\gamma_r)\gamma_r - \mathrm{Nrd}(\gamma_r) = -\deg(\gamma_r)$. Therefore $m_{000} = 1$, $m_{rr0} = -\deg(\gamma_r)$ for $1 \le r \le 3$, and $m_{rrt} = 0$ for $0 \le r \le 3$ and $1 \le t \le 3$. 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

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

Therefore

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

so it suffices to express $\gamma_r\gamma_s$ as a linear combination of $\gamma_0, \ldots, \gamma_3$ for $1 \leq r < s \leq 3$.

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 $1 \leq r < s \leq 3$ a system of four equations in the indeterminates $m_{rs0}, m_{rs1}, m_{rs2}, m_{rs3}$:

$$\operatorname{Trd}(\gamma_r\gamma_s\widehat{\gamma_k}) = \sum_{t=0}^{3} m_{rst} \operatorname{Trd}(\gamma_t\widehat{\gamma_k}). \tag{6.1}$$

We will show that the left-hand side of Equation 6.1 can be determined up to sign by the entries of G, but we need to make one choice of a square root (of $\det(G)$).

We compute the left hand side of Equation 6.1 for each $0 \leq r < s \leq 3$, $0 \leq k \leq 3$. 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 $1 \leq r < s \leq 3$. 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

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

We conclude that $m(\gamma_1,\gamma_2,\gamma_3)^2 = \det(G)$. We have that $m(\gamma_{\sigma(1)},\gamma_{\sigma(2)},\gamma_{\sigma(3)}) = \mathrm{sgn}(\sigma)m(\gamma_1,\gamma_2,\gamma_3)$ 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 $\mathrm{Trd}(\gamma_{\sigma(1)}\gamma_{\sigma(2)}\widehat{\gamma_{\sigma(3)}})$ by choosing, for example, $\mathrm{Trd}(\gamma_1\gamma_2\widehat{\gamma_3}) = \frac{1}{2}\sqrt{\det(G)}$ and then setting

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

We see the same phenomenon we observed earlier: 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 isomoprhism of $\Lambda \otimes \mathbb{Q}$ *as a quaternion algebra* with $\mathrm{End}^0(E)$ vs $(\mathrm{End}^0(E))^{\mathrm{op}}$. Having made this choice of square root, we have computed the left hand side of Equation 6.1 for all values of r, s, t. This system can then be solved with linear algebra, and the solutions yield the desired multiplication law.

One may ask if the two approaches are compatible. This is the case: first of all, G determines the structure of $\mathrm{End}^0(E)$ as a quadratic space, and there are only two (up to isomorphism) quaternion algebras isomorphic to $\mathrm{End}^0(E)$ whose trace-zero subspaces are isomorphic to the quadratic module determined by $G_0 = (G_{ij})_{1\le i,j\le 3}$. In particular, let $LDL^T = G$ with D diagonal and L lower-triangular with 1's on its diagonal. Let $\tilde{\gamma_i}$ be defined as above for $i = 1, 2, 3$. 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 c are equal.

6.3 Computing an order in $\mathbb{Z} + P$

We assume 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 lattices $f\colon (\mathbb{Q}^4, G) \otimes \mathbb{Q} \to H(a,b)$ and $g\colon (\mathrm{End}^0(E), \mathrm{Nrd}) \to (\mathbb{Q}^4, G)$ which sends γ_r to e_r, the rth standard basis vector of $\mathbb{Q}^4$. Let m_{rst} satisfy

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

the elements of the multiplication table for the basis $\mathcal{B} = \{\gamma_0, \gamma_1, \gamma_2, \gamma_3\}$. Let M_r be the matrix $M_r = (m_{rst})_{0\le s,t\le 3}$, so M_r^T is the image of γ_r in $M_4(\mathbb{C})$ under the left regular representation of $\mathrm{End}(E)$ using the basis $\mathcal{B}$. Let M_{rs} denote the sth row of M_r. To compute the order generated by $\mathcal{B}$, we compute the Hermite normal form H of the matrix A whose rows are the rows of M_0 along with M_{rs} for $0 < r < s \le 3$. The top four rows of H form a lattice L in $\mathbb{Z}^4$ such that $g^{-1}(L) = \mathcal{O}$, where $\mathcal{O}$ is the minimal order in $\mathrm{End}(E)$ containing Λ.

6.4 Augmenting an order with an endomorphism

We now assume we have computed a suborder $\mathcal{O}$ of $\mathbb{Z} + P$ generated by $\gamma_0 = 1$ and three inseparable endomorphisms $\gamma_1, \gamma_2, \gamma_3$. We represent $\mathcal{O}$ by a basis. To be precise, we represent a basis of $\mathcal{O}$ 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 $g^{-1}(L_{\mathcal{O}[\gamma]}) = \mathcal{O}$.

6.5 Computing $\mathbb{Z} + P$ and $\mathrm{End}(E)$

1. We have an order $\Lambda = \langle \gamma_0, \gamma_1, \gamma_2, \gamma_3 \rangle$ where $\gamma_0 = 1 \in \mathrm{End}(E)$ and $\gamma_i = \widehat{\pi} \circ \phi_i$ as before
2. While $\mathrm{discrd}(\Lambda) \neq p^2$:
   (a) Compute $\gamma \in P$ by computing $\phi \colon E \to E^{(p)}$ as before
   (b) Compute $x_0, \ldots, x_3$ such that $\gamma = \sum_i x_i \gamma_i$. To do this, note that we have
   $$\mathrm{Trd}(\gamma_i \widehat{\gamma}) = \sum_j x_j \, \mathrm{Trd}(\gamma_i \widehat{\gamma_j})$$
   and we have already computed $\mathrm{Trd}(\gamma_i \widehat{\gamma_j})$ (this is the ij-entry of the Gram matrix.) Also, we can compute
   $$\mathrm{Trd}(\gamma_i \widehat{\gamma}) = p \cdot \mathrm{Trd}(\phi_i \widehat{\phi})$$
   as before (using a generalized version of Schoof's algorithm) in time polylog p. This yields a system of four equations in the four variables x_0, x_1, x_2, x_3 which we can thus solve for using linear algebra.

(c) Compute the order generated by $\gamma_0, \ldots, \gamma_3, \gamma$ (using, e.g., the hermite normal form)

3. Compute $\mathrm{End}(E) \supset \mathbb{Z} + P$ using the algorithm of Voight

6.6 From $\mathbb{Z} + P$ to $\mathrm{End}(E)$

Definition 6.1. 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 will show that for quaternion algebras over $\mathbb{Q}$ ramified at p, orders which are p-saturated must also be p-maximal.

Proposition 6.2. *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 6.3. *Let $\mathcal{O} \subseteq \mathrm{End}^0(E)$ be a p-saturated order such that $\mathbb{Z} + P \subseteq \mathcal{O}$. Then $\mathcal{O} = \mathrm{End}(E)$.*

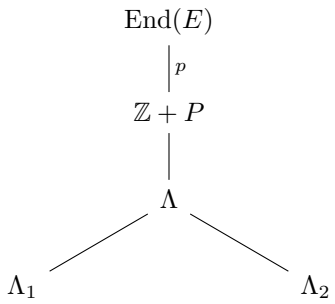
Proof. By Proposition 3.1, the reduced discriminant of $\mathbb{Z} + P$ is p^2, so $\mathbb{Z} + P$ is ℓ-maximal for all $\ell \neq p$. Since $\mathbb{Z} + P \subseteq \mathcal{O} \subseteq \mathrm{End}(E)$, the order $\mathcal{O}$ is also ℓ-maximal for all $\ell \neq p$. Moreover $\mathcal{O}$ is p-saturated, so $\mathcal{O}$ is p-maximal. 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 a p-saturated order that contains $\mathbb{Z} + P$. This is done by Algorithm 3.12 and Algorithm 7.9 in [Voi21].

6.7 How many endomorphisms do we need?

A natural question is whether we can bound the number of calls to Algorithm 1 before producing enough endomorphisms to generate $\mathrm{End}(E)$. We do not prove a bound here, leaving this to future work, however we argue that the expected number of calls is bounded by a constant independent of p and of E.

Suppose we run Algorithm 2 twice on input a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, producing two (not necessarily Bass) orders Λ_1, Λ_2 in $\mathrm{End}(E)$ generated 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 the bases of Λ_1, Λ_2.



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 $\mathrm{discrd}(\Lambda_1) = p^2 \,\mathrm{disc}(\rho_1)$ and $\mathrm{discrd}(\Lambda_2) = p^2 \,\mathrm{disc}(\rho_2)$, where $\rho_1 = \frac{\alpha_1\alpha_2}{p}$ and $\rho_2 = \frac{\alpha_3\alpha_4}{p}$. So, in particular, $[\mathbb{Z} + P : \Lambda] = \frac{\mathrm{discrd}(\Lambda)}{p^2}$ divides $\gcd(\mathrm{disc}(\rho_1), \mathrm{disc}(\rho_2))$. If we assume that the distribution of the factorization patterns of $\mathrm{disc}(\rho_1)$ and $\mathrm{disc}(\rho_2)$ follows the same distribution as two random integers, then they are coprime with probability approximately $6/\pi^2 \approx 0.6$. Thus we expect that after computing four suborders of $\mathrm{End}(E)$ with Algorithm 2 we have collected enough endomorphisms to find a basis of $\mathbb{Z} + P$.

Remark 6.4. If instead of working with the orders Λ_1, Λ_2 we work with Λ_{ρ_1} and Λ_{ρ_2} generated respectively by $1, \alpha_1, \alpha_2, \rho_1$ and $1, \alpha_3, \alpha_4, \rho_2$, then, with an analogous argument, we expect that after computing four suborders of this kind we have collected enough endomorphisms to find a basis of $\mathrm{End}(E)$.

This argument applies to any order generated by two non-commuting endomorphisms. Let α_1, α_2 be two arbitrary non-commuting elements of a quaternion order $\mathcal{O}$ and let $\Lambda = \langle \alpha_1, \alpha_2 \rangle \coloneqq \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_1\alpha_2$ 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

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

We introduce two heuristic assumptions on the distribution of the discriminants of elements of a maximal order in a quaternion algebra. Let $\mathcal{O}$ be a maximal order in a quaternion algebra ramified at $\{p, \infty\}$ and for a real number X, define $S_{\mathcal{O}}(X) := \{\alpha \in \mathcal{O} : \mathrm{Nrd}(\alpha) \leq X\}$. Our first assumption is that for a random α chosen from $S_{\mathcal{O}}(X)$ that $\mathrm{disc}(\alpha)$ is distributed approximately like a random discriminant $-4X \leq d \leq 0$ such that p is not split in $\mathbb{Q}(\sqrt{d})$. Our second assumption is that if we sample α, β from $S_{\mathcal{O}}(X)$ uniformly and independently, then the element

$$\mathrm{Trd}(\alpha)\beta + \mathrm{Trd}(\beta)\alpha - 2\alpha\beta$$

is uniformly distributed in $S_{\mathcal{O}}(X^2)$. Suppose now that we sample $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ uniformly and that $\alpha_{i1}\alpha_{i2} \neq \alpha_{i2}\alpha_{i1}$ for $i = 1, 2$. Let

$$D_i = \mathrm{disc}\left(\mathrm{Trd}(\alpha_{i2})\alpha_{i1} + \mathrm{Trd}(\alpha_{i1})\alpha_{i2} - 2\alpha_{i1}\alpha_{i2}\right).$$

Then the α_{ij} will generate a maximal order with probability at least the probability that

$$\gcd(D_1, D_2) = 1,$$

which will hold with probability bounded below by a constant given our two assumptions above.

A Non-backtracking random walks

Let $p > 3$ be a prime. Let $V = V(p) = \{E_i\}_{1 \leq i \leq n}$ denote a complete set of representatives of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$. We form a directed graph $G = G(p, \ell)$ whose vertex set is V and where an arrow from E_i to E_j is a choice of representative from the set $\mathrm{Aut}(E_j)\phi$, where $\phi\colon E_i \to E_j$ is an ℓ-isogeny. For a prime $\ell \neq p$, let a_{ij} denote the number of cyclic subgroups C of $E_i[\ell]$ such that $E_i/C \simeq E_j$. Consider the $\mathbb{C}$-vector space H with basis V. Define an inner product on H by $\langle E_i, E_j \rangle = w_i \delta_{ij}$ and extended via linearity, where δ_{ij} is the Kronecker delta function and $w_i \coloneqq \#\,\mathrm{Aut}(E_i)/2$. Define the operator A on H by $AE_i = \sum_j a_{ij} E_j$. Then A is self-adjoint as an operator on H with respect to $\langle , \rangle$. A walk on the graph G 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 if $\phi_{i+1} \neq u\widehat{\phi_i}$ for any automorphism u. Thus non-backtracking walks in $G(p, \ell)$ beginning at E_i are in bijection with cyclic subgroups of $E_i[\ell^\infty]$.

Proposition A.1. *Let $J \subseteq \{1, 2, \ldots, n\}$ and $X = \{E_j\}_{j \in J} \subseteq V$. If*

$$t/2 - \log_\ell\left(t + \frac{\ell - 1}{\ell + 1}\right) \geq \log_\ell\left(\frac{(p-1)^{3/2}}{24\sum_{j \in J} w_j^{-1}}\right)$$

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

$$\frac{6}{p-1}\sum_{j \in J} w_j^{-1}.$$

Proof. Let $P^{(t)}$ be the transition matrix for the non-backtracking random walk on G of length t. Let $\pi^{(t)} = P^{(t)}E_i$ be the probability distribution on V resulting from a random non-backtracking walk of length t beginning at E_i. Also, let $\mathcal{E} = \sum w_j^{-1}E_j$ so $s = \frac{1}{\langle \mathcal{E}, \mathcal{E} \rangle}$ is the stationary distribution for the random walk on G. Then by Theorem 11 of [BCC+22],

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

We have

$$s(X) = \frac{12}{p-1} \sum_{j \in J} w_j^{-1}.$$

We see that if

$$t/2 - \log_\ell \left(t + \frac{\ell - 1}{\ell + 1}\right) \geq \log_\ell \left(\frac{(p-1)^{3/2}}{24 \sum_{j \in J} w_j^{-1}}\right)$$

then

$$\frac{(p-1)^{1/2}}{4} \cdot \left(t + \frac{\ell - 1}{\ell + 1}\right) \cdot \ell^{-t/2} \leq \frac{6}{p-1} \sum_{j \in J} w_j^{-1}$$

so

$$\pi^{(t)}(X) \geq \frac{6}{p-1} \sum_{j \in J} w_j^{-1},$$

as desired. □

References

[ACNL+19] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. Adventures in supersingularland. Preprint, 2019. arxiv:1909.07779.

[BCC+22] 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. Cryptology ePrint Archive, Paper 2022/1469, 2022. `https://eprint.iacr.org/2022/1469`.

[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.

[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.

[EHL+] 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. *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, pages 215–232.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. *Eurocrypt 2018, LNCS 10822*, pages 329–368, 2018.

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

[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.

[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.

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

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

[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] ©2021.

[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.