SUPERSINGULAR CURVES WITH SMALL NON-INTEGER ENDOMORPHISMS

JONATHAN LOVE AND DAN BONEH

Abstract. We introduce a special class of supersingular curves over $\mathbb{F}_{p^2}$, 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 when 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 small-degree isogenies 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 ℓ-isogeny graphs.

1. Introduction

Given an elliptic curve E over a field F, let $\mathrm{End}(E)$ denote the ring of endomorphisms of E that are defined over $\overline{F}$. The curve E is **supersingular** if $\mathrm{End}(E)$ is non-abelian; this can only occur if E is defined over $\mathbb{F}_{p^2}$ for some prime p [25, Theorem V.3.1]. While the set of all supersingular curves can be quite complicated, in this paper we define collections of supersingular curves which are relatively easy to compute with and to classify.

Definition 1.1. *Given $M < p$, an elliptic curve E over a finite field of characteristic p is M-**small** (we also say that the j-invariant of E is M-small) if there exists $\alpha \in \mathrm{End}(E)$ with $\deg \alpha \leq M$ such that α is not multiplication by an integer. The set of M-small j-invariants of* supersingular *curves over $\mathbb{F}_{p^2}$ is denoted $\mathcal{S}_M$ (with the prime p being assumed from context).*

An M-small curve 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. Assuming for the rest of this paper that $p \geq 5$, a few notable properties that will be discussed are as follows:

(a) The set of all M-small curves in characteristic p can be generated by finding roots of Hilbert class polynomials for orders of discriminant $O(M)$ (Proposition 2.3).
(b) If $M < \frac{\sqrt{p}}{2}$, the set $\mathcal{S}_M$ of M-small supersingular curves partitions into $O(M)$ subsets, each connected by small-degree isogenies, such that there is no isogeny of degree less than $\frac{\sqrt{p}}{2M}$ between distinct subsets (Theorem 1.3).
(c) 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).

Date: February 2020.
Supported by NSF grant #1701567.

A number of other properties are discussed in an appendix:

(d) The number of M-small curves up to $\overline{\mathbb{F}_p}$-isomorphism is $O(M^{3/2})$.
(e) When $M \ll p$, approximately half of all M-small curves appear to be supersingular (heuristically and experimentally).
(f) When $M \geq \frac{1}{2}p^{2/3} + \frac{1}{4}$, every supersingular curve is M-small.

Let us state point (b) more precisely. Given an elliptic curve E over $\mathbb{F}_{p^2}$, 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 $\mathbb{F}_p$, then $E = E^{(p)}$; otherwise we have $E = (E^{(p)})^{(p)}$ and so this map will swap conjugate pairs of curves.[1] For $j \in \mathbb{F}_{p^2}$, let E_j be an elliptic curve over $\mathbb{F}_{p^2}$ with j-invariant equal to j.

Definition 1.2. *Let E and E' be supersingular elliptic curves over $\mathbb{F}_{p^2}$. The **distance from E to E'**, denoted $d(E, E')$, is the minimum degree of an isogeny $E \to E'$ or $E \to E'^{(p)}$ defined over $\overline{\mathbb{F}_p}$. We also define $d(j, j') = d(E_j, E_{j'})$ for supersingular j-invariants $j, j' \in \mathbb{F}_{p^2}$.*

By basic properties of isogenies (e.g., [25, Chapter III]), $\log d$ is a pseudometric on the set of supersingular curves over $\mathbb{F}_{p^2}$, and it descends to a metric on the set of Galois orbits $\{E, E^{(p)}\}$.

Theorem 1.3. *Suppose $p > 4M^2$, and let $\mathcal{S}_M$ denote the set of M-small supersingular curves. Then there exists a partition*

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

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:

(a) If j, j' are in distinct subsets $T_D \neq T_{D'}$, then

$$d(j, j') \geq \frac{\sqrt{p}}{2M}.$$

(b) 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 such that for each $i = 1, \ldots, r$, there exists an isogeny $E_{j_{i-1}} \to E_{j_i}$ or $E_{j_{i-1}} \to E_{j_i}^{(p)}$ with prime degree at most $\frac{4}{\pi}\sqrt{M}$.

See Figure 1 for an illustration of Theorem 1.3. Intuitively, this is saying that the set of supersingular curves has "isogeny valleys"[2] indexed by certain fundamental discriminants; each valley consists of a number of M-small curves that are all linked

[1] The map $E \to E^{(p)}$ on supersingular curves is called the "mirror involution" in [1], where the relationship between conjugate pairs, along with many other structural properties of supersingular isogeny graphs, is studied in detail.

[2] 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 [29]. 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.

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 $E \to E'$ of degree 2 or 3 (the primes less than $\frac{4}{\pi}\sqrt{12}$). 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 [2], plotted using Mathematica [33].

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 B.

The fact that the sets T_D are connected by small-degree isogenies (as described in Theorem 1.3(b)) will not be evident in the ℓ-isogeny graph for any individual prime ℓ. In fact, if ℓ is any prime such that one of the sets T_D contains an (M/ℓ^2)-small curve, then there are two curves in T_D such that the degree of any isogeny between them is either divisible by ℓ or greater than $p\ell/(4M)$ (Corollary C.2). So if we exclude any sufficiently small prime, Theorem 1.3(b) does not hold.

Motivation. We say that a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is "hard" if it is computationally infeasible to compute its endomorphism ring. A number of

applications in cryptography (e.g., [12]) 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 $p \equiv 2 \bmod 3$ and let E_0 be the supersingular curve with j-invariant 0. Let ℓ be a small prime. One can generate a large number of supersingular curves by taking a random walk along the graph of degree ℓ 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 (b) tells us that E could not reasonably be found by searching from E_0 on ℓ-isogeny graphs for any small primes ℓ. 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 (c) demonstrates that this is likely not the case.

This suggests that a hard curve will not be M-small; by the classification results of Section 2.1, this rules out roots of low-degree Hilbert class polynomials as reasonable candidates for hard curves. It remains an open problem to construct a single explicit hard supersingular curve.

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.

Sections 3–6 are devoted to the proof of Theorem 1.3. This proof depends on the fact that the endomorphism ring of a supersingular curve is a maximal order in a quaternion algebra,[3] so a brief review of some necessary background is given in Section 3. In Section 4 we lay the groundwork for a proof of Theorem 1.3, and prove an analogue of Theorem 1.3(a) for quaternion algebras. We discuss the theory of optimal embeddings of quadratic orders in Section 5, which enables us to prove a quaternion algebra analogue of Theorem 1.3(b). These two results are translated into facts about supersingular curves in Section 6, where we finish the proof of Theorem 1.3.

In Section 7, we discuss an algorithm that finds an isogeny between any two M-small supersingular curves. Appendix A includes more detail on these algorithms, 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 B. Appendix C depends on the results of Section 5, and shows that certain isogenies of degree ℓ cannot be replaced by short isogenies of degree relatively prime to ℓ.

Acknowledgments. We would like to thank John Voight for fruitful discussion without which we would not have found the algorithms in Section 7, and Akshay Venkatesh for pointing us towards the key ideas in Section 5. Thanks also to the anonymous reviewers for many improvements, including local proofs for Lemma 4.2

[3]This viewpoint lays the foundation for many prior papers on supersingular isogenies; see for instance [20], [22], and [15].

and Lemma 5.4, as well as pointing out a strengthening of Proposition 4.5 that leads to a better bound in Theorem 1.3.

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 [3] 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 quadratic order. If D is the discriminant of K, then $d := f^2 D$ is the discriminant of $\mathcal{O}_{K,f}$ (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 $1 \pmod 4$ 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 $\mathcal{O}_{K,f} \subseteq \mathcal{O}_{K,g}$ if and only if $g \mid f$.

Definition 2.1. *Let $\mathcal{O}$ be a quadratic order. The **Hilbert class polynomial** $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$ is the monic irreducible polynomial characterized by the following property:*[4] *for $j \in \mathbb{C}$, $H_{\mathcal{O}}(j) = 0$ if and only if j is the j-invariant of an elliptic curve $\widetilde{E}$ over $\mathbb{C}$ with $\mathrm{End}(\widetilde{E}) \cong \mathcal{O}$.*

Bröker's algorithm [3, Algorithm 2.4] proceeds as follows. To construct a supersingular curve over $\mathbb{F}_p$ with $p \equiv 1 \pmod 4$,[5] one first finds a prime $q \equiv 3 \pmod 4$ with Legendre symbol $\left(\frac{-q}{p}\right) = -1$. One can typically find very small values of q satisfying these constraints. The algorithm proceeds by computing the Hilbert class polynomial $H_{\mathcal{O}_K}(x)$ for $K = \mathbb{Q}(\sqrt{-q})$, and finding a root of $H_{\mathcal{O}_K}(x) \pmod p$ in $\mathbb{F}_p$. The condition $\left(\frac{-q}{p}\right) = -1$ then guarantees that this root is the j-invariant of a supersingular curve (Proposition 2.3). This algorithm generates M-small curves for a reasonably small value of M, as the following proposition shows.

Proposition 2.2. *The supersingular curves found by Algorithm 2.4 of [3] are $\left(\frac{q+1}{4}\right)$-small. Assuming GRH, they are M-small for $M = O(\log^2 p)$.*

Proof. The output of the algorithm is a curve E over $\mathbb{F}_p$ with the following property: there exists a curve $\widetilde{E}$ over the Hilbert class field of $\mathbb{Q}(\sqrt{-q})$ such that $\mathrm{End}(\widetilde{E}) \cong \mathcal{O}_K$ and E is the reduction of $\widetilde{E}$ modulo some prime of $\mathcal{O}_L$. In particular, $\frac{1+\sqrt{-q}}{2} \in \mathcal{O}_K$ is a non-integer endomorphism of $\widetilde{E}$ with norm $\frac{q+1}{4}$. The reduction map $\mathrm{End}(\widetilde{E}) \to \mathrm{End}(E)$ is a degree-preserving injection [24, Proposition

[4] See for example [10, Proposition 13.2] for proof that such a polynomial exists.

[5] For $p = 2$, the curve $y^2 + y = x^3$ is supersingular, and for $p \equiv 3 \pmod 4$ the curve $y^2 = x^3 + x$ is supersingular.

II.4.4], so $\mathrm{End}(E)$ also contains a non-integer endomorphism of norm $\frac{q+1}{4}$, proving that E is $\left(\frac{q+1}{4}\right)$-small.

As discussed in the proof of Lemma 2.5 in [3], under GRH we can find $q = O(\log^2 p)$ with the desired properties. □

2.1. **Classification of M-small curves.** A suitable generalization of Bröker's algorithm [3] can be used to generate the set of all M-small curves. Instead of only considering roots of the Hilbert class polynomial $H_{\mathcal{O}_K}(x)$, we will consider the set of roots of $H_{\mathcal{O}}(x) \pmod p$ for all quadratic orders with discriminant $-4M \leq \operatorname{disc}\mathcal{O} < 0$. This set is the set of j-invariants of M-small curves (Proposition 2.3), and we can determine whether a j-invariant is supersingular or ordinary by a Legendre symbol calculation as in [3].

Sutherland gives an algorithm for computing $H_{\mathcal{O}}(x) \pmod p$ in time $O(|\operatorname{disc}\mathcal{O}|^{1+\varepsilon})$ [30, Theorem 1]. Computing $H_{\mathcal{O}}(x)$ for all quadratic orders of discriminant $-4M \leq d < 0$ can therefore be done in time $O(M^{2+\varepsilon})$.

Proposition 2.3. *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 $H_{\mathcal{O}}(j) = 0 \pmod p$ for some quadratic order $\mathcal{O}$ with discriminant $-4M \leq \operatorname{disc}\mathcal{O} < 0$. Further, E is supersingular if and only if p does not split in the field of fractions of $\mathcal{O}$.*

Proof. First suppose E is M-small, and take $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ for which $\deg\alpha \leq M$. By Deuring's Lifting Theorem [21, Theorem 13.14], there is an elliptic curve $\widetilde{E}$ defined over a number field L, an endomorphism $\widetilde{\alpha}$ of $\widetilde{E}$, and a prime $\mathfrak{p}$ of L, such that $\widetilde{E}$ has good reduction at $\mathfrak{p}$, the reduction of $\widetilde{E}$ at $\mathfrak{p}$ is isomorphic over $\overline{\mathbb{F}_p}$ to E, and that the endomorphism on E induced by $\widetilde{\alpha}$ is equal to α. Since the map $\mathrm{End}(\widetilde{E}) \to \mathrm{End}(E)$ induced by reduction preserves degree [24, Proposition II.4.4], $\widetilde{\alpha} \in \mathrm{End}(\widetilde{E}) - \mathbb{Z}$ has degree at most M. For some quadratic order $\mathcal{O}$ in an imaginary quadratic field K, we will have $\mathrm{End}(\widetilde{E}) \cong \mathcal{O}$ [25, Corollary III.9.4]. Letting $d = \operatorname{disc}\mathcal{O}$, we will have $\widetilde{\alpha} = \frac{a+b\sqrt{d}}{2}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then

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

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

Conversely, suppose $H_{\mathcal{O}}(j) = 0 \pmod p$ for some quadratic order $\mathcal{O}$ with discriminant $-4M \leq \operatorname{disc}\mathcal{O} < 0$. Let $L/\mathbb{Q}$ be the splitting field of $H_{\mathcal{O}}(x)$, and let $\mathfrak{p}$ be a prime over p in L. Then by considering the reductions mod $\mathfrak{p}$ of the linear factors of $H_{\mathcal{O}}(x)$, we can conclude that j is the reduction mod $\mathfrak{p}$ of some $\widetilde{j} \in L$ with $H_{\mathcal{O}}(\widetilde{j}) = 0$. If $\widetilde{E}$ is an elliptic curve over L with j-invariant $\widetilde{j}$, then $\mathrm{End}(\widetilde{E}) \cong \mathcal{O}$, and its reduction modulo $\mathfrak{p}$ is isomorphic over $\overline{\mathbb{F}_p}$ to E. If $d = \operatorname{disc}\mathcal{O}$ is congruent to $0 \pmod 4$, then the element $\widetilde{\alpha} := \frac{\sqrt{d}}{2} \in \mathcal{O}$ satisfies $\mathrm{N}_{\mathcal{O}/\mathbb{Z}}(\widetilde{\alpha}) = \frac{|d|}{4} \leq M$. If $d \equiv 1 \pmod 4$, then we have $-4M + 1 \leq d$, and the element $\widetilde{\alpha} := \frac{1+\sqrt{d}}{2} \in \mathcal{O}$ satisfies $\mathrm{N}_{\mathcal{O}/\mathbb{Z}}(\widetilde{\alpha}) = \frac{|d|+1}{4} \leq M$. Since the map $\mathrm{End}(\widetilde{E}) \to \mathrm{End}(E)$ induced by reduction is a degree-preserving injection [24, Proposition II.4.4], the reduction of $\widetilde{\alpha}$ in either case gives $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ 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 [21, 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 [31].

3.1. **Quaternion Algebras and Subfields.** There is a quaternion algebra B over $\mathbb{Q}$, unique up to isomorphism, that ramifies exactly at p and ∞. For $p \neq 2$, we can take

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

for an appropriate integer q depending on $p \pmod 8$ (for $p \equiv 1 \pmod 8$, this agrees with the value of q [23, Proposition 5.1].

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 $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ for all $\alpha, \beta \in B$.
- its **reduced norm**, $\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = w^2 + qx^2 + py^2 + qpz^2$.
- its **reduced trace**, $\mathrm{trd}(\alpha) := \alpha + \overline{\alpha} = 2w$.

From these definitions, we see that any $\alpha \in B$ is the root of a polynomial

$$x^2 - \mathrm{trd}(\alpha)x + \mathrm{nrd}(\alpha)$$

with rational coefficients; if $\alpha \notin \mathbb{Q}$ this is the **minimal polynomial** of α. Noting that $\mathrm{trd}(\alpha)^2 - 4\,\mathrm{nrd}(\alpha) < 0$, any $\alpha \notin \mathbb{Q}$ generates an imaginary quadratic subfield $\mathbb{Q}(\alpha) \subseteq B$. The following result (a consequence of the Skolem-Noether Theorem) tells us exactly when two elements of B have the same minimal polynomial.

Theorem 3.1 ([31, Corollary 7.7.3])**.** *Let $\alpha, \beta \in B - \mathbb{Q}$. Then α and β satisfy the same minimal polynomial if and only if there exists $\gamma \in B^\times$ such that $\gamma^{-1}\alpha\gamma = \beta$.*

In particular, given any two isomorphic quadratic subfields of B, 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 [31, 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** $\mathfrak{O} \subseteq B$ is an ideal which contains 1 and is closed under multiplication (and is hence a subring of B). An element $\alpha \in B$ with $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in \mathbb{Z}$ is called **integral**; α 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,

$$\mathfrak{O}_L(I) := \{x \in B : xI \subseteq I\}, \qquad \mathfrak{O}_R(I) := \{x \in B : Ix \subseteq I\}.$$

We say that I is a **left ideal of** $\mathfrak{O}$ if $\mathfrak{O}_L(I) = \mathfrak{O}$, and that I is a **right ideal of** $\mathfrak{O}'$ if $\mathfrak{O}_R(I) = \mathfrak{O}'$. In this scenario we say I **links** $\mathfrak{O}$ **to** $\mathfrak{O}'$.

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 $\mathrm{nrd}(\alpha) \in$

$\mathbb{Z}$ for all α in an integral ideal. Given an integral ideal $I \subseteq B$, the **reduced norm** of I is defined to be

$$\mathrm{nrd}(I) := \gcd\{\mathrm{nrd}(\alpha) \mid \alpha \in I\}.$$

Observe that $I \subseteq J$ implies $\mathrm{nrd}(J) \mid \mathrm{nrd}(I)$.

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 $\mathfrak{O} \subseteq B$ we say that $\mathcal{O}$ is **optimally embedded** in $\mathfrak{O}$ if $\mathcal{O} \cong \mathfrak{O} \cap K$ for some subfield $K \subseteq B$.

3.3. **The Deuring Correspondence.** (See Chapter 42 of [31] for details.)

Let $\mathcal{S} \subseteq \mathbb{F}_{p^2}$ denote the set of j-invariants of supersingular curves. Given $j \in \mathcal{S}$, $\mathrm{End}(E_j)$ will be isomorphic to a maximal order in B. If j and j^p are $\mathbb{F}_{p^2}$-conjugates, then $\mathrm{End}(E_j)$ and $\mathrm{End}(E_{j^p})$ 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*:

$$\mathcal{S}/(j \sim j^p) \leftrightarrow \{\text{maximal orders of } B\}/\cong$$

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 $\mathrm{End}(E_j)$ for some j. Then we have a one-to-one correspondence

$$\{\text{separable isogenies out of } E_j\}/\cong \leftrightarrow \{\text{left ideals of } \mathfrak{O}_j\}.$$

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 $\mathrm{End}(E')$ (that is, I is a left $\mathfrak{O}_j$-ideal and a right $\mathfrak{O}_{j'}$-ideal), and $\deg \phi = \mathrm{nrd}(I)$.

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 $\mathrm{nrd}(\alpha) \leq M$.*

Then 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. We observe that these values are equal if and only if the corresponding quantities obtained by localizing at each prime are all equal [31, Lemma 9.5.7].

There is a unique maximal order at the ramified prime p, and so all three of the local quantities at p are equal to 1.

For $\ell \neq p$, the statement follows from the theory of the Bruhat-Tits Tree [31, Section 23.5]. Specifically, we have $B_\ell \cong M_2(\mathbb{Q}_\ell)$. With respect to an appropriate basis, if we set $\varpi = \left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we will have $\mathfrak{O}_\ell = M_2(\mathbb{Z}_\ell)$ and $\mathfrak{O}'_\ell = \varpi^{-e}\mathfrak{O}_\ell\varpi^e$ for some exponent e [31, Lemma 23.5.14]. Then $\mathfrak{O}_\ell\varpi^e = \varpi^e\mathfrak{O}'_\ell$ is the linking ideal of smallest reduced norm, and we can check directly that

$$|\mathfrak{O}_\ell : \mathfrak{O}_\ell \cap \mathfrak{O}'_\ell| = |\mathfrak{O}'_\ell : \mathfrak{O}_\ell \cap \mathfrak{O}'_\ell| = \mathrm{nrd}(\mathfrak{O}_\ell\varpi^e) = \ell^e. \qquad \square$$

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.*

Note that $\log d$ defines a metric on the set of maximal orders of B. Positive-definiteness and symmetry follow immediately from definition. If I and J are the integral ideals of smallest reduced norm linking $\mathfrak{O}$ to $\mathfrak{O}'$ and $\mathfrak{O}'$ to $\mathfrak{O}''$, respectively, then IJ is an integral ideal linking $\mathfrak{O}$ to $\mathfrak{O}''$. Since $\mathrm{nrd}(IJ) \leq \mathrm{nrd}(I)\,\mathrm{nrd}(J)$ for any compatible ideals I and J [31, Example 16.3.6], $\log d$ satisfies the triangle inequality. 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*

$$d(E, E') = \min\{d(\mathfrak{O}, \mathfrak{O}') \mid \mathfrak{O} \cong \mathrm{End}(E), \mathfrak{O}' \cong \mathrm{End}(E')\}.$$

Proof. By the Deuring correspondence, both sides are equal to

$$\min\{\deg \phi \mid \phi : E \to E'' \text{ for some } E'' \text{ with } \mathrm{End}(E'') \cong \mathrm{End}(E')\}. \qquad \square$$

4.2. **Two Key Propositions.** Suppose that $\mathfrak{O}$ and $\mathfrak{O}'$ are each M-small maximal orders in B. Let $\alpha \in \mathfrak{O} - \mathbb{Z}$ and $\alpha' \in \mathfrak{O}' - \mathbb{Z}$ each have reduced norm at most M. We will show that the distance from $\mathfrak{O}$ to $\mathfrak{O}'$ is small if $\mathbb{Q}(\alpha)$ is isomorphic to $\mathbb{Q}(\alpha')$, and is large otherwise. Precisely, we will prove the following two results, which are quaternion algebra analogues of results (a) and (b) of Theorem 1.3.

Proposition 4.5. *If $\mathbb{Q}(\alpha) \ncong \mathbb{Q}(\alpha')$, then $d(\mathfrak{O}, \mathfrak{O}')^2 \geq \frac{p}{4M^2}$.*

Proposition 4.6. *If $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha')$, then there exists a sequence of (not necessarily distinct) maximal orders*

$$\mathfrak{O} = \mathfrak{O}_0, \mathfrak{O}_1, \ldots, \mathfrak{O}_r \cong \mathfrak{O}'$$

such that

- *the distance between two consecutive terms is at most $\frac{4}{\pi}\sqrt{M}$, and*
- *each $\mathfrak{O}_i$ contains an element with the same minimal polynomial as either α or α'.*

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 $\frac{4}{\pi}\sqrt{M}$.

Proposition 4.6 will be proven in Section 5; we will proceed with a proof of Proposition 4.5. We begin by quoting a theorem due to Kaneko:

Theorem 4.7. *[19, Theorem 2′] Let $\mathfrak{O} \subseteq B$ be a maximal order. If $\mathcal{O}$ and $\mathcal{O}'$ are quadratic orders of imaginary quadratic fields, optimally embedded into $\mathfrak{O}$ with distinct images, then $\mathrm{disc}\,\mathcal{O}\,\mathrm{disc}\,\mathcal{O}' \geq 4p$. If in addition $\mathcal{O}$ and $\mathcal{O}'$ have isomorphic fields of fractions, then $\mathrm{disc}\,\mathcal{O}\,\mathrm{disc}\,\mathcal{O}' \geq p^2$.*

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. Let

$$\mathcal{O} := \mathbb{Q}(\alpha) \cap \mathfrak{O} \qquad \text{and} \qquad \mathcal{O}' := \mathbb{Q}(\alpha') \cap \mathfrak{O}.$$

both be optimally embedded in $\mathfrak{O}$. Since $\mathbb{Q}(\alpha) \ncong \mathbb{Q}(\alpha')$, these are distinct, so Theorem 4.7 implies that $\operatorname{disc}\mathcal{O} \operatorname{disc}\mathcal{O}' \geq 4p$.

Let D denote the discriminant of $K = \mathbb{Q}(\alpha)$. Since $\alpha \in \mathcal{O} - \mathbb{Z}$, and the quadratic order $\mathcal{O}$ must be of the form $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for some positive integer f, we have

$$\operatorname{nrd}(\alpha) \geq \mathrm{N}_{K/\mathbb{Q}}\left(\tfrac{1}{2}f\sqrt{D}\right) = \frac{f^2 D}{4} = \frac{1}{4}\operatorname{disc}\mathcal{O}.$$

Letting $d = d(\mathfrak{O}, \mathfrak{O}') = |\mathfrak{O}' : \mathfrak{O} \cap \mathfrak{O}'|$, we have $d\alpha' \in \mathfrak{O} \cap \mathfrak{O}' \subseteq \mathfrak{O}$. As above, we can compute $d^2 \operatorname{nrd}(\alpha') \geq \frac{1}{4}\operatorname{disc}\mathcal{O}'$. Hence

$$d^2 \geq \frac{\operatorname{disc}\mathcal{O}'}{4\operatorname{nrd}(\alpha')}\frac{\operatorname{disc}\mathcal{O}}{4\operatorname{nrd}(\alpha)} \geq \frac{p}{4M^2}. \qquad \square$$

5. Optimal Embeddings

Let K be an imaginary quadratic field of discriminant 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 relations between maximal orders. If two maximal orders have the same quadratic order optimally embedded in each, we call the relationship between them a "horizontal step"; if one of the optimally embedded orders is a proper subset of the other, the relationship is called a "vertical step".[6]

Remark 5.1. A fixed embedding $K \hookrightarrow B$ defines a unique optimally embedded quadratic order $K \cap \mathfrak{O}$. However, there is not a unique embedding of K into B (see Theorem 3.1), so it is possible for multiple distinct quadratic orders of K to all optimally embed into a single maximal order. Strictly speaking, "horizontal" and "vertical" steps are not relations between maximal orders, but rather between pairs of the form $(\mathfrak{O}, \mathcal{O})$, where $\mathcal{O}$ is a quadratic order optimally embedded in a maximal order $\mathfrak{O}$; if we do not specify $\mathcal{O}$, then these relations will not be well-defined.

5.1. Horizontal Steps.

First we consider the case in which the same quadratic 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 5.2 ([14, Satz 7])**.** *Let $\mathfrak{O}, \mathfrak{O}' \subseteq B$ be two maximal orders, and suppose*

$$\mathcal{O} \cong K \cap \mathfrak{O} = K \cap \mathfrak{O}'$$

[6]The 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 [29].

is optimally embedded in each. Then there is an invertible ideal[7] $\mathfrak{a}$ *of* $\mathcal{O}$ *such that* $\mathfrak{O}\mathfrak{a} = \mathfrak{a}\mathfrak{O}'$.

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 $\mathcal{O}$. Recall from Section 2 that we set $\mathcal{O}_{K,f} := \mathbb{Z} + f\mathcal{O}_K$, the order of conductor f in $\mathcal{O}_K$.

Lemma 5.3. *Let* K *be an imaginary quadratic field of discriminant* D. *Let* $\mathfrak{O}, \mathfrak{O}' \subseteq B$ *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*

$$d(\mathfrak{O}, \phi(\mathfrak{O}')) \leq \frac{2}{\pi} f\sqrt{|D|}.$$

Proof. By the Skolem-Noether theorem (Theorem 3.1), there exists $\gamma \in B$ such that

$$\mathfrak{O} \cap K = (\gamma^{-1}\mathfrak{O}'\gamma) \cap K$$

for some embedding $K \hookrightarrow B$. Since conjugation by γ is an automorphism of B, we can replace $\mathfrak{O}'$ with $\gamma^{-1}\mathfrak{O}'\gamma$, so that $\mathfrak{O} \cap K = \mathfrak{O}' \cap K$ is identified with the quadratic order $\mathcal{O}$.

By Theorem 5.2, there exists an invertible ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $\mathfrak{O}\mathfrak{a} = \mathfrak{a}\mathfrak{O}'$. We can find an ideal $\mathfrak{b}$ in the same ideal class as $\mathfrak{a}$ (so $\mathfrak{b} = \mathfrak{a}\delta$ for some $\delta \in K$) with $N_{\mathcal{O}/\mathbb{Z}}(\mathfrak{b}) \leq \frac{2}{\pi} f\sqrt{|D|}$ by Minkowski's bound [28, Theorem 5.4]. Then

$$\mathfrak{O}\mathfrak{b} = \mathfrak{O}\mathfrak{a}\delta = \mathfrak{a}\mathfrak{O}'\delta = (\mathfrak{b}\delta^{-1})\mathfrak{O}'\delta = \mathfrak{b}\phi(\mathfrak{O}'),$$

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

$$\operatorname{nrd}(\mathfrak{O}\mathfrak{b}) = \gcd\{\operatorname{nrd}(x) \mid x \in \mathfrak{O}\mathfrak{b}\} \leq \gcd\{\mathrm{N}_{\mathcal{O}/\mathbb{Z}}(x) \mid x \in \mathfrak{b}\} = \mathrm{N}_{\mathcal{O}/\mathbb{Z}}(\mathfrak{b}) \leq \frac{2}{\pi} f\sqrt{|D|},$$

which gives the upper bound on $d(\mathfrak{O}, \phi(\mathfrak{O}'))$. □

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 $\mathfrak{O}$, the following lemma explicitly constructs a new maximal order with an optimally embedded quadratic order of smaller conductor.

Lemma 5.4. *Let* ℓ *be a prime, and* $\beta \in \mathcal{O}_K$. *Let* $\mathfrak{O} \subseteq B$ *be a maximal order in which* $\mathbb{Z}[\ell\beta]$ *optimally embeds. Then there exists a maximal order* $\mathfrak{O}'$ *in which* $\mathbb{Z}[\beta]$ *optimally embeds, with* $d(\mathfrak{O}, \mathfrak{O}') = \ell$.

Proof. Consider $\mathfrak{O}_\ell \subseteq B_\ell$, given by completing at ℓ. By [31, Proposition 30.5.3], there are no optimal embeddings of $\mathbb{Z}[p\beta]$ in $\mathfrak{O}_p$ (so the conditions of the lemma cannot be satisfied if $\ell = p$), and for $\ell \neq p$ there is a unique optimal embedding of $\mathbb{Z}[\ell\beta]$ in $\mathfrak{O}_\ell$ up to conjugation. Explicitly, for $\ell \neq p$ we will have $\mathfrak{O}_\ell \cong M_2(\mathbb{Z}_p)$ [31, Corollary 10.5.5], and if $\beta^2 - t\beta + n = 0$ is the minimal polynomial for β, then the embedding $K \to M_2(\mathbb{Q}_p)$ defined by

$$\ell\beta \mapsto \begin{pmatrix} 0 & -\ell^2 n \\ 1 & \ell t \end{pmatrix},$$

[7] Eichler simply states that there must exist an ideal $\mathfrak{a}$ of $\mathcal{O}$ with $\mathfrak{O}\mathfrak{a} = \mathfrak{a}\mathfrak{O}'$, but he defines ideals to be locally principal [14, p. 133] and this implies invertibility.

induces an optimal embedding of $\mathbb{Z}[\ell\beta]$ into $M_2(\mathbb{Z}_p)$, unique up to conjugation by $\mathsf{GL}_2(\mathbb{Z}_p)$. The maximal order

$$\mathfrak{O}'_\ell := \begin{pmatrix} \mathbb{Z}_\ell & \ell\mathbb{Z}_\ell \\ \ell^{-1}\mathbb{Z}_\ell & \mathbb{Z}_\ell \end{pmatrix} \subseteq M_2(\mathbb{Q}_p)$$

contains $\left(\begin{smallmatrix} 0 & -\ell n \\ 1/\ell & t \end{smallmatrix}\right)$, the image of β, but does not contain the image of $\frac{1}{\ell}\beta$.

Now let

$$\mathfrak{O}' := \mathfrak{O}'_\ell \cap \bigcap_{q \neq \ell} \mathfrak{O}_q.$$

This is a maximal order because it is maximal at every prime. For all $q \neq \ell$ we have $\ell^{-1} \in \mathbb{Z}_q$, so $\mathcal{O}_{K,f}$ embeds into $\mathfrak{O}_q$, and hence $\mathcal{O}_{K,f}$ optimally embeds into $\mathfrak{O}'$. Finally, since $\mathfrak{O}$ and $\mathfrak{O}'$ are equal at every prime besides ℓ, we have

$$d(\mathfrak{O}, \mathfrak{O}') = |\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'| = |\mathfrak{O}_\ell : \mathfrak{O}_\ell \cap \mathfrak{O}'_\ell| = \ell. \qquad \square$$

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

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 $\mathfrak{O} =: \mathfrak{O}_0, \mathfrak{O}_1, \ldots, \mathfrak{O}_k = \widetilde{\mathfrak{O}}$, where $\mathcal{O}_{K,f_i}$ optimally embeds in $\mathfrak{O}_i$. Then

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

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 $\mathfrak{O}'$. Let $K \cong \mathbb{Q}(\alpha)$. To begin, take a vertical step from each of $\mathfrak{O}$ and $\mathfrak{O}'$ using Corollary 5.5: we obtain maximal orders $\widetilde{\mathfrak{O}}$ and $\widetilde{\mathfrak{O}'}$, both containing an optimally embedded $\mathcal{O}_K$, as well as bounds on $d(\mathfrak{O}, \widetilde{\mathfrak{O}})$ and $d(\mathfrak{O}', \widetilde{\mathfrak{O}'})$. Now join $\widetilde{\mathfrak{O}}$ and $\widetilde{\mathfrak{O}'}$ by a horizontal step using Lemma 5.3: this gives us an automorphism $\phi : B \to B$ and a bound on $d(\widetilde{\mathfrak{O}}, \phi(\widetilde{\mathfrak{O}'}))$. Combining these steps, we obtain a sequence

$$\mathfrak{O},\ \widetilde{\mathfrak{O}},\ \phi(\widetilde{\mathfrak{O}'}),\ \phi(\mathfrak{O}') \cong \mathfrak{O}'$$

with bounds on the consecutive distances; we can check that these are all bounded above by $\frac{4}{\pi}\sqrt{M}$. Since each of these orders contains an element with the same minimal polynomial as α or α', 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, we can factor the conductor of the optimally embedded orders into primes and take one step for each prime, as in the proof of Corollary 5.5. For the horizontal step, We can factor $\mathfrak{b}$ (from the proof of Lemma 5.3) into prime ideals as $\mathfrak{p}_1 \cdots \mathfrak{p}_s$. Set $\mathfrak{O}_0 = \mathfrak{O}$, and for each $i = 1, \ldots, s$, recursively define

$$\mathfrak{O}_i := \mathfrak{p}_i^{-1} \mathfrak{O}_{i-1} \mathfrak{p}_i.$$

Then $\mathcal{O}_K$ is optimally embedded in each $\mathfrak{O}_i$, and consecutive orders $\mathfrak{O}_{i-1}$ and $\mathfrak{O}_i$ are linked by the ideal $\mathfrak{O}_{i-1}\mathfrak{p}_i = \mathfrak{p}_i\mathfrak{O}_i$ of norm $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}_i)$. If we assume $\mathfrak{b}$ was chosen to be minimal, none of the $\mathfrak{p}_i$ 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 $\mathcal{S} \subseteq \mathbb{F}_{p^2}$ 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

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

We must prove that the sets T_D are disjoint, nonempty, and that every $j \in \mathcal{S}_M$ is in some T_D.

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

For any $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$, either $\alpha = \frac{\sqrt{D}}{2}$ or $\alpha = \frac{1+\sqrt{D}}{2}$ is an integral element of $\alpha \in \mathbb{Q}(\sqrt{D}) - \mathbb{Q}$, and the norm of α will be respectively $\frac{-D}{4} \leq M$ or $\frac{1-D}{4} \leq M$ (since it must be an integer). By the constraints on D, $\mathbb{Q}(\alpha)$ embeds into B [31, Proposition 14.6.7], and so the integral element α is contained in some maximal order. By the Deuring correspondence, this order is isomorphic to $\mathrm{End}(E_j)$ for some $j \in \mathcal{S}$. Hence there is an embedding $\iota : \mathbb{Z}[\alpha] \to \mathrm{End}(E_j)$, so j is M-small. Since $\mathbb{Q}(\iota(\alpha)) \cong \mathbb{Q}(\sqrt{D})$, we have $j \in T_D$, and so T_D is nonempty.

Suppose $j \in \mathcal{S}_M$, so there exists $\alpha \in \mathrm{End}(E_j) - \mathbb{Z}$ with $\deg(\alpha) \leq M$. Taking the minimal polynomial $x^2 - tx + \deg(\alpha)$ of α, $\deg(\alpha) \leq M$ implies $-4M \leq t^2 - 4\deg(\alpha) < 0$. 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 $\left(\frac{D}{p}\right) = -1$. 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 $D \neq D'$. For any $\mathfrak{O} \cong \mathrm{End}(E_j)$ and $\mathfrak{O}' \cong \mathrm{End}(E_{j'})$, we have $d(\mathfrak{O}, \mathfrak{O}')^2 \geq \frac{p}{4M^2}$ by Proposition 4.5. Thus Lemma 4.4 tells us that

$$d(j, j') = \min\{d(\mathfrak{O}, \mathfrak{O}') \mid \mathfrak{O} \cong \mathrm{End}(E_j),\ \mathfrak{O}' \cong \mathrm{End}(E_{j'})\} \geq \frac{\sqrt{p}}{2M}.$$

6.3. **Distances within T_D.** Suppose $j, j' \in T_D$, and let α, α' 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

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

with consecutive distances bounded by $\frac{4}{\pi}\sqrt{M}$, and each containing an element with the same minimal polynomial as either α or α'.

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

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

Because each E_{j_i} has an element with the same minimal polynomial as α or α', 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 $\mathfrak{O}_{i-1}$ to $\mathfrak{O}_i$ with prime norm at most $\frac{4}{\pi}\sqrt{M}$ 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 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 $\mathfrak{O}$ and $\mathfrak{O}'$, an ideal linking $\mathfrak{O}$ to $\mathfrak{O}'$ with S-powersmooth norm ($S \approx \frac{7}{2}\log p$) can be computed efficiently [20, Sections 4.5–4.7].
- (Oii) Given a supersingular elliptic curve E with known endomorphism ring $\mathrm{End}(E)$, and a left ideal of $\mathrm{End}(E)$ with S-powersmooth norm ($S \approx \frac{7}{2}\log p$), an isogeny out of E corresponding to I under the Deuring correspondence can be computed efficiently [15, Proposition 4].
- (Oiii) Given a maximal order $\mathfrak{O}$, a j-invariant such that $\mathrm{End}(E_j) \cong \mathfrak{O}$ can be computed efficiently [15, Section 7.1].

For each T_D, we can construct a maximal order $\mathfrak{O}_D$, and use Observation (Oiii) to find a j-invariant $j_D \in T_D$ 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 $j_{D'}^p$ as a composition of many small isogenies. 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. These algorithms are discussed further in Appendix A.

Isogenies defined over $\mathbb{F}_p$. Suppose j_1 and j_2 are M-small j-invariants in $\mathbb{F}_p$. Some situations, such as key recovery for the CSIDH protocol [6], require being able to find an $\mathbb{F}_p$-isogeny $E_{j_1} \to E_{j_2}$. While our algorithm allows us to construct an isogeny between these curves, this isogeny will not necessarily be defined over $\mathbb{F}_p$. This is solved by concurrent work of Castryck, Panny, and Vercauteren [7], in which they provide an algorithm to compute an $\mathbb{F}_p$-isogeny $E_{j_1} \to E_{j_2}$, given the endomorphism rings of E_{j_1} and E_{j_2} (which we are able to compute).

References

[1] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková. *Adventures in Supersingularland.* 2019. arXiv: 1909.07779 [math.NT].

[2] 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.

[3] Reinier Bröker. "Constructing supersingular elliptic curves". In: *Frontiers of Combinatorics and Number Theory* (Jan. 2009).

[4] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. "Modular Polynomials via Isogeny Volcanoes". In: *Mathematics of Computation* 81.278 (2012), pp. 1201–1231.

[5] John W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer, 1997. ISBN: 978-3-540-61788-4.

[6] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *IACR Cryptology ePrint Archive*. 2018.

[7] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. *Rational isogenies from irrational endomorphisms*. Cryptology ePrint Archive, Report 2019/1202. 2019. URL: https://eprint.iacr.org/2019/1202.

[8] 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.

[9] 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/S0305004100061697.

[10] 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.

[11] Harold Davenport. *Multiplicative number theory*. Ed. by Hugh L. Montgomery. 2nd ed. Springer, 2000.

[12] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. "Verifiable Delay Functions from Supersingular Isogenies and Pairings". In: *IACR Cryptology ePrint Archive* 2019 (2019), p. 166.

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

[14] Martin Eichler. "Zur Zahlentheorie der Quaternionen-Algebren". German. In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1955 (1955), pp. 127–151. DOI: 10.1515/crll.1955.195.127.

[15] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Cham: Springer International Publishing, 2018, pp. 329–368. ISBN: 978-3-319-78372-7.

[16] Noam D. Elkies. "The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$". In: *Inventiones mathematicae* 89.3 (Oct. 1987), pp. 561–567. DOI: 10.1007/BF01388985.

[17] Andrew Granville and Kannan Soundararajan. *Upper bounds for $|L(1,\chi)|$*. 2019. arXiv: math/0106176 [math.NT].

[18] Werner Hürlimann. "Dedekind's arithmetic function and primitive four squares counting functions". In: *Journal of Algebra and Number Theory: Advances and Applications* 14 (Dec. 2015), pp. 73–88. DOI: 10.18642/jantaa_7100121599.

[19] Masanobu Kaneko. "Supersingular j-invariants as singular moduli mod p". In: *Osaka Journal of Mathematics* 26.4 (1989), pp. 849–855. ISSN: 0030-6126.

[20] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. "On the quaternion ℓ-isogeny path problem". In: *LMS Journal of Computation and Mathematics* 17 (A June 2014), pp. 418–432. DOI: 10.1112/S1461157014000151.

[21] Serge Lang. *Elliptic functions*. Springer, 1987. ISBN: 978-1-4612-9142-8.

[22] Christophe Petit and Kristin E. Lauter. "Hard and Easy Problems for Supersingular Isogeny Graphs". In: (2017).

[23] Arnold Pizer. "An algorithm for computing modular forms on $\Gamma_0(N)$". In: *Journal of Algebra* 64 (1980), pp. 340–390.

[24] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994. ISBN: 978-0-387-09493-9.

[25] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. 2nd ed. Springer-Verlag, 2009. ISBN: 978-0-387-09493-9.

[26] Denis Simon. "Solving norm equations in relative number fields using S-units". In: *Mathematics of Computation* 71 (239 July 2002), pp. 1287–1305. DOI: 10.1090/S0025-5718-02-01309-1.

[27] Patrick Solé and Michel Planat. "Extreme Values of the Dedekind Ψ Function". In: *Journal of Combinatorics and Number Theory* 3.1 (2011), pp. 33–38.

[28] P. Stevenhagen. *Number Rings*. Oct. 2017. URL: http://websites.math.leidenuniv.nl/algebra/ant.pdf.

[29] Andrew Sutherland. "Isogeny Volcanoes". In: *The Open Book Series* 1 (Aug. 2012). DOI: 10.2140/obs.2013.1.507.

[30] Andrew V. Sutherland. "Computing Hilbert Class Polynomials with the Chinese Remainder Theorem". In: *Mathematics of Computation* 80.273 (2011), pp. 501–538.

[31] John Voight. *Quaternion Algebras*. Version v.0.9.19. May 2020. URL: https://math.dartmouth.edu/~jvoight/quat-book.pdf.

[32] John Michael Voight. "Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic". PhD thesis. Berkeley, CA, USA, 2005. ISBN: 0-542-29154-1.

[33] Wolfram Research, Inc. *Mathematica, Version 10.0*. Champaign, IL. 2014. URL: https://www.wolfram.com/mathematica.

[34] 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.

Appendix A. Computing Isogenies Between M-small Supersingular Curves

Let us elaborate on the approach described in Section 7. One subtle issue with this method 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.

A.1. Assumptions.

Recall 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 A.3 we carry out computations that depend on these assumptions for $p \approx 2^{256}$, $M = 100$, 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 $\mathrm{N}_{L/K}(z) = -p$ can be computed efficiently, if one exists.[8]

(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 $\mathrm{trd}(\omega\beta)$, it will not take too long before a choice of β such that the discriminant of the order $\mathbb{Z}\langle \omega, n\beta \rangle$ can be efficiently factored into primes.[9]

Lemma A.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 α with $\mathrm{nrd}(\alpha) \leq M$ 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 [31, Proposition 14.6.7]; this implies that $B \otimes_{\mathbb{Q}} K$ is split [31, Lemma 5.4.7], which implies by Theorem 5.4.6(vi) that there is a solution $\mathrm{N}_{K(i)/K}(z) = -p$ for some $z \in K[i]^\times$. Using assumption (Ai), we can solve for

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

in the norm equation, giving

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

After multiplying through by pq we have

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

---

[8] The algorithm for doing so is described in [26, Section 6], and is implemented in Magma [2] as `NormEquation(L, -p)`. In general, the bottleneck of the algorithm used to solve $\mathrm{N}_{L/K}(z) = m$ is to factor m into primes of K, but this is easy in our case because p is already an integer prime.

[9] 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.

Setting $\gamma = pi + qzj + xk$ and $\delta = qwj + yk$, we will have $\mathrm{trd}(\gamma\delta^{-1}) = 0$ and $\mathrm{nrd}(\gamma\delta^{-1}) = -D$ by the proof of Lemma 5.4.7 in [31], so that $\sqrt{D} \mapsto \gamma\delta^{-1}$ defines an embedding $\mathbb{Q}(\sqrt{D}) \hookrightarrow B$.

Take α to be whichever of $\frac{\sqrt{D}}{2}$ or $\frac{1+\sqrt{D}}{2}$ is integral (depending on whether $D \equiv 0$ or $1 \pmod 4$), considered now as an element of B. Take a random integral element $\beta \in B$ such that $\{1, \alpha, \beta\}$ is linearly independent. Setting n to be the denominator of $\mathrm{trd}(\alpha\beta)$, $\mathbb{Z}\langle\alpha, n\beta\rangle$ will be an order in B. If the discriminant of this order can be factored into primes (by assumption (Aii), this can be done after relatively few tries for β), we can efficiently compute a maximal order $\mathfrak{O}$ containing this using Proposition 4.3.4 of [32]. Noting that α has norm at most M, $\mathfrak{O}$ is the desired maximal order. □

A.2. **Algorithms for Computing Isogenies.** In order to compute isogenies, we will need to use modular polynomials.

Definition A.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^{6n} [9], 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 Φ_{659}, and 30 terabytes to store Φ_{20011} [4, 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 ℓ prime (the only case we will need) in time $O(\ell^{3+\varepsilon})$ [4, 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 $\frac{4}{\pi}\sqrt{M}$; 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 $\mathrm{End}(E_{j_D})$. Proposition 2.3 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 B.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 $\mathbb{F}_{p^2}$, 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 $\mathbb{F}_{p^2}$, 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

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 $\mathfrak{O}_D \subseteq B$ isomorphic to $\mathrm{End}(E_{j_D})$.

Compute $\Phi_\ell(x, y) \pmod p$ for all prime $\ell \leq \frac{4}{\pi}\sqrt{M}$ [4, Theorem 1].
Initialize an empty list $\mathcal{S}_M$.
for $-4M \leq d < 0$, $d \equiv 0$ *or* $1 \pmod 4$, $\left(\frac{d}{p}\right) = -1$ **do**
    Compute $H_{\mathcal{O}}(x)$, where $\mathcal{O}$ is the quadratic order of discriminant d [30, Theorem 1].
    Append all $j \in \mathbb{F}_{p^2}$ satisfying $H_{\mathcal{O}}(j) = 0$ to $\mathcal{S}_M$.
end
for *valid fundamental discriminants* D **do**
    Compute a maximal order $\mathfrak{O}_D$ that has some $\alpha \in \mathfrak{O}_D - \mathbb{Z}$ with $\mathrm{nrd}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D})$ (Lemma A.1).
    Compute $j_D \in \mathbb{F}_{p^2}$ such that $\mathrm{End}(E_{j_D}) \cong \mathfrak{O}_D$ (Oiii).
    Initialize queue $Q_D := (j_D)$ and empty list E'_D. Set $j := j_D$.
    while $j \in Q_D$ **do**
        for *prime* $2 \leq \ell \leq \frac{4}{\pi}\sqrt{M}$ **do**
            for $j' \in \mathcal{S}_M$ *such that* $\Phi_\ell(j', j) = 0 \pmod p$ *or* $\Phi_\ell(j', j^p) = 0 \pmod p$ **do**
                Append j' to the end of the queue Q_D.
                Append (j, j') to E'_D.
            end
        end
        Set j to be the next element of the queue Q_D. If no such element exists, break.
    end
    Set $T_D := Q_D \cup Q_D^p$.
    Set $E_D := \bigcup_{(j,j') \in E'_D} \{(j, j'), (j, j'^p), (j^p, j'), (j^p, j'^p)\}$.
end
For each valid fundamental discriminant D, return T_D, E_D, j_D, and $\mathfrak{O}_D$.

lemma gives us a condition on M under which such a curve will be guaranteed to exist.

Lemma A.3. *Let $q = -i^2$. If $M \geq q$, then there exists an M-small supersingular j-invariant in $\mathbb{F}_p$.*

Proof. There is a maximal order $\mathfrak{O}$ containing $\{1, i, j, k\}$, which corresponds by the Deuring correspondence to some supersingular j-invariant j. Since $i \in \mathfrak{O}$ and $\mathrm{nrd}(i) = q \leq M$, j is M-small. Since $j \in \mathfrak{O}$ and $\mathbb{Z}[j] \cong \mathbb{Z}[\sqrt{-p}]$, we have $j \in \mathbb{F}_p$ [13, 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

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 $E_{j_1} \to E_{j_2}$, given as a sequence of ℓ-isogenies for primes ℓ.

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 $\phi_{D_i} : E_{j_i} \to E_{j_{D_i}}$ or $\phi_{D_i} : E_{j_i} \to E^{(p)}_{j_{D_i}}$.
5 **end**
6 **for** $i \in \{1, 2\}$ **do** `// long paths between T_D`
7 Using $\mathfrak{O}_D$ and $\mathfrak{O}_{D_0}$ with Observations (Oi) and (Oii), find an isogeny $\Psi_i : E_{j_{D_0}} \to E_{j_{D_i}}$ or $\Psi_i : E_{j_{D_0}} \to E^{(p)}_{j_{D_i}}$.
8 Let $\widehat{\phi_{D_i}}$ denote the dual of ϕ_{D_i}. Choose $\alpha, \beta \in \{1, p\}$ such that the composition $\Gamma_i := \widehat{\phi_{D_i}} \circ \Psi_i^{\alpha} \circ \phi_{D_0}^{\beta} : E_{j_0} \to E_{j_i}$ is defined.
9 **end**
10 Return $\Gamma_2 \circ \widehat{\Gamma_1} : E_{j_1} \to E_{j_2}$.

curves $j_1, j_2 \in \mathcal{S}_M$. At each step in the algorithm, the isogenies in question may be recorded as a sequence of ℓ-isogenies for relatively small primes ℓ (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 $j_0 \in \mathcal{S}_M \cap \mathbb{F}_p$, a modification of Algorithm 2 can still produce isogenies between M-small supersingular curves. If we obtain an isogeny $E_{j_1} \to E^{(p)}_{j_2}$, we may simply compose this isogeny with the p^{th} power Frobenius $E^{(p)}_{j_2} \to E_{j_2}$. However, the resulting isogeny will be inseparable, and will not be expressible as a composition of ℓ-isogenies for small primes ℓ.

A.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 $p = 2^{256}+297$; 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 $\mathfrak{O}_D$ as in Algorithm 1, 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.

Appendix B. 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 B.1. *Let $\mathcal{O}$ have discriminant $-4M \leq \operatorname{disc}\mathcal{O} < 0$. Let $C_{\mathcal{O}}$ denote the set of isomorphism classes of elliptic curves E over $\overline{\mathbb{F}_p}$ such that $\mathcal{O}$ optimally embeds in $\operatorname{End}(E)$. Then*

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

Proof. The first inequality follows from Proposition 2.3 by counting roots, and we have the middle equality $\deg H_{\mathcal{O}}(x) = |\operatorname{Cl}(\mathcal{O})|$ by [10, 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

$$|\operatorname{Cl}(\mathcal{O})| \leq h(D) f \prod_{\text{prime } \ell \mid f} \left(1 - \left(\frac{D}{p}\right)\frac{1}{p}\right)$$

using the formula for the class number of nonmaximal orders [10, Theorem 7.24]. We can bound this above by $h(D)\psi(f)$ using the Dedekind ψ function, defined on positive integers as

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

We have $\psi(n) = O(n \log\log n)$ [27, Corollary 3.2], and the classical bound $h(D) = O(|D|^{1/2} \log D)$ (for instance, by Dirichlet's class number formula [11, §6 (15)] and bounds of the form $|L(1, \chi_D)| = O(\log D)$ [17]). Together these give the bound

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

using $f^2|D| = \operatorname{disc}\mathcal{O} \leq 4M$. □

Proposition B.2. *Let D be a fundamental discriminant, and*

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

be the set from Theorem 1.3 (defined 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 many different quadratic orders optimally embed into endomorphism rings of curves in T_D (N is large), but each quadratic order embeds in only a couple of these endomorphism rings ($h(D)$ is small). If D is comparable to M, then there are very few quadratic orders that optimally embed into endomorphism rings of curves in T_D (N is small), but each quadratic order optimally embeds into many different endomorphism rings ($h(D)$ 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 α with $\operatorname{nrd}(\alpha) \leq M$ 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 $\operatorname{nrd}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong K$. We have $\alpha \in \mathfrak{O} \cap \mathbb{Q}(\alpha) \cong \mathcal{O}_{K,f}$ for some conductor f. We must have $f^2|D|/4 \leq \operatorname{nrd}(\alpha) \leq M$, implying that

$f \leq \lfloor \sqrt{4M/|D|} \rfloor = N$. Hence, summing over all possible quadratic orders of K with conductors in this range, we have

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

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

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

by [18, Lemma 2.1]. 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 B.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 $\operatorname{nrd}(\alpha) \leq M$. Then α is in some quadratic order $\mathcal{O}$, and $|\operatorname{disc} \mathcal{O}|/4 \leq \operatorname{nrd}(\alpha)$ implies $-4M \leq \operatorname{disc} \mathcal{O} < 0$. For every possible quadratic order, there are at most $|\operatorname{Cl}(\mathcal{O})|$ isomorphism classes of maximal orders in which $\mathcal{O}$ is optimally embedded, meaning that we obtain an upper bound for the number of M-small maximal orders by summing $|\operatorname{Cl}(\mathcal{O})|$ over all quadratic orders with $-4M \leq \operatorname{disc} \mathcal{O} < 0$.

A quadratic order $\mathcal{O}$ is uniquely determined by its discriminant, and there is a bijection between $\operatorname{Cl}(\mathcal{O})$ and the set of reduced primitive positive-definite binary quadratic forms of discriminant $\operatorname{disc} \mathcal{O}$ (Theorem 7.7(ii) and Theorem 2.8 of [10]). 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 $a \leq c \leq \frac{a}{4} + \frac{M}{a}$. Together with $-a < b \leq a$ we conclude that there are at most

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

valid pairs (b, c) for a given a; summing over the $\sqrt{4M/3}$ options for a gives $O(M^{3/2})$ triples. □

Remark B.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 A.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 $H_{\mathcal{O}}(x) \pmod p$ is supersingular if and only if p does not split in the field of fractions of $\mathcal{O}$ (Proposition 2.3). 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.

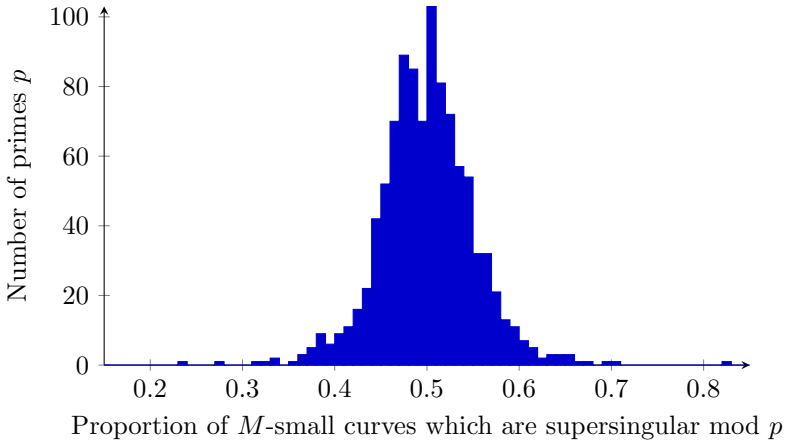

FIGURE 2. A histogram (bins of width 0.01) of the proportion of 100-small curves that are supersingular mod p, as p varies over 1000 consecutive primes $2^{40} < p \leq 2^{40} + 27201$. Discussed in Remark B.4. Data computed using Magma [2].

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 $H_{\mathcal{O}}(x) \pmod p$ 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 $-4M \leq \operatorname{disc} \mathcal{O} < 0$, by Theorem 4.7. So for $M \ll p$, we expect the set roots of $H_{\mathcal{O}}(x) \pmod p$ for $-4M \leq \operatorname{disc} \mathcal{O} < 0$ to have similar numbers of ordinary and supersingular curves.

Proposition B.5. *All supersingular j-invariants are $\left(\frac{1}{2}p^{2/3} + \frac{1}{4}\right)$-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 $\left(Cp^{\theta}\right)$-small.*

The sufficiency of $\frac{2}{3}$ was noted by Elkies [16, Section 4], and Yang showed that no smaller exponent could be taken [34, 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.

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 $\mathfrak{O} \subseteq B$ will be a 4-dimensional lattice of covolume $\frac{p}{4}$ under this embedding [8, (2.2)]. Projecting $\mathfrak{O}$ onto the orthogonal complement of 1 gives a 3-dimensional lattice of covolume $\frac{p}{4}$. By Theorem II.III.A of [5], any such lattice must have a nonzero element v with

length

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

An element of $\mathfrak{O}$ that projected onto v must be of the form $\frac{k}{2}+v$ for some integer k, because the reduced trace of an integral element is an integer. Hence either $v \in \mathfrak{O}$ or $\frac{1}{2}+v \in \mathfrak{O}$, and the reduced norm is either $\frac{1}{2}p^{2/3}$ or $\frac{1}{2}p^{2/3}+\frac{1}{4}$. This shows $\mathfrak{O}$ is $\left(\frac{1}{2}p^{2/3}+\frac{1}{4}\right)$-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 B.3). So if $\theta < \frac{2}{3}$ then the number of (Cp^θ)-small curves will be $O(p^{3\theta/2})$, with $\frac{3\theta}{2} < 1$. But the number of supersingular curves is $\frac{p}{12}+O(1)$ [25, Theorem V.4.1(c)], which grows faster than the set of (Cp^θ)-small curves. □

Appendix C. Prime-to-ℓ isogenies repel length-ℓ vertical steps

For this appendix, we assume the setup of Sections 3–5.

Recall Lemma 5.4, which states that given any maximal order $\mathfrak{O}$ with $\mathbb{Z}[\ell\beta]$ optimally embedded, there is a maximal order $\mathfrak{O}'$ with $\mathbb{Z}[\beta]$ optimally embedded which is distance ℓ away. If we replace $\mathfrak{O}'$ with an isomorphic order $\mathfrak{O}''$, the following proposition and corollary show that $d(\mathfrak{O},\mathfrak{O}'')$ must be either a multiple of ℓ or extremely large. This indicates why we must consider all primes in order to find a short path in Proposition 4.6 and Theorem 1.3(b).

Proposition C.1. *Let ℓ be a prime, and $\beta \in \mathcal{O}_K$. Suppose maximal orders $\mathfrak{O}$ and $\mathfrak{O}'$ have $\mathbb{Z}[\ell\beta]$ and $\mathbb{Z}[\beta]$ optimally embedded, respectively. If $d(\mathfrak{O},\mathfrak{O}')$ is not divisible by ℓ, then $d(\mathfrak{O},\mathfrak{O}') \ge \frac{p}{4\ell\,\mathrm{nrd}(\beta)}$.*

Proof. If the optimal embeddings of $\mathbb{Z}[\ell\beta]$ and $\mathbb{Z}[\beta]$ were to land in the same subfield $K \subseteq B$, then $|\mathfrak{O}' : \mathfrak{O}\cap\mathfrak{O}'|$ would be divisible by ℓ, a contradiction. Hence we must have $\mathfrak{O}\cap K \cong \mathbb{Z}[\ell\beta]$ and $\mathfrak{O}'\cap K' \cong \mathbb{Z}[\beta]$ for distinct (but isomorphic) fields K. let $\mathcal{O} := \mathfrak{O}\cap K$ and $\mathcal{O}' := \mathfrak{O}\cap K'$ both be optimally embedded in $\mathfrak{O}$. Since K and K' are isomorphic but distinct, Theorem 4.7 tells us that $\operatorname{disc}\mathcal{O}\operatorname{disc}\mathcal{O}' \ge p^2$.

Now $\ell\beta \in \mathcal{O}$ and $d\beta \in \mathcal{O}'$, so as in the proof of Proposition 4.5, we can conclude that

$$d^2 \ge \frac{\operatorname{disc}\mathcal{O}}{4\ell^2\,\mathrm{nrd}(\beta)}\frac{\operatorname{disc}\mathcal{O}'}{4\,\mathrm{nrd}(\beta)} \ge \frac{p^2}{16\ell^2\,\mathrm{nrd}(\beta)^2}.$$ □

Corollary C.2. *Let ℓ be a prime, $M \in \mathbb{Z}$, and E an (M/ℓ^2)-small supersingular curve over $\mathbb{F}_{p^2}$. Then there exists an M-small supersingular curve E' over $\mathbb{F}_{p^2}$ connected to E by an ℓ-isogeny, such that if $\phi : E \to E'$ is any isogeny with degree relatively prime to ℓ, then*

$$\deg\phi \ge \frac{p\ell}{4M}.$$

Proof. For some imaginary quadratic field K and some $\beta \in K$ with norm at most M/ℓ^2, the quadratic order $\mathbb{Z}[\beta]$ is optimally embedded in $\mathrm{End}(E)$. Modifying the proof of Lemma 5.4, we can find a maximal order $\mathfrak{O}'$ with $\mathbb{Z}[\ell\beta]$ optimally embedded, and such that $d(\mathrm{End}(E),\mathfrak{O}') = \ell$. By the Deuring correspondence, we obtain an M-small curve E' connected to E by an ℓ-isogeny.

Now any isogeny $\phi : E \to E'$ corresponds to an ideal I linking $\mathrm{End}(E)$ to some maximal order $\mathfrak{O}'' \cong \mathrm{End}(E')$. In particular, I must be contained in $\mathfrak{O}\cap\mathfrak{O}''$, so

if $\deg \phi = \mathrm{nrd}(I)$ is not divisible by ℓ, then neither is $d(\mathrm{End}(E), \mathfrak{O}'')$. Hence, by Proposition C.1,

$$\deg \phi = \mathrm{nrd}(I) \geq d(\mathrm{End}(E), \mathfrak{O}'') \geq \frac{p}{4\ell \,\mathrm{nrd}(\beta)} \geq \frac{p\ell}{4M}. \qquad \square$$

(Jonathan Love) Stanford University, Dept. of Mathematics
E-mail address: jonlove@stanford.edu

(Dan Boneh) Stanford University, Dept. of Computer Science
E-mail address: dabo@cs.stanford.edu