Computing isogeny classes of typical principally polarized abelian surfaces over the rationals

Edgar Costa (MIT)
Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation

January 4, 2023
Joint Mathematics Meetings

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

A more informal title

Computing isogeny classes of typical principally polarized abelian surfaces over the rationals

- isogeny class = "friendship graph"
- typical = "ordinary"
- principally polarized = "popular"
- typical + principally polarized + surface $\Rightarrow \text{Jac}(\text{genus 2 curve})$

Computing friendship graphs of ordinary genus 2 curves over the rationals

Isogeny classes

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 subgps.

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

Isogeny classes

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 subgps.

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

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

- L-function
- Rank
- Endomorphism algebra

In particular, the class must be finite (Faltings 1983).

Isogeny classes

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 subgps.

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

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

- L-function
- Rank
- Endomorphism algebra

In particular, the class must be finite (Faltings 1983).

What shape can these take?

Elliptic curves

If one goes to `www.LMFDB.org`, one will find:

- all the degrees of irreducible isogenies are primes

Elliptic curves

If one goes to `www.LMFDB.org`, one 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

If one goes to `www.LMFDB.org`, one 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

If one goes to www.LMFDB.org, one 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 1978): $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.

Elliptic curves

If one goes to www.LMFDB.org, one 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 1978): $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.
- the largest isogeny graph has rank 8

Elliptic curves

If one goes to www.LMFDB.org, one 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 1978): $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.
- the largest isogeny graph has rank 8 (Kenku 1982)

Elliptic curves

If one goes to www.LMFDB.org, one 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 1978): $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.
- the largest isogeny graph has rank 8 (Kenku 1982)
- 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

If one goes to www.LMFDB.org, one 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 1978): $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.
- the largest isogeny graph has rank 8 (Kenku 1982)
- 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.

Abelian surfaces

Very little is know away from elliptic curves over $\mathbb{Q}$.

www.LMFDB.org has genus 2 curves grouped by isogeny class of their Jacobian.

However, the isogeny classes are not complete.

Problem

Given an abelian surface A compute its isogeny class.

Generic approach

1. List irreducible isogeny types
2. Bound the prime divisors of their degree
3. Search for all isogenies of a given type and degree.

Generic approach

1. **List irreducible isogeny types**
   These depend on the dimension of A and $\mathrm{End}(A)^\dagger$.
2. **Bound the prime divisors of their degree**
3. **Search for all isogenies of a given type and degree.**

Generic approach

1. **List irreducible isogeny types**
   These depend on the dimension of A and $\mathrm{End}(A)^{\dagger}$.
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
2. **Bound the prime divisors of their degree**
3. **Search for all isogenies of a given type and degree.**

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
3. **Search for all isogenies of a given type and degree.**

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
3. **Search for all isogenies of a given type and degree.**

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
   Typical surfc: No global result known. Algorithmically one surface at a time. Given a surface compute a finite set of primes ℓ that includes all the possible prime divisors of the degree. (Dieulefait)
3. **Search for all isogenies of a given type and degree.**

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
   Typical surfc: No global result known. Algorithmically one surface at a time.
   Given a surface compute a finite set of primes ℓ that includes all the possible prime divisors of the degree. (Dieulefait)
3. **Search for all isogenies of a given type and degree.**
   $E/\mathbb{Q}$: using modular polynomials $\phi_\ell(x, y)$. Size of $\phi_\ell(x, y) = \widetilde{O}(\ell^3)$.
   e.g.: $\ell = 17$ requires about 8 pages of paper to print.

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
   Typical surfc: No global result known. Algorithmically one surface at a time.
3. **Search for all isogenies of a given type and degree.**
   $E/\mathbb{Q}$: using modular polynomials $\phi_\ell(x, y)$. Size of $\phi_\ell(x, y) = \widetilde{O}(\ell^3)$.
   e.g.: $\ell = 17$ requires about 8 pages of paper to print.
   Surface: modular polynomials are impractical to write down, size = $\widetilde{O}(\ell^{15})$

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
   Typical surfc: No global result known. Algorithmically one surface at a time.
3. **Search for all isogenies of a given type and degree.**
   $E/\mathbb{Q}$: using modular polynomials $\phi_\ell(x, y)$. Size of $\phi_\ell(x, y) = \widetilde{O}(\ell^3)$.
   e.g.: $\ell = 17$ requires about 8 pages of paper to print.
   Surface: modular polynomials are impractical to write down, size = $\widetilde{O}(\ell^{15})$
   The size is 1.4 MB for $\ell = 2$, 400 MB for $\ell = 3$.

Generic approach

1. **List irreducible isogeny types**
   $E/\mathbb{Q}$: maximal isotropic subgroups of $E[\ell]$, i.e., kernel of size ℓ.
   Typical surface: maximal isotropic subgroups $A[\ell^2]$ are also a possibility, i.e., kernels of size ℓ^2 or ℓ^4.
2. **Bound the prime divisors of their degree**
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$ (Mazur).
   Typical surfc: No global result known. Algorithmically one surface at a time.
3. **Search for all isogenies of a given type and degree.**
   $E/\mathbb{Q}$: using modular polynomials $\phi_\ell(x, y)$. Size of $\phi_\ell(x, y) = \widetilde{O}(\ell^3)$.
   e.g.: $\ell = 17$ requires about 8 pages of paper to print.
   Surface: modular polynomials are impractical to write down, size = $\widetilde{O}(\ell^{15})$
   The size is 1.4 MB for $\ell = 2$, 400 MB for $\ell = 3$.
   We will instead use analytical methods.

Analytic approach

Input: Genus 2 curve C

Output: All genus 2 curves such that their Jacobians are isogenous to C

- Dieulefait's tests tell us that degrees to consider. For

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

  the only possibility is 31^2.
- Compute $\tau \in \mathbb{H}_2$ as a ball that represents the isomorphism class of C.

Theorem

There exist M_k with $k \in 4, 6, 10, 12$ of weight k with integral Fourier coefficients that generate the graded $\mathbb{C}$-algebra of Siegel modular forms of $\mathbb{H}_2$.

- Compute $\lambda \in C^\times$ such that $\lambda^k M_k(\tau) = M_k(C)$ (via Igusa–Clebsch invariants) λ accounts for converting a big period matrix to a small period matrix $\tau \in \mathbb{H}_2$.

Analytic approach

Theorem

There exist M_k with $k \in 4, 6, 10, 12$ of weight k with integral Fourier coefficients that generate the graded $\mathbb{C}$-algebra of Siegel modular forms of $\mathbb{H}_2$.

- Compute $\lambda \in C^\times$ such that $\lambda^k M_k(\tau) = M_k(C)$ (via Igusa–Clebsch invariants)
- We now loop over all coset representative γ of the Hecke operator $T(\ell)$ (or $T_1(\ell^2)$) and compute $\left(\lambda c_\gamma\right)^k M_k(\gamma\tau) \in \mathbb{C}$ as balls.
  The constant c_γ such that they form Galois orbits of algebraic integers.
- Keep the γ's such that the computed balls for $\left(\lambda c_\gamma\right)^k M_k(\gamma\tau)$ contain an integer.

Analytic approach

- Keep the γ's such that the computed balls for $(\lambda c_\gamma)^k M_k(\gamma\tau)$ contain an integer.
  For our example, there is only one such γ, and
  $$(\lambda c_\gamma)^4 M_4(\gamma\tau) = \alpha^2 \cdot 318972640 \pm 7.8 \times 10^{-47}$$
  $$(\lambda c_\gamma)^6 M_6(\gamma\tau) = \alpha^3 \cdot 1225361851336 \pm 5.5 \times 10^{-39}$$
  $$(\lambda c_\gamma)^{10} M_{10}(\gamma\tau) = \alpha^5 \cdot 10241530643525839 \pm 1.6 \times 10^{-29}$$
  $$(\lambda c_\gamma)^{12} M_{12}(\gamma\tau) = -\alpha^6 \cdot 307105165233242232724 \pm 4.6 \times 10^{-22}$$
  where $\alpha = 2^2 \cdot 3^2 \cdot 31$.
- Recompute $(\lambda c_\gamma)^k M_k(\gamma\tau)$ with enough precision to certify the vanishing of
  $$\prod_\gamma ((\lambda c_\gamma)^k M_k(\gamma\tau) - m'_k) \in \mathbb{Z}.$$
- Reapply the method to the new invariants obtained.

Reconstructing curves

In our example, the isogeny class only contains one other curve.

We find it by first applying Mestre's algorithm to obtain

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

a quadratic twist by -83761 of the desired curve

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

Computing the isogeny class of this example took 113 minutes of CPU time.

Almost all of the time is spent on certifying the results.

One can independently obtain a certificate for the isogeny (6.5 hours and 3 MB).

Reconstructing curves

In our example, the isogeny class only contains one other curve.

We find it by first applying Mestre's algorithm to obtain

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

a quadratic twist by -83761 of the desired curve

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

Computing the isogeny class of this example took 113 minutes of CPU time.

Almost all of the time is spent on certifying the results.

One can independently obtain a certificate for the isogeny (6.5 hours and 3 MB).

We would like to do the same for the completeness of the isogeny graph.

LMFDB

We ran our algorithm on LMFDB. The whole computation took 75 hours of CPU time.

Originally 63 107 typical genus 2 curves, split amongst 62 600 isogeny classes.

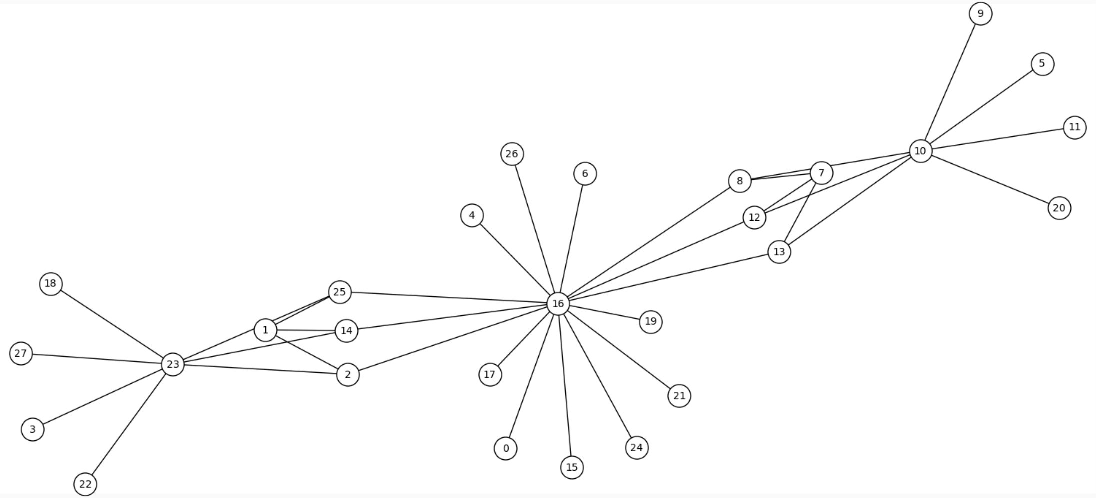
By computing isogeny classes, we found 21 923 new curves.

Size	1	2	3	4	5	6	7	8	9	10	12	16	18
Count	51549	2672	6936	420	756	164	40	45	3	2	3	9	1

Only 3 classes took more than 10 minutes.

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

Rank 28 graph



All Richolet isogenies.

3 isogeny classes with this graph with conductor $50274 = 2 \cdot 3^3 \cdot 7^2 \cdot 19$