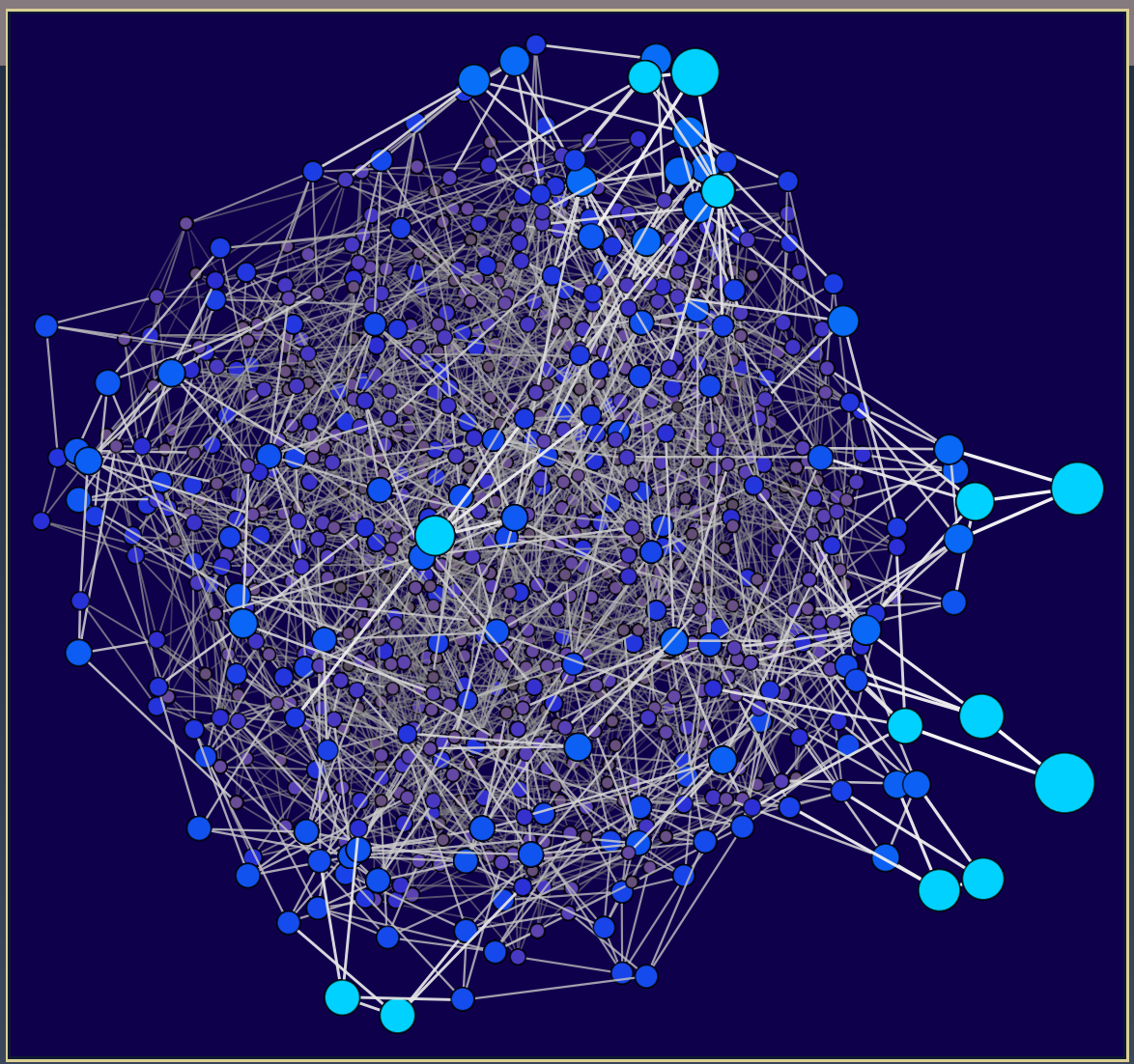
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Supersingular curves with small noninteger endomorphisms

Jonathan Love and Dan Boneh



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.7

msp

Supersingular curves with small noninteger endomorphisms

Jonathan Love and Dan Boneh

We introduce a special class of supersingular curves over $\mathbb{F}_{p^2}$, characterized by the existence of noninteger endomorphisms of small degree. We prove a number of properties about this set. Most notably, we can partition this set into subsets such 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 distinct subsets can heuristically be computed efficiently, giving a technique for computing isogenies between certain prescribed curves that cannot be efficiently found by searching on ℓ-isogeny graphs.

1. Introduction

Given an elliptic curve E over a field k, let $\mathrm{End}(E)$ denote the ring of endomorphisms of E that are defined over $\overline{k}$. The curve E is *supersingular* if $\mathrm{End}(E)$ is noncommutative; this can only occur if E is defined over $\mathbb{F}_{p^2}$ for some prime p [19, Theorem V.3.1]. The set $\mathrm{SS}(p)$ of all supersingular curves up to $\overline{\mathbb{F}}_p$-isomorphism can be quite complicated, but in this paper we define subsets of $\mathrm{SS}(p)$ which are relatively straightforward 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 $\overline{\mathbb{F}}_p$-isomorphism classes of *supersingular* M-small curves over $\mathbb{F}_{p^2}$ is denoted $\mathrm{SS}^M(p)$.

Assume for the rest of this paper that $p \geq 5$. We will study the structure of the set $\mathrm{SS}^M(p)$ of supersingular M-small curves, and in particular, we will discuss the following properties of this set:

(a) If $M < \sqrt{p}/2$, the set $\mathrm{SS}^M(p)$ 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 $\sqrt{p}/(2M)$ between distinct subsets (Theorem 1.3).

This research was supported by NSF grant #1701567.
MSC2010: 11G20, 11R52, 11T71.
Keywords: supersingular, elliptic curve, isogeny graph, M-small, endomorphism, quaternion, maximal order, Deuring correspondence, partition, archipelago, island, airport, orientation, Hilbert class polynomial.

(b) 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 (a) 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]

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 $\overline{\mathbb{F}}_p$.

By basic properties of isogenies (e.g., [19, 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 $\{E, E^{(p)}\}$.

Given a positive integer M and a fundamental discriminant D, we can define the following subset of $\mathrm{SS}^M(p)$:

$$T_D^M := \{E \in \mathrm{SS}(p) : \mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D}) \text{ for some } \alpha \in \mathrm{End}(E) - \mathbb{Z} \text{ with } \deg \alpha \leq M\}.$$

Theorem 1.3. *Let M be a positive integer. Then $\mathrm{SS}^M(p)$ is a union*

$$\mathrm{SS}^M(p) = \bigcup_D T_D^M,$$

of nonempty subsets T_D^M, indexed by fundamental discriminants $-4M \leq D < 0$ which are not congruent to a square mod p. These sets have the following properties:

(a) *If E, E' are in distinct subsets $T_D^M \neq T_{D'}^M$, then*

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

(b) *If E, E' are in the same T_D^M, then there is a sequence $E = E_0, E_1, \ldots, E_r = E'$ of elements of T_D^M such that*

$$d(E_{i-1}, E_i) \leq \tfrac{2}{3}\sqrt{3M}$$

for all $i = 1, \ldots, r$. We can take $r \leq 3$, or alternatively, we can take $r \leq 3\log_2\left(\frac{2}{3}\sqrt{3M}\right)$ and require all $d(E_{i-1}, E_i)$ to be prime.

Remark 1.4. If $M < \frac{1}{2}\sqrt{p}$, then Theorem 1.3(a) implies that the sets T_D^M are disjoint, and hence form a partition of $\mathrm{SS}^M(p)$.

Figure 1 illustrates Theorem 1.3 for $p = 20011$ and $M = 12$. In particular, since $\sqrt{20011}/(2 \cdot 12) \approx 5.9$, Theorem 1.3(a) predicts that curves in distinct sets T_D^M are at least two steps apart in the graph. Also, as the primes less than $\frac{2}{3}\sqrt{3 \cdot 12}$ are 2 and 3, Theorem 1.3(b) predicts that the sets T_D^M are connected components of the subgraph of 12-small curves. One can see that both these claims are true in the figure.

[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.

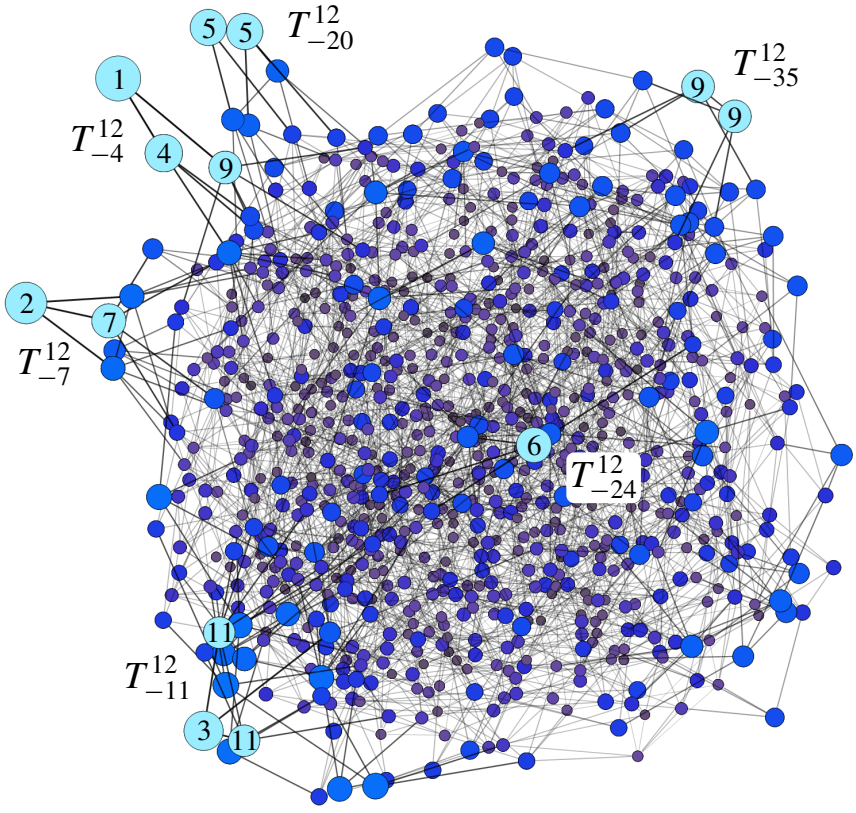


Figure 1. Supersingular curves in characteristic 20011 with conjugate pairs $\{E, E^{(p)}\}$ identified. The 12-small curves are highlighted and labeled with the smallest degree of a noninteger endomorphism. The sets T_D^M from Theorem 1.3 are indicated. Two curves E, E' are connected by an edge if there is an isogeny $E \to E'$ of degree 2 or 3. Data computed using Magma, plotted using Mathematica.

If we think of M minus the degree of the smallest noninteger endomorphism as a measure of elevation, then the set of supersingular curves can be thought of as an archipelago. The M-small curves are above sea level, and hence are easy to find and to study (Section 2). Each set T_D^M is an island: curves on the same island are close enough to walk between, but distinct islands are very far from each other. We shall see in Section 5 that the islands T_D^M are closely related to the craters of isogeny volcanoes (which appear in ordinary isogeny graphs [22] and in oriented supersingular isogeny graphs [7; 16]), so perhaps we can say that this archipelago was formed by volcanic activity! In Section 7 we will construct "airports" that allow us to efficiently travel between the islands, allowing us to find isogenies between any two M-small supersingular curves. Unfortunately, most supersingular curves remain deep underwater, shrouded in mystery.

The fact that the sets T_D^M are connected by small-degree isogenies (as described in Theorem 1.3(b)) will not be evident if we only consider isogenies of a single prime degree. In fact, if ℓ is a small prime, then under relatively mild conditions on M (Remark 6.2), there are two M-small curves that are connected by a degree ℓ isogeny, but such that any isogeny of degree relatively prime to ℓ will have degree greater

than $p\ell/(4M)$. So if we exclude isogenies of degree divisible by ℓ for any sufficiently small prime ℓ, the sets T_D^M will no longer be connected by short paths.

1A. ***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., [9]) 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. One can generate a large number of supersingular curves by starting at E_0 and taking a random walk along the graph of degree ℓ isogenies for some small prime ℓ. However, for any curve E found in this way, we can compute $\mathrm{End}(E)$ using the isogeny path from E_0 to E.

We may consider 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 (a) 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 (b) suggests that this is likely not the case, and that a hard curve will not be M-small. By the classification results of Section 2, this rules out using roots of low-degree Hilbert class polynomials as a reasonable candidate for a method of constructing hard curves. It remains an open problem to construct a single explicit hard supersingular curve.

1B. ***Organization.*** We briefly discuss how to generate M-small curves in Section 2, and begin the proof of Theorem 1.3 with Lemma 2.3. An overview of some concepts we will need from the theory of quaternion algebras[2] can be found in Section 3. In Section 4 we define a notion of distance for maximal orders of quaternion algebras, and use it to prove Theorem 1.3(a). We review the theory of orientations of supersingular curves in Section 5 and use this theory to prove Theorem 1.3(b). In Section 6 we show that certain isogenies of degree ℓ cannot be replaced by short isogenies of degree relatively prime to ℓ. We finish by describing an algorithm for computing isogenies between elliptic curves in Section 7.

A list of (mostly standard) results on the sizes of various sets of M-small curves can be found in an appendix, available with the unpublished version of this paper [15].

2. Hilbert class polynomials and M-small curves

Most well-known examples of supersingular curves are M-small for relatively small values of M. For instance, supersingular curves with a nontrivial 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 [2] proposes a general algorithm for producing a supersingular

[2]Many prior papers on supersingular isogenies use the structure of quaternion algebras to study supersingular isogenies; see for instance [13] and [10].

curve over an arbitrary finite field. We will show that his algorithm returns M-small curves, and then discuss how to generalize his approach to generate all M-small curves.

A ring $\mathcal{O}$ is a *quadratic order* if it is a finite-index subring of the ring of integers $\mathcal{O}_K$ of some imaginary quadratic field K. To each quadratic order $\mathcal{O}$, we can associate its *Hilbert class polynomial* $H_{\mathcal{O}}(x) \in \mathbb{Z}[x]$, which has the property that $z \in \mathbb{C}$ is a root of $H_{\mathcal{O}}$ if and only if z is the j-invariant of an elliptic curve $\widetilde{E}$ over $\mathbb{C}$ with endomorphism ring isomorphic to $\mathcal{O}$ [8, Proposition 13.2]. The degree of $H_{\mathcal{O}}$ equals the class number of $\mathcal{O}$.

Bröker's algorithm [2, Algorithm 2.4] proceeds as follows. To construct a supersingular curve over $\mathbb{F}_p$ with $p \equiv 1 \pmod 4$,[3] one first finds a small prime $q \equiv 3 \pmod 4$ with Legendre symbol $(-q/p) = -1$. We compute the Hilbert class polynomial $H_{\mathcal{O}_K}(x)$ for $K = \mathbb{Q}(\sqrt{-q})$, and find a root of $H_{\mathcal{O}_K}(x) \pmod p$ in $\mathbb{F}_p$. The condition $(-q/p) = -1$ then guarantees that this root is the j-invariant of a supersingular curve. This algorithm generates M-small curves for a reasonably small value of M, as the following proposition shows.

Proposition 2.1. *The supersingular curves found by Algorithm* 2.4 *of* [2] *are* $((q+1)/4)$*-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 is 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, $(1+\sqrt{-q})/2 \in \mathcal{O}_K$ is a noninteger endomorphism of $\widetilde{E}$. The reduction map $\mathrm{End}(\widetilde{E}) \to \mathrm{End}(E)$ is a degree-preserving injection [20, Proposition II.4.4], so $\mathrm{End}(E)$ contains a noninteger endomorphism of norm $(q+1)/4$, proving that E is $((q+1)/4)$-small. As discussed in the proof of [2, Lemma 2.5], under GRH we can take $q = O(\log^2 p)$. □

A natural generalization of Bröker's algorithm is to compute all roots (not just those in $\mathbb{F}_p$) of $H_{\mathcal{O}}(x) \pmod p$, for all imaginary quadratic orders $\mathcal{O}$ with sufficiently small discriminant. By Proposition 2.2, this process can be used to generate the set of all M-small elliptic curves. Note that if M is an integer, then an imaginary quadratic order $\mathcal{O}$ has discriminant $|\mathrm{disc}\,\mathcal{O}| \le 4M$ if and only if $\mathcal{O} - \mathbb{Z}$ has an element with norm at most M.

Proposition 2.2. *Let* $M \in \mathbb{Z}$ *satisfy* $3 \le M < p$, *let* E *be an elliptic curve over a finite field of characteristic* p, *and let* $z \in \overline{\mathbb{F}}_p$ *be the* j*-invariant of* E. *Then* E *is* M*-small if and only if* $H_{\mathcal{O}}(z) = 0$ *for some quadratic order* $\mathcal{O}$ *with discriminant* $-4M \le \mathrm{disc}\,\mathcal{O} < 0$. *In this setting* $\mathrm{End}(E)$ *contains an isomorphic copy of* $\mathcal{O}$, *and* E *is supersingular if and only if* p *does not split in the field of fractions of* $\mathcal{O}$.

The proof is analogous to that of Proposition 2.1, applying Deuring's lifting theorem [14, Theorem 13.14] to show that every M-small curve arises in this way. This result allows us to prove the first portion of Theorem 1.3.

Lemma 2.3. *The sets* T_D^M *appearing in Theorem 1.3 are nonempty, and their union is* $\mathrm{SS}^M(p)$.

[3] 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.

Proof. Given any fundamental discriminant $-4M \leq D < 0$ with $(D/p) = -1$, p does not split in the quadratic field K with discriminant D. So by Proposition 2.2, the roots of $H_{\mathcal{O}_K}(x) \pmod p$ are j-invariants of M-small supersingular curves in T_D^M.

Now consider $E \in \mathrm{SS}^M(p)$. By Proposition 2.2, $\mathrm{End}(E)$ contains a quadratic order $\mathcal{O}$ with discriminant $-4M < \operatorname{disc} \mathcal{O} < 0$, and p does not split in the field of fractions of $\mathcal{O}$. Letting D be the discriminant of the field of fractions of $\mathcal{O}$, we hence have $-4M \leq D < 0$ and $(D/p) = -1$. Since M is an integer, $\mathcal{O} - \mathbb{Z}$ contains an element with norm at most M, so that $E \in T_D^M$. □

3. Maximal orders of quaternion algebras

Unless otherwise cited, all the material in this section can be found in [25].

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

$$B := \{w + xi + yj + zk : w, x, y, z \in \mathbb{Q}\}, \qquad i^2 = -q,\ j^2 = -p,\ ij = -ji = k$$

for an appropriate integer q depending on $p \pmod 8$ [17, Proposition 5.1].

Given $\alpha = w + xi + yj + zk \in B$, we define its *conjugate*, $\overline{\alpha} := w - ix - jy - kz$, its *reduced norm*, $\mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = w^2 + qx^2 + py^2 + qpz^2$, and its *reduced trace*, $\mathrm{trd}(\alpha) := \alpha + \overline{\alpha} = 2w$. 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. Any $\alpha \notin \mathbb{Q}$ generates an imaginary quadratic subfield $\mathbb{Q}(\alpha) \subseteq B$. Conversely, an imaginary quadratic field K embeds into B if and only if p does not split in K [25, Proposition 14.6.7], or equivalently, if the Legendre symbol $((\operatorname{disc} K)/p)$ is not equal to 1.

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. An order is *maximal* if there are no orders properly containing it. 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

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

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 $K \subseteq B$. The map $\mathcal{O} \to B$ with image $\mathfrak{O} \cap K$ is an *optimal embedding*.

3A. ***The Deuring correspondence.*** Let $\mathrm{SS}(p) \subseteq \mathbb{F}_{p^2}$ denote the set of supersingular curves up to $\overline{\mathbb{F}}_p$-isomorphism. Given $E \in \mathrm{SS}(p)$, $\mathrm{End}(E)$ will be isomorphic to a maximal order in B. If E and $E^{(p)}$ are Frobenius conjugates, then $\mathrm{End}(E)$ and $\mathrm{End}(E^{(p)})$ will be isomorphic orders. Aside from this relation, nonisomorphic curves will always have nonisomorphic endomorphism rings. In fact, we have a bijection, known as the *Deuring correspondence*

$$\mathrm{SS}(p)/(E \sim E^{(p)}) \;\leftrightarrow\; \{\text{maximal orders of } B\}/\cong$$

sending E to the set of maximal orders isomorphic to $\mathrm{End}(E)$. 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, if we fix $E \in \mathrm{SS}(p)$ and a maximal order $\mathfrak{O}_E \cong \mathrm{End}(E)$, then we have a one-to-one correspondence

$$\{\text{separable isogenies out of } E\}/\cong \;\leftrightarrow\; \{\text{left ideals of } \mathfrak{O}_E\}.$$

An isogeny $\phi : E \to E'$ will correspond to an ideal I linking $\mathfrak{O}_E$ to some maximal order $\mathfrak{O}_{E'}$ isomorphic to $\mathrm{End}(E')$, and $\deg \phi = \mathrm{nrd}(I)$.

4. Large distances between T_D^M

We first define a notion of distance between maximal orders and prove some of its properties. We will then use this notion to prove part (a) of Theorem 1.3.

4A. ***Distance between maximal orders.***

Definition 4.1. Given maximal orders $\mathfrak{O}, \mathfrak{O}' \subseteq B$, the *distance from* $\mathfrak{O}$ *to* $\mathfrak{O}'$, $d(\mathfrak{O}, \mathfrak{O}')$, is any of the following quantities:

(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 $\mathfrak{O}'$.

Lemma 4.2. *The three quantities in Definition 4.1 are all equal.*

Proof. We observe that these values are equal if and only if the corresponding quantities obtained by localizing at each prime are all equal [25, 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 [25, 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 [25, 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

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

Note that $\log d$ defines a metric on the set of maximal orders of B; the triangle inequality follows because $\mathrm{nrd}(IJ) \leq \mathrm{nrd}(I)\,\mathrm{nrd}(J)$ for any compatible ideals I and J [25, Example 16.3.6]. Unlike distances between elliptic curves, Definition 4.1 is *not* isomorphism-invariant, but we can relate the two notions of distance as follows.

Lemma 4.3. *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

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

4B. ***Proof of Theorem 1.3(a).*** Suppose that $E \in T_D^M$ and $E' \in T_{D'}^M$. Let $\mathfrak{O} \cong \mathrm{End}(E)$ and $\mathfrak{O}' \cong \mathrm{End}(E')$ be maximal orders in B. Thus there exist $\alpha \in \mathfrak{O} - \mathbb{Z}$ and $\alpha' \in \mathfrak{O}' - \mathbb{Z}$, each with reduced norm at most M. The quadratic orders

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

are both optimally embedded in $\mathfrak{O}$. Since $\mathbb{Q}(\alpha) \ncong \mathbb{Q}(\alpha')$, $\mathcal{O}$ and $\mathcal{O}'$ are distinct. Hence

$$\mathrm{disc}\,\mathcal{O}\,\mathrm{disc}\,\mathcal{O}' \geq 4p,$$

as a result of the following theorem due to Kaneko.

Theorem 4.4 [12, 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* $\mathrm{disc}\,\mathcal{O}\,\mathrm{disc}\,\mathcal{O}' \geq p^2$.

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

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

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 we did with $\mathrm{nrd}(\alpha)$, we can compute $d^2\,\mathrm{nrd}(\alpha') \geq \frac{1}{4}\,\mathrm{disc}\,\mathcal{O}'$. Hence

$$d^2 M^2 \geq d^2\,\mathrm{nrd}(\alpha)\,\mathrm{nrd}(\alpha') \geq \frac{1}{16}\,\mathrm{disc}\,\mathcal{O}\,\mathrm{disc}\,\mathcal{O}' \geq \frac{p}{4}.$$

This implies that $d(\mathfrak{O}, \mathfrak{O}') \geq \sqrt{p}/(2M)$. Since this bound holds for all maximal orders $\mathfrak{O} \cong \mathrm{End}(E)$ and $\mathfrak{O}' \cong \mathrm{End}(E')$, Lemma 4.3 allows us to conclude that $d(E, E') \geq \sqrt{p}/(2M)$, concluding the proof of Theorem 1.3(a).

5. Short paths within T_D^M

We first introduce the theory of orientations[4] as defined by Colò and Kohel [7]. We then use these results to prove part (b) of Theorem 1.3.

5A. *Orientations.*

Definition 5.1. Given a supersingular curve $E \in \mathrm{SS}(p)$ and an imaginary quadratic field K, a *K-orientation* of E is a fixed embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$. Given a quadratic order $\mathcal{O} \subseteq K$, a K-orientation is a *primitive $\mathcal{O}$-orientation* if $\mathrm{End}(E) \cap \iota(K) \cong \mathcal{O}$, or in other words, if ι restricted to $\mathcal{O}$ is an optimal embedding of $\mathcal{O}$ in $\mathrm{End}(E)$.

Definition 5.2. If $E, E' \in \mathrm{SS}(p)$ have K-orientations ι and ι', respectively, an isogeny $\phi : E \to E'$ is *K-oriented* if

$$\iota'(x) = \frac{1}{\deg \phi} \phi \circ \iota(x) \circ \widehat{\phi}, \qquad x \in K,$$

where $\widehat{\phi}$ denotes the dual isogeny of ϕ.

Let $\mathrm{SS}_{\mathcal{O}}(p)$ denote the set of elliptic curves equipped with a primitive $\mathcal{O}$-orientation, up to K-oriented isomorphism. Onuki describes two types of isogenies that we will use to construct paths. First there are "ascending" isogenies, which can be used to decrease the conductor of the optimally embedded quadratic order.

Proposition 5.3 [16, Proposition 4.1]. *Suppose ℓ is a prime and f is a positive integer. Let $\mathcal{O} \subseteq K$ have conductor ℓf, and $\mathcal{O}' \subseteq K$ have conductor f. Then for any $(E, \iota) \in \mathrm{SS}_{\mathcal{O}}(p)$, there exists $(E', \iota') \in \mathrm{SS}_{\mathcal{O}'}(p)$ with a K-oriented isogeny $E \to E'$ of degree ℓ.*

In order to describe "horizontal" isogenies, we first describe an action of the class group $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{SS}_{\mathcal{O}}(p)$. Given an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ relatively prime to p, and a curve E with a primitive $\mathcal{O}$-orientation, define the $\mathfrak{a}$-torsion subgroup

$$E[\mathfrak{a}] := \bigcap_{x \in \mathfrak{a}} \ker \iota(x).$$

Up to K-oriented isomorphism, there is a unique elliptic curve $(\mathfrak{a} * E)$ with a primitive $\mathcal{O}$-orientation and a separable isogeny $\phi_{\mathfrak{a}} : E \to (\mathfrak{a} * E)$ such that $\ker \phi_{\mathfrak{a}} = E[\mathfrak{a}]$ [16, Proposition 3.5]. Since principal ideals act by endomorphisms, the action $(\mathfrak{a}, E) \mapsto \mathfrak{a} * E$ is well-defined on ideal classes.

Proposition 5.4 [16, Proposition 3.3 and Theorem 3.4]. *Suppose p does not divide the conductor of $\mathcal{O}$. Either the ideal class group $\mathrm{Cl}(\mathcal{O})$ acts transitively on $\mathrm{SS}_{\mathcal{O}}(p)$, or $\mathrm{SS}_{\mathcal{O}}(p)$ splits into two conjugate orbits: (E, ι) is in one orbit if and only if $(E^{(p)}, \iota^{(p)})$ is in the other.*

[4] A previous version of this paper took a different approach to proving analogues of Propositions 5.3 and 5.4. While the underlying ideas are similar, we have found that the language of orientations provides a much cleaner framework for these results.

Suppose $E \in \mathrm{SS}_{\mathcal{O}}(p)$ and $\mathfrak{a}$ is an invertible ideal of $\mathcal{O}$ relatively prime to p. The proof of [16, Proposition 3.5] shows that the dual isogeny of $\phi_{\mathfrak{a}}$ has kernel $(\mathfrak{a} * E)[\overline{\mathfrak{a}}]$, and so by the proof of [16, Proposition 3.6], $\widehat{\phi}_{\mathfrak{a}} \circ \phi_{\mathfrak{a}}$ has kernel $E[\overline{\mathfrak{a}}\mathfrak{a}] = E[\mathrm{N}(\mathfrak{a})]$. Thus

$$\begin{aligned}(\deg \phi_{\mathfrak{a}})^2 &= \deg(\widehat{\phi}_{\mathfrak{a}} \circ \phi_{\mathfrak{a}}) \\ &= |E[\mathrm{N}(\mathfrak{a})]| = \mathrm{N}(\mathfrak{a})^2,\end{aligned}$$

so we can conclude that $\deg \phi_{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})$.

5B. ***Proof of Theorem 1.3(b).*** Suppose $E, E' \in T_D^M$, so there exist $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ and $\alpha' \in \mathrm{End}(E') - \mathbb{Z}$ with $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha')$. Set $K \cong \mathbb{Q}(\alpha)$.

Ascending isogenies. We may equip E with a K-orientation ι that has image $\mathbb{Q}(\alpha) \subseteq \mathrm{End}(E) \otimes \mathbb{Q}$. This K-orientation is a primitive $\mathcal{O}$-orientation for some quadratic order $\mathcal{O} \subseteq K$. By Proposition 5.3, a sequence of K-oriented isogenies of prime degree can take us from E to a curve $F \in \mathrm{SS}_{\mathcal{O}_K}(p)$, successively dividing the conductor of the optimally embedded order by one prime factor at a time. We can use the fact that $\alpha \in \iota(\mathcal{O})$ to bound the conductor f of $\mathcal{O}$:

$$\frac{3}{4} f^2 \leq \frac{f^2 |D|}{4} \leq \deg(\alpha) \leq M,$$

so that $f \leq b := \frac{2}{3}\sqrt{3M}$. Hence, the isogeny $E \to F$ obtained by composing all the prime-degree isogenies has degree at most b.

In the same way, we can find a sequence of prime-degree isogenies from E' to a curve $F' \in \mathrm{SS}_{\mathcal{O}_K}(p)$, and the degree of their composition is at most b. Take the dual to obtain an isogeny $F' \to E'$.

Horizontal isogenies. We first consider the case that F and F' are in the same orbit under the action of $\mathrm{Cl}(\mathcal{O}_K)$. By Proposition 5.4, there is an ideal $\mathfrak{a}$ of $\mathcal{O}_K$ such that $\mathfrak{a} * F = F'$. Since this action depends only on the ideal class, we may take $\mathfrak{a}$ to have norm at most $\frac{1}{\sqrt{3}}\sqrt{|D|}$,[5] which is at most $b = \frac{2}{3}\sqrt{3M}$ since $|D| \leq 4M$. Hence there is an isogeny $F \to F'$ of degree at most b.

Combining this isogeny with the vertical isogenies found above, the sequence E, F, F', E' has consecutive distances at most b. The curves F and F' are in T_D^M because they have an optimally embedded quadratic order strictly larger than $\mathcal{O}$ and $\mathcal{O}'$. This shows that we can find a sequence as in Theorem 1.3(b) with $r = 3$.

If F and F' are in different orbits, first apply Frobenius conjugation to F' and E' (as well as to the isogeny connecting them). Then F and $F'^{(p)}$ are in the same $\mathrm{Cl}(\mathcal{O}_K)$-orbit, so the argument above shows that the sequence E, F, $F'^{(p)}$, $E'^{(p)}$ has consecutive distances at most b. But by Definition 1.1, replacing $E'^{(p)}$ with E' does not change distances.

[5] Minkowski's bound has the coefficient $\frac{2}{\pi}$ instead of $\frac{1}{\sqrt{3}}$, but we get a stronger bound using the Hermite constant $\gamma_2 = \frac{2}{\sqrt{3}}$. Namely, the fractional ideal $\mathfrak{a}^{-1}$ must contain an element x of norm at most $\gamma_2(\frac{1}{2}\sqrt{|D|})\,\mathrm{N}(\mathfrak{a})^{-1}$, and we can take the ideal $x\mathfrak{a} \sim \mathfrak{a}$.

Prime-degree isogenies. We decompose each of the isogenies $E \to F$, $F \to F'$, and $F' \to E'$ into isogenies of prime degree. Note that $E \to F$ and $E' \to F'$ were defined as compositions of prime-degree isogenies to begin with, and every curve along the way is in T_D^M because the optimally embedded quadratic order grows at each step. For the isogeny $F \to F'$, write the ideal $\mathfrak{a}$ as a product of prime ideals. We can choose $\mathfrak{a}$ so that none of its prime ideal factors will be principal, so that they will all have prime norm. These ideals therefore induce prime-degree isogenies, and their composition is an isogeny $F \to F'$.

Since the isogenies $E \to F$, $F \to F'$, and $F' \to E'$ each have degree b, the full sequence of prime-degree isogenies

$$E = E_0 \to E_1 \to \cdots \to E_r \cong E'$$

must satisfy

$$2^r \leq \prod_{i=1}^{r} d(E_{i-1}, E_i) \leq b^3,$$

which gives us the bound $r \leq 3 \log_2 b$.

Combining Lemma 2.3, Section 4B, and Section 5B, we have a complete proof of Theorem 1.3.

6. Vertical ℓ-isogenies have no short detours

As discussed in Section 5, M-small curves within a single set T_D^M may be given a $\mathbb{Q}(\sqrt{D})$-orientation, and then connected by "horizontal" or "vertical" isogenies. In this section we prove that if two oriented curves are connected by a vertical ℓ-isogeny, then there is no short isogeny between them with degree relatively prime to ℓ.[6] As a result, the short paths described in Theorem 1.3(b) will only exist if all sufficiently small primes are allowed as degrees of isogenies.

Proposition 6.1. *Let ℓ be a prime, $M \in \mathbb{Z}$, and β be an imaginary quadratic integer with norm at most M/ℓ^2. Suppose $E, E' \in \mathrm{SS}^M(p)$ have $\mathbb{Z}[\beta]$ optimally embedded in $\mathrm{End}(E)$ and $\mathbb{Z}[\ell\beta]$ optimally embedded in $\mathrm{End}(E')$. If $\phi : E \to E'$ is any isogeny with degree relatively prime to ℓ, then*

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

Remark 6.2. Given $M \in \mathbb{Z}$ and prime ℓ, if $\mathrm{SS}^{M/\ell^2}(p)$ is nonempty then there are $E, E' \in \mathrm{SS}^M(p)$ satisfying the conditions of Proposition 6.1: we can take $E \in \mathrm{SS}^{M/\ell^2}(p)$ and follow a "descending" ℓ-isogeny [16, Proposition 4.1] to E'.

Proof of Proposition 6.1. Let $\phi : E \to E'$ be an isogeny with degree relatively prime to ℓ. Fix a maximal order $\mathfrak{O} \subseteq B$ with $\mathfrak{O} \cong \mathrm{End}(E)$. By the Deuring correspondence, ϕ corresponds to an ideal I linking $\mathfrak{O}$ to some maximal order $\mathfrak{O}' \cong \mathrm{End}(E')$. Since I is a sublattice of $\mathfrak{O} \cap \mathfrak{O}'$, $\mathrm{nrd}(I)^2 = |\mathfrak{O} : I|$ [25, Main Theorem 16.1.3] is a multiple of $d(\mathfrak{O}, \mathfrak{O}') = |\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'|$. Thus, since $\mathrm{nrd}(I) = \deg \phi$ is not divisible by ℓ, neither is $d(\mathfrak{O}, \mathfrak{O}')$.

[6] A result of this form does not hold for horizontal isogenies, because a single ideal class may have multiple representatives with small, relatively prime norms.

If the optimal embeddings $\mathbb{Z}[\beta] \hookrightarrow \mathfrak{O}$ and $\mathbb{Z}[\ell\beta] \hookrightarrow \mathfrak{O}'$ were to land in the same subfield of 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 and 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 4.4 tells us that $\operatorname{disc}\mathcal{O} \operatorname{disc}\mathcal{O}' \geq p^2$.

Letting $d := d(\mathfrak{O}, \mathfrak{O}')$, we have $\ell\beta \in \mathcal{O}$ and $d\beta \in \mathcal{O}'$. So just as in Section 4B,

$$d^2\ell^2 \operatorname{nrd}(\beta)^2 \geq \frac{1}{16} \operatorname{disc}\mathcal{O} \operatorname{disc}\mathcal{O}' \geq \frac{p^2}{16}.$$

Finally, applying Definition 4.1(c),

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

7. Isogenies between M-small supersingular curves

Despite the large distances between M-small curves in distinct subsets T_D^M, we show that isogenies between them can nonetheless be computed efficiently under certain heuristic assumptions. On each "island" T_D^M, we will construct an "airport," a curve with known endomorphism ring. To find an isogeny between two M-small curves, we will apply Theorem 1.3(b) to find a path from each curve to the airport on its respective island, and then compute an isogeny between the airports.

7A. ***Locating the airports.*** From our definition of B, we have $j^2 = -p$ and $i^2 = -q$ for some relatively small value of q; for $p \equiv 3 \pmod 4$ we can use $q = 1$, and for $p \equiv 1 \pmod 4$ we can use the same q as in Proposition 2.1, so that under GRH we have $q = O(\log^2 p)$. Let $K \neq \mathbb{Q}(i)$ be a quadratic field of discriminant $-4M \leq D < 0$. We must make an assumption which we leave unproven, but is plausible both heuristically and experimentally (see Remark 7.3).

Assumption 7.1. Let $\alpha \in B$ satisfy $4\alpha^2 = D$ (if $D \equiv 0 \pmod 4$) or $4\alpha^2 - 4\alpha + 1 = D$ (if $D \equiv 1 \pmod 4$). Then it is feasible to find an integral element $\beta \in B$ with the following property: if n is the denominator of $\operatorname{trd}(\alpha\beta)$, then the discriminant of the order $\mathbb{Z}\langle\alpha, n\beta\rangle$ can be efficiently factored into primes.[7]

Lemma 7.2. *Assume GRH and an oracle for Assumption 7.1. Given a fundamental discriminant $-4M \leq D < 0$ with $(D/p) = -1$, a maximal order of B containing an integral element α with $\operatorname{nrd}(\alpha) \leq M$ and $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\sqrt{D})$ can be computed in probabilistic polynomial time in M and $\log p$.*

Proof. The computation is as follows. First find $x, y, z, w \in \mathbb{Q}$ such that

$$(x + y\sqrt{D})^2 + q(z + w\sqrt{D})^2 = -p. \tag{1}$$

If we set

$$\gamma = pi + qzj + xk \quad \text{and} \quad \delta = qwj + yk,$$

[7]The definition of n guarantees that $\mathbb{Z}\langle\alpha, n\beta\rangle$ is in fact an order. Aside from the fact that the discriminant will be divisible by p^2 (since any order is contained in a maximal order), we expect this discriminant to behave in some sense as a "random integer" as we vary β. In the range of values that seem to arise in practice, integers that can be easily factored are relatively common.

the proof of [25, Lemma 5.4.7] shows that $(\gamma\delta^{-1})^2 = D$, giving us an explicit embedding of $\mathbb{Q}(\sqrt{D})$ into B. Let $\alpha = \frac{1}{2}\gamma\delta^{-1}$ or $\alpha = \frac{1}{2}(1 + \gamma\delta^{-1})$, whichever is integral. Then α satisfies the conditions for Assumption 7.1, so we can use the oracle to find an order containing α and a factorization of its discriminant. Then use [24, Proposition 4.3.4] to construct a maximal order containing this order. The resulting maximal order contains α, and so the required conditions are satisfied.

We now discuss the validity and runtime of this process. If we set $K = \mathbb{Q}(\sqrt{D})$, there exists an embedding of $K = \mathbb{Q}(\sqrt{D})$ into B [25, Proposition 14.6.7]. This implies that $B \otimes_{\mathbb{Q}} K$ is split [25, Lemma 5.4.7], so there exists a solution $v \in K(i)^\times$ to the relative norm equation $\mathrm{N}_{K(i)/K}(v) = -p$ [25, Theorem 5.4.6(vi)], implying that (1) has a solution.

We can solve (1) using an algorithm due to Simon [21, Algorithm 6.5], which requires computing the relative class group of $K(i)/K$, factoring the norms of the generators of the relative class group into prime ideals of K, factoring p into prime ideals of K, and linear algebra. Under GRH, the discriminant Δ of $K(i) \cong \mathbb{Q}(\sqrt{D}, \sqrt{-q})$ is polynomial in M and $\log p$, so the first two of these tasks can be done in polynomial time.[8] Since $(D/p) = -1$, p is already prime in K, and the necessary linear algebra can also be done in polynomial time.

Constructing a maximal order containing $\operatorname{disc}\mathbb{Z}\langle\alpha, n\beta\rangle$ takes polynomial time in $\log p$ and the bit-lengths of α and $n\beta$, assuming the factorization of $\operatorname{disc}\mathbb{Z}\langle\alpha, n\beta\rangle$ is given, and a probabilistic algorithm (e.g., [18]) is used for factoring polynomials over finite fields. □

Remark 7.3. We checked Assumption 7.1 experimentally using Magma, by computing the maximal order of Lemma 7.2 for $p = 2^{256} + 297$ (in this case we can take $q = 7$), $M = 100$, and all 62 allowable values of D. We used the function `NormEquation` to solve the relative norm equation, and `MaximalOrder` to find a maximal order containing a given order. In every case, either $\beta = i$ or $\beta = j$ satisfied Assumption 7.1. Constructing all of these maximal orders took 60 seconds on a generic personal laptop (16 GB RAM, 1.80 GHz CPU).

7B. ***An algorithm for computing isogenies.*** We describe an algorithm[9] for computing an isogeny between any two curves $E, E' \in \mathrm{SS}(p)$. In general, the runtime will be exponential in $\log p$, but it is efficient when E and E' are both M-small for relatively small M. Note that the algorithm does not require knowledge of any noninteger endomorphisms of E or E', or even a nontrivial bound on M.

Lemma 7.4. *Let $M < p$ be such that $E, E' \in \mathrm{SS}^M(p)$ (the value of M may not be known to the algorithm).*[10] *Assuming GRH and an oracle for Assumption 7.1, Algorithm 1 runs successfully in probabilistic polynomial time in M and* $\log p$.

[8] The (absolute) class groups $\mathrm{Cl}(K(i))$ and $\mathrm{Cl}(K)$ can be computed in probabilistic subexponential time in $\log|\Delta|$ [3], and the relative class group can be efficiently computed from this data using linear algebra [6, Algorithm 7.3.1]. Under GRH, generators of the relative class group will have (absolute) norm $O(\log^2|\Delta|)$ [6, p. 369] and so factoring their (relative) norms can also be done efficiently.

[9] This algorithm is primarily a proof of concept; there is a lot of optimization that can be done if it is to be used in practice.

[10] Every $E \in \mathrm{SS}(p)$ is M-small for $M = \left\lfloor \frac{1}{2}p^{2/3} + \frac{1}{4} \right\rfloor$ [11, Section 4].

Algorithm 1: Computing isogenies between supersingular curves.

Input : $E, E' \in \mathrm{SS}(p)$.
Output : An isogeny $E \to E'$.

(1) Find the roots in $\mathbb{F}_{p^2}$ of the Hilbert class polynomials $H_{\mathcal{O}}(x) \pmod p$, for quadratic orders $\mathcal{O}$ of successively increasing discriminant. Stop when the j-invariant of E is found as a root of $H_{\mathcal{O}_E}(x) \pmod p$, for some order $\mathcal{O}_E$. Let S denote the set of all roots in $\mathbb{F}_{p^2}$ of all quadratic orders considered.
(2) Let D be the discriminant of the field of fractions of $\mathcal{O}_E$. Compute a maximal order $\mathfrak{O}_D \subseteq B$ as in Lemma 7.2.
(3) Compute an elliptic curve $E_D \in \mathrm{SS}(p)$ such that $\mathrm{End}(E_D) \cong \mathfrak{O}_D$.
(4) Find an isogeny in S from E to E_D by breadth-first search. That is, from the current curve, use modular polynomials to find all curves in S that are connected to the current curve by an isogeny of prime degree at most
$$\tfrac{2}{3}\sqrt{3\left\lceil \tfrac{1}{4}|\mathrm{disc}\,\mathcal{O}_E|\right\rceil}.$$
Continue until either E_D or $E_D^{(p)}$ is found. If $E_D^{(p)}$ is found, replace E_D with $E_D^{(p)}$.
(5) Repeat Steps (1) to (4) for E', obtaining a curve $E_{D'}$ with known endomorphism ring, as well as a path from E' to $E_{D'}$.
(6) Compute an isogeny from E_D to $E_{D'}$.
(7) Compose the isogeny $E \to E_D$ (from Step (4)), the isogeny $E_D \to E_{D'}$ (from Step (6)), and the isogeny $E_{D'} \to E'$ (dual of the isogeny from Step (5)).

Proof. First we examine Step (1). Each polynomial $H_{\mathcal{O}}(x) \pmod p$ can be computed in $O(|\mathrm{disc}\,\mathcal{O}|^{1+\varepsilon})$ time [23, Theorem 1]. The roots of this polynomial in $\mathbb{F}_{p^2}$ can be found by factoring it over $\mathbb{F}_p$, and keeping the linear and quadratic factors. There is a probabilistic algorithm for factoring which is polynomial time in $\deg H_{\mathcal{O}}(x)$ and $\log p$ [18]. The degree of $H_{\mathcal{O}}(x)$ equals the class number of $\mathcal{O}$, which is $O(|\mathrm{disc}\,\mathcal{O}|^{1/2+\varepsilon})$. By Proposition 2.2, the j-invariant of E is a root of $H_{\mathcal{O}_E}(x) \pmod p$ for an order $\mathcal{O}_E$ with $|\mathrm{disc}\,\mathcal{O}_E| \leq 4M$, so Step (1) computes S and $\mathcal{O}_E$ in time polynomial in M and $\log p$.

Step (2) requires an oracle for Assumption 7.1 but otherwise runs in polynomial time in M and $\log p$; note that $(D/p) = -1$ by Proposition 2.2 so the conditions of Lemma 7.2 are met. There are known algorithms for performing Steps (3) [10, Proposition 13] and (6) [10, Proposition 7] in polynomial time.

Now consider Step (4). Let $\widehat{M} = \left\lceil \frac{1}{4}|\mathrm{disc}\,\mathcal{O}_E|\right\rceil$, so that $-4\widehat{M} \leq \mathrm{disc}\,\mathcal{O}_E < 0$. Thus $E \in T_D^{\widehat{M}}$, and $E_D \in T_D^{\widehat{M}}$ by the properties of $\mathfrak{O}$ described in Lemma 7.2. Since S contains $\mathrm{SS}^{\widehat{M}}(p)$ by construction, Theorem 1.3(b) guarantees that Step (4) will find a path from E to either E_D or $E_D^{(p)}$. Since the number of elements of S is polynomial in M, the process can be done in time polynomial in M and $\log p$. Replacing E_D with $E_D^{(p)}$ does not change the endomorphism ring, and so Step (6) can still be done. □

7C. ***Isogenies defined over*** $\mathbb{F}_p$**.** Suppose E and E' are M-small curves defined over $\mathbb{F}_p$. Some situations, such as key recovery for the CSIDH protocol [4], require being able to find an $\mathbb{F}_p$-isogeny $E \to E'$. While Algorithm 1 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 [5], in which they provide an algorithm to compute an $\mathbb{F}_p$-isogeny $E \to E'$, given the endomorphism rings of E and E' (which can be computed from the isogenies $E \to E_D$ and $E' \to E_{D'}$, found in Steps (4) and (5) of Algorithm 1).

Acknowledgments

We would like to thank John Voight for crucial insights behind the results of Section 7, and Akshay Venkatesh for pointing us towards the key ideas necessary for Section 5. We also thank the anonymous reviewers for many improvements, including a local proof for Lemma 4.2, a significant improvement to the bound in Theorem 1.3(a), and catching many errors.

Several attendees of the XIVth Algorithmic Number Theory Symposium also helped to improve this paper after its initial presentation. We especially thank Boris Fouotsa Tako, Lorenz Panny, and Noam Elkies for pointing out ways to improve the presentation of Section 5, and Frederik Vercauteren and Steven Galbraith for attentive editing and constructive feedback.

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

[2] Reinier Bröker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory **1** (2009), no. 3, 269–273. MR 2681311

[3] Johannes A. Buchmann, *A subexponential algorithm for the determination of class groups and regulators of algebraic number fields*, Séminaire de Théorie des Nombres, Paris 1988–89 (Catherine Goldstein, ed.), Progress in Mathematics, no. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 27–41.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *CSIDH: an efficient post-quantum commutative group action*, Advances in Cryptology – ASIACRYPT 2018 (Thomas Peyrin and Steven Galbraith, eds.), Springer International Publishing, 2018, pp. 395–427.

[5] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren, *Rational isogenies from irrational endomorphisms*, Advances in Cryptology – EUROCRYPT 2020 (Anne Canteaut and Yuval Ishai, eds.), Springer International Publishing, 2020, pp. 523–548.

[6] Henri Cohen, *Advanced topics in computational number theory*, Springer, 2000.

[7] Leonardo Colò and David Kohel, *Orienting supersingular isogeny graphs*, Number-Theoretic Methods in Cryptology 2019, 2019.

[8] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2 ed., Wiley, 2013.

[9] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso, *Verifiable delay functions from supersingular isogenies and pairings*, Advances in Cryptology – ASIACRYPT 2019 (Steven D. Galbraith and Shiho Moriai, eds.), Springer International Publishing, 2019, pp. 248–277.

[10] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit, *Supersingular isogeny graphs and endomorphism rings: reductions and solutions*, Advances in Cryptology – EUROCRYPT 2018 (Jesper Buus Nielsen and Vincent Rijmen, eds.), Springer International Publishing, 2018, pp. 329–368.

[11] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Inventiones mathematicae **89** (1987), no. 3, 561–567.

[12] Masanobu Kaneko, *Supersingular j-invariants as singular moduli mod p*, Osaka Journal of Mathematics **26** (1989), no. 4, 849–855.

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

[14] Serge Lang, *Elliptic functions*, Springer, 1987.

[15] Jonathan Love and Dan Boneh, *Supersingular curves with smal non-integer endomorphisms*, 2020. arXiv 1910.03180

[16] Hiroshi Onuki, *On oriented supersingular elliptic curves*, 2020. arXiv 2002.09894

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

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

[19] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2 ed., Springer-Verlag, 2009.

[20] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, 1994.

[21] Denis Simon, *Solving norm equations in relative number fields using S-units*, Mathematics of Computation **71** (2002), 1287–1305.

[22] Andrew V. Sutherland, *Isogeny volcanoes*, The Open Book Series **1** (2012).

[23] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Mathematics of Computation **80** (2011), no. 273, 501–538.

[24] John Voight, *Quadratic forms and quaternion algebras: algorithms and arithmetic*, Ph.D. thesis, Berkeley, CA, USA, 2005.

[25] John Voight, *Quaternion algebras*, 2020.

Received 20 Feb 2020.

JONATHAN LOVE: jonlove@stanford.edu
Department of Mathematics, Stanford University, Stanford, CA, United States

DAN BONEH: dabo@cs.stanford.edu
Computer Science Department, Stanford University, Stanford, CA, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

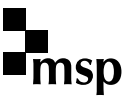
Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.



MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS