Computing Isogeny Classes of Principally Polarized Abelian Surfaces Over the Rationals

Edgar Costa (MIT)

April 13, 2023, Leibniz Universität Hannover

Slides available at edgarcosta.org

Joint work with Raymond van Bommel, Shiva Chidambaram, and Jean Kieffer.

Isogeny classes

Fix a number field k to be the base field. We can take $k = \mathbb{Q}$.

Definition

An isogeny between two abelian varieties is a $\varphi : A \twoheadrightarrow B$ such that $\# \ker \varphi < \infty$.

The isogeny class is obtained by taking quotients by finite rational subgroups.

This defines an equivalence relation, as we have $\varphi^\vee : B^\vee \to A^\vee$.

We are interested in computing the isogeny class of A over k.

Isogeny classes

Two abelian varieties in the same isogeny class share many properties, e.g.,

- L-function
- Mordell–Weil rank
- Endomorphism algebra $\mathrm{End}(A) \otimes \mathbb{Q}$

Isogeny classes

Two abelian varieties in the same isogeny class share many properties, e.g.,

- L-function
- Mordell–Weil rank
- Endomorphism algebra $\mathrm{End}(A) \otimes \mathbb{Q}$

Theorem (Faltings)

The isogeny class of an abelian variety over k is finite.

Can construct (finite, connected) isogeny graphs:

- Vertices are abelian varieties in an isogeny class.
- Edges are irreducible (labeled by degree = size of kernel)

Isogeny classes

Two abelian varieties in the same isogeny class share many properties, e.g.,

- L-function
- Mordell–Weil rank
- Endomorphism algebra $\mathbf{End}(A) \otimes \mathbb{Q}$

Theorem (Faltings)

The isogeny class of an abelian variety over k is finite.

Can construct (finite, connected) isogeny graphs:

- Vertices are abelian varieties in an isogeny class.
- Edges are irreducible (labeled by degree = size of kernel)

Question

What are the possibility isogeny graphs?

Elliptic curves

We can explore isogeny graphs of elliptic curves in the `www.LMFDB.org`.

We will find:

- all the degrees of irreducible isogenies are primes

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes
  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as

$$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$

  where $\deg \varphi_i = \ell_i$ are primes.

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes

  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as

  $$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$

  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes

  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as

  $$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$

  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up (Mazur)

  $\ell \in \{2, 3, 5, 7, 13, 11, 17, 37, 19, 43, 67, 163\}$.

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes

  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as

  $$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$

  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up (Mazur)

  $\ell \in \{2, 3, 5, 7, 13, 11, 17, 37, 19, 43, 67, 163\}$.
- the largest isogeny graph has size 8

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes
  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as
  $$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$
  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up (Mazur)
  $\ell \in \{2, 3, 5, 7, 13, 11, 17, 37, 19, 43, 67, 163\}$.
- the largest isogeny graph has size 8 (Kenku)

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes
  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as

$$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$

  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up (Mazur)
  $\ell \in \{2, 3, 5, 7, 13, 11, 17, 37, 19, 43, 67, 163\}$.
- the largest isogeny graph has size 8 (Kenku)
- not many graphs show up (only 10 if one ignores the degrees)
  1: 37.a 2: 26.b 3: 11.a 4: 27.a, 20.a, 17.a 6: 14.a, 21.a 8: 15.a, 30.a

Elliptic curves

We can explore isogeny graphs of elliptic curves in the www.LMFDB.org.

We will find:

- all the degrees of irreducible isogenies are primes
  Indeed, an isogeny $\varphi : E \to E'$ can always be factored as
  $$E \xrightarrow{[n]} E \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_n} E_n = E',$$
  where $\deg \varphi_i = \ell_i$ are primes.
- not all primes show up (Mazur)
  $\ell \in \{2, 3, 5, 7, 13, 11, 17, 37, 19, 43, 67, 163\}$.
- the largest isogeny graph has size 8 (Kenku)
- not many graphs show up (only 10 if one ignores the degrees)
  1: 37.a 2: 26.b 3: 11.a 4: 27.a, 20.a, 17.a 6: 14.a, 21.a 8: 15.a, 30.a
  (Chiloyan–Lozano-Robledo 2021) That is all, LMFDB has all the possibilities.

Higher dimensions?

No such complete picture is known away from elliptic curves over $\mathbb{Q}$.

One approach is to collect data:

Algorithmic problem

Given an abelian variety A over a number field k, compute its isogeny class.

Higher dimensions?

No such complete picture is known away from elliptic curves over $\mathbb{Q}$.

One approach is to collect data:

Algorithmic problem

Given an abelian variety A over a number field k, compute its isogeny class.

Eventually restrict to the simplest higher-dimensional case:

- Abelian surfaces
- endowed with principal polarizations
- over $k = \mathbb{Q}$
- that are typical, i.e. $\mathrm{End}(A^{\mathrm{al}}) = \mathbb{Z}$.

These are all Jacobians of genus 2 curves over $\mathbb{Q}$.

Higher dimensions?

No such complete picture is known away from elliptic curves over $\mathbb{Q}$.

One approach is to collect data:

Algorithmic problem

Given an abelian variety A over a number field k, compute its isogeny class.

Eventually restrict to the simplest higher-dimensional case:

- Abelian surfaces
- endowed with principal polarizations
- over $k = \mathbb{Q}$
- that are typical, i.e. $\mathrm{End}(A^{\mathrm{al}}) = \mathbb{Z}$.

These are all Jacobians of genus 2 curves over $\mathbb{Q}$.

`www.LMFDB.org` contains genus 2 curves with small discriminants, grouped by (heuristic) isogeny class of their Jacobians, but these classes are not complete.

Algorithmic approach

Algorithmic problem

Given an abelian variety A over a number field k, compute its isogeny class.

For an elliptic curve $E/\mathbb{Q}$:

1. Search for ℓ-isogenies $E \to E'$ for each ℓ in Mazur's list. This is a finite problem.
2. Reapply on E' as needed.

In general:

1. Reduce to finitely many isogeny types. (E.g., "prime degree" for elliptic curves)
2. Compute a finite number of possible degrees.
   We are now down to a finite problem.
3. Search for all isogenies of a given type and degree.
4. Reapply as needed.

Classification of isogenies

$\varphi : A \to B$ isogeny between principally polarized abelian varieties.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \wr\downarrow \lambda_A & & \wr\downarrow \lambda_B \\ A^\vee & \xleftarrow[\varphi^\vee]{} & B^\vee \end{array} \quad \rightsquigarrow \quad \mu = \lambda_A^{-1} \circ \varphi^\vee \circ \lambda_B \circ \varphi \in \mathrm{End}(A).$$

Recall that $\mathrm{End}(A)$ has a positive Rosati involution $\dagger$ defined by $\mu^\dagger = \lambda_A^{-1} \circ \mu^\vee \circ \lambda_A$.

Theorem (Mumford)

There is a bijection

$$\left\{\varphi : A \to B\right\} \longleftrightarrow \left\{(\mu, K) \ : \ \begin{array}{l} \mu \in \mathrm{End}(A)^\dagger, \ \mu > 0 \\ K \subseteq A[\mu] \ \text{ maximal isotropic} \end{array}\right\}$$

$$\varphi \longmapsto \left(\lambda_A^{-1} \circ \varphi^\vee \circ \lambda_B \circ \varphi, \ \ker \varphi\right).$$

Irreducible isogeny types

Assume now that $\mathrm{End}(A)^\dagger = \mathbb{Z}$. (True in particular if A is typical).

Any $\varphi : A \to B$ satisfies: $\ker(\varphi)$ is maximal isotropic in $A[n]$ for some $n \in \mathbb{Z}_{\geq 1}$.

Up to decomposing φ, can assume $n = \ell^e$ is a prime power.

Lemma

Assume $e \geq 3$. If $K \subset A[\ell^e]$ is maximal isotropic, then $\ell K \cap A[\ell^{e-2}]$ is maximal isotropic in $A[\ell^{e-2}]$.

Thus, any isogeny $\varphi : A \to B$ can always be factored as

$$A = A_0 \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} A_n = B,$$

where $\ker(\varphi_i)$ is maximal isotropic in $A_{i-1}[\ell_i]$ or $A_{i-1}[\ell_i^2]$, for ℓ_i prime.

Irreducible isogeny types for abelian surfaces

Further assume that A is an abelian surface (with p.p., and $\mathrm{End}(A)^\dagger = \mathbb{Z}$).
Then the other p.p. abelian surfaces in the isogeny class of A can be enumerated by looking at isogenies φ of the following types:

- 1-step: $K := \ker(\varphi)$ is a maximal isotropic subgroup of $A[\ell]$, so $K \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$,
- 2-step: K is a maximal isotropic subgroup of $A[\ell^2]$ and $K \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$.

of degree ℓ^2 and ℓ^4 respectively.

Remark

Over $\mathbb{Q}^{\mathrm{al}}$, every 2-step isogeny decomposes as a sequence of two 1-step isogenies, in $\ell + 1$ different ways (permuted by Galois).

Algorithmic problem

Given a p.p. abelian variety A over a number field k, compute its isogeny class.

	Elliptic curves $/\mathbb{Q}$	Typical p.p. abelian surfaces $/\mathbb{Q}$
Isogeny types	Prime degree	1-step or 2-step ✓
Possible degrees	Mazur's theorem	?
Search for isogenies		

Serre's open image theorem

Theorem (Mazur)

If $\varphi : E \to E'$ defined over $\mathbb{Q}$ has prime degree ℓ, then $\ell \in \{2, \ldots, 19, 37, 43, 67, 163\}$

Serre's open image theorem

Theorem (Mazur)

If $\varphi : E \to E'$ defined over $\mathbb{Q}$ has prime degree ℓ, then $\ell \in \{2, \ldots, 19, 37, 43, 67, 163\}$

No uniform result à la Mazur is known for abelian surfaces. However:

Serre's open image theorem

If A is a typical abelian surface, then its Galois representation ρ_A has open image in $\mathrm{GSp}_4(\widehat{\mathbb{Z}})$.

Theorem (Mazur)

If $\varphi : E \to E'$ defined over $\mathbb{Q}$ has prime degree ℓ, then $\ell \in \{2, \ldots, 19, 37, 43, 67, 163\}$

No uniform result à la Mazur is known for abelian surfaces. However:

Serre's open image theorem

If A is a typical abelian surface, then its Galois representation ρ_A has open image in $\mathrm{GSp}_4(\widehat{\mathbb{Z}})$.

This implies:

- The set $S := \{\ell : \rho_{A,\ell}(\mathrm{Gal}_{\mathbb{Q}}) \neq \mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})\}$ is finite.
- $A[\ell]$ has nontrivial rational subgroups only $\ell \in S$.
- The set S contains all primes for which 1-step and 2-step isogenies exist.

Dieulefait's algorithm

Can treat each A individually:

Algorithm (Dieulefait)[1]

Input: Conductor of A and a finite list of L-polynomials

Output: Finite superset of primes ℓ with reducible mod-ℓ Galois representation.

[1] See also Banwait–Brumer–Kim–Klagsbrun–Mayle–Srinivasan–Vogt (2023).

Dieulefait's algorithm

Can treat each A individually:

Algorithm (Dieulefait)[1]

Input: Conductor of A and a finite list of L-polynomials

Output: Finite superset of primes ℓ with reducible mod-ℓ Galois representation.

Example

$$C\colon y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$

the only possibilities are isogenies of degree 31^2:

[1] See also Banwait–Brumer–Kim–Klagsbrun–Mayle–Srinivasan–Vogt (2023).

Computing isogeny classes

Algorithmic problem

Given a p.p. abelian variety A over a number field k, compute its isogeny class.

	Elliptic curves $/\mathbb{Q}$	Typical p.p. abelian surfaces $/\mathbb{Q}$
Isogeny types	Prime degree	1-step or 2-step ✓
Possible degrees	Mazur's theorem	Dieulefait's algorithm ✓
Search for isogenies	?	??

Modular polynomials

Elliptic curves: usually search for ℓ-isogenies using algebraic equations for the cover of modular curves $X_0(\ell) \to X(1)$.

E.g., the modular polynomials $\Phi_\ell(x, y) \in \mathbb{Z}[x, y]$ defined by

$$\Phi_\ell(j, j') = 0 \iff \exists\, \varphi : E_j \longrightarrow E_{j'} \text{ such that } \ker \varphi \simeq \mathbb{Z}/\ell\mathbb{Z}.$$

Size grows as $O(\ell^{3+\varepsilon})$, big but manageable (28MB for $\ell = 163$).

Modular polynomials

Elliptic curves: usually search for ℓ-isogenies using algebraic equations for the cover of modular curves $X_0(\ell) \to X(1)$.

E.g., the modular polynomials $\Phi_\ell(x,y) \in \mathbb{Z}[x,y]$ defined by

$$\Phi_\ell(j,j') = 0 \iff \exists\,\varphi : E_j \longrightarrow E_{j'} \text{ such that } \ker\varphi \simeq \mathbb{Z}/\ell\mathbb{Z}.$$

Size grows as $O(\ell^{3+\varepsilon})$, big but manageable (28MB for $\ell = 163$).

Abelian surfaces: Modular polynomials for p.p. abelian surfaces are impractical.
More variables: $\Phi_\ell(x_1,x_2,x_3,y) \in \mathbb{Q}(x_1,x_2,x_3)[y]$.
Size grows as $O(\ell^{15+\varepsilon})$, already $\gg$ 29 GB for $\ell = 7$.

We use complex-analytic methods instead.

Moduli space of elliptic curves

Let $E/\mathbb{C}$ be an elliptic curve. Moduli space: $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}_1$.

Can choose $\tau \in \mathbb{H}_1$ and an equation $E : y^2 = x^3 - 27c_4x - 54c_6$ such that

$$\begin{array}{rcl} E(\mathbb{C}) & \simeq & \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), \\ \dfrac{dx}{2y} & \mapsto & \dfrac{1}{2\pi i}\, dz. \end{array}$$

Then c_4, c_6 are modular forms:

$$c_4 = E_4(\tau), \quad c_6 = E_6(\tau), \quad \text{hence} \quad j(E) = j(\tau) = 1728\frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2}.$$

Moduli space of elliptic curves

Let $E/\mathbb{C}$ be an elliptic curve. Moduli space: $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}_1$.

Can choose $\tau \in \mathbb{H}_1$ and an equation $E : y^2 = x^3 - 27c_4x - 54c_6$ such that

$$\begin{aligned} E(\mathbb{C}) &\simeq \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \\ \frac{dx}{2y} &\mapsto \frac{1}{2\pi i}\,dz. \end{aligned}$$

Then c_4, c_6 are modular forms:

$$c_4 = E_4(\tau), \quad c_6 = E_6(\tau), \quad \text{hence} \quad j(E) = j(\tau) = 1728\frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2}.$$

Theorem

The graded $\mathbb{C}$-algebra of modular forms on $\mathbb{H}_1$ for $\mathrm{SL}_2(\mathbb{Z})$ is $\mathbb{C}[E_4, E_6]$.

Moreover E_4, E_6 have integral, primitive Fourier expansions.
Hence c_4, c_6 are indeed “the right invariants” to consider.

Moduli space of p.p. abelian surfaces

A complex p.p. abelian surface takes the form $\mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2)$ with $\tau \in \mathbb{H}_2$.
Moduli space: $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathbb{H}_2$.

Theorem (Igusa)

The graded $\mathbb{C}$-algebra of (scalar-valued) Siegel modular forms of even weight on $\mathbb{H}_2$ for $\mathrm{Sp}_4(\mathbb{Z})$ is $\mathbb{C}[M_4, M_6, M_{10}, M_{12}]$, where the M_i are algebraically independent.

Normalized such that the M_j have primitive, integral Fourier expansions and M_{10}, M_{12} are cusp forms.
Explicit relations with the Igusa–Clebsch invariants I_2, I_4, I_6, I_{10} of a genus 2 curve:

$$M_4 = 2^{-2} I_4, \qquad M_6 = 2^{-3}(I_2 I_4 - 3 I_6),$$
$$M_{10} = -2^{-12} I_{10}, \qquad M_{12} = 2^{-15} I_2 I_{10}.$$

The M_j's are "the right invariants" on the moduli space of p.p. abelian surfaces.

Analytic isogenies

Enumerating isogenous abelian varieties is easy on the complex-analytic side.

- **Elliptic curves:** the complex tori ℓ-isogenous to $\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ are given by

  $$\mathbb{C}/(\mathbb{Z}+\tfrac{1}{\ell}\eta\tau\mathbb{Z})$$

  where $\eta \in \mathrm{SL}_2(\mathbb{Z})$ are coset representatives for $\Gamma^0(\ell)\backslash\mathrm{SL}_2(\mathbb{Z})$.
  Note: $\frac{1}{\ell}\eta\tau = \gamma\tau$ where $\gamma = \left(\begin{smallmatrix}1 & 0\\ 0 & \ell\end{smallmatrix}\right)\eta \in \mathrm{GL}_2(\mathbb{Q})^+$.

- **Abelian surfaces:** explicit sets $S_1(\ell), S_2(\ell) \subset \mathrm{GSp}_4(\mathbb{Q})^+$ such that for $i = 1, 2$,

  $$\{\text{ab. surfaces } i\text{-step } \ell\text{-isogenous to } \mathbb{C}^2/(\mathbb{Z}^2+\tau\mathbb{Z}^2)\} = \{\mathbb{C}^2/\left(\mathbb{Z}^2+\gamma\tau\mathbb{Z}^2\right)\}_{\gamma\in S_i(\ell)}.$$

Algorithmic problem

Decide when $\gamma\tau \in \mathbb{H}_2$ is attached to an abelian surface defined over $\mathbb{Q}$.

Construction of algebraic integers

Theorem (corollary of Igusa)

If f is a Siegel modular form of even weight k with integral Fourier coefficients, then $12^k f \in \mathbb{Z}[M_4, M_6, M_{10}, M_{12}]$.

Theorem

Let $\tau \in \mathbb{H}_2$ such that there exists $\lambda \in \mathbb{C}^\times$ with $\lambda^j M_j(\tau) \in \mathbb{Z}$ for $j \in \{4, 6, 10, 12\}$.
If f is a Siegel modular form of even weight k with integral Fourier coefficients, then

$$\prod_{\gamma \in S_i(\ell)} \left(X - \left(12\lambda\ell^{c_\gamma}\right)^k f(\gamma\tau) \right) \in \mathbb{Z}[X].$$

Thus, for each $j \in \{4, 6, 10, 12\}$, the complex numbers

$$N(j, \gamma) := \left(12\lambda\ell^{c_\gamma}\right)^j M_j(\gamma\tau) \qquad \text{for } \gamma \in S_i(\ell),\ i = 1 \text{ or } 2,$$

form a Galois-stable set of algebraic integers.

Algorithm and certification

Input: Invariants $m_4, m_6, m_{10}, m_{12} \in \mathbb{Z}$ of a genus 2 curve, a prime ℓ, and $i \in \{1, 2\}$.

Output: Invariants of all i-step ℓ-isogenous abelian surfaces.

1. Compute complex balls that provably contain:
   - $\tau \in \mathbb{H}_2$
   - $\lambda \in \mathbb{C}^\times$ such that $\lambda^j M_j(\tau) = m_j$ for $j \in \{4, 6, 10, 12\}$
   - $N(j, \gamma)$, for each $j \in \{4, 6, 10, 12\}$ and $\gamma \in S_i(\ell)$.
2. Keep the γ_0's such that $N(j, \gamma_0)$ contains an integer m'_j for $j \in \{4, 6, 10, 12\}$. The m'_j are putative invariants for the abelian surface attached to $\gamma_0 \tau$.
3. Confirm that $N(j, \gamma_0) = m'_j$ by certifying the vanishing of

$$\prod_{\gamma \in S_i(\ell)} \left(N(j, \gamma) - m'_j \right) \in \mathbb{Z}.$$

   We need to recompute $N(j, \gamma_0)$ (only!) to a much higher precision.

Example, continued

Let $\ell = 31$, $i = 1$ and

$$C\colon y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$

Working at 300 bits of precision, there is only one γ_0 such that the complex balls for $N(j, \gamma_0)$ for $j \in \{4, 6, 10, 12\}$ contain integers:

$$N(4, \gamma_0) = \alpha^2 \cdot 318972640 \pm 7.8 \times 10^{-47},$$
$$N(6, \gamma_0) = \alpha^3 \cdot 1225361851336 \pm 5.5 \times 10^{-39},$$
$$N(10, \gamma_0) = \alpha^5 \cdot 10241530643525839 \pm 1.6 \times 10^{-29},$$
$$N(12, \gamma_0) = -\alpha^6 \cdot 307105165233242232724 \pm 4.6 \times 10^{-22}$$

where $\alpha = 2^2 \cdot 3^2 \cdot 31$.

We certify these equalities by working at 4 128 800 bits of precision. Use certified quasi-linear time algorithms for the evaluation of modular forms (Kieffer 2022).

Reconstructing a genus 2 curve

Given $(m'_4, m'_6, m'_{10}, m'_{12}) = (318972640, 1225361851336, 10241530643525839, \ldots)$, find a corresponding curve C' such that $\mathbf{Jac}(C)$ and $\mathbf{Jac}(C')$ are isogenous over $\mathbb{Q}$.

Mestre's algorithm yields

$$y^2 = -1624248x^6 + 5412412x^5 - 6032781x^4 + 876836x^3 - 1229044x^2 - 5289572x - 1087304,$$

a quadratic twist by -83761 of the desired curve

$$C' : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862.$$

We reapply the algorithm to C', and we only find the original curve.

Reconstructing a genus 2 curve

Given $(m'_4, m'_6, m'_{10}, m'_{12}) = (318972640, 1225361851336, 10241530643525839, \ldots)$, find a corresponding curve C' such that $\mathrm{Jac}(C)$ and $\mathrm{Jac}(C')$ are isogenous over $\mathbb{Q}$.

Mestre's algorithm yields

$$y^2 = -1624248x^6 + 5412412x^5 - 6032781x^4 + 876836x^3 - 1229044x^2 - 5289572x - 1087304,$$

a quadratic twist by -83761 of the desired curve

$$C' : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862.$$

We reapply the algorithm to C', and we only find the original curve.

Remarks

- 113 minutes of CPU time for this example
- 90% of the time is spent certifying the results
- Can independently create a certificate for the isogeny (6.5 hours and 3 MB)

LMFDB data

Originally 63 107 typical genus 2 curves in 62 600 isogeny classes.

By computing isogeny classes, we found 21 923 new curves.

Size	1	2	3	4	5	6	7	8	9	10	12	16	18
Count	51 549	2 672	6 936	420	756	164	40	45	3	2	3	9	1

LMFDB data

Originally 63 107 typical genus 2 curves in 62 600 isogeny classes.

By computing isogeny classes, we found 21 923 new curves.

Size	1	2	3	4	5	6	7	8	9	10	12	16	18
Count	51 549	2 672	6 936	420	756	164	40	45	3	2	3	9	1

Observation

A 2-step 2-isogeny (of degree 16) always implies an existence of a second one. This explains the 6913 $\triangle$ and the 756 $\bowtie$ we found.

The whole computation took 75 hours. Only 3 classes took more than 10 minutes:

- 349.a: 56 min, isogeny of degree 13^4.
- 353.a: 23 min, isogeny of degree 11^4.
- 976.a: 19 min, checking that no isogeny of degree 29^4 exists.

Upcoming to LMFDB

A new set of 5 235 806 curves due to Sutherland is soon to be added to the LMFDB. Of these, 1 823 592 are typical, split amongst 1 538 149$\pm\varepsilon$ isogeny classes.

We found 688 094 new curves (in 97 days). Counts per size:

Size	1	2	3	4	5	6	7	8	≥ 9
Count	1 098 812	125 694	212 000	58 310	16 925	15 459	498	6 073	4 270

We discovered isogenies of degrees $\{2^2, 2^4, 3^2, 3^4, 5^2, 5^4, 7^2, 7^4, 11^4, 13^2, 13^4, 17^2, 31^2\}$.

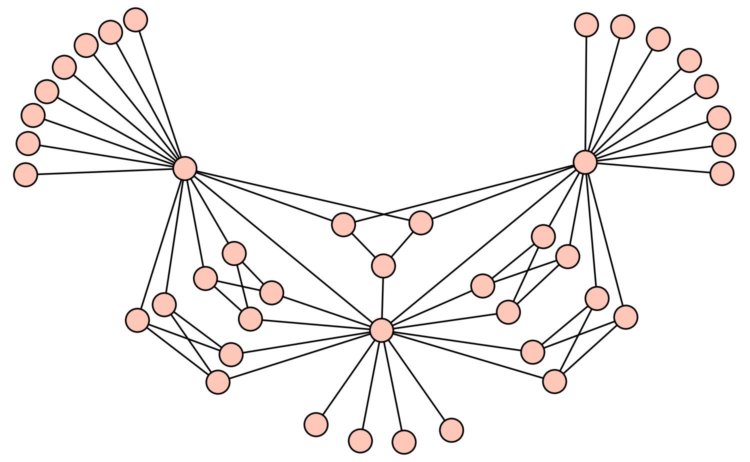
Some observations by size of isogeny class:

- 2: 75% have degree 2^2, 22% have degree 3^4, and then 3^2, 5^4, 5^2, 7^4, 7^2, . . .
- 3: 99.2% are $\triangle$ of degree 2^4 isogenies.
- 4: 97.8% are $\succ\!\!-$ of Richelot isogenies.
- 5: 99.8% are $\bowtie$ of degree 2^4 isogenies.
- 6: 75% + 15% are two graphs consisting of Richelot isogenies.

All data and graphs at https://github.com/edgarcosta/genus2classes

Life, the universe, and everything

Isogeny graph consisting of 42 Richelot isogenous curves outside our database, with conductor $497051100 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17^2$:



https://arxiv.org/abs/2301.10118