Abelian surfaces with good reduction away from 2

Young Researchers in Algebraic Number Theory (Y-RANT) conference

Robin Visser
Mathematics Institute
University of Warwick

7 September 2023

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.

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.

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Cases for which we have effective algorithms:

- elliptic curves ($d = 1$)

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a degree d number field)

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a degree d number field)
- hyperelliptic curves

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a degree d number field)
- hyperelliptic curves
- $K = \mathbb{Q}$ and $S = \emptyset$

Motivation

Faltings proof not fully effective (can give weak bound on number of isogeny classes)!

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 $h_F(A) \leq c_{K,d,S}$.

Cases for which we have effective algorithms:

- elliptic curves ($d = 1$)
- abelian varieties of GL_2-type (i.e. $\mathrm{End}(A) \otimes \mathbb{Q}$ contains a degree d number field)
- hyperelliptic curves
- $K = \mathbb{Q}$ and $S = \emptyset$

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

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 502 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 $\{2, 3, 5, 7, 13\}$.

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 $\{2, 3, 5, 7, 13\}$.

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 $\{2, 3, 5, 7, 13\}$.

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

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

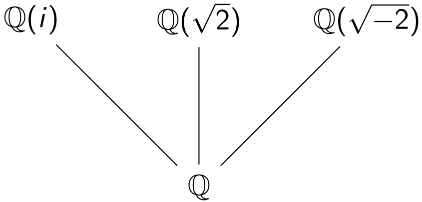

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

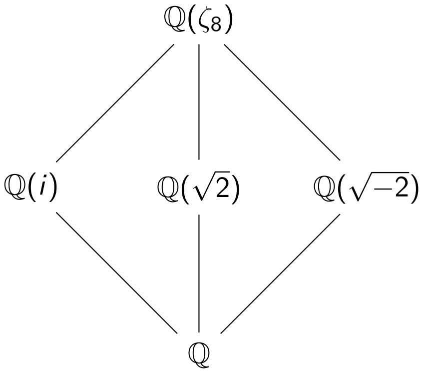

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

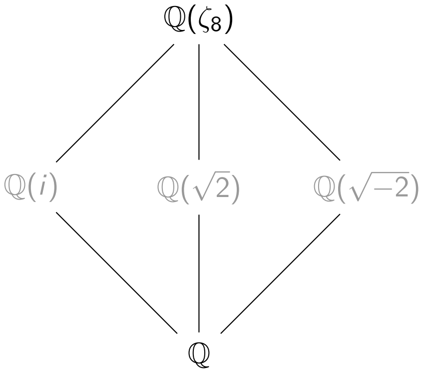

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

Elliptic curves

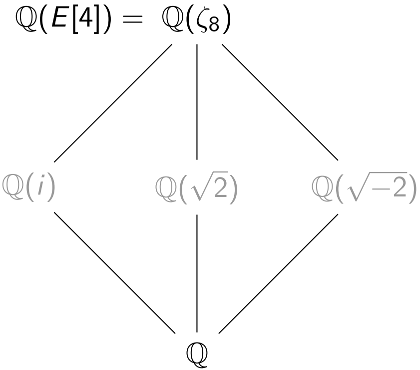

Figure: Field diagram of quadratic extensions of $\mathbb{Q}$ unramified away from 2, and their compositum.

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

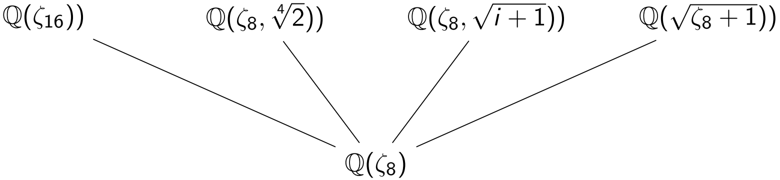

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

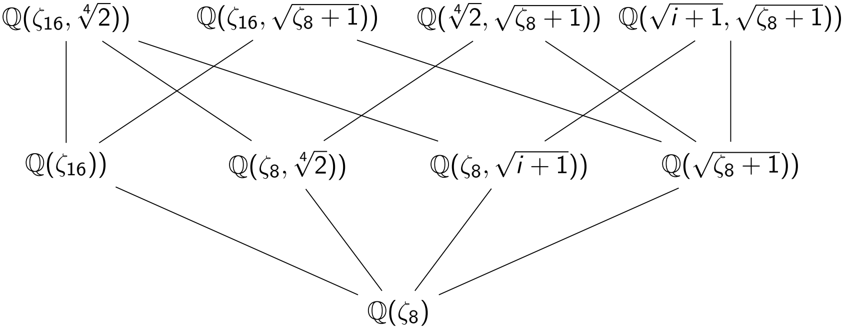

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

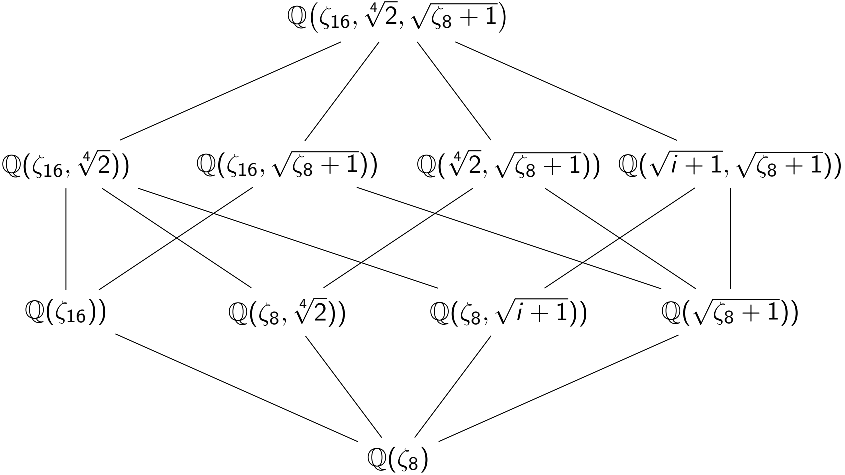

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

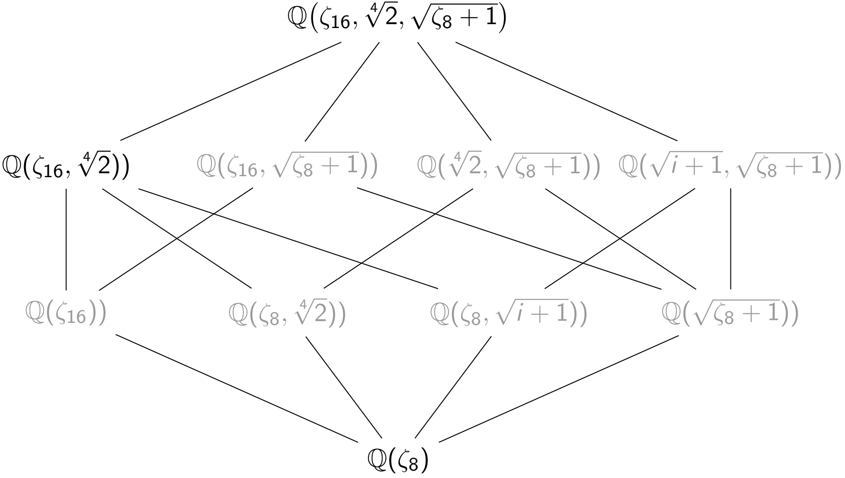

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

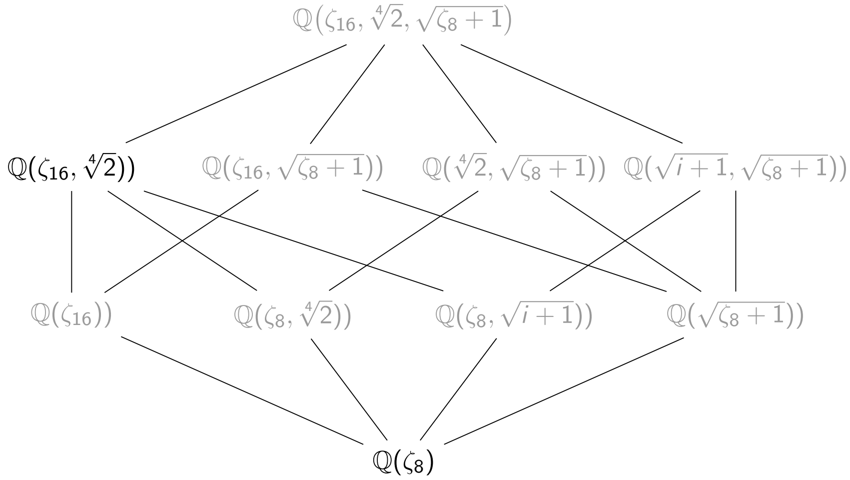

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

Elliptic curves

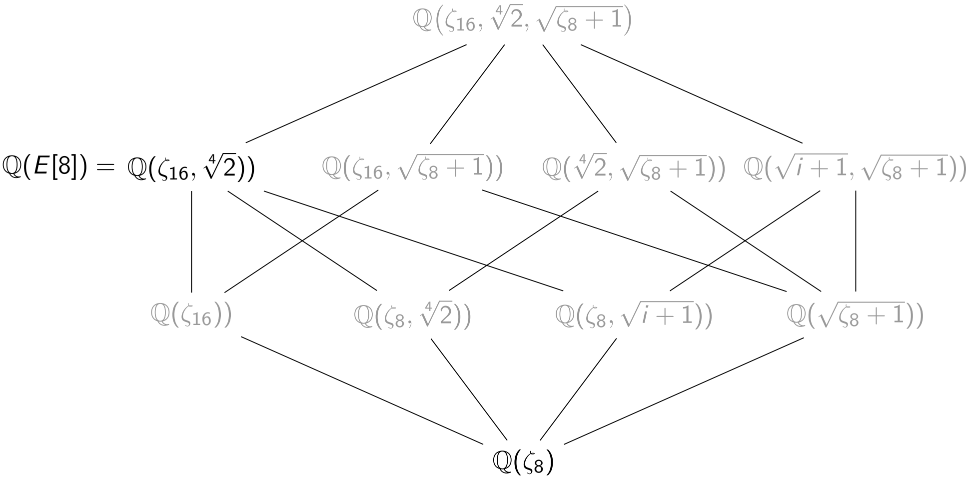

Figure: Field diagram of quadratic extensions of $\mathbb{Q}(\zeta_8)$ unramified away from 2, and their compositums.

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. 2023)

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. 2023)

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. 2023)

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!