Computing genus 2 curves over $\mathbb{Q}$ whose Jacobian has good reduction away from 2

British Mathematical Colloquium, University of Manchester

Robin Visser
Mathematics Institute
University of Warwick

19 June 2024

Motivation

Conjecture (Mordell 1922)

Any smooth curve C over a number field K of genus at least 2 has only finitely many K-rational points.

Motivation

Conjecture (Mordell 1922)

Any smooth curve C over a number field K of genus at least 2 has only finitely many K-rational points.

Conjecture (Shafarevich 1962)

Let K be a number field, $d \geq 1$ a positive integer, and S a finite set of primes of K. Then there are only finitely many K-isomorphism classes of abelian varieties A/K of dimension d with good reduction outside S.

Motivation

Conjecture (Mordell 1922)

Any smooth curve C over a number field K of genus at least 2 has only finitely many K-rational points.

Conjecture (Shafarevich 1962)

Let K be a number field, $d \geq 1$ a positive integer, and S a finite set of primes of K. Then there are only finitely many K-isomorphism classes of abelian varieties A/K of dimension d with good reduction outside S.

Theorem (Parshin 1968)

The Shafarevich conjecture implies the Mordell conjecture.

Motivation

Theorem (Faltings 1983; conjectured by Mordell 1922)

Any smooth curve C over a number field K of genus at least 2 has only finitely many K-rational points.

Theorem (Faltings 1983; conjectured by Shafarevich 1962)

Let K be a number field, $d \geq 1$ a positive integer, and S a finite set of primes of K. Then there are only finitely many K-isomorphism classes of abelian varieties A/K of dimension d with good reduction outside S.

Theorem (Parshin 1968)

The Shafarevich conjecture implies the Mordell conjecture.

Motivation

Theorem (Faltings 1983; conjectured by Mordell 1922)

Any smooth curve C over a number field K of genus at least 2 has only finitely many K-rational points.

Theorem (Faltings 1983; conjectured by Shafarevich 1962)

Let K be a number field, $d \geq 1$ a positive integer, and S a finite set of primes of K. Then there are only finitely many K-isomorphism classes of abelian varieties A/K of dimension d with good reduction outside S.

Theorem (Parshin 1968)

The Shafarevich conjecture implies the Mordell conjecture.

- Unfortunately Faltings' proof doesn't give a fully effective algorithm to find all such abelian varieties ☹.

Effective Shafarevich

Conjecture (Effective Mordell)

There exists an algorithm which can explicitly compute $C(K)$ given any smooth curve C over a number field K of genus at least 2.

Effective Shafarevich

Conjecture (Effective Mordell)

There exists an algorithm which can explicitly compute $C(K)$ given any smooth curve C over a number field K of genus at least 2.

Conjecture (Effective Shafarevich)

There exists an algorithm which can explicitly compute all dimension d abelian varieties A/K with good reduction outside S, for any number field K, positive integer d, and finite set of primes S of K.

Effective Shafarevich

Conjecture (Effective Mordell)

There exists an algorithm which can explicitly compute $C(K)$ given any smooth curve C over a number field K of genus at least 2.

Conjecture (Effective Shafarevich)

There exists an algorithm which can explicitly compute all dimension d abelian varieties A/K with good reduction outside S, for any number field K, positive integer d, and finite set of primes S of K.

Theorem (Rémond 1999)

The effective Shafarevich conjecture implies the effective Mordell conjecture.

Effective Shafarevich

Conjecture (Effective Mordell)

There exists an algorithm which can explicitly compute $C(K)$ given any smooth curve C over a number field K of genus at least 2.

Conjecture (Effective Shafarevich)

There exists an algorithm which can explicitly compute all dimension d abelian varieties A/K with good reduction outside S, for any number field K, positive integer d, and finite set of primes S of K.

Theorem (Rémond 1999)

The effective Shafarevich conjecture implies the effective Mordell conjecture.

- Many techniques available to solve effective Mordell in many cases (e.g. local methods, quotients, descent, Chabauty–Coleman, Mordell–Weil sieve).

Effective Shafarevich

Some cases for which effective Shafarevich is known:

Effective Shafarevich

Some cases for which effective Shafarevich is known:

- elliptic curves (Coates 1970, Masser–Wüstholz 1988, Brumer–Silverman 1996, Poulakis 1999, Kida 2001, Cremona–Lingham 2007, Fuchs–von Känel–Wüstholz 2011, Koutsianas 2015, ...).

Effective Shafarevich

Some cases for which effective Shafarevich is known:

- elliptic curves (Coates 1970, Masser–Wüstholz 1988, Brumer–Silverman 1996, Poulakis 1999, Kida 2001, Cremona–Lingham 2007, Fuchs–von Känel–Wüstholz 2011, Koutsianas 2015, ...).
- $S = \varnothing$ for $K = \mathbb{Q}$ (Abrashkin 1976-77, Fontaine 1985), for small quadratic and cyclotomic fields K (Fontaine 1985, Abrashkin 1987, Schoof 2001–2019, Dembéle 2019).

Effective Shafarevich

Some cases for which effective Shafarevich is known:

- elliptic curves (Coates 1970, Masser–Wüstholz 1988, Brumer–Silverman 1996, Poulakis 1999, Kida 2001, Cremona–Lingham 2007, Fuchs–von Känel–Wüstholz 2011, Koutsianas 2015, ...).
- $S = \varnothing$ for $K = \mathbb{Q}$ (Abrashkin 1976-77, Fontaine 1985), for small quadratic and cyclotomic fields K (Fontaine 1985, Abrashkin 1987, Schoof 2001–2019, Dembéle 2019).
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3, 5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Brumer–Kramer 2001, Calegari 2004, Schoof 2005-12).

Effective Shafarevich

Some cases for which effective Shafarevich is known:

- elliptic curves (Coates 1970, Masser–Wüstholz 1988, Brumer–Silverman 1996, Poulakis 1999, Kida 2001, Cremona–Lingham 2007, Fuchs–von Känel–Wüstholz 2011, Koutsianas 2015, ...).
- $S = \varnothing$ for $K = \mathbb{Q}$ (Abrashkin 1976-77, Fontaine 1985), for small quadratic and cyclotomic fields K (Fontaine 1985, Abrashkin 1987, Schoof 2001–2019, Dembéle 2019).
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3,5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Brumer–Kramer 2001, Calegari 2004, Schoof 2005-12).
- abelian varieties of GL_2-type (von Känel 2020).

Effective Shafarevich

Some cases for which effective Shafarevich is known:

- elliptic curves (Coates 1970, Masser–Wüstholz 1988, Brumer–Silverman 1996, Poulakis 1999, Kida 2001, Cremona–Lingham 2007, Fuchs–von Känel–Wüstholz 2011, Koutsianas 2015, ...).
- $S = \varnothing$ for $K = \mathbb{Q}$ (Abrashkin 1976-77, Fontaine 1985), for small quadratic and cyclotomic fields K (Fontaine 1985, Abrashkin 1987, Schoof 2001–2019, Dembéle 2019).
- semistable abelian varieties over $\mathbb{Q}$, where $S = \{2\}$, $\{3\}$, $\{5\}$, $\{3, 5\}$, $\{7\}$, $\{11\}$, $\{13\}$, $\{23\}$ (Brumer–Kramer 2001, Calegari 2004, Schoof 2005-12).
- abelian varieties of GL_2-type (von Känel 2020).

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

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more!

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves 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

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

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

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

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

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

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

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

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

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.
- $C : y^2 = x^5 + 478x^3 + 57122x$ has bad reduction at $\{2, 13\}$.
- $C : y^2 = x^5 + 28x^4 - 868x^3 - 6160x^2 + 43076x - 149072$ has bad reduction at $\{2, 3, 11\}$.

Genus 2 curves

Problem (Poonen 1996)

List all genus 2 curves $C/\mathbb{Q}$ whose Jacobians have good reduction away from 2.

Smart (1997) computed all 366 genus 2 curves with good reduction outside 2. But there are more! Examples of other curves $C/\mathbb{Q}$ where $\mathrm{Jac}(C)$ good outside 2:

- $C : y^2 = x^5 - 14x^3 + 81x$ has bad reduction at $\{2, 3\}$.
- $C : y^2 = 2x^5 - 9x^4 - 24x^3 + 22x^2 + 78x - 41$ has bad reduction at $\{2, 5\}$.
- $C : y^2 = 2x^5 + x^4 - 16x^3 - 72x^2 + 240x + 136$ has bad reduction at $\{2, 7\}$.
- $C : y^2 = x^5 + 478x^3 + 57122x$ has bad reduction at $\{2, 13\}$.
- $C : y^2 = x^5 + 28x^4 - 868x^3 - 6160x^2 + 43076x - 149072$ has bad reduction at $\{2, 3, 11\}$.

So far, we've found 512 examples of genus 2 curves $C/\mathbb{Q}$ such that $\mathrm{Jac}(C)$ is good outside 2.

Genus 2 curves

Easier Problem

Fix a small set of primes S. Find all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobian has good reduction away from 2.

Genus 2 curves

Easier Problem

Fix a small set of primes S. Find all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobian has good reduction away from 2.

Strategy:

- Let $C/\mathbb{Q} : y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ be such a curve, where $\alpha_i \in \mathbb{Q}(J[2])$.

Genus 2 curves

Easier Problem

Fix a small set of primes S. Find all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobian has good reduction away from 2.

Strategy:

- Let $C/\mathbb{Q} : y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ be such a curve, where $\alpha_i \in \mathbb{Q}(J[2])$.
- Use Siegel's identity: $\dfrac{(\alpha_i-\alpha_j)(\alpha_k-\alpha_\ell)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} + \dfrac{(\alpha_i-\alpha_\ell)(\alpha_j-\alpha_k)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} = 1$

Genus 2 curves

Easier Problem

Fix a small set of primes S. Find all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobian has good reduction away from 2.

Strategy:

- Let $C/\mathbb{Q} : y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ be such a curve, where $\alpha_i \in \mathbb{Q}(J[2])$.
- Use Siegel's identity: $\dfrac{(\alpha_i-\alpha_j)(\alpha_k-\alpha_\ell)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} + \dfrac{(\alpha_i-\alpha_\ell)(\alpha_j-\alpha_k)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} = 1$
- Compute all possible 2-torsion fields $\mathbb{Q}(J[2])$.

Genus 2 curves

Easier Problem

Fix a small set of primes S. Find all genus 2 curves $C/\mathbb{Q}$ with good reduction outside S and whose Jacobian has good reduction away from 2.

Strategy:

- Let $C/\mathbb{Q} : y^2 = c(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)(x-\alpha_6)$ be such a curve, where $\alpha_i \in \mathbb{Q}(J[2])$.
- Use Siegel's identity: $\dfrac{(\alpha_i-\alpha_j)(\alpha_k-\alpha_\ell)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} + \dfrac{(\alpha_i-\alpha_\ell)(\alpha_j-\alpha_k)}{(\alpha_i-\alpha_k)(\alpha_j-\alpha_\ell)} = 1$
- Compute all possible 2-torsion fields $\mathbb{Q}(J[2])$.
- Solve the T-unit equations $x+y=1$ for $x, y \in O_T^\times$ over $\mathbb{Q}(J[2])$ where T is the primes in $\mathbb{Q}(J[2])$ lying above S.

Further optimisations

Let $\psi_1, \psi_2, \ldots, \psi_t$ be a set of T-unit generators over $\mathbb{Q}(J[2])$. Let $a_{k,i,j} \in \mathbb{Z}$ be given by

$$\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \cdots \psi_t^{a_{t,i,j}}$$

Further optimisations

Let $\psi_1, \psi_2, \ldots, \psi_t$ be a set of T-unit generators over $\mathbb{Q}(J[2])$. Let $a_{k,i,j} \in \mathbb{Z}$ be given by

$$\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \cdots \psi_t^{a_{t,i,j}}$$

Constraints on $a_{k,i,j}$:

- Galois constraints: For all $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$, $a_{f_\sigma(k), g_\sigma(i), g_\sigma(j)} = a_{k,i,j}$.
- Cluster pictures (using that J has good reduction at odd primes).
- Solving simple T-unit equations (i.e. $\tau + \sigma(\tau) = 1$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$).

Further optimisations

Let $\psi_1, \psi_2, \ldots, \psi_t$ be a set of T-unit generators over $\mathbb{Q}(J[2])$. Let $a_{k,i,j} \in \mathbb{Z}$ be given by

$$\alpha_i - \alpha_j = \psi_1^{a_{1,i,j}} \psi_2^{a_{2,i,j}} \cdots \psi_t^{a_{t,i,j}}$$

Constraints on $a_{k,i,j}$:

- Galois constraints: For all $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$, $a_{f_\sigma(k),g_\sigma(i),g_\sigma(j)} = a_{k,i,j}$.
- Cluster pictures (using that J has good reduction at odd primes).
- Solving simple T-unit equations (i.e. $\tau + \sigma(\tau) = 1$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(J[2])/\mathbb{Q})$).

Solving the linear system:

- Brute force
- Closest vector problem
- Integer programming

Summary

Theorem (V. WIP)

There are at least 512 $\mathbb{Q}$-isomorphism classes of genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2. These include all such curves where $C/\mathbb{Q}$ has good reduction away from either $\{2,3\}$, $\{2,5\}$, or $\{2,7\}$. In particular,

1. *There are exactly 78 genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2 and such that $rad(\Delta_{min}) = 6$.*
2. *There are exactly 28 genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2 and such that $rad(\Delta_{min}) = 10$.*
3. *There are exactly 24 genus 2 curves $C/\mathbb{Q}$ whose Jacobian has good reduction away from 2 and such that $rad(\Delta_{min}) = 14$.*

All genus 2 curves $C/\mathbb{Q}$ whose Jacobian is good outside 2 and such that $|\Delta_{min}| \leq 10^{14}$ is contained in our table.

Summary

- All curves (and more stats) given at: `bit.ly/genus2`

Summary

- All curves (and more stats) given at: `bit.ly/genus2`
- Are there any curves $C/\mathbb{Q}$ with $\mathrm{Jac}(C)$ good outside 2 not in our list?

Summary

- All curves (and more stats) given at: `bit.ly/genus2`
- Are there any curves $C/\mathbb{Q}$ with $\mathrm{Jac}(C)$ good outside 2 not in our list?
- If you can find any more curves, please let me know!

Summary

- All curves (and more stats) given at: `bit.ly/genus2`
- Are there any curves $C/\mathbb{Q}$ with $\mathrm{Jac}(C)$ good outside 2 not in our list?
- If you can find any more curves, please let me know!

Thank you!