Isogeny classes of typical, principally polarized abelian surfaces over $\mathbb{Q}$

Raymond van Bommel (Massachusetts Institute of Technology)

LMFDB, Computation, and Number Theory (LuCaNT), ICERM, 10 July 2023

Joint work with Edgar Costa, Shiva Chidambaram, and Jean Kieffer

Isogenies

Definition

An isogeny between two abelian varieties over $\mathbb{Q}$ is a morphism $\varphi\colon A \twoheadrightarrow B$ such that $\#\ker\varphi < \infty$.

Isogenies are obtained by taking quotients by finite subgroups defined over $\mathbb{Q}$. Being isogenous is an equivalence relation.

Theorem (Faltings)

The isogeny class of A over $\mathbb{Q}$ is finite.

Two abelian varieties in the same isogeny class share many properties, including

- dimension
- L-function
- Mordell–Weil rank $\mathrm{rk}_{\mathbb{Z}} A(\mathbb{Q})$
- endomorphism algebra $\mathrm{End}(A) \otimes \mathbb{Q}$

Isogeny classes

Theorem (Faltings)

The isogeny class of A over $\mathbb{Q}$ is finite.

Can construct (finite, connected) isogeny graphs:

- vertices: abelian varieties in an isogeny class,
- edges: indecomposable isogenies and labelled by degree.

Questions

- What are the possible isogeny graphs when $\dim(A)$ is fixed?
- Can we compute the isogeny graph of a given abelian variety A?

Elliptic curves over the rationals

We can explore isogeny graphs of elliptic curves over $\mathbb{Q}$ at the LMFDB.

- Ignoring degrees, we find 10 non-isomorphic graphs:

Size	1	2	3	4	6	8
Examples	37.a	26.b	11.a	27.a, 20.a, 17.a	14.a, 21.a	15.a, 30.a

- All edge labels, i.e. degrees of indecomposable isogenies, are prime.
- Not all primes ℓ appear as isogeny degrees: only

$$\ell \in \{2, \ldots, 19, 37, 43, 67, 163\}.$$

Lemma

Any isogeny $\varphi \colon E \to E'$ can 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 and φ_i are defined over $\mathbb{Q}$.

Elliptic curves over the rationals

Theorem (Mazur)

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

Theorem (Kenku)

Any isogeny class of elliptic curves over $\mathbb{Q}$ has size at most 8.

Chiloyan, Lozano-Robledo 2021

Complete classification of possible labelled isogeny graphs.

The LMFDB contains examples for all of these graphs.

Higher dimensions?

Algorithmic problem

Given an abelian surface A (i.e. $g = 2$) over $\mathbb{Q}$, compute its isogeny class.

In this work, we add two additional assumptions:

- A is principally polarized, i.e. equipped with $A \simeq A^\vee$. True for ECs and Jacobians.
- A is typical, i.e. $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$.

Then A is the Jacobian of genus 2 curves over $\mathbb{Q}$:

$$y^2 = f(x), \qquad \deg(f) = 5 \text{ or } 6 \text{ and } f \text{ has distinct roots.}$$

The LMFDB contains genus 2 curves with small discriminants, grouped by isogeny class of their Jacobians, but these isogeny classes are currently not complete.

Algorithmic approach

Algorithmic problem

Given an abelian variety A over $\mathbb{Q}$, 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. Classify the possible isogeny types. (E.g., "prime degree" for elliptic curves.)
2. Compute a finite number of possible degrees. We now face a finite problem.
3. Search for all isogenies of a given type and degree.
4. Reapply as needed.

Classification of isogenies

Let A be typical, principally polarized abelian surface.

Proposition

The isogeny class of A can be enumerated using isogenies φ of the following types:

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

These isogenies are of degree ℓ^2 and ℓ^4 respectively. Here "isotropic" means: isotropic w.r.t. the Weil pairing on $A[\ell]$ or $A[\ell^2]$, so that the quotient abelian surface A/K is still principally polarized.

We need to know which primes ℓ can arise. However no analogue of Mazur's isogeny theorem is known for $g > 1$.

Dieulefait's algorithm

Serre's open image theorem

If A is a typical abelian surface, then $A[\ell]$ has a nontrivial subgroup defined over $\mathbb{Q}$ only for finitely many primes ℓ.

This is good: if φ is a 1-step isogeny, then $A[\ell]$ contains a 2-dimensional subspace defined over $\mathbb{Q}$. If φ is 2-step, then $A[\ell]$ contains a 1-dimensional subspace over $\mathbb{Q}$.

Algorithm (Dieulefait, 2002)

Input: Genus 2 curve C such that $A = \mathrm{Jac}(C)$

Output: Finite set of primes ℓ containing those for which $A[\ell]$ has nontrivial subgroups defined over $\mathbb{Q}$.

Example where the only possibilities are isogenies of degree 31^2:

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

The only reasonable algorithm to actually find isogenies is to use analytic methods, i.e. $\mathbb{Q} \hookrightarrow \mathbb{C}$.

We have $A(\mathbb{C}) = \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2)$ for some period matrix $\tau \in \mathbb{H}_2$: this means τ is a 2×2 complex, symmetric matrix such that $\mathrm{Im}(\tau)$ is positive definite. $\mathbb{H}_2$ carries an action of $\mathrm{GSp}_4(\mathbb{R})^+$, analogous to the "usual" action of $\mathrm{GL}_2^+(\mathbb{R})$ on $\mathbb{H}_1$.

Lemma

There are explicit sets $S_1(\ell)$ and $S_2(\ell) \subset \mathrm{GSp}_4(\mathbb{Q})^+$ such that for $i = 1, 2$,

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

We need to decide when $\gamma\tau \in \mathbb{H}_2$ is attached to an abelian surface defined over $\mathbb{Q}$, and if so, reconstruct the associated genus 2 curve.

Finding isogenous curves

Task

Decide which $\gamma\tau$, for $\gamma \in S_1(\ell)$ or $S_2(\ell)$, are period matrices of $\mathbf{Jac}(C)$ for some genus 2 curve $C/\mathbb{Q}$.

Problem

Modular polynomials are of size $\mathcal{O}(\ell^{15+\varepsilon})$, which is too big! ($\gg$ 29 GB for $\ell = 7$)

1. Evaluate Siegel modular forms at $\gamma\tau$. This yields $\mathbb{C}$-valued invariants of the curve C. (Think: the j-invariant of elliptic curves is also an analytic function.) Call these invariants $N(j, \gamma)$ for $j \in \{4, 6, 10, 12\}$.
2. If C is defined over $\mathbb{Q}$, then $N(j, \gamma)$ is a rational number, and even an integer if properly constructed. We can certify this with interval arithmetic.
3. Given these invariants in $\mathbb{Z}$, reconstruct an equation for C by "standard methods" (Mestre's algorithm, computing the correct twist.)

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 $\gamma_0 \in S_1(\ell)$ such that the invariants $N(j,\gamma_0)$ for $j \in \{4, 6, 10, 12\}$ could possibly be integers:

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

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

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

Example, finding the 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.

Remarks

- 113 minutes of CPU time for this example
- 90% of the time is spent certifying the results

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 1 743 737 typical genus 2 curves due to Sutherland is soon to be added to the LMFDB, split in 1 440 894 isogeny classes. We found 600 948 new curves (in 111 CPU days). Counts per size:

1	2	3	4	5	6	7	8	≥ 9
1 032 456	116 847	197 253	54 543	15 547	14 323	430	5 594	3 901

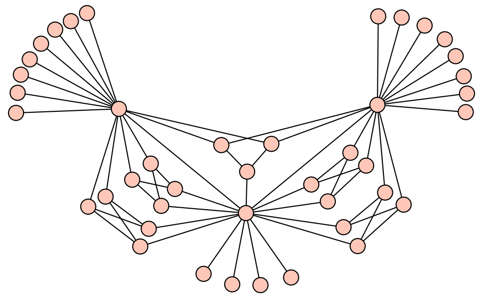
We discovered indecomposable isogenies of degree

$$2^2 \text{ (= Richelot isogenies)}, \ 2^4, 3^2, 3^4, 5^2, 5^4, 7^2, 7^4, 11^4, 13^2, 13^4, 17^2, 31^2.$$

- Size 2: 75% have degree 2^2, 22% have degree 3^4, and then 3^2, 5^4, 5^2, 7^4, 7^2, ...
- Size 3: 99% are $\triangle$ of degree 2^4 isogenies.
- Size 4: 98% are $\succ\!\!-$ of Richelot isogenies.
- Size 5: 99.8% are $\bowtie$ of degree 2^4 isogenies.
- Size 6: 75% + 15% are two graphs consisting of Richelot isogenies.

Life, the universe, and everything

Isogeny graph consisting of 42 Richelot isogenous curves (outside our database):



Preprint: https://arxiv.org/abs/2301.10118

Code and data: https://github.com/edgarcosta/genus2isogenies