Supersingular Curves With Small Non-integer Endomorphisms

Jonathan Love Dan Boneh

October 9, 2019

Abstract

We introduce a special class of supersingular curves over \( F_{p^2} \), characterized by the existence of non-integer endomorphisms of small degree. A number of properties of this set is proved. Most notably, we show that this set partitions into subsets in such a way that curves within each subset have small-degree isogenies between them, but curves in distinct subsets have no isogenies of degree \( O(p^{1/4-\varepsilon}) \) between them. Despite this, we show that isogenies between these curves can be computed efficiently, giving a technique for computing isogenies between certain prescribed curves that cannot be reasonably connected by searching on \( \ell \)-isogeny graphs.

1 Introduction

Fix an odd prime \( p \geq 5 \). An elliptic curve \( E \) is supersingular if its endomorphism ring is non-abelian [Sil09, Theorem V.3.1].

Definition 1.1. Given \( M < p \), an elliptic curve \( E \) over a finite field of characteristic \( p \) (or its \( j \)-invariant) is \( M \)-small if there exists an endomorphism \( \alpha \) of \( E \) with \( \deg \alpha \leq M \) such that \( \alpha \) is not multiplication by an integer. The set of \( M \)-small \( j \)-invariants of supersingular curves is denoted \( S_M \).

\( M \)-small curves may be ordinary or supersingular. This paper will focus primarily on the set of \( M \)-small supersingular curves, though some results will hold for any \( M \)-small elliptic curve. Some notable properties that will be discussed:

(a) The set of all \( M \)-small curves can be generated efficiently by finding roots of Hilbert class polynomials (Proposition 2.4).

(b) The number of \( M \)-small curves up to \( \overline{F}_p \)-isomorphism is \( O(M^{3/2}) \) (Proposition A.3).

(c) When \( M \ll p \), approximately half of all \( M \)-small curves appear to be supersingular (Remark A.4).

(d) When \( M \geq \frac{1}{2}p^{2/3} + \frac{1}{4} \), every supersingular curve is \( M \)-small (Proposition A.5).

(e) When \( M \ll p \), the set \( S_M \) of \( M \)-small supersingular curves partitions into \( O(M) \) subsets, such that there is no isogeny of degree \( O(p^{1/4-\varepsilon}) \) between any two elements in distinct subsets (Theorem 1.3).

(f) The endomorphism rings of \( M \)-small supersingular curves, and isogenies between any two of them, can heuristically be computed in time polynomial in \( M \) and \( \log p \) (Section 7).

Let us state point (e) more precisely. Recall that every supersingular curve can be defined over \( F_{p^2} \) [Sil09, Theorem V.3.1(a)]. Given an elliptic curve \( E \) over \( F_{p^2} \), let \( E^{(p)} \) denote its image under the \( p^{th} \) power Frobenius map \( (x, y) \mapsto (x^p, y^p) \). If \( E \) is defined over \( F_p \), then \( E = E^{(p)} \); otherwise we have \( E = (E^{(p)})^{(p)} \) and so this map will swap conjugate pairs of curves.\(^1\) For \( j \in F_{p^2} \), let \( E_j \) be an elliptic curve with \( j \)-invariant equal to \( j \).

\(^1\)The map \( E \rightarrow E^{(p)} \) on supersingular curves is called the “mirror involution” in [Arp+19], where the relationship between conjugate pairs, along with many other structural properties of supersingular isogeny graphs, is studied in detail.
\textbf{Definition 1.2.} Let $E$ and $E'$ be supersingular elliptic curves over $\mathbb{F}_p$. The \textbf{distance from $E$ to $E'$}, denoted $d(E, E')$, is the minimum degree of an isogeny $E \to E'$ or $E \to E'(^p)$. We also define $d(j,j') = d(E_j, E_{j'})$ for supersingular $j$-invariants $j,j'$.

This definition identifies conjugate pairs $E, E(^p)$ of supersingular curves. For any curves $E$, $E'$, and $E''$, we have

$$d(E, E) = 1, \quad d(E, E') = d(E', E), \quad d(E, E'') \leq d(E, E')d(E', E'')$$

by basic properties of isogenies (e.g., [Sil09, Sections III.4, III.6]).

A \textbf{fundamental discriminant} is either a squarefree integer $D \equiv 1 \pmod{4}$, or $D = 4m$ where $m \equiv 2,3 \pmod{4}$ is squarefree. We can now state the main theorem:

\textbf{Theorem 1.3.} Suppose $p > 64M^2$, and let $\mathcal{S}_M$ denote the set of $M$-small supersingular curves. There exists a partition

$$\mathcal{S}_M = \bigcup_D T_D$$

of $\mathcal{S}_M$ into nonempty subsets, indexed by fundamental discriminants $-4M \leq D < 0$ which are not congruent to a square mod $p$. This partition has the following properties:

- If $j,j'$ are in distinct subsets $T_D \neq T_{D'}$, then
  $$d(j,j') \geq \frac{p^{1/4}}{\sqrt{2M}}.$$

- If $j,j'$ are in the same subset $T_D$, then there is a chain $j = j_0, j_1, \ldots, j_r = j'$ of elements of $T_D$ such that
  $$d(j_{i-1}, j_i) \leq \frac{4}{\pi} \sqrt{M}$$
  for all $i = 1, \ldots, r$. We can find such a chain with $r \leq 3$, or alternatively, we can find such a chain for which there is an isogeny $E_{j_{i-1}} \to E_j$ of prime degree at most $\frac{1}{2} \sqrt{M}$ for each $i$.

See Figure 1 for an illustration of the Theorem. Intuitively, this is saying that the set of supersingular curves has “isogeny valleys”\footnote{Perhaps they should be called “isogeny peaks” because we shall see in Section 5 that they are very closely related to the volcanic “craters” of ordinary isogeny graphs, as discussed in [Sut12]. However, it feels more natural to associate $M$-small curves with valleys, both so that we can think of endomorphism degree as a measure of height, and because they are in practice easier to reach, as discussed in Section 2.} indexed by the mathy certain fundamental discriminants; each valley consists of a number of $M$-small curves that are all linked together by low-degree isogenies, but are very far away from the $M$-small curves in other isogeny valleys. The sizes and shapes of these valleys are discussed in Appendix A.

\textbf{Motivation.} We say that a supersingular elliptic curve $E$ over $\mathbb{F}_{p^2}$ is \textbf{hard} if it is computationally infeasible to compute its endomorphism ring. A number of applications in cryptography (e.g., [Feo+19]) need an explicit hard curve $E$ where no one, including the party who generated the curve, can compute its endomorphism ring. Currently, there is no known method to generate such a curve.

To illustrate the problem, suppose $p \equiv 2 \pmod{3}$ and let $E_0$ be the supersingular curve with $j$-invariant 0. Let $\ell$ be a small prime. One can generate a large number of supersingular curves by taking a random walk along the graph of degree $\ell$ isogenies, starting at $E_0$. However, every curve $E$ generated this way will have a known endomorphism ring: the endomorphism ring of $E$ can be computed using the isogeny path from $E_0$ to $E$.

Point (a) raises the possibility of using the set of $M$-small supersingular elliptic curves, for some polynomial size $M$, as a candidate set of explicit hard curves. If $E$ is a typical $M$-small curve, then point (e) tells us that $E$ could not reasonably be found by searching from $E_0$ on $\ell$-isogeny graphs for
Figure 1: A graph which illustrates Theorem 1.3. The vertices are supersingular elliptic curves in characteristic $p = 20011$, with conjugate pairs $\{E, E^{(p)}\}$ identified. The 12-small curves are highlighted, and labelled with the smallest degree of a non-integer endomorphism. The square vertex is the curve $y^2 = x^3 + x$ with $j$-invariant 1728. Two curves $E, E'$ are connected by an edge if there is an isogeny $E \rightarrow E'$ of degree 2 or 3 (the primes less than $\frac{1}{2}\sqrt{12}$). The connected components of the $M$-small subgraph correspond to the sets $T_D$ for $D = -4, -7, -11, -24, -35, -20$ (starting from the square and proceeding clockwise). Data computed using Magma [BCP97], plotted using Mathematica [Wol14].
any small primes $\ell$. A priori, this might suggest that it would be difficult to compute the isogeny path from $E_0$ to $E$, and therefore there is hope that the endomorphism ring of $E$ will remain unknown. However, point (f) demonstrates that this is likely not the case.

This suggests that a candidate hard curve should not be $M$-small; by the classification results of Section 2.1, this rules out taking roots of Hilbert class polynomials as a technique for finding hard curves. Constructing an explicit hard supersingular curve remains an open problem.

**Organization.** The content of this paper is as follows. In Section 2, we note that several known examples of supersingular curves are in fact $M$-small for very small values of $M$, and show that an algorithm due to Bröker used to generate supersingular curves will typically output $M$-small curves. We will then see how to generate all such curves by generalizing Bröker’s algorithm.

At this point, we will start to depend on the fact that the endomorphism ring of a supersingular curve is an order in a quaternion algebra. Section 3 will briefly review the necessary background about quaternion algebras and their orders, culminating in the statement of the Deuring correspondence, which gives us a precise dictionary between the world of supersingular curves and the world of maximal orders of a certain quaternion algebra. The material in this section is standard and can be found in other sources.\(^4\)

Sections 4–6 contain the proof of Theorem 1.3. Section 4 lays out the skeleton of the proof; after developing a notion of distance between quaternion orders that is compatible with Definition 1.1 under the Deuring correspondence, we state two key bounds on distances between maximal orders that will imply Theorem 1.3. The first of these, which tells us that certain pairs of maximal orders will be very far apart from each other, is also proven in Section 4. In Section 5 we develop the theory of optimal embeddings of quadratic orders in maximal orders, and use this to prove the second proposition, which allows us to find short paths between certain pairs of maximal orders. Once these propositions have been shown, they can be translated into a proof of Theorem 1.3 via the Deuring correspondence; this is carried out in Section 6.

Finally, in Section 7 (which applies Theorem 1.3 and the topics reviewed in Section 3, but does not depend on the material of Sections 4–6), we discuss an algorithm that finds an isogeny between any two $M$-small supersingular curves, and give an example of its performance for $p \approx 2^{256}$ and $M = 100$. We include bounds on the sizes of various sets of $M$-small curves in Appendix A.

**Acknowledgments.** Thanks to John Voight for fruitful discussion without which we would not have found the algorithms in Section 7, and to Akshay Venkatesh for pointing us towards the key ideas in Section 5. This work was supported by NSF grant #1701567.

## 2 Generating $M$-small curves

Most well-known examples of supersingular curves are all $M$-small for relatively small values of $M$. For instance, supersingular curves with a non-trivial automorphism are 1-small. This includes the curve $y^2 = x^3 + x$ with $j$-invariant 1728 when $p \equiv 3 \pmod{4}$, and the curve $y^2 = x^3 + 1$ with $j$-invariant 0 when $p \equiv 2 \pmod{3}$.

More generally, Bröker in [Brö09] proposes a general algorithm for producing a supersingular curve over an arbitrary finite field. We will discuss the algorithm here, and then see in Section 2.1 how to generalize his approach to generate all $M$-small curves.

Given an imaginary quadratic field $K$, a **quadratic order** $\mathcal{O}$ in $K$ is a subring of $K$ such that the field of fractions of $\mathcal{O}$ is equal to $K$. If $\mathcal{O}_K$ is the ring of integers of $K$, the only quadratic orders in $K$ are of the form $\mathcal{O}_{K,f} := \mathbb{Z} + f\mathcal{O}_K$ for some positive integer $f$, called the **conductor** of the

---

\(^4\)In addition to the papers referenced in the previous footnote, John Voight has a particularly thorough introduction to these concepts in [Voi19].
quadratic order [Cox13, Lemma 7.2]. If $D$ is the discriminant of $K$, then $d := f^2 D$ is the discriminant of $O_{K,f}$ [Cox13, (7.3)] (throughout this paper, we will use $D$ to refer to fundamental discriminants, and $d$ to refer to discriminants of arbitrary quadratic orders). Further, any $d \equiv 0$ or $1$ (mod 4) can be written uniquely as $d = f^2 D$ for $f > 1$ and a fundamental discriminant $D$, so that quadratic orders are uniquely determined by their discriminant. We have $O_{K,f} \subseteq O_{K,g}$ if and only if $g \mid f$.

**Definition 2.1.** Let $O$ be a quadratic order. We say an elliptic curve $E$ has complex multiplication by $O$ if $O$ embeds in $\text{End}(E)$, and there is no quadratic order $O'$ that embeds in $\text{End}(E)$ such that its image strictly contains the image of $O$.

This definition is not standard; often “complex multiplication by $O$” simply means that $O$ embeds into $\text{End}(E)$. For example, if $E$ is an ordinary elliptic curve in characteristic $p$, $E$ has complex multiplication by $O$ in the sense of Definition 2.1 if and only if $\text{End}(E) \cong O$. Elliptic curves with complex multiplication by $O$ can be classified by the roots of a polynomial:

**Definition 2.2.** Let $O$ be a quadratic order. The Hilbert class polynomial $H_O(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial characterized by the following property: $H_O(j) = 0$ if and only if $j$ is the $j$-invariant of an elliptic curve with complex multiplication by $O$ [Cox13, Proposition 13.2].

Bröker’s algorithm [Brö09, Algorithm 2.4] proceeds as follows. To construct a supersingular curve over $\mathbb{F}_p$ with $p \equiv 1 \pmod{4}$, one first finds a prime $q \equiv 3 \pmod{4}$ with Legendre symbol $\left(\frac{-2}{p}\right) = -1$. One can typically find very small values of $q$ satisfying these constraints. The algorithm proceeds by computing the Hilbert class polynomial $H_{O_K}(x) \pmod{p}$ for $K = \mathbb{Q}(\sqrt{-q})$, and finding a root of this polynomial in $\mathbb{F}_p$. The condition $\left(\frac{-2}{p}\right) = -1$ then guarantees that this root is the $j$-invariant of a supersingular curve (Proposition 2.4). This algorithm generates $M$-small curves for a reasonably small value of $M$, as the following proposition shows.

**Proposition 2.3.** The supersingular curves found by Algorithm 2.4 of [Brö09] will be $(\frac{1}{2}+\frac{1}{4})$-small. Assuming GRH, they will be $M$-small for $M = O(\log^2 p)$.

**Proof.** The output of the algorithm will be a curve $\overline{E}$, which is a reduction of a curve $E$ with complex multiplication by $O_K$. In particular, $\frac{1+\sqrt{-7}}{2} \in O_K$ is a non-integer endomorphism of $E$ with norm $\frac{1}{2}+\frac{1}{4}$. The reduction map $\text{End}(E) \to \text{End}(\overline{E})$ is a degree-preserving injection [Sil94, Proposition II.4.4], so $\text{End}(\overline{E})$ also contains a non-integer endomorphism of norm $\frac{1}{2}+\frac{1}{4}$, proving that $\overline{E}$ is $(\frac{1}{2}+\frac{1}{4})$-small.

As discussed in the proof of Lemma 2.5 in [Brö09], under GRH we can find $q = O(\log^2 p)$ with the desired properties. \hfill \Box

### 2.1 Classification of $M$-small curves

A suitable generalization of Bröker’s algorithm [Brö09] can be used to generate the set of all $M$-small curves. Instead of only considering the Hilbert class polynomial $H_{O_K}(x)$, we will consider the set of roots of $H_O(x) \pmod{p}$ for all quadratic orders with discriminant $-4M \leq \text{disc} O < 0$. This set will be the set of $j$-invariants of $M$-small curves (Proposition 2.4), and we will be able to tell supersingular from ordinary by a Legendre symbol calculation as in [Brö09].

Sutherland gives an algorithm for computing $H_O(x) \pmod{p}$ in time $O(\text{disc} O^{1+\varepsilon})$ [Sut11, Theorem 1]. Computing $H_O(x)$ for all quadratic orders of discriminant $-4M \leq d < 0$ can therefore be done in time $O(M^{2+\varepsilon})$.

**Proposition 2.4.** Let $3 \leq M < p$, let $E$ be an elliptic curve over a finite field of characteristic $p$, and let $j$ be the $j$-invariant of $E$. Then $E$ is $M$-small if and only if $H_O(j) = 0 \pmod{p}$ for some quadratic order $O$ with discriminant $-4M \leq \text{disc} O < 0$. Further, $E$ is supersingular if and only if $p$ does not split in the field of fractions of $O$.

\footnotetext[5]{For $p = 2$, the curve $y^2 + y = x^3$ will be supersingular, and for $p \equiv 3 \pmod{4}$ the curve $y^2 = x^3 + x$ will be supersingular.
Proof. First suppose $E$ is $M$-small, and take $\alpha \in \text{End}(E) - \mathbb{Z}$ for which $\deg \alpha \leq M$. By Deuring’s Lifting Theorem [Lan87, Theorem 13.14], there is an elliptic curve $\tilde{E}$ defined over a number field $L$, an endomorphism $\tilde{\alpha}$ of $\tilde{E}$, and a prime $p$ of $L$, such that the reduction of $\tilde{E}$ at $p$ is isomorphic to $E$ and the reduction of $\tilde{\alpha}$ corresponds to $\alpha$ under this isomorphism. Since the map $\text{End}(\tilde{E}) \to \text{End}(E)$ induced by reduction preserves degree [Sil94, Proposition II.4.4], $\tilde{\alpha} \in \text{End}(\tilde{E}) - \mathbb{Z}$ has degree at most $M$. Thus $\text{End}(\tilde{E}) \cong \mathcal{O}$ for some quadratic order $\mathcal{O}$ in an imaginary quadratic field $K$ [Sil94, Corollary III.9.4]. Letting $d = \text{disc}\mathcal{O}$, we will have $\tilde{\alpha} = \frac{a + b\sqrt{d}}{2}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then

$$\frac{|d|}{4} = N_{K/\mathbb{Q}} \left( \sqrt{d} \right) \leq N_{\mathcal{O}/\mathbb{Z}} \left( \frac{a + b\sqrt{d}}{2} \right) = \deg \tilde{\alpha} \leq M,$$

implying $-4M \leq \text{disc}\mathcal{O} < 0$. By definition of the Hilbert class polynomial, this implies that the $j$-invariant $\tilde{j} \in L$ of $\tilde{E}$ is a root of the Hilbert class polynomial $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$. Reducing modulo $p$, we see that $j$ is a root of $H_{\mathcal{O}}(x)$ (mod $p$).

Conversely, suppose $H_{\mathcal{O}}(j) = 0$ (mod $p$) for some quadratic order $\mathcal{O}$ with discriminant $-4M \leq \text{disc}\mathcal{O} < 0$. Let $L/\mathbb{Q}$ be the splitting field of $H_{\mathcal{O}}(x)$, and let $p$ be a prime over $p$ in $L$. Then by considering the reductions mod $p$ of the linear factors of $H_{\mathcal{O}}(x)$, we can conclude that $j$ is the reduction mod $p$ of some $\tilde{j} \in L$ with $H_{\mathcal{O}}(\tilde{j}) = 0$. If $\tilde{E}$ is an elliptic curve over $L$ with $j$-invariant $\tilde{j}$, then $\tilde{E}$ has complex multiplication by $\mathcal{O}$, and its reduction modulo $p$ is isomorphic to $E$. If $d = \text{disc}\mathcal{O}$ is congruent to $0$ (mod $4$), then the element $\tilde{\alpha} := \sqrt{d} \in \mathcal{O}$ satisfies $N_{\mathcal{O}/\mathbb{Z}}(\tilde{\alpha}) = \frac{|d|}{4} \leq M$. If $d \equiv 1$ (mod $4$), then we have $-4M + 1 \leq d$, and the element $\tilde{\alpha} := \frac{1 + \sqrt{d}}{2} \in \mathcal{O}$ satisfies $N_{\mathcal{O}/\mathbb{Z}}(\tilde{\alpha}) = \frac{|d| + 1}{4} \leq M$. Since the map $\text{End}(\tilde{E}) \to \text{End}(E)$ induced by reduction is a degree-preserving injection [Sil94, Proposition II.4.4], the reduction of $\tilde{\alpha}$ in either case gives $\alpha \in \text{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$, so that $E$ is $M$-small.

The fact that $E$ is supersingular if and only if $p$ does not split in the field of fractions of $\mathcal{O}$ is a theorem of Deuring [Lan87, Theorem 13.12].

3 Maximal Orders of Quaternion Algebras

In order to prove further results about $M$-small curves which are supersingular, we will need to review the theory of quaternion algebras. Unless otherwise cited, all the material in this section can be found in [Voi19].

3.1 Quaternion Algebras and Subfields

If $E$ is a supersingular elliptic curve over $\mathbb{F}_p$, its endomorphism ring will be isomorphic to a maximal order in a particular quaternion algebra:

**Lemma 3.1** ([PL17, Proposition 1]). There is a quaternion algebra $B$ over $\mathbb{Q}$, unique up to isomorphism, that ramifies exactly at $p$ and $\infty$. For $p \neq 2$, we can take

$$\mathbb{Q}(i, j, k) := \{w + xi + yj + zk : i^2 = -q, j^2 = -p, ij = -ji = k\},$$

where

- $q = 1$ if $p \equiv 3$ (mod 4);
- $q = 2$ if $p \equiv 5$ (mod 8);
- $q \equiv 3$ (mod 4) is a prime with $\left( \frac{p}{q} \right) = -1$ (that is, $p$ is not a quadratic residue mod $q$) if $p \equiv 1$ (mod 8).

Assuming GRH, we can always take $q = O(\log^2 p)$. 

6
Given $\alpha = w + xi + yj + zk \in B$, we define:

- its **conjugate**, $\overline{\alpha} := w - ix - jy - kZ$. This satisfies the property that $\overline{\overline{\alpha}} = \alpha$, $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, and $\overline{\alpha \beta} = \overline{\alpha} \overline{\beta}$ for all $\alpha, \beta \in B$.
- its **reduced norm**, $\text{nr}(\alpha) := \alpha \overline{\alpha} = w^2 + qx^2 + py^2 + qz^2$.
- its **reduced trace**, $\text{tr}(\alpha) := \alpha + \overline{\alpha} = 2w$.

From these definitions, we see that any $\alpha \notin \mathbb{Q}$ is the root of a polynomial

$$x^2 - \text{tr}(\alpha)x + \text{nr}(\alpha)$$

with rational coefficients, the **minimal polynomial** of $\alpha$. Noting that $\text{tr}(\alpha)^2 - 4\text{nr}(\alpha) < 0$, $\alpha$ generates an imaginary quadratic subfield $\mathbb{Q}(\alpha) \subseteq B$.

It is important to note that $\alpha$ and $\overline{\alpha}$ are not the only roots of this minimal polynomial; indeed, if $\alpha \in B$ and $\gamma \in B - \mathbb{Q}(\alpha)$, then $\gamma^{-1}\alpha\gamma$ will typically not lie in $\mathbb{Q}(\alpha)$, but will satisfy the same minimal polynomial $x^2 - \text{tr}(\alpha)x + \text{nr}(\alpha)$ and will hence generate a distinct but isomorphic subfield. Fortunately, the following result (a consequence of the Skolem-Noether Theorem) tells us that all the roots are related in this way:

**Theorem 3.2 ([Voi19, Corollary 7.7.3]).** $\alpha$ and $\beta$ satisfy the same minimal polynomial if and only if there exists $\gamma \in B$ such that $\gamma^{-1}\alpha\gamma = \beta$.

In particular, given any two isomorphic subfields, applying this theorem to the generators shows that there is an automorphism of $B$ that takes one subfield onto the other. An imaginary quadratic field $K$ embeds into $B$ if and only if $p$ does not split in $K$ [Voi19, Proposition 14.6.7], which is equivalent to requiring that the Legendre symbol $\left(\frac{D}{p}\right)$ is not equal to 1, where $D$ is the discriminant of $K$.

### 3.2 Ideals and Orders

An **ideal** $I \subseteq B$ is a subgroup under addition which is generated by a basis of $B$ considered as a vector space over $\mathbb{Q}$. An **order** $\mathcal{O} \subseteq B$ is an ideal which contains 1 and is closed under multiplication (and is hence a subring of $B$). An element $\alpha \in B$ with $\text{tr}(\alpha), \text{nr}(\alpha) \in \mathbb{Z}$ is called **integral**: $\alpha$ is integral if and only if it is contained in some order of $B$.

Given an ideal $I \subseteq B$, we can define **left and right orders of $I$**, $\mathcal{O}_L(I) := \{x \in B : xI \subseteq I\}$, $\mathcal{O}_R(I) := \{x \in B :Ix \subseteq I\}$. We say that $I$ is a **left ideal of $\mathcal{O}$** if $\mathcal{O}_L(I) = \mathcal{O}$, and that $I$ is a **right ideal of $\mathcal{O'}$** if $\mathcal{O}_R(I) = \mathcal{O'}$. In this scenario we say $I$ **links $\mathcal{O}$ to $\mathcal{O'}$**.

An ideal $I$ that is closed under multiplication is called an **integral ideal**. An integral ideal is necessarily contained in its left and right orders, and hence $\text{nr}(\alpha) \in \mathbb{Z}$ for all $\alpha$ in an integral ideal. Given an integral ideal $I \subseteq B$, the **reduced norm** of $I$ is defined to be

$$\text{nr}(I) := \gcd\{\text{nr}(\alpha) \mid \alpha \in I\}.$$ 

Observe that $I \subseteq J$ implies $\text{nr}(J) | \text{nr}(I)$.

An order is **maximal** if there are no orders properly containing it. Unlike number fields, for which the ring of integers is the unique maximal order, a quaternion algebra will typically have many distinct maximal orders.

Given a quadratic order $\mathcal{O}$ and a maximal order $\mathcal{D} \subseteq B$ we say that $\mathcal{O}$ is **optimally embedded** in $\mathcal{D}$ if $\mathcal{O} \cong \mathcal{D} \cap K$ for some subfield $K \subseteq B$. 


3.3 The Deuring Correspondence

(See Chapter 42 of [Voi19] for details.)

Let \( \mathcal{S} \subseteq \mathbb{F}_p^2 \) denote the set of \( j \)-invariants of supersingular curves. Given \( j \in \mathcal{S} \), \( \text{End}(E_j) \) will be isomorphic to a maximal order in \( B \). If \( j \) and \( j^p \) are \( \mathbb{F}_p^2 \)-conjugates, then \( \text{End}(E_j) \) and \( \text{End}(E_{j^p}) \) will be isomorphic orders. Aside from this relation, non-isomorphic curves will always have non-isomorphic endomorphism rings. In fact, we have a bijection, known as the Deuring correspondence:

\[
\mathcal{S} / (j \mapsto j^p) \leftrightarrow \{ \text{maximal orders of } B \} / \equiv
\]

sending \( j \) to the endomorphism ring of \( E_j \). The degree (resp. trace, resp. dual) of an endomorphism is equal to the norm (resp. trace, resp. conjugate) of the corresponding element of \( B \), and composition of endomorphisms corresponds to multiplication of elements of \( B \). Further, suppose we fix a maximal order \( \mathfrak{O}_j \) associated to \( \text{End}(E_j) \) for some \( j \). Then we have a one-to-one correspondence

\[
\{ \text{separable isogenies out of } E_j \} / \equiv \leftrightarrow \{ \text{left ideals of } \mathfrak{O}_j \}.
\]

An isogeny \( \phi : E_j \to E' \) will correspond to an ideal \( I \) linking \( \mathfrak{O}_j \) to some maximal order \( \mathfrak{O}_{j'} \) isomorphic to \( \text{End}(E') \) (that is, \( I \) is a left \( \mathfrak{O}_j \)-ideal and a right \( \mathfrak{O}_{j'} \)-ideal), and \( \deg \phi = \text{nrd}(I) \).

4 Distance Between Maximal Orders

4.1 Definitions for Maximal Orders

In order to use the Deuring correspondence to express Theorem 1.3 in the language of maximal orders, we must have a notion of \( M \)-small and a notion of distance for maximal orders. The first of these is straightforward:

**Definition 4.1.** An order \( \mathfrak{O} \subseteq B \) is **\( M \)-small** if there exists \( \alpha \in \mathfrak{O} - \mathbb{Z} \) with \( \text{nrd}(\alpha) \leq M \).

A supersingular curve is \( M \)-small if and only if its endomorphism ring is an \( M \)-small maximal order.

Our next task is to come up with a definition of distance between maximal orders that is compatible with Definition 1.1.

**Lemma 4.2.** If \( \mathfrak{O}, \mathfrak{O}' \subseteq B \) are maximal orders, the following quantities are all equal:

(a) \( |\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'| \) (the index of \( \mathfrak{O} \cap \mathfrak{O}' \) in \( \mathfrak{O} \)).

(b) \( |\mathfrak{O}' : \mathfrak{O} \cap \mathfrak{O}'| \) (the index of \( \mathfrak{O} \cap \mathfrak{O}' \) in \( \mathfrak{O}' \)).

(c) The smallest reduced norm of an integral ideal linking \( \mathfrak{O} \) to \( \mathfrak{O}' \).

**Proof.** Lemma 8 of [Koh+14] tells us (a) and (b) are equal to a common integer \( d \), and that the ideal

\[
I(\mathfrak{O}, \mathfrak{O}') := \{ \alpha \in B_{p, \infty} | \alpha \mathfrak{O}' \mathfrak{O} \subseteq d \mathfrak{O} \}
\]

is an integral ideal linking \( \mathfrak{O} \) to \( \mathfrak{O}' \) with reduced norm \( d \); this proves (c) \( \leq \) (a) = (b).

Now let \( I \) be any integral ideal linking \( \mathfrak{O} \) to \( \mathfrak{O}' \). If \( I \) is a subset of \( n \mathfrak{O} \), then \( \frac{1}{n} I \) is still an integral ideal linking \( \mathfrak{O} \) to \( \mathfrak{O}' \), with smaller reduced norm. Hence, the \( I \) of smallest reduced norm must not be a subset of \( n \mathfrak{O} \) for any \( n > 1 \). But Lemma 8 of [Koh+14] then tells us that \( I = I(\mathfrak{O}, \mathfrak{O}') \), so \( d = \text{nrd}(I(\mathfrak{O}, \mathfrak{O}')) \) is the smallest reduced norm of an integral ideal linking \( \mathfrak{O} \) to \( \mathfrak{O}' \).

**Definition 4.3.** The **distance from \( \mathfrak{O} \) to \( \mathfrak{O}' \)**, \( d(\mathfrak{O}, \mathfrak{O}') \), is any of the equivalent quantities in Lemma 4.2.
By definition, we have
\[ d(\mathcal{O}, \mathcal{O}) = 1, \quad d(\mathcal{O}, \mathcal{O}') = d(\mathcal{O}', \mathcal{O}). \]
For any maximal orders \( \mathcal{O}, \mathcal{O}', \) and \( \mathcal{O}'' \), \( I(\mathcal{O}, \mathcal{O}')I(\mathcal{O}', \mathcal{O}'') \) is an integral ideal linking \( \mathcal{O} \) to \( \mathcal{O}'' \). Since \( \text{nr}(I) \leq \text{nr}(J) \) for any ideals \( I \) and \( J \) [Voi19, p. 226], we have
\[ d(\mathcal{O}, \mathcal{O}'') \leq \text{nr}(I(\mathcal{O}, \mathcal{O}')I(\mathcal{O}', \mathcal{O}'')) \leq d(\mathcal{O}, \mathcal{O}')d(\mathcal{O}', \mathcal{O}''). \]
We can compare distances between elliptic curves and distances between maximal orders as follows:

**Lemma 4.4.** Let \( E \) and \( E' \) be supersingular curves. Then
\[ d(E, E') = \min \{d(\mathcal{O}, \mathcal{O}') | \mathcal{O} \cong \text{End}(E), \mathcal{O}' \cong \text{End}(E')\}. \]

**Proof.** By the Deuring correspondence, both sides are equal to
\[ \min \{\deg \phi | \phi : E \to E'' \text{ for some } E'' \text{ with } \text{End}(E'') \cong \text{End}(E')\}. \]

### 4.2 Two Key Propositions

Suppose that \( \mathcal{O} \) and \( \mathcal{O}' \) are each \( M \)-small maximal orders in \( B \). Let \( \alpha \in \mathcal{O} - \mathbb{Z} \) and \( \alpha' \in \mathcal{O}' - \mathbb{Z} \) each have reduced norm at most \( M \). We will show that the distance from \( \mathcal{O} \) to \( \mathcal{O}' \) is small if \( \mathbb{Q}(\alpha) \) is isomorphic to \( \mathbb{Q}(\alpha') \), and is large otherwise. Precisely, we have the following:

**Proposition 4.5.** If \( \mathbb{Q}(\alpha) \not\cong \mathbb{Q}(\alpha') \), then \( d(\mathcal{O}, \mathcal{O}')^4 \geq \frac{p}{4M^2} \).

**Proposition 4.6.** If \( \mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha') \), then there exists a sequence of (not necessarily distinct) maximal orders
\[ \mathcal{O} = \mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_r \cong \mathcal{O}' \]
 such that

- the distance between two consecutive terms is at most \( \frac{1}{\pi} \sqrt{M} \), and
- each \( \mathcal{O}_i \) contains an element with the same minimal polynomial as either \( \alpha \) or \( \alpha' \).

We can find such a sequence with \( r \leq 3 \), or alternatively we can find such a sequence such that consecutive orders are linked by an ideal of prime norm at most \( \frac{1}{\pi} \sqrt{M} \).

Proposition 4.5 will be in Section 4.3, and Proposition 4.6 will be proven in Section 5.

Before we continue, we note that in order to prove each of these propositions, we will study lattice structures at very different scales. The “large-scale” viewpoint, used to prove Proposition 4.5, depends on the fact that orders in \( B \) are 4-dimensional lattices with large discriminant [Voi19, p. 208] and uses lattice geometry to deduce facts about sizes of elements. On the other hand, the “small-scale” viewpoint, used to prove Proposition 4.6, zooms in on the quadratic orders that contain small non-integer elements, and studies 2-dimensional lattices of small discriminant related to these quadratic orders. For a different example of how each of these viewpoints can be applied, see Proposition A.5.

### 4.3 Proof of Proposition 4.5

We quote a theorem due to Kaneko that leverages the large-scale structure of orders:

**Theorem 4.7.** [Kan89, Theorem 2'] Let \( \mathcal{O} \subseteq B \) be an order.\(^6\) If \( \mathcal{O} \) and \( \mathcal{O}' \) are quadratic orders of distinct imaginary quadratic fields and both optimally embed into \( \mathcal{O} \), then \( \text{disc} \mathcal{O} \text{disc} \mathcal{O}' \geq 4p \).

\(^6\)In [Kan89] the theorem requires \( \mathcal{O} \) to be maximal; however, this is not used anywhere in the proof.
The proof proceeds by explicitly computing the discriminant of the suborder generated by \( \mathcal{O} \) and \( \mathcal{O}' \); noting that it must be a multiple of \( p^2 \) gives the desired inequality. Using this, we can prove our first bound.

**Proof of Proposition 4.5.** Consider the order \( \mathfrak{O} \cap \mathfrak{O}' \). Let

\[
\mathfrak{O} := \mathbb{Q}(\alpha) \cap (\mathfrak{O} \cap \mathfrak{O}') \quad \text{and} \quad \mathfrak{O}' := \mathbb{Q}(\alpha') \cap (\mathfrak{O} \cap \mathfrak{O}')
\]

both be optimally embedded; since \( \mathbb{Q}(\alpha) \not\cong \mathbb{Q}(\alpha') \), Theorem 4.7 implies that \( \text{disc } \mathfrak{O} \text{ disc } \mathfrak{O}' \geq 4p \).

Now let \( n \) be the smallest positive integer such that \( n\alpha \in \mathfrak{O} \cap \mathfrak{O}' \), and \( n' \) the minimal positive integer such that \( n'\alpha' \in \mathfrak{O} \cap \mathfrak{O}' \). Let \( \mathcal{D} \) denote the discriminant of \( \mathbb{Q}(\alpha) \). Since \( n\alpha \in \mathcal{O} - \mathbb{Z} \), and the quadratic order \( \mathcal{O} \) must be of the form \( \mathcal{O} = \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{\mathcal{D}})} \) for some positive integer \( f \), we have

\[
n^2 \text{nrd}(\alpha) = \text{nrd}(n\alpha) \geq \text{nrd} \left( \frac{\sqrt{\mathcal{D}}}{2} \right) = \frac{f^2 \mathcal{D}}{4} = \frac{1}{4} \text{ disc } \mathcal{O}.
\]

Likewise we have \( n'^2 \text{nrd}(\alpha') \geq \frac{1}{4} \text{ disc } \mathcal{O}' \).

Without loss of generality, suppose \( n \geq n' \). Since \( \alpha \) has order \( n \in \mathfrak{O} \), the index of \( \mathfrak{O} \cap \mathfrak{O}' \) in \( \mathfrak{O} \) is at least \( n \), and so

\[
d(\mathfrak{O}, \mathfrak{O}')^4 = |\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'|^4 \geq n^4 \geq n^2 n'^2 \geq \frac{\text{disc } \mathfrak{O} \text{ disc } \mathfrak{O}'}{16 \text{nrd}(\alpha) \text{nrd}(\alpha')} \geq \frac{p}{4M^2}. \quad \square
\]

## 5 Optimal Embeddings

We now move on the studying the small-scale structure of maximal orders. Let \( K \) be an imaginary quadratic field of discriminant \( \mathcal{D} \), and let two maximal orders \( \mathfrak{O}, \mathfrak{O}' \) of \( B \) each admit an optimal embedding of some quadratic order of \( K \). If these optimally embedded quadratic orders both have small discriminant, our goal is to construct a sequence of maximal orders from \( \mathfrak{O} \) to \( \mathfrak{O}' \) such that the distance between two consecutive orders is small.

To do this, we will need to consider two types of relationships between orders. If two maximal orders have the same quadratic order optimally embedded in each, we call the relationship between them a **horizontal step:** if the optimally embedded orders are not equal, the relationship is called a **vertical step.**

Let \( \mathfrak{O} \) be a maximal order, and \( \mathfrak{O} \) a quadratic order of \( K \) optimally embedded in \( \mathfrak{O} \). We will see that both horizontal and vertical steps from \( \mathfrak{O} \) can be taken by considering some lattice \( \Lambda \subseteq K \), and using the ideal \( \{ x \in \mathfrak{O} \mid x\Lambda \subseteq \mathfrak{O} \} \) to link \( \mathfrak{O} \) to another maximal order. For horizontal steps we will let \( \Lambda \) be an ideal of \( \mathfrak{O} \) (Theorem 5.1), and for vertical steps we will let \( \Lambda \) be a quadratic order containing \( \mathfrak{O} \) (Lemma 5.4).

### 5.1 Horizontal Steps

First we consider the case in which the same \( K \)-order \( \mathcal{O} \) is optimally embedded in two maximal orders \( \mathfrak{O} \) and \( \mathfrak{O}' \). For this we will use a version of the Chevalley-Hasse-Noether Theorem proved by Eichler:

**Theorem 5.1 ([Eic55, Satz 7]).** Let \( \mathfrak{O}, \mathfrak{O}' \subseteq B \) be two maximal orders, and suppose

\[
\mathcal{O} \cong K \cap \mathfrak{O} = K \cap \mathfrak{O}'
\]

7The terminology is meant to draw a comparison with isogeny graphs of ordinary elliptic curves, in which there are horizontal isogenies which preserve the endomorphism ring and vertical isogenies which change it [Sut12].

8The original theorem, published independently by Chevalley [Che34], Hasse [Has34], and Noether [Noc34] in 1934, is at once more general (\( B \) may be replaced with any central simple algebra) and less general (the optimally embedded \( K \)-order must be the full ring of integers of \( K \)) than Eichler’s version, as Eichler discusses in a footnote [Eic55, p. 134]. Eichler’s version is in fact slightly more general than what is stated here, replacing maximal orders with orders of squarefree level.
is optimally embedded in each. Then there is an invertible ideal \( a \) of \( \mathcal{O} \) such that \( \mathcal{O}a = a\mathcal{O}' \).\(^9\)

The proof uses a local-global principle for orders in quaternion algebras. After setting up an appropriate theory of localization, Eichler finds an element \( \alpha_\ell \in K_\ell \) such that \( \mathcal{O}_\ell \alpha_\ell = \alpha_\ell \mathcal{O}'_\ell \) for each prime \( \ell \), and concludes that there is an ideal \( a \) which localizes to \( \alpha_\ell \mathcal{O}_\ell \) for all \( \ell \).

Observe that \( \mathcal{O}a = a\mathcal{O}' \) is an ideal linking \( \mathcal{O} \) to \( \mathcal{O}' \), and since \( a \subseteq \mathcal{O} \) we can equivalently describe this ideal as \( \{ x \in \mathcal{O} \mid xa^{-1} \subseteq \mathcal{O} \} \). Using this theorem, we will show that the distance between orders related by a horizontal step can be bounded in terms of norms of ideals of the common optimally embedded order \( \mathcal{O} \).

**Lemma 5.2.** Let \( K \) be an imaginary quadratic field of discriminant \( D \). Let \( \mathcal{O}, \mathcal{O}' \subseteq B \) be maximal orders, and suppose \( \mathcal{O} := \mathcal{O}_{K,f} \) optimally embeds into each. Then there exists an automorphism \( \phi : B \to B \) such that

\[
d(\mathcal{O}, \phi(\mathcal{O}')) \leq \frac{2}{\pi} f|\sqrt{D}|.
\]

**Proof.** By the Skolem-Noether theorem (Theorem 3.2), there exists some \( \gamma \in B \) such that

\[
\mathcal{O} = \mathcal{O} \cap K = \gamma^{-1}\mathcal{O}'\gamma \cap K.
\]

Then by Theorem 5.1, there exists an invertible ideal \( a \) of \( \mathcal{O} \) such that \( \mathcal{O}a = a(\gamma^{-1}\mathcal{O}'\gamma) \). We can find an ideal \( b \) in the same ideal class as \( a \) (so \( b = a\delta \) for some \( \delta \in K \)) with \( N_{\mathcal{O}/\mathbb{Z}}(b) \leq \frac{2}{\pi} f|\sqrt{D}| \) by Minkowski’s bound [Ste17, Theorem 5.4]. Then

\[
\mathcal{O}b = \mathcal{O}a\delta = a(\gamma^{-1}\mathcal{O}'\gamma)\delta = (b\delta^{-1})(\gamma^{-1}\mathcal{O}'\gamma)\delta = b\phi(\mathcal{O}'),
\]

where \( \phi : B \to B \) is the inner automorphism \( \phi(x) := (\gamma\delta)^{-1}x(\gamma\delta) \). Hence \( \mathcal{O}b = b\phi(\mathcal{O}') \) is an ideal linking \( \mathcal{O} \) to \( \phi(\mathcal{O}') \). We have

\[
\text{nrd}(\mathcal{O}b) = \gcd\{\text{nrd}(x) \mid x \in \mathcal{O}b\} \leq \gcd\{N_{\mathbb{K}/\mathbb{Q}}(x) \mid x \in b\} = N_{\mathbb{K}/\mathbb{Q}}(b) \leq \frac{2}{\pi} f|\sqrt{D}|,
\]

which gives an upper bound on \( d(\mathcal{O}, \phi(\mathcal{O}')) \).

**Remark 5.3.** One can prove this result directly on the elliptic curve side of the Deuring correspondence, without using the Chevalley-Hasse-Noether Theorem. Namely, if \( \mathcal{O} \cong \text{End}(E) \) and \( \mathcal{O}' \cong \text{End}(E') \), we can use Deuring’s Lifting Theorem [Lan87, Theorem 13.14] to lift \( E \) and \( E' \) to curves \( \tilde{E} \) and \( \tilde{E}' \) over a number field \( L \), each of which have complex multiplication by \( \mathcal{O} \). Then \( \text{Cl}(\mathcal{O}) \) acts transitively on these curves [Sil94, Proposition II.1.2], with an integral ideal \( a \) yielding an isogeny \( \tilde{E} \to \tilde{E}' \) of degree \( N_{\mathbb{K}/\mathbb{Q}}(a) \) [Sil94, Corollary II.1.5], which can be bounded as above by Minkowski’s bound. Reduction preserves degree of isogenies [Sil94, Proposition II.4.4], so that the distance from \( E \) to \( E' \) is at most \( \frac{2}{\pi} f|\sqrt{D}| \). This implies the desired upper bound on distance between \( \mathcal{O} \) and \( \phi(\mathcal{O}') \) for some automorphism \( \phi \) of \( B \) by Lemma 4.4.

However, it is less clear from this approach how the full endomorphism rings of \( E \) and \( E' \) are related. The advantage of proving the result using the Chevalley-Hasse-Noether Theorem is that it provides an explicit ideal linking two maximal orders that are related by a horizontal step.

### 5.2 Vertical Steps

Now we must determine how to step between maximal orders that have different quadratic orders optimally embedded into each. If a quadratic order \( \mathcal{O} \neq \mathcal{O}_K \) optimally embeds into a maximal order \( \mathcal{O} \), the following lemma explicitly constructs a new maximal order with an optimally embedded quadratic order of smaller conductor.

---

\(^9\)Eichler simply states that there must exist an ideal \( a \) of \( \mathcal{O} \) with \( \mathcal{O}a = a\mathcal{O}' \). However, in his definition of ideals, he adds a local condition that guarantees invertibility: “Unter einem \( \mathcal{O} \)-Ideal verstehen wir den Durchschnitt von \( \mathcal{O}_p \)-Idealen \( \mathfrak{a}_p = \mathcal{O}_p \mathfrak{a}_p \) mit irgendwelchen \( \mathfrak{a}_p \neq 0 \in \mathcal{O}_p \) für alle \( p \) wobei höchstens endlich viele \( \mathfrak{a}_p \neq \mathfrak{O}_p \) sein sollen (für \( \mathfrak{O}_p \) vgl. (8)). Bei dieser Fassung des Idealebegriffs bilden die \( \mathcal{O} \)-I Ideale für eine beliebige Ordnung \( \mathcal{O} \) eine Gruppe” [Eic56, p. 133].
Lemma 5.4. Let $f$ be a positive integer and $\ell$ a prime. Let $\mathfrak{O} \subseteq B$ be a maximal order in which $O_{K, f}$ optimally embeds. Then there exists a maximal order $\mathfrak{O}'$ in which $O_{K, f}$ optimally embeds, with $d(\mathfrak{O}, \mathfrak{O}') = \ell$.

Proof. Let $K \subseteq B$ be the subfield $O_{K, f}$ embeds into, and let $\omega \in K$ denote a generator of the ring of integers of $K$. Setting $\beta = f\omega$, we have $\mathbb{Z}[\beta] \cong O_{K, f}$ and $\mathbb{Z}[\ell\beta] \cong O_{K, f}$; hence $\ell\beta \in \mathfrak{O}$ but $\beta \notin \mathfrak{O}$. Let

$$I = \{x \in \mathfrak{O} \mid x\beta \in \mathfrak{O}\}.$$ 

$I$ is a left ideal of $\mathfrak{O}$ (that is, $\mathfrak{O}I = I$), because for any $y \in \mathfrak{O}$ and $x \in I$, we have $yx \in \mathfrak{O}$ and $(yx)\beta = y(x\beta) \in \mathfrak{O}$, proving that $yx \in I$. $I$ contains $\ell\mathfrak{O}$, because for any $\ell x \in \ell\mathfrak{O}$, we have $\ell x\beta = x(\ell\beta) \in \mathfrak{O}$. However, this containment is proper, because $\ell\beta \in \mathfrak{O} - \ell\mathfrak{O}$, but

$$\ell\beta^2 = \text{trd}(\ell\beta) - \ell \text{nr}(\beta) \in \mathfrak{O}$$

so $\ell\beta \in I$. Hence we have strict containments $\ell\mathfrak{O} \subsetneq I \subsetneq \mathfrak{O}$. Since $\text{nr}(\ell\mathfrak{O}) = \ell^2$, this implies $\text{nr}(I) = \ell$.

Now let $\mathfrak{O}'$ be the right order of $I$. Observe that $\beta \in \mathfrak{O}'$, because if $x \in I$ then $x\beta \in \mathfrak{O}$ and

$$x\beta^2 = \text{trd}(\beta)(x\beta) - \text{nr}(\beta)x \in \mathfrak{O},$$

showing that $x\beta \in I$. Hence $O_{K, f}$ embeds into $\mathfrak{O}'$.

To show $O_{K, f}$ optimally embeds into $\mathfrak{O}'$, suppose $O_{K, k}$ also embeds for some $k \mid f$. The element $k\omega \in O_{K, k}$ will reduce to an element of order $\frac{\ell\beta}{k}$ in $\mathfrak{O}'/I$, because the smallest multiple of $\omega$ in $I$ is $\ell\beta \omega = \ell\beta$. By $[\mathfrak{O}' : I] = \text{nr}(I)^2 = \ell^2$, see [Vo19, Theorem 16.1.3,], we must have $\frac{\ell\beta}{k} \in \{1, \ell, \ell^2\}$ by Lagrange’s Theorem, and since we assumed $k \mid f$ we have either $k = f$ or $\ell k = f$. Suppose $\ell k = f$, and let $x \in \mathfrak{O} - I$, so $x\beta \notin \mathfrak{O}$. Since $\ell x \in I$ and $k\omega \in \mathfrak{O}'$, we must have

$$(\ell x)(k\omega) = x(f\omega) = x\beta \in I \subsetneq \mathfrak{O},$$

a contradiction. Hence $k = f$, proving that $O_{K, f}$ is optimally embedded in $\mathfrak{O}'$. $\square$

Corollary 5.5. Let $f$ be a positive integer, and $\mathfrak{O} \subseteq B$ be a maximal order in which $O_{K, f}$ optimally embeds. Then there exists a maximal order $\widetilde{\mathfrak{O}}$ in which $O_{K}$ optimally embeds, with $d(O_{\mathfrak{O}}, \widetilde{\mathfrak{O}}) = f$.

Proof. Factor $f = \ell_1 \cdots \ell_k$ into primes, and set $f_i = \ell_{i+1} \cdots \ell_k$ (so $f_0 = f$ and $f_k = 1$). Apply Lemma 5.4 successively, obtaining maximal orders $\mathfrak{O} = \mathfrak{O}_0, \mathfrak{O}_1, \ldots, \mathfrak{O}_k = \mathfrak{O}$, where $O_{K, f_i}$ optimally embeds in $\mathfrak{O}_i$. Then

$$d(\mathfrak{O}, \widetilde{\mathfrak{O}}) \leq \prod_{i=1}^{k} d(\mathfrak{O}_{i-1}, \mathfrak{O}_i) = \prod_{i=1}^{k} \ell_i = f.$$ 

$\square$

5.3 Proof of Proposition 4.6

We are now ready to combine our vertical and horizontal steps to create a path between two maximal orders $\mathfrak{O}$ and $\mathfrak{O}'$. From each of these two orders, we will take vertical steps to an order which has the ring of integers embedded; the two resulting orders will then be separated by horizontal steps.

Let $D$ denote the discriminant of $Q(\alpha) \cong Q(\alpha')$, and suppose $\mathfrak{O} \cap Q(\alpha) \cong O_{K, f}$ and $\mathfrak{O}' \cap Q(\alpha') \cong O_{K, g}$ are optimally embedded orders. We start by computing a few inequalities. Notice that any element of $O_{K, f} - Z$ will have norm at least that of $f\sqrt{D}$, so

$$\frac{f^2 |D|}{4} = N_{Q(\sqrt{D})/Q} \left(\frac{f \sqrt{D}}{2}\right) \leq \text{nr}(\alpha) \leq M,$$

which implies $f \leq \sqrt{\frac{4M}{|D|}}$.

Since $\sqrt{\frac{4}{|D|}} \leq \frac{4}{f}$ for all negative fundamental discriminants ($D \leq -3$), we in fact have $f \leq \frac{4}{\sqrt{2}} \sqrt{M}$. The same bound clearly holds for $g$. 

12
Likewise, any element of $\mathcal{O}_K - \mathbb{Z}$ will have norm at least that of $\frac{\sqrt{D}}{2}$, so

$$\frac{|D|}{4} = N_{\mathbb{Q}(\sqrt{p})/\mathbb{Q}}\left(\frac{\sqrt{D}}{2}\right) \leq \text{nr}(\alpha) \leq M,$$

which implies $|D| \leq 4M$.

To begin constructing the path, take a vertical step from each of $\mathcal{O}$ and $\mathcal{O}'$ using Corollary 5.5: there are maximal orders $\mathcal{O}$ and $\mathcal{O}'$ into which $\mathcal{O}_K$ optimally embeds with $d(\mathcal{O}, \mathcal{O}) \leq f$ and $d(\mathcal{O}', \mathcal{O}') \leq g$. Now take a horizontal step using Lemma 5.2: there is an automorphism $\phi: B \to B$ such that

$$d(\mathcal{O}, \phi(\mathcal{O}')) \leq \frac{2}{\pi} \sqrt{|D|} \leq \frac{4}{\pi} \sqrt{M}.$$ 

This gives us a sequence

$$\mathcal{O}, \mathcal{O}, \phi(\mathcal{O}'), \phi(\mathcal{O}') \cong \mathcal{O}'$$

with consecutive distances bounded above by $\frac{2}{\pi} \sqrt{M}$. Since the optimally embedded order only became larger with each vertical step, each of these orders contains an element with the same minimal polynomial as $\alpha$ or $\alpha'$. This settles the $r \leq 3$ case of the Proposition.

If instead we want all consecutive terms to be linked by ideals of prime norm, we can break up each step into smaller ones. For the vertical steps, rather than stepping all the way down to orders with $\mathcal{O}_K$ optimally embedded, we can factor $f$ and $g$ into primes and take one step for each prime, as in the proof of Corollary 5.5.

We can also break down the horizontal step in a similar way. Following the proof of Lemma 5.2, first factor $b$ into prime ideals $p_1 \cdots p_s$. Set $\mathcal{O}_0 = \mathcal{O}$, and for each $i = 1, \ldots, s$, recursively define

$$\mathcal{O}_i := p_i^{-1} \mathcal{O}_{i-1} p_i.$$ 

Then $\mathcal{O}_K$ is optimally embedded in each $\mathcal{O}_i$, and consecutive orders $\mathcal{O}_{i-1}$ and $\mathcal{O}_i$ are linked by the ideal $\mathcal{O}_{i-1} p_i = p_i \mathcal{O}_i$ of norm $N_{\mathcal{O}/\mathbb{Q}}(p_i)$. If we assume $b$ was chosen to be minimal, none of the $p_i$ can be principal, and so they will all have prime norm. \(\square\)

6 Proof of Theorem 1.3

6.1 Existence of Partition

Recall that we defined $S \subseteq \mathbb{F}_{p^2}$ to be the set of all $j$-invariants of supersingular curves. For each fundamental discriminant $-4M \leq D < 0$ which is not congruent to a square mod $p$ (that is, for which the Legendre symbol $\left(\frac{D}{p}\right)$ is equal to $-1$), set

$$T_D := \{ j \in S : \mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D}) \text{ for some } \alpha \in \text{End}(E_j) - \mathbb{Z}, \deg \alpha \leq M \}.$$ 

We must prove that the sets $T_D$ are disjoint, nonempty, and that every $j \in S_M$ is in some $T_D$.

If $j \in T_D \cap T_{D'}$, then $\text{End}(E_j)$ contains elements $\alpha, \alpha'$ generating nonisomorphic subfields, each with degree at most $M$. Applying Proposition 4.5 to $D = \mathcal{O}' \cong \text{End}(E_j)$, we obtain $1 = d(\mathcal{O}, \mathcal{O})^4 \geq \frac{64}{3\pi^2 M^2}$, contradicting $p > 3\pi^2 M^2$. Hence the sets $T_D$ are all disjoint.

For any $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$, we can construct an integral element $\alpha \in \mathbb{Q}(\sqrt{D}) - \mathbb{Q}$ with $\text{nr}(\alpha) \leq M$:

- If $D \equiv 0 \pmod{4}$, take $\alpha = \frac{\sqrt{D}}{2}$; this has norm $\frac{-D}{4} \leq M$.
- If $D \equiv 1 \pmod{4}$, take $\alpha = \frac{1+\sqrt{D}}{2}$; in this case $D \geq -4M + 1$, so $\alpha$ has norm $\frac{1-D}{4} \leq M$. 

13
Given a supersingular elliptic curve $E$ shows that the sequence $Q_r$ with orders linked by an ideal of prime order. In the first case, we would have a sequence of $j_4$ with consecutive distances bounded by $\alpha$. By the Deuring correspondence, this order is isomorphic to $\text{End}(E_j)$ for some $j \in S$. Hence there is an embedding $\iota : \mathbb{Z}[\alpha] \to \text{End}(E_j)$, so $j$ is $M$-small. Since $\mathbb{Q}(\iota(\alpha)) \cong \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D})$, we have $j \in T_D$, and so $T_D$ is nonempty.

Suppose $j \in S_M$, so there exists $\alpha \in \text{End}(E_j) - \mathbb{Z}$ with $\deg(\alpha) \leq M$. As an element of a quaternion algebra, $\alpha$ must satisfy a minimal polynomial $x^2 - tx + \deg(\alpha)$ with $t^2 - 4 \deg(\alpha) < 0$; by $\deg(\alpha) \leq M$ we in fact have $-4M \leq t^2 - 4 \deg(\alpha) < 0$. Dividing by perfect square factors does not affect these inequalities, and so the discriminant $D$ of $\mathbb{Q}(\alpha)$ must be in the range $-4M \leq D < 0$. Since $\mathbb{Q}(\alpha)$ embeds into $B$ and $D < p$ we must have $(D/p) = -1$. Hence $j$ is in $T_D$ for some $D$.

### 6.2 Distance between $T_D$ and $T_{D'}$

Suppose $j \in T_D$ and $j' \in T_{D'}$ for $D \neq D'$. Take any $\mathcal{O} \cong \text{End}(E_j)$ and $\mathcal{O}' \cong \text{End}(E_{j'})$. By Proposition 4.5, $d(\mathcal{O}, \mathcal{O}')^4 \geq \frac{p^{1/4}}{\sqrt{2M}}$. Since this holds for any such $\mathcal{O}$ and $\mathcal{O}'$, Lemma 4.4 tells us that

$$d(j, j') = \min \{d(\mathcal{O}, \mathcal{O}') \mid \mathcal{O} \cong \text{End}(E_j), \mathcal{O}' \cong \text{End}(E_{j'})\} \geq \frac{p^{1/4}}{\sqrt{2M}}.$$

### 6.3 Distances within $T_D$

Suppose $j, j' \in T_D$, and let $\alpha, \alpha'$ be the corresponding small non-integer endomorphisms with $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha') \cong \mathbb{Q}(\sqrt{D})$. By Proposition 4.6, there exists a chain

$$\text{End}(E_j) \cong \mathcal{O}_0, \mathcal{O}_1, \ldots, \mathcal{O}_r \cong \text{End}(E_{j'})$$

with consecutive distances bounded by $\frac{2}{\pi} \sqrt{M}$, and each containing an element with the same minimal polynomial as either $\alpha$ or $\alpha'$.

Now set $j_0 := j, j_r := j'$, and for each $i = 1, \ldots, r - 1$, set $j_i$ so that $\text{End}(E_{j_i}) \cong \mathcal{O}_i$. By Lemma 4.4, for $i = 1, \ldots, r$ we have

$$d(E_{j_{i-1}}, E_{j_i}) \leq d(\mathcal{O}_{i-1}, \mathcal{O}_i) \leq \frac{4}{\pi} \sqrt{M}.$$

Because each $E_{j_i}$ has an element with the same minimal polynomial as $\alpha$ or $\alpha'$, each $j_i \in T_D$. This shows that the sequence $j_0, j_1, \ldots, j_r$ has the desired properties.

Note that we could have chosen our sequence of maximal orders to have $r \leq 3$, or to have consecutive orders linked by an ideal of prime order. In the first case, we would have a sequence of $j$-invariants with $r \leq 3$. In the second case, an ideal linking $\mathcal{O}_{i-1}$ to $\mathcal{O}_i$ with prime norm at most $\frac{2}{\pi} \sqrt{M}$ will correspond by the Deuring correspondence to an isogeny $E_{j_{i-1}} \to E_{j_i}$ of prime degree at most $\frac{4}{\pi} \sqrt{M}$. This concludes the proof.

### 7 Isogenies Between $M$-small Supersingular Curves

Despite the large distances between $M$-small curves in distinct subsets $T_D$ (as in Theorem 1.3), we will show that isogenies between them can nonetheless be computed efficiently (probabilistic polynomial time in $M$ and $\log p$) under certain heuristic assumptions. To begin with, we recall the following observations, made in other papers:

(Oi) Given two maximal orders $\mathcal{O}$ and $\mathcal{O}'$, an ideal linking $\mathcal{O}$ to $\mathcal{O}'$ with $S$-powersmooth norm $(S \approx \frac{1}{2} \log p)$ can be computed efficiently [Koh+14, Sections 4.5–4.7].

(Oii) Given a supersingular elliptic curve $E$ with known endomorphism ring $\text{End}(E)$, and a left ideal of $\text{End}(E)$ with $S$-powersmooth norm $(S \approx \frac{1}{2} \log p)$, an isogeny out of $E$ corresponding to $I$ under the Deuring correspondence can be computed efficiently [Eis+18, Proposition 4].
(Oiii) Given a maximal order $\mathcal{O}$, a $j$-invariant such that $\text{End}(E_j) \cong \mathcal{O}$ can be computed efficiently [Eis+18, Section 7.1].

For each $T_D$, we will construct a maximal order $\mathcal{O}_{T_D}$, and use Observation (Oiii) to find a $j$-invariant $j_D \in T_p$ with known endomorphism ring. Then for $D \neq D'$, we can use Observations (Oi) and (Oii) to find a (large degree) isogeny from $j_D$ to either $j_{D'}$ or $j_{D''}$. These specified $j$-invariants $j_D$ will act as “airports,” knowing that each isogeny valley $T_D$ is connected by small-degree isogenies, we can connect any two $M$-small supersingular curves by first finding a path from each to the closest airport, then following the large degree path between the airports.

One subtle issue with this approach comes from the fact that the Deuring correspondence is not one-to-one; it’s quite possible that for some $D, T_D$ is actually a disjoint union of two subsets that are very far apart, one being the set of conjugates of the other. To remedy this, it suffices to have a single $M$-small supersingular $j$-invariant $j_0 \in \mathbb{F}_p$ to route all paths through. For then if we have a path from $j_0$ to $j^p$, we can simply apply the $p^{th}$ power Frobenius map to this path to obtain a path from $j_0$ to $j$. This technique will be used in Algorithm 2.

### 7.1 Assumptions

Recall in Lemma 3.1 that $i^2 = -q$ and $j^2 = -p$ for some relatively small value of $q$. Let $K \neq \mathbb{Q}(i)$ be a quadratic field of discriminant $-4M \leq D < 0$. We will make two assumptions which are unproven but heuristically reasonable. In Section 7.3 we carry out computations that depend on these assumptions for $p \approx 2^{56}$, $M = 100$, and all allowable values of $D$, showing that in practice these assumptions seem to be valid.

(Ai) A solution $z \in L := K(i)$ to the norm equation $N_{L/K}(z) = -p$ can be computed efficiently, if one exists.\(^{10}\)

(Aii) Let $\omega \in B$ satisfy $4\omega^2 = D$ (if $D \equiv 0 \pmod{4}$) or $4\omega^2 - 4\omega + 1 = D$ (if $D \equiv 1 \pmod{4}$). Then if we randomly select integral elements $\beta \in B$, and let $n$ be the denominator of $\text{trd}(\omega \beta)$, it will not take too long before a choice of $\beta$ such that the discriminant of the order $\mathbb{Z}[\omega, n\beta]$ can be efficiently factored into primes.\(^{11}\)

**Lemma 7.1.** Take assumptions (Ai) and (Aii). Given any fundamental discriminant $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$, a maximal order of $B$ containing an integral element $\alpha$ with $\text{nr}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D})$ can be computed efficiently.

**Proof.** For $D$ satisfying the above conditions, there is an embedding of $K = \mathbb{Q}(\sqrt{D})$ into $B$ by [Voi19, Proposition 14.6.7]; this implies that $B \otimes_{\mathbb{Q}} K$ is split [Voi19, Lemma 5.4.7], which implies by Theorem 5.4.6(vi) that there is a solution $N_{K(i)/K}(z) = -p$ for some $z \in K[i]^\times$. Using assumption (Ai), we can solve for

$$z = (x + y\sqrt{D}) + i(z + w\sqrt{D}), \quad x, y, z, w \in \mathbb{Q},$$

in the norm equation, giving

$$(x + y\sqrt{D})^2 + q(z + w\sqrt{D})^2 = -p.$$  

After multiplying through by $pq$ we have

$$p^2q + (qz + qw\sqrt{D})^2p + (x + y\sqrt{D})^2pq = 0.$$

\(^{10}\) The algorithm for doing so is described in [Sim02, Section 6], and is implemented in Magma [BCP97] as $\text{NormEquation}(L, -p)$. In general, the bottleneck of the algorithm used to solve $N_{L/K}(z) = m$ is to factor $m$ into primes of $K$, but this is easy in our case because $p$ is already an integer prime.

\(^{11}\) Aside from the fact that the discriminant will be divisible by $p^2$ (since any order is contained in a maximal order), we expect it to behave like a “random integer” in some sense, and easily-factorable integers are not too rare in the range of values that appear to arise in practice.
Proof. There is a maximal order $\mathcal{O}$ containing $\{1, i, j, k\}$, which corresponds by the Deuring correspondence to some supersingular $j$-invariant $j$. Since $i \in \mathcal{O}$ and $\text{nr}(i) = q \leq M$, $j$ is $M$-small. Since $j \in \mathcal{O}$ and $\mathbb{Z}[j] \cong \mathbb{Z}[(\sqrt{-p})]$ we have $j \in \mathbb{F}_p$ [DG16, Proposition 2.4].

Suppose we have completed Algorithm 1. If we have some $j_0 \in \mathcal{S}_M \cap \mathbb{F}_p$, then we can apply Algorithm 2 to compute an isogeny between any two $M$-small supersingular curves $j_1, j_2 \in \mathcal{S}_M$. At each step

7.2 Algorithms for Computing Isogenies

In order to compute isogenies, we will need to use modular polynomials.

Definition 7.2. The $n$th modular polynomial $\Phi_n(x, y) \in \mathbb{Z}[x]$ is characterized by the following property: $\Phi_n(j_1, j_2) = 0$ if and only if there is a degree $n$ cyclic isogeny $E_{j_1} \to E_{j_2}$ (i.e., an isogeny with a cyclic group as its kernel).

Modular polynomials are symmetric in $x$ and $y$ ($\Phi_n(x, y) = \Phi_n(y, x)$), and if $n$ is prime, then the degree of each variable in $\Phi_n(x, y)$ is $n + 1$. The largest coefficient of $\Phi_n(x, y)$ grows faster than $n^n$ [Coh84], which makes even the storage (let alone the computation) of modular polynomials very difficult as $n$ grows large; for instance it takes more than a gigabyte to store the binary representation of $\Phi_{659}$, and 30 terabytes to store $\Phi_{20011}$ [BLS12, pp. 1201, 1228]. However, it is possible to compute $\Phi_n(x, y) \pmod{p}$ directly, without first computing it with integer coefficients; for instance, an algorithm given by Bröker et. al. computes $\Phi_\ell(x, y) \pmod{p}$ for $\ell$ prime (the only case we will need) in time $O(e^{3 + \varepsilon})$ [BLS12, Theorem 1].

Say a fundamental discriminant $D$ is valid if $-4M \leq D < 0$ and $\left( \frac{D}{p} \right) = -1$. For each valid fundamental discriminant $D$, let $T_D$ be as in Theorem 1.3 (defined in Section 6.1). Let $E_D$ be the set of pairs $(j, j') \in T_D \times T_D$ such that there is an isogeny $j \to j'$ or $j \to j'^p$ of prime degree at most $\frac{2}{3} \sqrt{M}$; Theorem 1.3 implies that the graph $(T_D, E_D)$ is connected.

Using these definitions, we can apply Algorithm 1 to compute the sets $T_D$, the edges $E_D$, and a specified $j_D \in T_D$ with known endomorphism ring $\text{End}(E_{j_D})$. Proposition 2.4 guarantees that the algorithm correctly builds the set $\mathcal{S}_M$ of supersingular $M$-small curves.

Note that $H_{\mathcal{O}}(x)$ will have degree $O(M^{1/2 + \varepsilon})$ (Proposition A.1), and the polynomials $\Phi_\ell(x, j)$ will have degree $\ell + 1 = O(M^{1/2})$. Assuming the conditions under which each appear in the algorithm, these polynomials will split in $\mathbb{F}_{2^\ell}$, because their roots will be $j$-invariants of supersingular curves. Thus, assuming an oracle for Assumptions (Ai) and (Aii), and an oracle that finds all roots of a polynomial of degree $O(M^{1/2 + \varepsilon})$ that splits over $\mathbb{F}_{2^\ell}$, Algorithm 1 can be shown to run in time polynomial in $M$ and $\log p$.

As noted above, if we want to guarantee existence of a path from any $M$-small supersingular curve to any other one (and not just to one out of a conjugate pair), we will need to be able to route isogenies through an $M$-small supersingular curve defined over $\mathbb{F}_p$. Such a curve should typically be fairly easy to find; the following lemma gives us a condition on $M$ under which such a curve will be guaranteed to exist.

Lemma 7.3. Let $q = -i^2$ as in Lemma 3.1. If $M \geq q$, then there exists an $M$-small supersingular $j$-invariant in $\mathbb{F}_p$.

Proof. There is a maximal order $\mathcal{O}$ containing $\{1, i, j, k\}$, which corresponds by the Deuring correspondence to some supersingular $j$-invariant $j$. Since $i \in \mathcal{O}$ and $\text{nr}(i) = q \leq M$, $j$ is $M$-small. Since $j \in \mathcal{O}$ and $\mathbb{Z}[j] \cong \mathbb{Z}[\sqrt{-p}]$, we have $j \in \mathbb{F}_p$ [DG16, Proposition 2.4].

Suppose we have completed Algorithm 1. If we have some $j_0 \in \mathcal{S}_M \cap \mathbb{F}_p$, then we can apply Algorithm 2 to compute an isogeny between any two $M$-small supersingular curves $j_1, j_2 \in \mathcal{S}_M$. At each step
Algorithm 1: Precomputing the $M$-small partition and a selected curve in each subset.

**Input**: $p$ and $M$.
**Output**: For each valid fundamental discriminant $D$, output $T_D$, $E_D$, a specified $j_D \in T_D$, and a maximal order $O_D \subseteq \mathcal{B}$ isomorphic to $\text{End}(E_{j_D})$.

1. Compute $\Phi_\ell(x, y) \pmod{p}$ for all prime $\ell \leq \frac{2}{3} \sqrt{M}$ \cite[Theorem 1]{BLS12}.
2. Initialize an empty list $\mathcal{S}_M$.
3. for $-4M \leq d < 0$, $d \equiv 0$ or $1 \pmod{4}$, $\left(\frac{d}{p}\right) = -1$ do
   4. Compute $\mathcal{O}_D(x)$, where $\mathcal{O}$ is the quadratic order of discriminant $d$ \cite[Theorem 1]{Sut11}.
   5. Append all $j \in \mathbb{F}_p^2$ satisfying $\mathcal{O}_D(j) = 0$ to $\mathcal{S}_M$.
4. end
5. for valid fundamental discriminants $D$ do
   6. Compute a maximal order $\mathcal{O}_D$ that has some $\alpha \in \mathcal{O}_D - \mathbb{Z}$ with $\text{nrd}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D})$ (Lemma 7.1).
   7. Compute $j_D \in \mathbb{F}_p^2$ such that $\text{End}(E_{j_D}) \cong \mathcal{O}_D \ (\text{Oi})$.
   8. Initialize queue $Q_D := (j_D)$ and empty list $E_D$. Set $j := j_D$.
   9. while $j \in Q_D$ do
      10. for prime $2 \leq \ell \leq \frac{2}{3} \sqrt{M}$ do
          11. for $j' \in \mathcal{S}_M$ such that $\Phi_\ell(j', j) = 0 \pmod{p}$ or $\Phi_\ell(j', j^\ell) = 0 \pmod{p}$ do
              12. Append $j'$ to the end of the queue $Q_D$.
              13. Append $(j, j')$ to $E_D$.
      14. end
   15. end
   16. Set $j$ to be the next element of the queue $Q_D$. If no such element exists, break.
   17. end
   18. Set $T_D := Q_D \cup Q_D^p$.
   19. Set $E_D := \bigcup_{(j, j') \in E_D} \{ (j, j'), (j, j^p), (j^p, j'), (j^p, j^p) \}$.
20. end
21. for each valid fundamental discriminant $D$, return $T_D$, $E_D$, $j_D$, and $\mathcal{O}_D$.

Algorithm 2: Computing isogenies between $M$-small supersingular curves.

**Input**: $j_1, j_2 \in \mathcal{S}_M$, $j_0 \in \mathcal{S}_M \cap \mathbb{F}_p$, and the output of Algorithm 1.
**Output**: An isogeny $E_{j_i} \rightarrow E_{j_i}$, given as a sequence of $\ell$-isogenies for primes $\ell = 1$.

1. Find $D_0, D_1, D_2$ such that $j_i \in T_{D_i}$ for each $i$.
2. for $i \in \{0, 1, 2\}$ do // short paths within $T_D$
   3. Find a sequence of edges in $E_{D_i}$ connecting $j_i$ to $j_{D_i}$.
   4. By following these edges, compute an isogeny $\phi_{D_i} : E_{j_i} \rightarrow E_{j_{D_i}}$ or $\phi_{D_i} : E_{j_i} \rightarrow E_{j_{D_i}}(p)$.
   5. end
6. for $i \in \{1, 2\}$ do // long paths between $T_D$
   7. Using $\mathcal{D}_D$ and $\mathcal{D}_{D_0}$ with Observations (Oi) and (Oii), find an isogeny $\Psi_i : E_{j_{D_0}} \rightarrow E_{j_{D_i}}$ or $\Psi_i : E_{j_{D_0}} \rightarrow E_{j_{D_i}}^{(p)}$.
   8. Let $\tilde{\phi}_{D_i}$ denote the dual of $\phi_{D_i}$. Choose $\alpha, \beta \in \{1, p\}$ such that the composition $\Gamma_i := \tilde{\phi}_{D_i} \circ \Psi_i^\alpha \circ \phi_{D_0}^\beta : E_{j_0} \rightarrow E_{j_i}$ is defined.
   9. end
10. Return $\Gamma_2 \circ \Gamma_1 : E_{j_1} \rightarrow E_{j_2}$.

17
in the algorithm, the isogenies in question may be recorded as a sequence of \( \ell \)-isogenies for relatively small primes \( \ell \) (in particular, \( \ell = O(\sqrt{M}) \) in step 4 by Theorem 1.3, and \( \ell = O(\log p) \) in step 7 by Observations (Oi) and (Oii)).

Even if we do not have a \( j \)-invariant \( j_0 \in S_M \cap \mathbb{F}_p \), a modification of Algorithm 2 can still produce isogenies between \( M \)-small supersingular curves. If we obtain an isogeny \( E_{j_1} \to E_{j_2}^{(p)} \), we may simply compose this isogeny with the \( p \)th power Frobenius \( E_{j_2}^{(p)} \to E_{j_2} \). However, the resulting isogeny will be inseparable, and will not be expressible as a composition of \( \ell \)-isogenies for small primes \( \ell \).

7.3 Example

It is worth examining how well Algorithm 1 works in practice; in particular, line 8 depends on the unproven assumptions (Ai) and (Aii), so we will focus on the time this step takes.

Let \( p = 2^{236} + 297 \); we can take \( B \) defined by \( i^2 = -7 \) and \( j^2 = -p \). Let \( M = 100 \). There are 62 valid fundamental discriminants \( D \):

\[-7, -15, -20, -40, -43, -47, -55, -56, -59, -79, -83, -84, -91, -95, \ldots, -399.\]

For each of these \( D \), we computed \( \mathcal{O}_D \) as in line 8. To do this for all valid \( D \) took 60 seconds on a generic personal laptop. In each case, we were able to take \( \beta = i \) or \( \beta = j \) in Assumption (Aii).

In practice, it seems as though the real bottleneck of Algorithm 1 is the edge-finding algorithm (lines 11–19); this took 4105 seconds on the same laptop.

A Counting \( M \)-small Curves

We will estimate the size of various sets of \( M \)-small curves, starting small and working up to progressively larger sets.

Proposition A.1. Let \( \mathcal{O} \) have discriminant \(-4M \leq \text{disc} \mathcal{O} < 0 \). Let \( C_\mathcal{O} \) denote the set of isomorphism classes of elliptic curves over a finite field of characteristic \( p \) that have complex multiplication by \( \mathcal{O} \). Then

\[ |C_\mathcal{O}| \leq \deg H_\mathcal{O}(x) = |\text{Cl}(\mathcal{O})| = O(M^{1/2+\varepsilon}). \]

Proof. The first inequality follows from Proposition 2.4 by counting roots, and we have the middle equality \( \deg H_\mathcal{O}(x) = |\text{Cl}(\mathcal{O})| \) by [Cox13, Proposition 13.2]. Let \( \mathcal{O} = \mathcal{O}_{K,f} \), let \( D \) be the discriminant of \( K \), and \( h(D) \) the class number of \( K \). Then

\[ |\text{Cl}(\mathcal{O})| \leq h(D)^f \prod_{\text{prime } \ell \mid f} \left( 1 - \left( \frac{D}{\ell} \right) \frac{1}{\ell} \right) \]

using the formula for the class number of nonmaximal orders [Cox13, Theorem 7.24]. We can bound this above by \( h(D) \psi(f) \) using the Dedekind \( \psi \) function, defined on positive integers as

\[ \psi(n) := n \prod_{\text{prime } \ell \mid n} \left( 1 + \frac{1}{\ell} \right). \]

We have \( \psi(n) = O(n \log \log n) \) [SP11, Corollary 3.2], and the classical bound \( h(D) = O(|D|^{1/2} \log D) \) (for instance, by Dirichlet’s class number formula [Dav00, §6 (15)] and bounds of the form \( |L(1, \chi_D)| = O(\log D) \) [GS19]). Together these give the bound

\[ |\text{Cl}(\mathcal{O})| = O(f|D|^{1/2} \log D \log \log f) = O(M^{1/2+\varepsilon}), \]

using \( f|D| = \text{disc} \mathcal{O} \leq 4M \). \( \square \)
Proposition A.2. Let $D$ be a fundamental discriminant, and

$$T_D := \{ j \in S : \mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D}) \text{ for some } \alpha \in \text{End}(E_j) - \mathbb{Z}, \deg \alpha \leq M \}$$

be the set from Theorem 1.3 (defined as such in Section 6.1). Then

$$|T_D| = O \left( \frac{M \log |D|}{\sqrt{|D|}} \right).$$

The structure of $T_D$ will depend heavily on its relationship to $M$, as the proof will illustrate. If $D$ is very small, then $T_D$ represents many different quadratic orders ($N$ is large), but each embeds in only a couple of maximal orders ($h(D)$ is small). If $D$ is comparable to $M$, then $T_D$ represents only a couple of different quadratic orders ($N$ is small), but each embeds in many different maximal orders ($h(D)$ is large). Intuitively, the “isogeny valley” $T_D$ is deep and narrow for small $|D|$, but shallow and wide for large $|D|$.

Proof. Let $K$ be a field of discriminant $D$, and let $C_D$ be the set of isomorphism classes of maximal orders $\mathfrak{O} \subseteq B$ containing an element $\alpha$ with $\text{nr}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong K$. By the Deuring correspondence we have $|T_D| \leq 2|C_D|$, so it suffices to count $C_D$.

Suppose $\alpha \in \mathfrak{O}$ has $\text{nr}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong K$. We have $\alpha \in \mathfrak{O} \cap \mathbb{Q}(\alpha) \cong \mathfrak{O}_{K,f}$ for some conductor $f$. As in the proof of Proposition 4.6, we must have $f^2 |D|/4 \leq \text{nr}(\alpha) \leq M$, implying that $f \leq \sqrt{4M/|D|} = N$. Hence, summing over all possible quadratic orders of $K$ with conductors in this range, we have

$$|C_D| \leq \sum_{f=1}^{N} |\text{Cl}(\mathfrak{O}_{K,f})| \leq h(D) \sum_{f=1}^{N} \psi(f)$$

using the proof of Proposition A.1. This value is

$$h(D) \left( \frac{30M}{\pi^2 |D|} + O(N \log N) \right)$$

by Lemma 2.1 of [H"ur15]. Applying $h(D) = O(|D|^{1/2} \log |D|)$, we get the desired bound $|T_D| = O \left( M \log |D|/\sqrt{|D|} \right)$.

Proposition A.3. The number of $M$-small curves is $O(M^{3/2})$.

Proof. Given an $M$-small order $\mathfrak{O}$, let $\alpha \in \mathfrak{O} - \mathbb{Z}$ have $\text{nr}(\alpha) \leq M$. Then $\alpha$ is in some quadratic order $\mathfrak{O}$, and $|\text{disc} \mathfrak{O}|/4 \leq \text{nr}(\alpha)$ implies $-4M \leq \text{disc} \mathfrak{O} < 0$. For every possible quadratic order, there are at most $|\text{Cl}(\mathfrak{O})|$ isomorphism classes of maximal orders in which $\mathfrak{O}$ is optimally embedded, meaning that we obtain an upper bound for the number of $M$-small maximal orders by summing $|\text{Cl}(\mathfrak{O})|$ over all quadratic orders with $-4M \leq \text{disc} \mathfrak{O} < 0$.

A quadratic order $\mathfrak{O}$ is uniquely determined by its discriminant, and there is a bijection between $\text{Cl}(\mathfrak{O})$ and the set of reduced primitive positive-definite binary quadratic forms of discriminant disc $\mathfrak{O}$ (Theorem 7.7(ii) and Theorem 2.8 of [Cox13]). That is, it suffices to bound the number of triples $(a,b,c) \in \mathbb{Z}^3$ with $-a < b \leq a \leq c$ and $b \geq 0$ if $a = c$, gcd$(a,b,c) = 1$, and $-4M \leq b^2 - 4ac < 0$.

From $|b| \leq a \leq c$, we have $-4M \leq b^2 - 4ac \leq -3a^2$, so $a \leq \sqrt{4M/3}$. Likewise $-4M \leq b^2 - 4ac \leq a^2 - 4ac$ implies $a \leq c \leq \frac{a}{4} + \frac{M}{a^2}$. Together with $-a < b \leq a$ we conclude that there are at most

$$\left( \frac{a}{4} + \frac{M}{a^2} - a + 1 \right) (2a) \leq 2M + 1$$

valid pairs $(b,c)$ for a given $a$; summing over the $\sqrt{4M/3}$ options for $a$ gives $O(M^{3/2})$ triples.
Remark A.4. When $M \ll p$, we observe that roughly half of all $M$-small curves are supersingular; for instance, with $p = 2^{256} + 297$ and $M = 100$ (the example discussed in Section 7.3), there are 1108 $M$-small curves, of which 528 (about 0.48 of the total) are supersingular. In Figure 2, we see that the proportion of $M$-small curves that are supersingular appears to follow a distribution centered at 0.5; for 94% of the primes $p$ considered, between 0.4 and 0.6 of $M$-small curves were supersingular modulo $p$.

Heuristically, this follows from the observation that a root of $H_{\mathcal{O}}(x)$ (mod $p$) is supersingular if and only if $p$ does not split in the field of fractions of $\mathcal{O}$ (Proposition 2.4). For each quadratic order $\mathcal{O}$, the set of primes which split in the field of fractions of $\mathcal{O}$ have density $\frac{1}{2}$ (Chebotarev’s Density Theorem), so for a set of quadratic orders with discriminants in a given range, we might expect that $p$ will split in the field of fractions of about half of them.

This observation clearly fails for $M$ large enough, because there are only finitely many supersingular curves, but infinitely many ordinary ones. This is because supersingular curves have complex multiplication by infinitely many distinct quadratic orders; that is, even though half (i.e. infinitely many) of the polynomials $H_{\mathcal{O}}(x)$ (mod $p$) should have supersingular roots, each individual supersingular $j$-invariant will be a root of infinitely many of them. But for small enough values of $M$, at most one of these quadratic orders can have $-4M \leq \text{disc } \mathcal{O} < 0$, by Theorem 4.7. So for $M \ll p$, we expect the set roots of $H_{\mathcal{O}}(x)$ (mod $p$) for $-4M \leq \text{disc } \mathcal{O} < 0$ to have similar numbers of ordinary and supersingular curves.

Proposition A.5. All supersingular $j$-invariants are $(\frac{1}{2}p^{2/3} + \frac{1}{3})$-small. The exponent is the best possible: if $\theta < \frac{2}{3}$ then for any constant $C$, there exists a prime $p$ and a supersingular $j$-invariant mod $p$ which is not $(Cp^\theta)$-small.

The sufficiency of $\frac{2}{3}$ was noted by Elkies [Elk87, Section 4], and Yang showed that no smaller exponent could be taken [Yan06, Proposition 1.1]. The proof given here roughly follows each of their approaches. Notice that Elkies’ bound uses the “large-scale” structure of maximal orders, namely the geometry of the full 4-dimensional lattice, while Yang’s bound uses the “small-scale” structure, counting embedded quadratic orders of small discriminant.

Figure 2: A histogram (bins of width 0.01) of the proportion of 100-small curves that are supersingular mod $p$, as $p$ varies over 1000 consecutive primes $2^{40} < p \leq 2^{40} + 27201$. Data computed using Magma [BCP97].
Proof. We can embed $B$ into $\mathbb{R}^4$ as follows:

$$a + bi + cj + dk \mapsto (a, b\sqrt{q}, c\sqrt{p}, d\sqrt{qp}).$$

This makes the reduced norm $(a + bi + cj + dk) \mapsto a^2 + qb^2 + pc^2 + qpd^2$ agree with the standard Euclidean norm on $\mathbb{R}^4$. A maximal order $\mathcal{O} \subseteq B$ will be a 4-dimensional lattice of covolume $\frac{q}{4}$ under this embedding [CG14, (2.2)]. Projecting $\mathcal{O}$ onto the orthogonal complement of 1 gives a 3-dimensional lattice of covolume $\frac{q}{4}$. By Theorem II.III.A of [Cas97], any such lattice must have a nonzero element $v$ with length

$$|v| \leq \left(\frac{p\sqrt{2}}{4}\right)^{1/3} = \frac{p^{1/3}}{\sqrt{2}}.$$

An element of $\mathcal{O}$ that projected onto $v$ must be of the form $\frac{v}{2} + v$ for some integer $k$, because the reduced trace of an integral element is an integer. Hence either $v \in \mathcal{O}$ or $\frac{v}{2} + v \in \mathcal{O}$, and the reduced norm is either $\frac{1}{2}p^{2/3}$ or $\frac{1}{2}p^{2/3} + \frac{1}{4}$. This shows $\mathcal{O}$ is $(\frac{1}{2}p^{2/3} + \frac{1}{4})$-small.

Conversely, we saw that the number of $M$-small curves is $O(M^{3/2})$, by summing sizes of ideal class groups of embedded quadratic orders (Proposition A.3). So if $\theta < \frac{2}{3}$ then the number of $(Cp^\theta)$-small curves will be $O(p^{3\theta/2})$, with $\frac{3\theta}{2} < 1$. But the number of supersingular curves is $p^{12} + O(1)$ [Sil09, Theorem V.4.1(c)], which grows faster than the set of $(Cp^\theta)$-small curves. \qed

References

[Arp+19] Sarah Arpin et al. Adventures in Supersingularland. 2019. arXiv: 1909.07779 [math.NT] (cit. on p. 1).

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: J. Symbolic Comput. 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125 (cit. on pp. 3, 15, 20).

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. “Modular Polynomials via Isogeny Volcanoes”. In: Mathematics of Computation 81.278 (2012), pp. 1201–1231 (cit. on pp. 16, 17).

[Brö09] Reinier Bröker. “Constructing supersingular elliptic curves”. In: Frontiers of Combinatorics and Number Theory (Jan. 2009) (cit. on pp. 4, 5).

[Cas97] John W. S. Cassels. An Introduction to the Geometry of Numbers. Springer, 1997. ISBN: 978-3-540-61788-4 (cit. on p. 21).

(CG14) Ilya Chevyrev and Steven D. Galbraith. “Constructing supersingular elliptic curves with a given endomorphism ring”. In: LMS Journal of Computation and Mathematics 17.A (2014), pp. 71–91. DOI: 10.1112/S1461157014000254 (cit. on p. 21).

[Che34] C. Chevalley. “Sur certains idéaux d’une algèbre simple”. French. In: Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 10.1 (June 1934), pp. 83–105. DOI: 10.1007/BF02940666 (cit. on p. 10).

[Coh84] Paula Cohen. “On the coefficients of the transformation polynomials for the elliptic modular function”. In: Mathematical Proceedings of the Cambridge Philosophical Society 95.3 (1984), pp. 389–402. DOI: 10.1017/S0305004100028046 (cit. on p. 16).

[Cox13] David A. Cox. Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. 2nd ed. Wiley, 2013. ISBN: 978-0-471-19079-0 (cit. on pp. 5, 18, 19).

[Dav00] Harold Davenport. Multiplicative number theory. Ed. by Hugh L. Montgomery. 2nd ed. Springer, 2000 (cit. on p. 18).
Andrew Sutherland. “Isogeny Volcanoes”. In: The Open Book Series 1 (Aug. 2012). doi: 10.2140/obs.2013.1.507 (cit. on pp. 2, 10).

John Michael Voight. “Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic”. PhD thesis. Berkeley, CA, USA, 2005. isbn: 0-542-29154-1 (cit. on p. 16).

John Voight. Quaternion Algebras. Version v.0.9.15. May 2019. url: https://math.dartmouth.edu/~jvoight/quat-book.pdf (cit. on pp. 4, 6–9, 12, 14–16).

Wolfram Research, Inc. Mathematica, Version 10.0. Champaign, IL. 2014. url: https://www.wolfram.com/mathematica (cit. on p. 3).

Tonghai Yang. “Minimal CM Liftings of Supersingular Elliptic Curves”. In: Pure and Applied Mathematics Quarterly 4 (4 Jan. 2006). doi: 10.4310/PAMQ.2008.v4.n4.a14 (cit. on p. 20).