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

Jean Kieffer (Harvard)

Arithmetic Statistics conference, CIRM Luminy, May 16, 2023

Joint work with Raymond van Bommel, Shiva Chidambaram, and Edgar Costa (MIT)

Elliptic curves and abelian varieties

Fix a number field k. (Later on, $k = \mathbb{Q}$).

Definition

An abelian variety over k is a smooth, projective variety over k with a group law.

Call the dimension g. Example: elliptic curve (= dimension 1)

$$E : y^2 = x^3 + ax + b \qquad (a, b \in k,\ 4a^3 + 27b^2 \neq 0.)$$

More generally, the Jacobian of a smooth curve of genus g.

Even though elliptic curves and abelian varieties are equally important in number theory, there is a wide complexity gap between $g = 1$ and $g > 1$.

Isogenies

Definition

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

Isogenies are obtained by taking quotients by finite subgroups defined over k. Being isogenous is an equivalence relation.

Theorem (Faltings)

The isogeny class of A over k is finite.

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

- Dimension
- L-function
- Mordell–Weil rank $\mathrm{rk}_{\mathbb{Z}}\, A(k)$
- Endomorphism algebra $\mathrm{End}(A) \otimes \mathbb{Q}$...

Isogeny graphs

Theorem (Faltings)

The isogeny class of A over k is finite.

Can construct (finite, connected) isogeny graphs:

- Vertices are abelian varieties in an isogeny class,
- Edges are irreducible isogenies, e.g. labeled by degree.

Questions

- What are the possible isogeny graphs?
- Can we compute them?
- Which statistical behaviors occur?

Elliptic curves over the rationals: the LMFDB

From now on, $k = \mathbb{Q}$.

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

- 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 irreducible isogenies, are prime.
- Not all primes ℓ appear as isogeny degrees: only

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

Elliptic curves over the rationals: classification

Lemma

Any isogeny $\varphi : E \to E'$ 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 $\mathbb{Q}$.

Theorem (Mazur)

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

Theorem (Kenku)

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

Chiloyan, Lozano-Robledo 2021

Complete classification of possible labeled isogeny graphs.

The LMFDB contains examples for all of these graphs.

Elliptic curves over the rationals: statistics

Ongoing effort to answer counting problems for isogenies between elliptic curves over $\mathbb{Q}$. Ordered by height: $\mathrm{ht}(E) = \max\{4|a|^3, 27|b|^2\}$.

Theorem (Molnar, Voight 2022)

For each $\varepsilon > 0$, there are effectively computable constants c, c' such that

$$\#\{E/\mathbb{Q} : E \text{ admits a 7-isogeny, } \mathrm{ht}(E) \leq X\} = c\, X^{1/6} \log X + c' X^{1/6} + O(X^{1/8+\varepsilon}).$$

Related to counting points on stacky curves, as modular curves parametrize elliptic curves endowed with isogenies of a certain type.

Side question

What are estimates on the number of elliptic curves with each type of isogeny graph?

Higher dimensions?

One approach is to collect data:

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. $\mathrm{End}(A^{\mathrm{al}}) = \mathbb{Z}$.

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

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

www.LMFDB.org 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 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. 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 $K \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$.

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 ℓ's.

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 stable line.

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:

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

Analytic isogenies

The only reasonable algorithm 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 $i = 1, 2$,

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

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 $\mathrm{Jac}(C)$ for some genus 2 curve $C/\mathbb{Q}$.

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 in fact an integer if properly constructed. Can detect this in a certified way 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:

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

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

We certify equality by working at 4 128 800 bits of precision. Use certified quasi-linear time algorithms for the evaluation of modular forms, via theta functions (K. 2022).

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 1 823 592 typical genus 2 curves* due to Sutherland is soon to be added to the LMFDB, split in 1 538 149 isogeny classes.

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

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

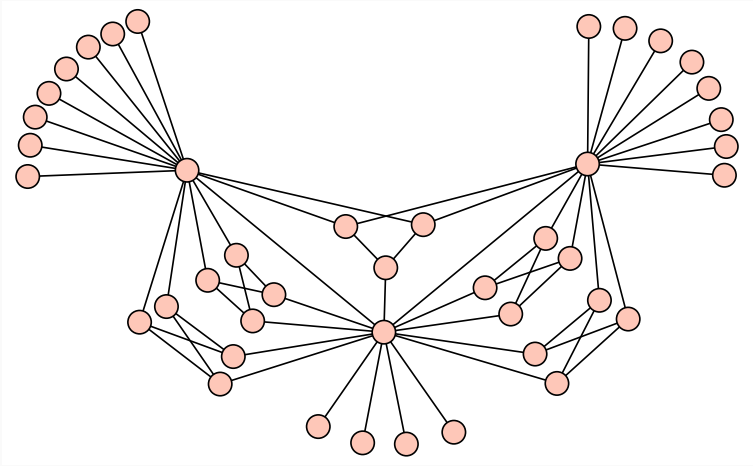
We discovered irreducible isogenies of degree

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

- 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: 99.2% are $\triangle$ of degree 2^4 isogenies.
- Size 4: 97.8% 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):



Conclusion

https://arxiv.org/abs/2301.10118

Thank you.