

Supersingular Curves with Small Non-integer Endomorphisms

Live Event

Jonathan Love¹ Dan Boneh²

¹Department of Mathematics, Stanford University
<https://stanford.edu/~jonlove>

²Department of Computer Science, Stanford University
<https://stanford.edu/~dabo>

Algorithmic Number Theory Symposium, June 2020

Definition

An elliptic curve E over a finite field of characteristic p is **M -small** if there exists $\alpha \in \text{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$.

Discussion of Theorem 1.3:

- 1 Classification into sets T_D
- 2 Two distinct T_D are far apart
- 3 Short paths within each T_D

Classification into T_D

Let E be a supersingular curve over \mathbb{F}_{p^2} .

- Suppose there exists $\alpha \in \text{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$.
- $\mathbb{Q}(\alpha)$ is an imaginary quadratic field, say with discriminant D .
- We say that E is in T_D .

From Supersingular Curves to Maximal Orders

- B : the unique quaternion algebra ramified at p and ∞
- $E^{(p)}$: The image of E/\mathbb{F}_{p^2} under $(x, y) \mapsto (x^p, y^p)$

Deuring Correspondence

There is a bijection

$$\frac{\{\text{supersingular curves over } \mathbb{F}_{p^2}\}}{\cong, E \sim E^{(p)}} \leftrightarrow \frac{\{\text{maximal orders of } B\}}{\cong}$$
$$E \mapsto \text{End}(E).$$

An isogeny $E \rightarrow E'$ corresponds to a lattice that is a left ideal of some $\mathfrak{O} \cong \text{End}(E)$ and right ideal of some $\mathfrak{O}' \cong \text{End}(E')$.

Use this to translate Theorem 1.3 into a result about maximal orders.

From Supersingular Curves to Maximal Orders

Definition / Lemma 4.2

If $\mathfrak{O}, \mathfrak{O}' \subseteq B$ are maximal orders, the *distance* $d(\mathfrak{O}, \mathfrak{O}')$ is any of the following equal quantities:

$$|\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'| = |\mathfrak{O}' : \mathfrak{O} \cap \mathfrak{O}'| = \min_{\substack{\text{integral ideals } I \subseteq B \\ O_L(I) = \mathfrak{O}, O_R(I) = \mathfrak{O}'}} \text{nrd}(I).$$

Warning: This is not isomorphism-invariant!

From Supersingular Curves to Maximal Orders

Definition / Lemma 4.2

If $\mathfrak{O}, \mathfrak{O}' \subseteq B$ are maximal orders, the *distance* $d(\mathfrak{O}, \mathfrak{O}')$ is any of the following equal quantities:

$$|\mathfrak{O} : \mathfrak{O} \cap \mathfrak{O}'| = |\mathfrak{O}' : \mathfrak{O} \cap \mathfrak{O}'| = \min_{\substack{\text{integral ideals } I \subseteq B \\ O_L(I) = \mathfrak{O}, O_R(I) = \mathfrak{O}'}} \text{nrd}(I).$$

Warning: This is not isomorphism-invariant!

Lemma 4.3

The smallest degree of an isogeny from E to either E' or $E'^{(p)}$ is equal to

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

Two distinct T_D are far apart

Let \mathfrak{O} and \mathfrak{O}' be maximal orders in B , and $\alpha \in \mathfrak{O} - \mathbb{Z}$ and $\alpha' \in \mathfrak{O}' - \mathbb{Z}$ each have reduced norm at most M .

Proposition 4.5

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

Two distinct T_D are far apart

Let \mathfrak{O} and \mathfrak{O}' be maximal orders in B , and $\alpha \in \mathfrak{O} - \mathbb{Z}$ and $\alpha' \in \mathfrak{O}' - \mathbb{Z}$ each have reduced norm at most M .

Proposition 4.5

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

Proof Idea: If $d(\mathfrak{O}, \mathfrak{O}') = d$, then $1, \alpha, d\alpha', d\alpha\alpha'$ are linearly independent elements contained in \mathfrak{O} . Maximal orders of B have discriminant p^2 , so d can't be too small.

Short paths within each T_D

Let \mathfrak{D} and \mathfrak{D}' be maximal orders in B , and $\alpha \in \mathfrak{D} - \mathbb{Z}$ and $\alpha' \in \mathfrak{D}' - \mathbb{Z}$ each have reduced norm at most M .

Proposition 4.6

If $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha')$, then after replacing \mathfrak{D}' with an isomorphic maximal order, there is a sequence of maximal orders from \mathfrak{D} to \mathfrak{D}' , all containing either α or α' (as elements of B), with consecutive distances at most $\frac{4}{\pi}\sqrt{M}$.

Short paths within each T_D

Proof Idea:

- Arrange so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ as subfields of B (Skolem-Noether).

Short paths within each T_D

Proof Idea:

- Arrange so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ as subfields of B (Skolem-Noether).
- “Vertical steps:” $\mathbb{Q}(\alpha) \cap \mathfrak{D}$ will be a not-necessarily maximal quadratic order of $\mathbb{Q}(\alpha)$. Explicitly construct nearby maximal orders \mathfrak{D}_i such that $\mathbb{Q}(\alpha) \cap \mathfrak{D}_i$ is closer to being a maximal order (Lemma 5.4).

Short paths within each T_D

Proof Idea:

- Arrange so that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ as subfields of B (Skolem-Noether).
- “Vertical steps:” $\mathbb{Q}(\alpha) \cap \mathfrak{D}$ will be a not-necessarily maximal quadratic order of $\mathbb{Q}(\alpha)$. Explicitly construct nearby maximal orders \mathfrak{D}_i such that $\mathbb{Q}(\alpha) \cap \mathfrak{D}_i$ is closer to being a maximal order (Lemma 5.4).
- “Horizontal steps:” If $\mathbb{Q}(\alpha) \cap \mathfrak{D} = \mathbb{Q}(\alpha') \cap \mathfrak{D}'$, then there exists an ideal \mathfrak{a} of the quadratic order such that $\mathfrak{D}\mathfrak{a} = \mathfrak{a}\mathfrak{D}'$ (Chevalley-Hasse-Noether). If \mathfrak{a} is small then $d(\mathfrak{D}, \mathfrak{D}')$ is small.

Put it all together

Compile results, get Theorem 1.3.