The Effective Shafarevich Conjecture

London Junior Number Theory Seminar

Robin Visser
Mathematics Institute
University of Warwick

13 February 2024

Motivation

- Let K be a number field and S a finite set of places of K.

Motivation

- Let K be a number field and S a finite set of places of K.

Conjecture (Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Motivation

- Let K be a number field and S a finite set of places of K.

Conjecture (Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Conjecture (Shafarevich 1962)

Let $g \geq 2$ be a positive integer. Then there are only finitely many K-isomorphism classes of smooth curves C/K of genus g with good reduction outside S.

Motivation

- Let K be a number field and S a finite set of places of K.

Conjecture (Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Conjecture (Shafarevich 1962)

Let $g \geq 2$ be a positive integer. Then there are only finitely many K-isomorphism classes of smooth curves C/K of genus g with good reduction outside S.

Conjecture (Shafarevich 1962)

Let $d \geq 1$ be a positive integer. Then there are only finitely many K-isomorphism classes of (p.p.) abelian varieties A/K of dimension d with good reduction outside S.

Motivation

- Let K be a number field and S a finite set of places of K.

Conjecture (Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Conjecture (Shafarevich 1962)

Let $g \geq 2$ be a positive integer. Then there are only finitely many K-isomorphism classes of smooth curves C/K of genus g with good reduction outside S.

Conjecture (Shafarevich 1962)

Let $d \geq 1$ be a positive integer. Then there are only finitely many K-isomorphism classes of (p.p.) abelian varieties A/K of dimension d with good reduction outside S.

$$\text{Shafarevich (abelian varieties)} \implies \text{Shafarevich (curves)} \implies \text{Mordell}$$

Motivation

- Let K be a number field and S a finite set of places of K.

Theorem (Faltings 1983)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Theorem (Faltings 1983)

Let $g \geq 2$ be a positive integer. Then there are only finitely many K-isomorphism classes of smooth curves C/K of genus g with good reduction outside S.

Theorem (Faltings 1983)

Let $d \geq 1$ be a positive integer. Then there are only finitely many K-isomorphism classes of (p.p.) abelian varieties A/K of dimension d with good reduction outside S.

$$\text{Shafarevich (abelian varieties)} \implies \text{Shafarevich (curves)} \implies \text{Mordell}$$

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

Sketch proof:

- Let C/K be a curve with genus $g > 1$ and with good reduction outside S.

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

Sketch proof:

- Let C/K be a curve with genus $g > 1$ and with good reduction outside S.
- For each point $P \in C(K)$, Kodaira–Parshin constructed a curve C_P/K' with genus g' and good reduction outside S' with a map $C_P \to C$ which is ramified only at P.

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

Sketch proof:

- Let C/K be a curve with genus $g > 1$ and with good reduction outside S.
- For each point $P \in C(K)$, Kodaira–Parshin constructed a curve C_P/K' with genus g' and good reduction outside S' with a map $C_P \to C$ which is ramified only at P.
- Crucially, K', g', and S' depend only on K, g and S (not on P).

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

Sketch proof:

- Let C/K be a curve with genus $g > 1$ and with good reduction outside S.
- For each point $P \in C(K)$, Kodaira–Parshin constructed a curve C_P/K' with genus g' and good reduction outside S' with a map $C_P \to C$ which is ramified only at P.
- Crucially, K', g', and S' depend only on K, g and S (not on P).
- Shafarevich implies there can only be finitely many such curves C_P/K'.

From Shafarevich to Mordell

Theorem (Parshin 1968)

The Shafarevich conjecture (for curves) implies the Mordell conjecture.

Sketch proof:

- Let C/K be a curve with genus $g > 1$ and with good reduction outside S.
- For each point $P \in C(K)$, Kodaira–Parshin constructed a curve C_P/K' with genus g' and good reduction outside S' with a map $C_P \to C$ which is ramified only at P.
- Crucially, K', g', and S' depend only on K, g and S (not on P).
- Shafarevich implies there can only be finitely many such curves C_P/K'.
- A classical theorem of De Franchis states that the set of (non-constant) morphisms from some curve Y to X of genus > 1 is finite. □

Motivation

Theorem (Torelli 1914-15)

Shafarevich conjecture for abelian varieties implies Shafarevich conjecture for curves.

Proof: Follows by a theorem of Torelli, which states that a curve C/K is determined by its Jacobian $\mathrm{Jac}(C)$, together with its principal polarisation. $\square$

Motivation

Theorem (Torelli 1914-15)

Shafarevich conjecture for abelian varieties implies Shafarevich conjecture for curves.

Proof: Follows by a theorem of Torelli, which states that a curve C/K is determined by its Jacobian $\mathrm{Jac}(C)$, together with its principal polarisation. $\square$

Theorem (Faltings 1983)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Motivation

Theorem (Torelli 1914-15)

Shafarevich conjecture for abelian varieties implies Shafarevich conjecture for curves.

Proof: Follows by a theorem of Torelli, which states that a curve C/K is determined by its Jacobian $\mathrm{Jac}(C)$, together with its principal polarisation. □

Theorem (Faltings 1983)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Some other proofs of the Mordell conjecture:

- Vojta–Bombieri (1990) gave proof using diophantine approximation. (simplified by Faltings)
- Lawrence–Venkatesh (2018) gave proof using p-adic Hodge theory.

Effective Mordell

None of these proofs are completely effective (but can give a weak bound on the number of points in Mordell conjecture and number of isogeny classes in Shafarevich conjecture)!

Effective Mordell

None of these proofs are completely effective (but can give a weak bound on the number of points in Mordell conjecture and number of isogeny classes in Shafarevich conjecture)!

Problem (Effective Mordell)

Given a smooth curve C/K of genus at least 2, compute $C(K)$.

Effective Mordell

None of these proofs are completely effective (but can give a weak bound on the number of points in Mordell conjecture and number of isogeny classes in Shafarevich conjecture)!

Problem (Effective Mordell)

Given a smooth curve C/K of genus at least 2, compute $C(K)$.

Many approaches one could try:

- Local methods
- Quotients
- Descent
- Mordell-Weil sieve
- Chabauty-Coleman (also quadratic Chabauty, Kim's non-abelian Chabauty)

Effective Shafarevich

- Let K be a number field and S a finite set of places of K.

Effective Shafarevich

- Let K be a number field and S a finite set of places of K.

Conjecture (Effective Mordell)

Given any smooth curve C/K of genus at least 2, there exists an effectively computable constant c such that $h(P) \leq c$ for all $P \in C(K)$.

Effective Shafarevich

- Let K be a number field and S a finite set of places of K.

Conjecture (Effective Mordell)

Given any smooth curve C/K of genus at least 2, there exists an effectively computable constant c such that $h(P) \leq c$ for all $P \in C(K)$.

Conjecture (Effective Shafarevich for curves)

Let $g \geq 2$. There exists an effectively computable constant $c_{K,g,S}$ such that, for any smooth genus g curve C/K with good reduction outside S, we have $h_F(C) \leq c_{K,g,S}$.

Effective Shafarevich

- Let K be a number field and S a finite set of places of K.

Conjecture (Effective Mordell)

Given any smooth curve C/K of genus at least 2, there exists an effectively computable constant c such that $h(P) \leq c$ for all $P \in C(K)$.

Conjecture (Effective Shafarevich for curves)

Let $g \geq 2$. There exists an effectively computable constant $c_{K,g,S}$ such that, for any smooth genus g curve C/K with good reduction outside S, we have $h_F(C) \leq c_{K,g,S}$.

Conjecture (Effective Shafarevich for abelian varieties)

Let $d \geq 1$. There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Effective Shafarevich

- Let K be a number field and S a finite set of places of K.

Conjecture (Effective Mordell)

Given any smooth curve C/K of genus at least 2, there exists an effectively computable constant c such that $h(P) \leq c$ for all $P \in C(K)$.

Conjecture (Effective Shafarevich for curves)

Let $g \geq 2$. There exists an effectively computable constant $c_{K,g,S}$ such that, for any smooth genus g curve C/K with good reduction outside S, we have $h_F(C) \leq c_{K,g,S}$.

Conjecture (Effective Shafarevich for abelian varieties)

Let $d \geq 1$. There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Effective Shafarevich (a.v.) $\Longrightarrow$ Effective Shafarevich (curves) $\Longrightarrow$ Effective Mordell

Effective Shafarevich

Effective Shafarevich

Conjecture (Effective Shafarevich)

There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Effective Shafarevich

Conjecture (Effective Shafarevich)

There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Some cases for which we have effective algorithms:

- elliptic curves ($d = 1$)

Effective Shafarevich

Conjecture (Effective Shafarevich)

There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Some cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3, 5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Schoof 2005-12).

Effective Shafarevich

Conjecture (Effective Shafarevich)

There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Some cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3, 5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Schoof 2005-12).
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a degree d number field) (von Känel 2020).

Effective Shafarevich

Conjecture (Effective Shafarevich)

There exists an effectively computable constant $c_{K,d,S}$ such that, for any dimension d abelian variety A/K with good reduction outside S, we have $h_F(A) \leq c_{K,d,S}$.

Some cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3, 5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Schoof 2005-12).
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a degree d number field) (von Känel 2020).

Even the case $d = 2$, $K = \mathbb{Q}$, $S = \{2\}$ is still an open problem!

Elliptic Curves

Elliptic Curves

Theorem (Tate 1960)

There are no elliptic curves over $\mathbb{Q}$ with good reduction everywhere.

Elliptic Curves

Theorem (Tate 1960)

There are no elliptic curves over $\mathbb{Q}$ with good reduction everywhere.

Proof: Let $E/\mathbb{Q}$ have global minimal model

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

with $a_i \in \mathbb{Z}$. Define the quantities:

$$b_2 = a_1^2 - 4a_2, \qquad c_4 = b_2^2 - 24b_4$$

$$b_4 = 2a_4 - a_1a_3, \qquad c_6 = b_2^3 - 36b_2b_4 + 216b_6$$

$$b_6 = a_3^2 - 4a_6, \qquad \Delta = b_2^2b_8 - 8b_3^4 - 27b_6^2 + 9b_2b_4b_6$$

$$b_8 = a_4^2 - a_1a_3a_4 + a_1^2a_6 + a_2a_3^2 - 4a_2a_6$$

where the discriminant Δ satisfies $1728\Delta = c_4^3 - c_6^2$.

Elliptic Curves

Theorem (Tate 1960)

There are no elliptic curves over $\mathbb{Q}$ with good reduction everywhere.

Proof: Let $E/\mathbb{Q}$ have global minimal model

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

with $a_i \in \mathbb{Z}$. Define the quantities:

$$b_2 = a_1^2 - 4a_2, \qquad c_4 = b_2^2 - 24b_4$$
$$b_4 = 2a_4 - a_1a_3, \qquad c_6 = b_2^3 - 36b_2b_4 + 216b_6$$
$$b_6 = a_3^2 - 4a_6, \qquad \Delta = b_2^2b_8 - 8b_3^4 - 27b_6^2 + 9b_2b_4b_6$$
$$b_8 = a_4^2 - a_1a_3a_4 + a_1^2a_6 + a_2a_3^2 - 4a_2a_6$$

where the discriminant Δ satisfies $1728\Delta = c_4^3 - c_6^2$.
If $E/\mathbb{Q}$ has good reduction everywhere, then $\Delta = \pm 1$.

Elliptic Curves

Can show this has no solutions by purely elementary methods:

Elliptic Curves

Can show this has no solutions by purely elementary methods:

- **Case a_1 even**:
  - Then $\pm 1 = \Delta \equiv 5b_6^2 \pmod 8$. As squares $\equiv 0, 1, 4 \pmod 8$, this is impossible!

Elliptic Curves

Can show this has no solutions by purely elementary methods:

- **Case a_1 even**:
  - Then $\pm 1 = \Delta \equiv 5b_6^2 \pmod 8$. As squares $\equiv 0, 1, 4 \pmod 8$, this is impossible!
- **Case a_1 odd**:
  - Let $x := c_4 \mp 12$. Then $x \equiv 5 \pmod 8$ and can show that $x(x^2 \pm 36x + 432) = c_6^2$.
  - $\pm x$ not square $\pmod 8 \implies \gcd(x, x^2 \pm 36x + 432) > 1 \implies 3$ divides x.
  - Let $x = 3y$, $c_6 = 9z$. Then $y(y^2 \pm 12y + 48) = 3z^2$ for some z. Note that $y \equiv 7 \pmod 8$ and $y > 0$ as $y((y \pm 6)^2 + 12) > 0$.
  - If $p > 3$ divides y, it does so to an even power. Similarly, 3 divides y, thus 3 divides z^2, and so 3 divides y to an even power. So y is a square, contradiction □

Elliptic Curves

Can show this has no solutions by purely elementary methods:

- **Case a_1 even**:
  - Then $\pm 1 = \Delta \equiv 5b_6^2 \pmod 8$. As squares $\equiv 0, 1, 4 \pmod 8$, this is impossible!
- **Case a_1 odd**:
  - Let $x := c_4 \mp 12$. Then $x \equiv 5 \pmod 8$ and can show that $x(x^2 \pm 36x + 432) = c_6^2$.
  - $\pm x$ not square $\pmod 8$ $\implies$ $\gcd(x, x^2 \pm 36x + 432) > 1$ $\implies$ 3 divides x.
  - Let $x = 3y$, $c_6 = 9z$. Then $y(y^2 \pm 12y + 48) = 3z^2$ for some z. Note that $y \equiv 7 \pmod 8$ and $y > 0$ as $y((y \pm 6)^2 + 12) > 0$.
  - If $p > 3$ divides y, it does so to an even power. Similarly, 3 divides y, thus 3 divides z^2, and so 3 divides y to an even power. So y is a square, contradiction $\square$

Ogg used similar methods to classify all elliptic curves $E/\mathbb{Q}$ with good reduction outside 2

Elliptic Curves

Theorem (Ogg 1965)

There are exactly 24 elliptic curves $E/\mathbb{Q}$ with good reduction outside 2.

Elliptic Curves

Theorem (Ogg 1965)

There are exactly 24 elliptic curves $E/\mathbb{Q}$ with good reduction outside 2.

They are:

$$
\begin{array}{llll}
y^2 = x^3 - x, & y^2 = x^3 - 8x. & y^2 = x^3 + x^2 + x + 1, & y^2 = x^3 + x^2 + 3x - 5 \\
y^2 = x^3 + x, & y^2 = x^3 + 8x, & , y^2 = x^3 - x^2 + x - 1, & y^2 = x^3 - x^2 + 3x + 5 \\
y^2 = x^3 - 2x, & y^2 = x^3 - 11x - 14, & y^2 = x^3 + x^2 - 3x + 1, & y^2 = x^3 + x^2 - 9x + 7 \\
y^2 = x^3 + 2x, & y^2 = x^3 - 11x + 14, & y^2 = x^3 - x^2 - 3x - 1 & y^2 = x^3 - x^2 - 9x - 7 \\
y^2 = x^3 - 4x, & y^2 = x^3 - 44x - 112, & y^2 = x^3 + x^2 - 2x - 2, & y^2 = x^3 + x^2 - 13x - 21 \\
y^2 = x^3 + 4x, & y^2 = x^3 - 44x + 112, & y^2 = x^3 - x^2 - 2x + 2, & y^2 = x^3 - x^2 - 13x + 21
\end{array}
$$

(divided into 10 $\mathbb{Q}$-isogeny classes and 5 $\overline{\mathbb{Q}}$-isomorphism classes).

Elliptic Curves Summary

Let $E(S)$ be the set of elliptic curves $E/\mathbb{Q}$ with good reduction outside S.

Set S	$\lvert E(S)\rvert$	**Authors**	**Year**
$\emptyset$	0	Tate (proof published by Ogg)	1965
$\{2\}$	24	Ogg	1965
$\{2,3\}$	752	Coghlan, Stephens	1967, 1965
$\{11\}$	12	Agrawal–Coates–Hunt–Van der Poorten	1980
$\{2,p\},\ p \in \{5,\ldots,23\}$	$280, 288, \ldots$	Cremona–Lingham	2007
$\{2,3,23\}$	5520	Koutsianas	2015
$\{2,3,5,7,11\}$	592 192	von Känel–Matschke	2016
$\{2,3,5,7,11,13\}$	4 576 128	Best–Matschke	2020
$\{2,3,5,7,\ldots,23\}$	1 390 818 304*	Matschke	2021

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Algorithm to compute all elliptic curves E/K with good reduction outside S:

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Algorithm to compute all elliptic curves E/K with good reduction outside S:

1. Compute all possible fields L/K of degree at most 6 and unramified outside S.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Algorithm to compute all elliptic curves E/K with good reduction outside S:

1. Compute all possible fields L/K of degree at most 6 and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x + y = 1$ in L.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Algorithm to compute all elliptic curves E/K with good reduction outside S:

1. Compute all possible fields L/K of degree at most 6 and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x + y = 1$ in L.
3. For each λ, compute the j-invariant: $j = 2^8 \frac{(\lambda^2 - \lambda + 1)^2}{\lambda^2 (1-\lambda)^2}$. Check if this lies in K.

Classifying elliptic curves

Let E/K be an elliptic curve with good reduction outside S.

- Write $E/K : y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ where $\alpha_i \in K(E[2])$.
- Let $\lambda := \frac{\alpha_3 - \alpha_1}{\alpha_2 - \alpha_1}$. Note that both λ and $1 - \lambda$ are $S \cup \{2\}$-units in $K(E[2])$.

Algorithm to compute all elliptic curves E/K with good reduction outside S:

1. Compute all possible fields L/K of degree at most 6 and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x + y = 1$ in L.
3. For each λ, compute the j-invariant: $j = 2^8 \frac{(\lambda^2 - \lambda + 1)^2}{\lambda^2 (1-\lambda)^2}$. Check if this lies in K.
4. For each valid $j \in K$, construct an elliptic curve E/K with j-invariant j, and compute all quadratic twists $E^{(u)}$ for $u \in K(S, 2)$ (for $j \neq 0, 1728$).

Classifying elliptic curves

More algorithms to compute all elliptic curves E/K with good reduction outside S:

Classifying elliptic curves

More algorithms to compute all elliptic curves E/K with good reduction outside S:

- **Mordell curves**: Given an elliptic curve E/K, we have $c_6^2 = c_4^3 - 1728\Delta$. Suffices to compute all S-integral points on $Y^2 = X^3 + n$ for finitely many n.

  Sage implements this over $\mathbb{Q}$ as:

  `EllipticCurves_with_good_reduction_outside_S`

Classifying elliptic curves

More algorithms to compute all elliptic curves E/K with good reduction outside S:

- **Mordell curves**: Given an elliptic curve E/K, we have $c_6^2 = c_4^3 - 1728\Delta$. Suffices to compute all S-integral points on $Y^2 = X^3 + n$ for finitely many n.

  Sage implements this over $\mathbb{Q}$ as:
  `EllipticCurves_with_good_reduction_outside_S`

- **Thue-Mahler equations**: Can construct a binary cubic form $F(u, v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$ such that $F(u, v)$ is a $S \cup \{2, 3\}$-smooth integer for some $u, v \in \mathbb{Z}$.

Classifying elliptic curves

More algorithms to compute all elliptic curves E/K with good reduction outside S:

- **Mordell curves**: Given an elliptic curve E/K, we have $c_6^2 = c_4^3 - 1728\Delta$. Suffices to compute all S-integral points on $Y^2 = X^3 + n$ for finitely many n.

  Sage implements this over $\mathbb{Q}$ as:
  `EllipticCurves_with_good_reduction_outside_S`

- **Thue-Mahler equations**: Can construct a binary cubic form $F(u,v) = \omega_0 u^3 + \omega_1 u^2 v + \omega_2 u v^2 + \omega_3 v^3$ such that $F(u,v)$ is a $S \cup \{2,3\}$-smooth integer for some $u, v \in \mathbb{Z}$.

- **Modular symbols**: If $K = \mathbb{Q}$ or a totally real quadratic or cubic field, then can compute the space of $\Gamma_0(N)$ modular symbols for finitely many N.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1 - \lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1 - \lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Algorithm to classify genus g hyperelliptic curves C/K with good reduction outside S:

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1 - \lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Algorithm to classify genus g hyperelliptic curves C/K with good reduction outside S:

1. Compute all fields L/K of degree at most $(2g+2)!$ and unramified outside S.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1 - \lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Algorithm to classify genus g hyperelliptic curves C/K with good reduction outside S:

1. Compute all fields L/K of degree at most $(2g+2)!$ and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x + y = 1$ in L.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1-\lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Algorithm to classify genus g hyperelliptic curves C/K with good reduction outside S:

1. Compute all fields L/K of degree at most $(2g+2)!$ and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x+y=1$ in L.
3. Compute all possible discriminants Δ.

Hyperelliptic Curves

Let C/K be a genus g hyperelliptic curve with good reduction outside S.

- Write $C/K : y^2 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{2g+2})$ where $\alpha_i \in K(J[2])$.
- Let $\lambda_i := \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_1}$. For all i, both λ_i and $1 - \lambda_i$ are $S \cup \{2\}$-units in $K(J[2])$.

Algorithm to classify genus g hyperelliptic curves C/K with good reduction outside S:

1. Compute all fields L/K of degree at most $(2g+2)!$ and unramified outside S.
2. For each L, compute all solutions λ to the S-unit equation $x + y = 1$ in L.
3. Compute all possible discriminants Δ.
4. For each combination of Δ and $\lambda_1, \lambda_2, \ldots, \lambda_{2g+2}$, compute $\alpha_i - \alpha_j$ using

$$(\alpha_i - \alpha_j)^{2(g+1)(2g+1)} = \Delta \left(\prod_{1 \leq k < \ell \leq n} \frac{\lambda_i - \lambda_j}{\lambda_k - \lambda_\ell} \right)^2 .$$

Hyperelliptic Curves

Whilst this is technically effective, its almost never practical!

Hyperelliptic Curves

Whilst this is technically effective, its almost never practical!

Theorem (von Känel 2014)

Let C/K be a genus g hyperelliptic curve with good reduction outside S. Then C/K is K-isomorphic to a Weierstrass model $y^2 = f(x)$ with absolute log height $ht(f)$ satisfying

$$ht(f) \leq \begin{cases} (\nu\sigma)^{5\nu\sigma} N_S^{\nu/2} D_K^{\nu(\lambda_S+1)/4} & \text{if } C \text{ has a } K\text{-rational WP}, \\ (\nu\sigma)^{c(2\nu)^3\sigma^4} p^{(3\nu)^3\sigma^4} D_K^{(3\nu)^3\sigma^4} & \text{if } C \text{ has no } K\text{-rational WP}, \end{cases}$$

where $d = deg(K/\mathbb{Q})$, D_K is the absolute discriminant of K over $\mathbb{Q}$, $\nu = 6(2g+1)(2g)(2g-1)d^2$, $\lambda_S = \log_2 h_S$, $\sigma = s + \lambda_S + 1$, h_S the class number of $\mathcal{O}_S$, s the number of finite places in S, p the maximum of the residue characteristics of the finite places in S, $N(v)$ the number of elements in the residue field of v, and $N_S = \prod_{v \text{ finite}} N(v)$.

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

If $A/\mathbb{Q}$ is a principally polarised abelian surface, then A is isomorphic to one of the following three cases:

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

If $A/\mathbb{Q}$ is a principally polarised abelian surface, then A is isomorphic to one of the following three cases:

1. $A \cong \mathrm{Jac}(C)$ where $C/\mathbb{Q}$ is smooth genus 2 curve.

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

If $A/\mathbb{Q}$ is a principally polarised abelian surface, then A is isomorphic to one of the following three cases:

1. $A \cong \mathrm{Jac}(C)$ where $C/\mathbb{Q}$ is smooth genus 2 curve.
2. $A \cong E_1 \times E_2$ where E_1, E_2 are elliptic curves over $\mathbb{Q}$.

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

If $A/\mathbb{Q}$ is a principally polarised abelian surface, then A is isomorphic to one of the following three cases:

1. $A \cong \mathrm{Jac}(C)$ where $C/\mathbb{Q}$ is smooth genus 2 curve.
2. $A \cong E_1 \times E_2$ where E_1, E_2 are elliptic curves over $\mathbb{Q}$.
3. $A \cong \mathrm{Res}_{K/\mathbb{Q}} E$; the Weil restriction of an elliptic curve E/K where K is a quadratic number field.

Abelian surfaces

Problem

Classify all abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2.

If $A/\mathbb{Q}$ is a principally polarised abelian surface, then A is isomorphic to one of the following three cases:

1. $A \cong \mathrm{Jac}(C)$ where $C/\mathbb{Q}$ is smooth genus 2 curve.
2. $A \cong E_1 \times E_2$ where E_1, E_2 are elliptic curves over $\mathbb{Q}$.
3. $A \cong \mathrm{Res}_{K/\mathbb{Q}} E$; the Weil restriction of an elliptic curve E/K where K is a quadratic number field.

Cases 2 and 3 can easily be dealt with. Case 1 seems to be hard (at least for me)!

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2. But there are more!

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C/\mathbb{Q} : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2.
But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C/\mathbb{Q} : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C/\mathbb{Q} : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2.
But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C/\mathbb{Q} : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.
- $C/\mathbb{Q} : y^2 = x^5 + 478x^3 + 57122x$ has bad reduction at $\{2, 13\}$.

Genus 2 curves

Theorem (Smart 1997)

There are exactly 366 genus 2 curves $C/\mathbb{Q}$ with good reduction away from 2, divided amongst 165 isogeny classes.

By taking $\mathrm{Jac}(C)$, we have examples of abelian surfaces with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C/\mathbb{Q} : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C/\mathbb{Q} : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.
- $C/\mathbb{Q} : y^2 = x^5 + 478x^3 + 57122x$ has bad reduction at $\{2, 13\}$.

So far, we've found 504 examples of genus 2 curves $C/\mathbb{Q}$ such that $\mathrm{Jac}(C)$ is good outside 2.

Abelian surfaces

Conjecture

If $C/\mathbb{Q}$ is a smooth genus 2 curve such that $\mathrm{Jac}(C)$ has good reduction away from 2, then C has good reduction away from $\{2, p\}$ for some prime $p \in \{3, 5, 7, 13\}$.

Abelian surfaces

Conjecture

If $C/\mathbb{Q}$ is a smooth genus 2 curve such that $\mathrm{Jac}(C)$ has good reduction away from 2, then C has good reduction away from $\{2, p\}$ for some prime $p \in \{3, 5, 7, 13\}$.

From here on, we'll focus on attempting to solve the (hopefully simpler) subproblem:

Abelian surfaces

Conjecture

If $C/\mathbb{Q}$ is a smooth genus 2 curve such that $\mathrm{Jac}(C)$ has good reduction away from 2, then C has good reduction away from $\{2, p\}$ for some prime $p \in \{3, 5, 7, 13\}$.

From here on, we'll focus on attempting to solve the (hopefully simpler) subproblem:

(Hopefully easier) subproblem

Classify all isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 and with full rational 2-torsion (i.e. $\mathbb{Q}(A[2]) = \mathbb{Q}$).

Faltings-Serre

Faltings-Serre

Definition (ℓ-adic Tate module)

Let A/K be an abelian variety of dimension d. The ℓ-**adic Tate module** is

$$T_\ell(A) := \varprojlim_m A[\ell^m]$$

where $A[\ell^m]$ are the ℓ^m-torsion points on A (over $\overline{K}$).

Faltings-Serre

Definition (ℓ-adic Tate module)

Let A/K be an abelian variety of dimension d. The **ℓ-adic Tate module** is

$$T_\ell(A) := \varprojlim_m A[\ell^m]$$

where $A[\ell^m]$ are the ℓ^m-torsion points on A (over $\overline{K}$).

Definition (ℓ-adic Galois representation)

For $\sigma \in \mathrm{Gal}(\overline{K}/K)$, let σ act on $T_\ell(A)$ in the natural way. Define the map

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell).$$

Faltings-Serre

Definition (ℓ-adic Tate module)

Let A/K be an abelian variety of dimension d. The **ℓ-adic Tate module** is

$$T_\ell(A) := \varprojlim_m A[\ell^m]$$

where $A[\ell^m]$ are the ℓ^m-torsion points on A (over $\overline{K}$).

Definition (ℓ-adic Galois representation)

For $\sigma \in \mathrm{Gal}(\overline{K}/K)$, let σ act on $T_\ell(A)$ in the natural way. Define the map

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell).$$

For some specific $n \geq 1$, we can factor this map as:

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K(A[\ell^n])/K) \to \mathrm{Aut} A[\ell^n] \cong \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z}).$$

Faltings-Serre

Theorem (Faltings-Serre)

Let K be a number field and S a finite set of places of K, Suppose $\rho_1, \rho_2 : Gal(\overline{K}/K) \to GL_n(\mathbb{Q}_2)$ are continuous representations unramified outside S. Then there exists a finite set of primes T disjoint from S, such that if

$$tr(\rho_1(Frob_{\mathfrak{p}})) = tr(\rho_2(Frob_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$, then ρ_1 is isomorphic to ρ_2.

Faltings-Serre

Theorem (Faltings-Serre)

Let K be a number field and S a finite set of places of K, Suppose $\rho_1, \rho_2 : Gal(\overline{K}/K) \to GL_n(\mathbb{Q}_2)$ are continuous representations unramified outside S. Then there exists a finite set of primes T disjoint from S, such that if

$$tr(\rho_1(Frob_{\mathfrak{p}})) = tr(\rho_2(Frob_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$, then ρ_1 is isomorphic to ρ_2.

Sketch proof:

Faltings-Serre

Theorem (Faltings-Serre)

Let K be a number field and S a finite set of places of K, Suppose $\rho_1, \rho_2 : Gal(\overline{K}/K) \to GL_n(\mathbb{Q}_2)$ are continuous representations unramified outside S. Then there exists a finite set of primes T disjoint from S, such that if

$$tr(\rho_1(Frob_{\mathfrak{p}})) = tr(\rho_2(Frob_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$, then ρ_1 is isomorphic to ρ_2.

Sketch proof:

- Use Hermite-Minkowski bounds to obtain finitely many number fields L/K with degree bounded by ℓ^{2d^2} and unramified away from S.

Faltings-Serre

Theorem (Faltings-Serre)

Let K be a number field and S a finite set of places of K, Suppose $\rho_1, \rho_2 : Gal(\overline{K}/K) \to GL_n(\mathbb{Q}_2)$ are continuous representations unramified outside S. Then there exists a finite set of primes T disjoint from S, such that if

$$tr(\rho_1(Frob_{\mathfrak{p}})) = tr(\rho_2(Frob_{\mathfrak{p}}))$$

for all $\mathfrak{p} \in T$, then ρ_1 is isomorphic to ρ_2.

Sketch proof:

- Use Hermite-Minkowski bounds to obtain finitely many number fields L/K with degree bounded by ℓ^{2d^2} and unramified away from S.
- Use the Chebatorev density theorem to obtain a finite set of primes T disjoint from S, such that $\{\text{Frob}_{\mathfrak{p}}\}_{\mathfrak{p} \in T}$ cover $\text{Gal}(L/K)$, for all L as above.

Faltings-Serre

Faltings-Serre

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K,s) = \prod_{\mathfrak{p} \text{ prime}} L_{\mathfrak{p}}(A/K, \mathrm{N}\mathfrak{p}^{-s}).$$

where, for primes $\mathfrak{p}$ of good reduction, $L_{\mathfrak{p}}(A/K, T)$ is given by the characteristic polynomial of $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ where $\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$.

Faltings-Serre

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K, s) = \prod_{\mathfrak{p} \text{ prime}} L_{\mathfrak{p}}(A/K, \mathrm{N}\mathfrak{p}^{-s}).$$

where, for primes $\mathfrak{p}$ of good reduction, $L_{\mathfrak{p}}(A/K, T)$ is given by the characteristic polynomial of $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ where $\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$.

Theorem (Faltings–Serre)

Let A/K and B/K be two abelian varieties. If $L_{\mathfrak{p}}(A/K, s) = L_{\mathfrak{p}}(B/K, s)$ for some effectively computable finite set of primes $\mathfrak{p}$, then $L(A/K, s) = L(B/K, s)$.

Faltings-Serre

Let A/K be an abelian variety. Its L-function factors as an Euler product,

$$L(A/K, s) = \prod_{\mathfrak{p} \text{ prime}} L_{\mathfrak{p}}(A/K, \mathrm{N}\mathfrak{p}^{-s}).$$

where, for primes $\mathfrak{p}$ of good reduction, $L_{\mathfrak{p}}(A/K, T)$ is given by the characteristic polynomial of $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ where $\rho_{A,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$.

Theorem (Faltings–Serre)

Let A/K and B/K be two abelian varieties. If $L_{\mathfrak{p}}(A/K, s) = L_{\mathfrak{p}}(B/K, s)$ for some effectively computable finite set of primes $\mathfrak{p}$, then $L(A/K, s) = L(B/K, s)$.

Theorem (Faltings–Serre–Livné)

Let $A/\mathbb{Q}$ and $B/\mathbb{Q}$ be two abelian varieties with good reduction away from 2 and with full rational 2-torsion. Then if $L_p(A/\mathbb{Q}, s) = L_p(B/\mathbb{Q}, s)$ for each $p \in \{3, 5, 7\}$, then A and B are isogenous over $\mathbb{Q}$.

Elliptic curves

To illustrate, let's use the Faltings-Serre method to classify elliptic curves with good reduction away from 2 and with full rational 2-torsion!

Elliptic curves

To illustrate, let's use the Faltings-Serre method to classify elliptic curves with good reduction away from 2 and with full rational 2-torsion!

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2, and with full rational 2-torsion. Then E is isomorphic to either $E_1 : y^2 = x^3 - x$ or $E_2 : y^2 = x^3 - 4x$.

Elliptic curves

To illustrate, let's use the Faltings-Serre method to classify elliptic curves with good reduction away from 2 and with full rational 2-torsion!

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2, and with full rational 2-torsion. Then E is isomorphic to either $E_1 : y^2 = x^3 - x$ or $E_2 : y^2 = x^3 - 4x$.

Quick proof: Let $E/\mathbb{Q}$ be given by $y^2 = x(x-a)(x-b)$ for some distinct nonzero $a, b \in \mathbb{Z}$. Then a, b and $a - b$ are all powers of 2. Can easily observe that $b \in \{-a, a/2, 2a\}$ and in every case, E is isomorphic to either E_1 or E_2. □

Elliptic curves

To illustrate, let's use the Faltings-Serre method to classify elliptic curves with good reduction away from 2 and with full rational 2-torsion!

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2, and with full rational 2-torsion. Then E is isomorphic to either $E_1 : y^2 = x^3 - x$ or $E_2 : y^2 = x^3 - 4x$.

Quick proof: Let $E/\mathbb{Q}$ be given by $y^2 = x(x-a)(x-b)$ for some distinct nonzero $a, b \in \mathbb{Z}$. Then a, b and $a - b$ are all powers of 2. Can easily observe that $b \in \{-a, a/2, 2a\}$ and in every case, E is isomorphic to either E_1 or E_2. □

Longer proof: Classify the possible Euler factors $L_3(E/\mathbb{Q}, T)$, $L_5(E/\mathbb{Q}, T)$, and $L_7(E/\mathbb{Q}, T)$ and apply the Faltings–Serre–Livné criterion!

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ *be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then* $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ *and* $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

- $\mathbb{Q}(E[2^n])$ is Galois and contains ζ_{2^n}.

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

- $\mathbb{Q}(E[2^n])$ is Galois and contains ζ_{2^n}.
- $\mathbb{Q}(E[2^n])$ is unramified outside 2.

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

- $\mathbb{Q}(E[2^n])$ is Galois and contains ζ_{2^n}.
- $\mathbb{Q}(E[2^n])$ is unramified outside 2.
- $\mathbb{Q}(E[2^n])$ is a compositum of quadratic extensions of $\mathbb{Q}(E[2^{n-1}])$.

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

- $\mathbb{Q}(E[2^n])$ is Galois and contains ζ_{2^n}.
- $\mathbb{Q}(E[2^n])$ is unramified outside 2.
- $\mathbb{Q}(E[2^n])$ is a compositum of quadratic extensions of $\mathbb{Q}(E[2^{n-1}])$.
- For each odd prime $\mathfrak{p}$ in $\mathbb{Q}(E[2^n])$, the Weil inequality implies

$$2^{2n} \leq |E(\mathbb{F}_{\mathfrak{p}})| \leq \mathrm{N}\mathfrak{p} + 1 + 2\sqrt{\mathrm{N}\mathfrak{p}}.$$

Elliptic curves

Theorem

Let $E/\mathbb{Q}$ be an elliptic curve with good reduction away from 2 and with full 2-torsion. Then $\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8)$ and $\mathbb{Q}(E[8]) = \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$

Proof: For any $n \geq 1$, we note the following properties for $\mathbb{Q}(E[2^n])$:

- $\mathbb{Q}(E[2^n])$ is Galois and contains ζ_{2^n}.
- $\mathbb{Q}(E[2^n])$ is unramified outside 2.
- $\mathbb{Q}(E[2^n])$ is a compositum of quadratic extensions of $\mathbb{Q}(E[2^{n-1}])$.
- For each odd prime $\mathfrak{p}$ in $\mathbb{Q}(E[2^n])$, the Weil inequality implies

$$2^{2n} \leq |E(\mathbb{F}_{\mathfrak{p}})| \leq \mathrm{N}\mathfrak{p} + 1 + 2\sqrt{\mathrm{N}\mathfrak{p}}.$$

- $\mathrm{Gal}(\mathbb{Q}(E[2^n])/\mathbb{Q})$ is a subgroup of $\{M \in \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z}) : M \equiv I \pmod 2\}$.

Elliptic curves

$\mathbb{Q}$

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

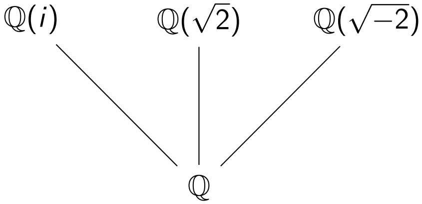

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

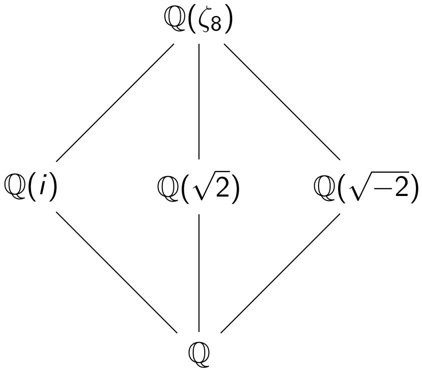

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

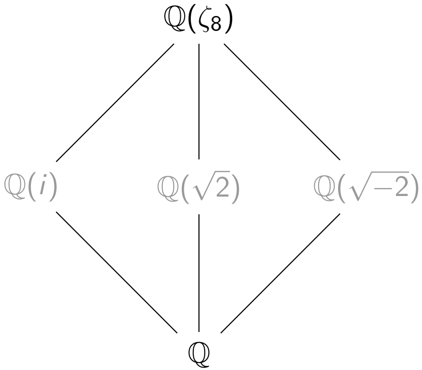

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

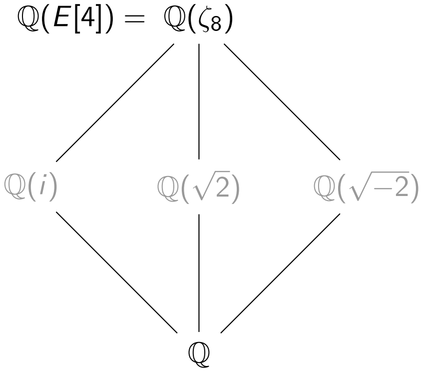

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

$\mathbb{Q}(\zeta_8)$

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

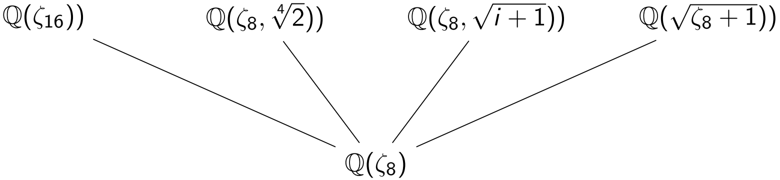

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

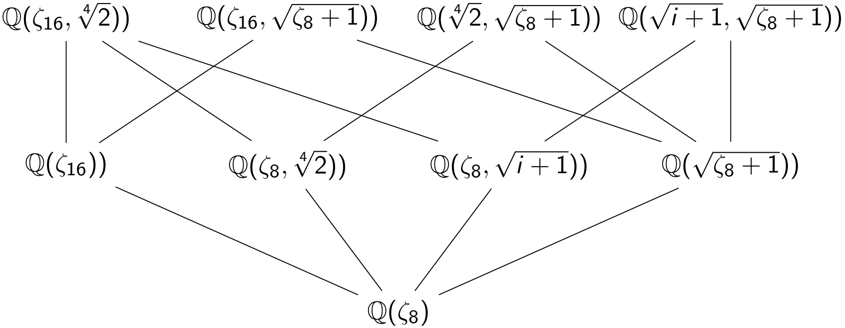

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

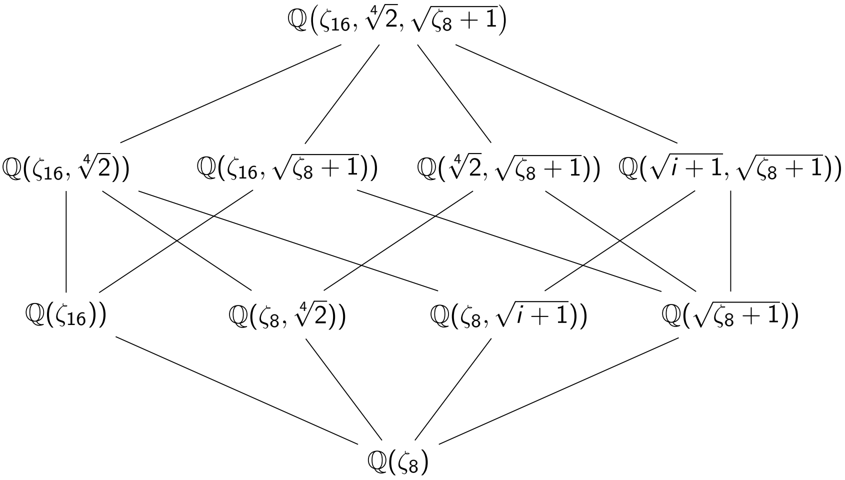

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

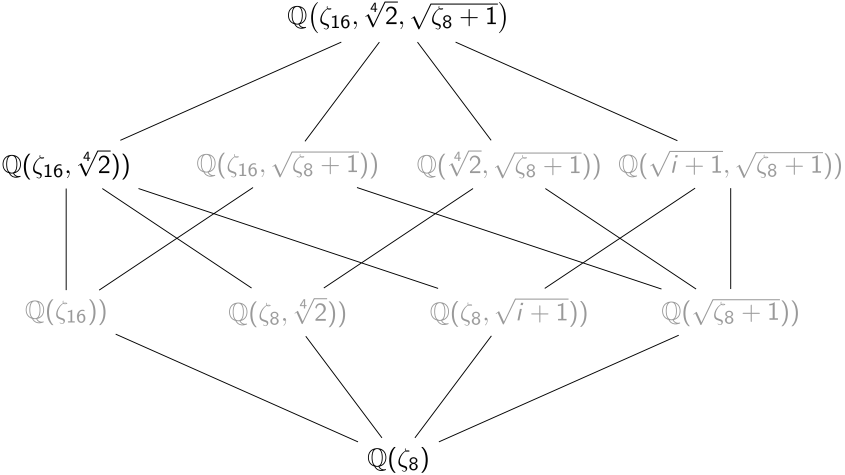

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

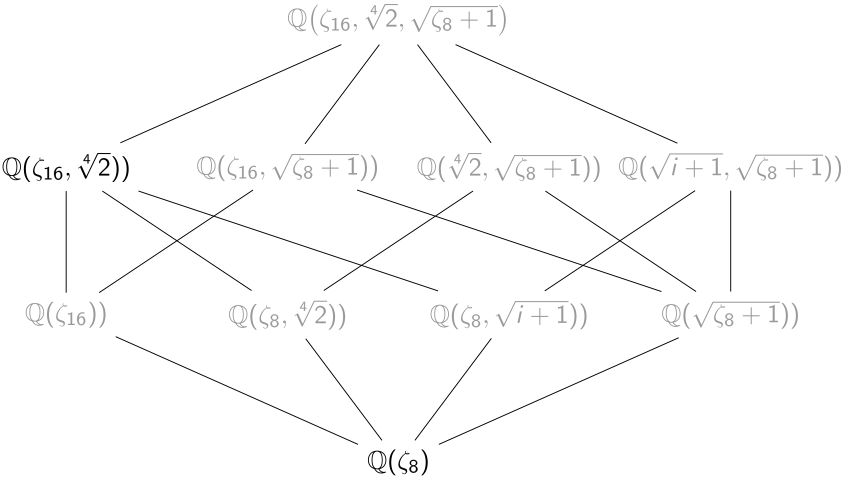

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

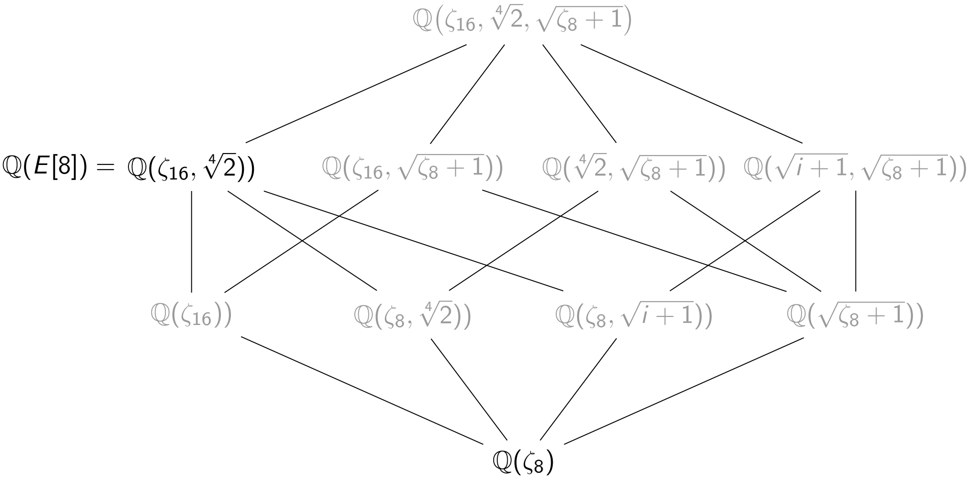

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

- As $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}) \cong C_2^2 \rtimes C_4$, we compute all possible embeddings of $C_2^2 \rtimes C_4$ into $\{M \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod 2\}$.

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

- As $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}) \cong C_2^2 \rtimes C_4$, we compute all possible embeddings of $C_2^2 \rtimes C_4$ into $\{M \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod 2\}$.
- Using that $\det(\mathrm{Frob}_p) = p$, a brute force computer search yields

$$\mathrm{tr}(\mathrm{Frob}_3) \equiv 0, \quad \mathrm{tr}(\mathrm{Frob}_5) \equiv 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) \equiv 0 \pmod 8.$$

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

- As $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}) \cong C_2^2 \rtimes C_4$, we compute all possible embeddings of $C_2^2 \rtimes C_4$ into $\{M \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod 2\}$.
- Using that $\det(\mathrm{Frob}_p) = p$, a brute force computer search yields

$$\mathrm{tr}(\mathrm{Frob}_3) \equiv 0, \quad \mathrm{tr}(\mathrm{Frob}_5) \equiv 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) \equiv 0 \pmod 8.$$

- By the Hasse-Weil bound, this implies

$$\mathrm{tr}(\mathrm{Frob}_3) = 0, \quad \mathrm{tr}(\mathrm{Frob}_5) = 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) = 0.$$

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

- As $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}) \cong C_2^2 \rtimes C_4$, we compute all possible embeddings of $C_2^2 \rtimes C_4$ into $\{M \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod 2\}$.
- Using that $\det(\mathrm{Frob}_p) = p$, a brute force computer search yields

$$\mathrm{tr}(\mathrm{Frob}_3) \equiv 0, \quad \mathrm{tr}(\mathrm{Frob}_5) \equiv 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) \equiv 0 \pmod 8.$$

- By the Hasse-Weil bound, this implies

$$\mathrm{tr}(\mathrm{Frob}_3) = 0, \quad \mathrm{tr}(\mathrm{Frob}_5) = 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) = 0.$$

- Using the Faltings–Serre–Livné criterion, this implies there are at most two isogeny classes of elliptic curves $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion.

Elliptic curves

Classifying $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion:

- As $\mathrm{Gal}(\mathbb{Q}(\zeta_{16}, \sqrt[4]{2}) \cong C_2^2 \rtimes C_4$, we compute all possible embeddings of $C_2^2 \rtimes C_4$ into $\{M \in \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) : M \equiv I \pmod 2\}$.
- Using that $\det(\mathrm{Frob}_p) = p$, a brute force computer search yields

$$\mathrm{tr}(\mathrm{Frob}_3) \equiv 0, \quad \mathrm{tr}(\mathrm{Frob}_5) \equiv 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) \equiv 0 \pmod 8.$$

- By the Hasse-Weil bound, this implies

$$\mathrm{tr}(\mathrm{Frob}_3) = 0, \quad \mathrm{tr}(\mathrm{Frob}_5) = 2 \text{ or } -2, \quad \text{and} \quad \mathrm{tr}(\mathrm{Frob}_7) = 0.$$

- Using the Faltings–Serre–Livné criterion, this implies there are at most two isogeny classes of elliptic curves $E/\mathbb{Q}$ good away from 2 with full rational 2-torsion.
- As E_1, E_2 not isogenous, there are exactly two such isogeny classes! Computing the isogeny class over $\mathbb{Q}$ for both E_1 and E_2 gives the result! □

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

1. Use the Faltings–Serre–Livné criterion to compute a finite set of primes T for which $\{L_{\mathfrak{p}}(A/K, T)\}_{\mathfrak{p} \in T}$ uniquely determines $L(A/K, s)$.

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

1. Use the Faltings–Serre–Livné criterion to compute a finite set of primes T for which $\{L_{\mathfrak{p}}(A/K, T)\}_{\mathfrak{p} \in T}$ uniquely determines $L(A/K, s)$.
2. For each $\mathfrak{p} \in T$, use the Weil inequalities to compute a finite set of possible L-factors $L_{\mathfrak{p}}(A/K, T)$.

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

1. Use the Faltings–Serre–Livné criterion to compute a finite set of primes T for which $\{L_{\mathfrak{p}}(A/K, T)\}_{\mathfrak{p} \in T}$ uniquely determines $L(A/K, s)$.
2. For each $\mathfrak{p} \in T$, use the Weil inequalities to compute a finite set of possible L-factors $L_{\mathfrak{p}}(A/K, T)$.
3. For a suitable prime ℓ and sufficiently large n, compute the possible ℓ^n-torsion fields $K(A[\ell^n])$ and thus the possible embeddings $\mathrm{Gal}(K(A[\ell^n])/K) \to \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$.

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

1. Use the Faltings–Serre–Livné criterion to compute a finite set of primes T for which $\{L_{\mathfrak{p}}(A/K, T)\}_{\mathfrak{p} \in T}$ uniquely determines $L(A/K, s)$.
2. For each $\mathfrak{p} \in T$, use the Weil inequalities to compute a finite set of possible L-factors $L_{\mathfrak{p}}(A/K, T)$.
3. For a suitable prime ℓ and sufficiently large n, compute the possible ℓ^n-torsion fields $K(A[\ell^n])$ and thus the possible embeddings $\mathrm{Gal}(K(A[\ell^n])/K) \to \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$.
4. Compute the possible characteristic polynomials (mod ℓ^n) to narrow down the possibilities for $L_{\mathfrak{p}}(A/K, T)$. For each remaining valid L-function $L(A/K, s)$, search for an abelian variety that has this L-function.

General algorithm

A "sometimes" effective algorithm to compute isogeny classes of dimension d abelian varieties A/K with good reduction outside S:

1. Use the Faltings–Serre–Livné criterion to compute a finite set of primes T for which $\{L_{\mathfrak{p}}(A/K, T)\}_{\mathfrak{p} \in T}$ uniquely determines $L(A/K, s)$.
2. For each $\mathfrak{p} \in T$, use the Weil inequalities to compute a finite set of possible L-factors $L_{\mathfrak{p}}(A/K, T)$.
3. For a suitable prime ℓ and sufficiently large n, compute the possible ℓ^n-torsion fields $K(A[\ell^n])$ and thus the possible embeddings $\mathrm{Gal}(K(A[\ell^n])/K) \to \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$.
4. Compute the possible characteristic polynomials (mod ℓ^n) to narrow down the possibilities for $L_{\mathfrak{p}}(A/K, T)$. For each remaining valid L-function $L(A/K, s)$, search for an abelian variety that has this L-function.
5. Hope that, for large enough n, the only remaining possible L-functions $L(A/K, s)$ correspond to explicit examples of abelian varieties already found!

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q},s)$	$\#L_5(A/\mathbb{Q},s)$	$\#L_7(A/\mathbb{Q},s)$
0	$\mathbb{Q}$	C_1	63	129	207

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q},s)$	$\#L_5(A/\mathbb{Q},s)$	$\#L_7(A/\mathbb{Q},s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q},s)$	$\#L_5(A/\mathbb{Q},s)$	$\#L_7(A/\mathbb{Q},s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, s)$	$\#L_5(A/\mathbb{Q}, s)$	$\#L_7(A/\mathbb{Q}, s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6
4	(many)†	$C_2^2 \rtimes C_8$, $D_4 \rtimes C_8$, $C_2^2.C_4 \wr C_2$	1	4	2

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q},s)$	$\#L_5(A/\mathbb{Q},s)$	$\#L_7(A/\mathbb{Q},s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6
4	(many)†	$C_2^2 \rtimes C_8,\ D_4 \rtimes C_8,$ $C_2^2.C_4 \wr C_2$	1	4	2
5	(many)	(many)	1	3	1

Abelian surfaces (revisited)

Let's apply this to abelian surfaces:

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q},s)$	$\#L_5(A/\mathbb{Q},s)$	$\#L_7(A/\mathbb{Q},s)$
0	$\mathbb{Q}$	C_1	63	129	207
1	$\mathbb{Q}$	C_1	17	35	53
2	$\mathbb{Q}(\zeta_8)$	$C_2 \times C_2$	6	12	16
3	$\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$	$C_2^2 \rtimes C_4$	2	5	6
4	(many)†	$C_2^2 \rtimes C_8$, $D_4 \rtimes C_8$, $C_2^2.C_4 \wr C_2$	1	4	2
5	(many)	(many)	1	3	1

†One possibility is $\mathbb{Q}(\alpha)$ with minimal polynomial $x^{32} - 16x^{31} + 120x^{30} - 528x^{29} + 1356x^{28} - 1232x^{27} - 4768x^{26} + 22128x^{25} - 41324x^{24} + 22672x^{23} + 73368x^{22} - 202720x^{21} + 227588x^{20} - 97728x^{19} - 7248x^{18} - 67344x^{17} + 130936x^{16} + 60384x^{15} - 322288x^{14} + 308080x^{13} - 66076x^{12} - 103424x^{11} + 108920x^{10} - 58864x^{9} + 24084x^{8} - 6448x^{7} + 48x^{6} +$

Results

Theorem (V. WIP (2024))

There are exactly 3 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by $E_1 \times E_1$, $E_1 \times E_2$ and $E_2 \times E_2$, where E_1, E_2 are the elliptic curves $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 - 4x$.

Results

Theorem (V. WIP (2024))

There are exactly 3 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces with full rational 2-torsion. These are given by $E_1 \times E_1$, $E_1 \times E_2$ and $E_2 \times E_2$, where E_1, E_2 are the elliptic curves $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 - 4x$.

Doing a similar (albeit more tedious) computation also gives the following result:

Theorem (V. WIP (2024))

There are exactly 23 isogeny classes of abelian surfaces $A/\mathbb{Q}$ with good reduction away from 2 which contain surfaces such that either $A[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^4$ or $A[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Thank you!