Simultaneous equidistribution of supersingular reductions of CM-curves

Joint with Menny Aka, Philippe Michel, and Andreas Wieser

Manuel Luethi

Tel Aviv University

May 7 2020

Weierstrass equations

In what follows k is an arbitrary field.

Definition

An elliptic curve over k is the locus of a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

together with a base point at infinity, such that the discriminant $\Delta(a_1, \ldots, a_6) \neq 0$.

The discriminant is a polynomial in the coefficients of the Weierstrass equation. Non-vanishing is a smoothness condition.

Weierstrass equations II

Assume k a field, $\mathrm{char}(k) \neq 2, 3$.

Lemma

Let $a, b \in k$ such that $a^3 - b^2 \neq 0$. The locus of

$$E : y^2 = x^3 - 27ax - 54b$$

together with a point O at infinity is an elliptic curve over k. Its discriminant satisfies

$$1728\Delta = a^3 - b^2.$$

The group law

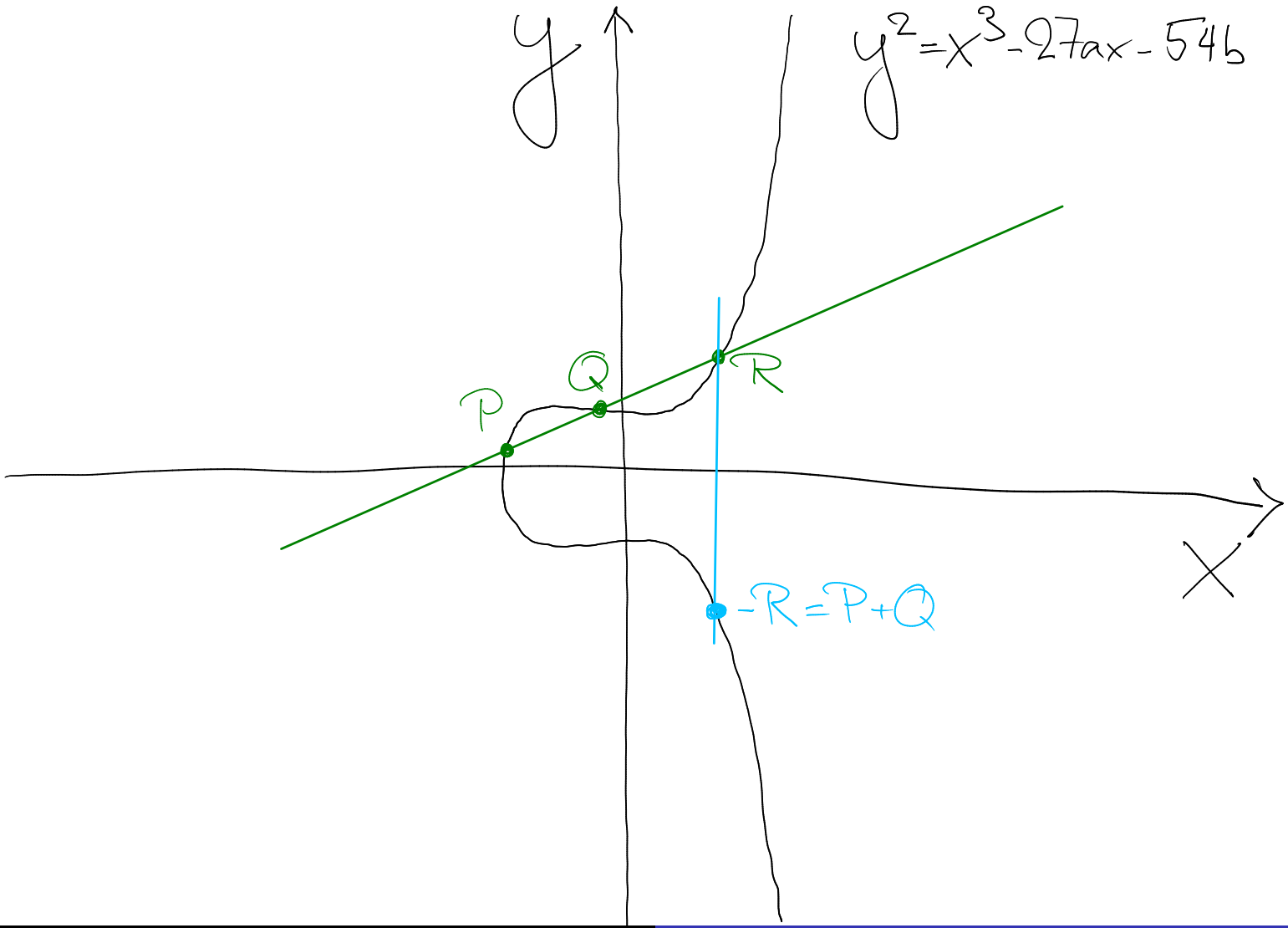
Curves given by Weierstrass equations admit a structure of commutative algebraic groups.

- Assume that E has the special form from before.
- $P = (x, y) \in E \implies -P := (x, -y) \in E$.
- Addition via *chord-tangent method*: Given $P, Q \in E(k)$, set

$$P + Q = -R,$$

where R is the third intersection point of E with the line through P, Q.

The group law II



Endomorphism rings I

$\mathrm{End}(E)$ is a torsion-free $\mathbb{Z}$-algebra, i.e. has characteristic 0.

Proposition

Let E be an elliptic curve. Then one of the following is true.

- $\mathrm{End}(E) = \mathbb{Z}$.
- $\mathrm{End}(E)$ *is an order in an imaginary quadratic number field, i.e. E has complex multiplication.*
- $\mathrm{End}(E)$ *is a maximal order in a quaternion algebra, i.e. E is supersingular.*

Endomorphism rings II

1. If $\mathrm{char}(k) = 0$, then E is *not* supersingular.
2. If $\mathrm{char}(k) = p > 0$ and E is supersingular, then E is defined over $\overline{\mathbb{F}_p}$ and isomorphic to a curve defined over $\mathbb{F}_{p^2}$.
3. In particular the set $\mathscr{S}_p$ of $\overline{\mathbb{F}_p}$-classes of supersingular elliptic curves is finite.

Complex multiplication

1. Assume $\mathrm{char}(k) \neq 2$ and $E : y^2 = x^3 + x$.
2. Let $\mathrm{i} \in \overline{k}$ s.t. $\mathrm{i}^2 = -1$. Then

$$[\mathrm{i}](x, y) = (-x, \mathrm{i}y) \quad ((x, y) \in E)$$

   defines a non-trivial automorphism of E.
3. Note $[\mathrm{i}] \notin \mathbb{Z}$ as $[\mathrm{i}]^2 = -1$.
4. For the curves
   - $E : y^2 = x^3 + x$ over $\mathbb{C}$,
   - $\tilde{E} : y^2 = x^3 + x$ over $\mathbb{F}_5$,
   - $\overline{E} : y^2 = x^3 + x$ over $\mathbb{F}_7$

   the endomorphism ring contains $\mathbb{Z}[\mathrm{i}] \supsetneq \mathbb{Z}$.

A supersingular curve

1. Consider $\overline{E} : y^2 = x^3 + x$ over $k = \mathbb{F}_7$. Let $K = \mathbb{F}_{7^2}$.
2. $\overline{E}(K) \setminus \overline{E}(k) \neq \emptyset$: $(2, 2\mathrm{i}) \in \overline{E}(K) \setminus \overline{E}(k)$.
3. Let $\varphi \in \mathrm{Gal}(K|k)$ be the non-trivial Galois automorphism, i.e. the Frobenius automorphism.
4. φ yields an automorphism of $\overline{E}(K)$, trivial on $\overline{E}(k)$.
5. $\varphi \notin \mathbb{Z}[\mathrm{i}]$ as $\varphi \circ [\mathrm{i}] \neq [\mathrm{i}] \circ \varphi$. Otherwise $\mathrm{i} = \mathrm{i}^7$, i.e. $\mathrm{i} \in k$.
6. Hence $\overline{E}$ is supersingular.

Complex uniformization

- There is a one-to-one correspondence

$$\{\Lambda \subseteq \mathbb{C} \text{ a lattice}\} / \mathbb{C}^\times$$
$$\updownarrow$$
$$\{E/\mathbb{C} \text{ elliptic curve}\} / \mathbb{C} - \text{Isomorphism}$$

- For every elliptic curve E over $\mathbb{C}$, there is a lattice $\Lambda \subseteq \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C} / \Lambda$ as complex Lie groups and vice versa.
- This is an equivalence of categories.
- Special case of GAGA.

Complex multiplication I

- Every holomorphic endomorphism of $\mathbb{C}/\Lambda$ has a unique lift to a holomorphic endomorphism of $\mathbb{C}$ preserving Λ.
- Therefore

$$\mathfrak{o} := \mathrm{End}(\mathbb{C}/\Lambda) = \{\omega \in \mathbb{C} : \omega\Lambda \subseteq \Lambda\}.$$

- W.l.o.g. $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\Im\tau \neq 0$. If $\omega \in \mathfrak{o}$, then $\omega \in \Lambda$.
- Applying ω to 1 and τ respectively shows

$$(a + b\tau)\tau = c + d\tau \quad (a, b, c, d \in \mathbb{Z}).$$

- Therefore $\mathfrak{o} = \mathbb{Z}$ or $\mathfrak{o} \subseteq \mathbb{Q}(\tau)$ is an order in an imaginary quadratic number field and Λ is a proper $\mathfrak{o}$-ideal.

Complex multiplication II

- Orders in quadratic number fields are parametrized by their discriminants D.
- The covolume of $\mathfrak{o}_D$ in $\mathbb{C}$ is $\mathrm{covol}(\mathfrak{o}_D) = \frac{\sqrt{|D|}}{2}$.
- Let

$$\mathrm{CM}_D = \{E/\mathbb{C} : E \text{ has CM by } \mathfrak{o}_D\}/\mathbb{C}\text{-isomorphism}.$$

- Let $\mathrm{Cl}(\mathfrak{o}_D)$ be the set of fractional proper $\mathfrak{o}_D$-ideals up to principal equivalence.
- Then $\mathrm{Cl}(\mathfrak{o}_D) \longleftrightarrow \mathrm{CM}_D$ via

$$[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{o}_D) \mapsto \left[\mathbb{C}/\mathfrak{a}\right]$$

by previous argument.

Summary

- Elliptic curves over $\mathbb{C}$ correspond to $\mathbb{C}^\times$-homothety classes of lattices in $\mathbb{C}$.
- Isomorphism classes of curves with CM by $\mathfrak{o}_D$ correspond to classes of proper fractional $\mathfrak{o}_D$-ideals.
- $\mathrm{Cl}(\mathfrak{o}_D)$ acts on CM_D by

$$[\mathfrak{a}] * \left[\mathbb{C}/\Lambda\right] := \left[\mathbb{C}/\mathfrak{a}^{-1}\Lambda\right].$$

Supersingular reduction

Assume that D is a negative fundamental discriminant, i.e. $\mathfrak{o}_D$ is the ring of integers in $\mathbb{Q}(\sqrt{D})$. We also assume $p > 3$.

1. All CM_D-curves can be defined over a numberfield.
2. There is a reduction map $E \mapsto E \bmod p$ whose image is a curve defined over $\overline{\mathbb{F}_p}$.
3. If p is not split in $\mathbb{Q}(\sqrt{D})$, then $E \bmod p$ is a supersingular elliptic curve.

Compare to reduction of $E : y^2 = x^3 + x$ over $\mathbb{Q}$ to $\overline{E} : y^2 = x^3 + x$ over $\mathbb{F}_p$.

- If $p = 5$, then $p = (2 + \mathrm{i})(2 - \mathrm{i})$ splits in $\mathbb{Z}[\mathrm{i}]$ and $\overline{E}$ is *not* supersingular.
- If $p = 7$, then p is prime in $\mathbb{Z}[\mathrm{i}]$ and $\overline{E}$ *is* supersingular.

Deuring's theorem

The following result is a simplified version of a result due to M. Deuring.

Theorem

Let $\overline{E}$ be a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. Then there exists an elliptic curve E with complex multiplication such that $\overline{E} \cong E \bmod p$.

Lifting supersingular curves I

- $\mathscr{S}_p$ is finite; in fact $|\mathscr{S}_p| = \frac{p}{12} + O(1)$.
- CM_D is finite; in fact $|\mathrm{CM}_D| \asymp |D|^{\frac{1}{2}+o(1)} \to \infty$ as $D \to -\infty$.
- Consider the sequence of reductions $\mathrm{CM}_D \to \mathscr{S}_p$ as $D \to -\infty$ along the condition that p is inert in $\mathbb{Q}(\sqrt{D})$. Question: Will the reduction eventually be surjective?

Lifting supersingular curves II

The following result is a simplified version of a result due to Ph. Michel.

Theorem

Let $\overline{E}$ be a supersingular elliptic curve defined over $\overline{\mathbb{F}_p}$. There exists $D_0 < 0$ such that for all fundamental discriminants $D \leq D_0$ for which p is inert there is $E \in \mathrm{CM}_D$ such that $\overline{E} \cong E \bmod p$.

In fact, Ph. Michel proves an effective equidistribution result for the natural (non-uniform) probability measure on $\mathscr{S}_p$.

Our result

Theorem (Aka-L.-Michel-Wieser)

Let $q_1, q_2, p_1, \ldots, p_s$ be distinct odd primes. There is $D_0 < 0$ such that for any fundamental discriminant $D \leq D_0$ satisfying that

- *$p_1, \ldots, p_s$ are inert in $\mathbb{Q}(\sqrt{D})$ and*
- *q_1, q_2 are split in $\mathbb{Q}(\sqrt{D})$*

the simultaneous reduction map

$$\mathrm{CM}_D \to \prod_{i=1}^{s} \mathscr{S}_{p_i} \qquad E \mapsto (E \bmod p_1, \ldots, E \bmod p_s)$$

is surjective.

In fact, we use a classification of joinings by Einsiedler and Lindenstrauss to prove an (ineffective) equidistribution result.

(Optimal) embeddings and supersingular reduction

- Let $D < 0$ a fundamental discriminant, p inert in $\mathbb{Q}(\sqrt{D})$.
- Let $E \in \mathrm{CM}_D$.
- Then $\mathbf{B}_{\infty,p} := \mathrm{End}(E \bmod p) \otimes \mathbb{Q}$ is a quaternion algebra.
- $\mathcal{O} = \mathrm{End}(E \bmod p)$ is a maximal order in $\mathbf{B}_{\infty,p}$.
- The isomorphism class of $\mathbf{B}_{\infty,p}$ only depends on p.
- Reduction mod p gives embedding

$$\iota : \mathrm{End}(E) \hookrightarrow \mathrm{End}(E \bmod p),$$

i.e. an embedding

$$\iota : \mathfrak{o}_D \hookrightarrow \mathcal{O}.$$

Equivalence of embeddings

Definition

Let $\iota_1, \iota_2 : \mathfrak{o}_D \hookrightarrow \mathcal{O}$ embeddings. Then $\iota_1 \sim \iota_2$ if

$$\exists u \in \mathcal{O}^\times \, \forall x \in \mathfrak{o}_D \quad \iota_2(x) = u\iota_1(x)u^{-1}.$$

We let $h(\mathfrak{o}_D, \mathcal{O})$ be the number of equivalence classes of embeddings $\iota : \mathfrak{o}_D \hookrightarrow \mathcal{O}$.

Deuring's theorem revisited

Consider the following version of Deuring's theorem, due to B. Gross and D. Zagier.

Theorem

Let $\mathcal{O} \subseteq \mathbf{B}_{\infty,p}$ be a maximal order and $\iota : \mathfrak{o}_D \hookrightarrow \mathcal{O}$ an embedding. Then there exists a unique $E \in \mathrm{CM}_D$ such that

$$\mathrm{End}(E \bmod p) \cong \mathcal{O}$$

and the embedding $\iota_E : \mathrm{End}(E) \hookrightarrow \mathrm{End}(E \bmod p)$ is equivalent to ι under the isomorphism.

In the theorem, we use that there is a natural way to choose the isomorphism $\mathfrak{o}_D \cong \mathrm{End}(E)$.

Counting embeddings

Recall: $D < 0$ is a fundamental discriminant and p inert in $\mathbb{Q}(\sqrt{D})$.

Lemma (N. Elkies, K. Ono, and T. Yang)

Let $\overline{E} \in \mathscr{S}_p$ and $\mathcal{O} = \mathrm{End}(\overline{E})$. Then

$$|\{E \in \mathrm{CM}_D : E \bmod p \cong \overline{E}\}| = \frac{1}{2} h(\mathfrak{o}_D, \mathcal{O}).$$

Surjectivity in one factor I

- By the lemma it suffices to prove that eventually $h(\mathfrak{o}_D, \mathcal{O}) > 0$ for all maximal orders $\mathcal{O} \subseteq \mathbf{B}_{\infty,p}$.
- Up to conjugacy, $\mathbf{B}_{\infty,p}$ contains only finitely many maximal orders.
- For surjectivity, it suffices to prove that for all maximal orders $\mathcal{O} \subseteq \mathbf{B}_{\infty,p}$ eventually $h(\mathfrak{o}_D, \mathcal{O}) > 0$.
- For equidistribution we need to show that $h(\mathfrak{o}_D, \mathcal{O})/|\mathrm{Cl}(\mathfrak{o}_D)|$ has the right asymptotics.

Surjectivity in one factor II

- Let $\iota : \mathfrak{o}_D \hookrightarrow \mathcal{O} \subseteq \mathbf{B}_{\infty,p}$ an embedding.
- ι is completely determined by $\iota(\sqrt{D})$.
- Let $\mathcal{O}^T = \{x \in \mathbb{Z} + 2\mathcal{O} : \mathrm{Tr}(x) = 0\}$ (Gross lattice). There is a one-to-one correspondence between embeddings $\iota : \mathfrak{o}_D \hookrightarrow \mathcal{O}$ and the set

$$\{v \in \mathcal{O}^T : v \text{ is primitive and } \mathrm{Nr}(v) = -D\}.$$

Surjectivity in one factor III

Therefore the surjectivity of the reduction map is equivalent to the following.

Theorem

Let p prime, $\mathcal{F}(p)$ the set of negative fundamental discriminants D s.t. p is inert in $\mathbb{Q}(\sqrt{D})$. Let $\mathcal{O}$ be a maximal order in $\mathbf{B}_{\infty,p}$. There exists $D_0 < 0$ such that for all $D \in \mathcal{F}(p)$ we have

$$D < D_0 \implies -D \in \mathrm{Nr}(\mathcal{O}^T).$$

This follows from a theorem of Duke. Under additional congruence conditions, this admits a dynamic proof due to Linnik and Skubenko.