Abelian surfaces with good reduction away from 2

Modular curves and Galois representations

Robin Visser
Mathematics Institute
University of Warwick

19 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.

Theorem (Faltings 1983; conjectured by 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.

Theorem (Faltings 1983; conjectured by Mordell 1922)

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

Theorem (Faltings 1983; conjectured by 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; conjectured by Mordell 1922)

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

Theorem (Faltings 1983; conjectured by 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.

- However Faltings proof not fully effective!

Motivation

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

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

Motivation

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
- hyperelliptic curves

Motivation

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
- hyperelliptic curves
- abelian varieties of GL_2-type

Motivation

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
- hyperelliptic curves
- abelian varieties of GL_2-type

What about $d = 2$, $K = \mathbb{Q}$, $S = \{2\}$?

Problem

Problem

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

Problem

Problem

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

- This seems very hard (at least for me)!

Problem

Problem

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

- This seems very hard (at least for me)!

(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.

Faltings–Serre–Livné method

Faltings–Serre–Livné method

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

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

Faltings–Serre–Livné method

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–Livné method

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 $L_{\mathfrak{p}}(A/K,T) = L_{\mathfrak{p}}(B/K,T)$ for some effectively computable finite set of primes $\mathfrak{p}$, then $L(A/K,s) = L(B/K,s)$.

Faltings–Serre–Livné method

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 $L_{\mathfrak{p}}(A/K, T) = L_{\mathfrak{p}}(B/K, T)$ 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 $L_p(A/\mathbb{Q}, T) = L_p(B/\mathbb{Q}, T)$ for each $p \in \{3, 5, 7\}$, then A and B are isogenous over $\mathbb{Q}$.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

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

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

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

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

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

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

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

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, T)$	$\#L_5(A/\mathbb{Q}, T)$	$\#L_7(A/\mathbb{Q}, T)$
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	?	$C_2^2 \rtimes C_8,\ D_4 \rtimes C_8,$ $C_2^2.C_4 \wr C_2$	1	4	2

Computations

We brute force the possible Euler factors $L_p(A/\mathbb{Q}, T)$ for $p = 3, 5, 7$!

- Use that $\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$ embeds in $\mathrm{GL}_4(\mathbb{Z}/2^n\mathbb{Z})$, for each $n \geq 1$.
- Compute the characteristic polynomials for each matrix in the image of each embedding. This gives a finite number of possibilities for $L_p(A/\mathbb{Q}, T)$ mod 2^n.

n	$\mathbb{Q}(A[2^n])$	$\mathrm{Gal}(\mathbb{Q}(A[2^n])/\mathbb{Q})$	$\#L_3(A/\mathbb{Q}, T)$	$\#L_5(A/\mathbb{Q}, T)$	$\#L_7(A/\mathbb{Q}, T)$
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	?	$C_2^2 \rtimes C_8$, $D_4 \rtimes C_8$, $C_2^2.C_4 \wr C_2$	1	4	2
5	?	(many)	1	3	1

Results

Theorem

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

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 much longer) computation also gives the following result:

Theorem

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 $A[2](\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.