Computing Isogeny Classes of Principally Polarized Abelian Surfaces Over the Rationals

Edgar Costa (MIT)

January 12, 2023, Simons Collaboration Annual Meeting

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

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 subgroups.

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 subgroups.

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
  $\Rightarrow$ the isogeny class of an abelian variety is finite (Faltings).

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 subgroups.

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
  $\Rightarrow$ the isogeny class of an abelian variety is finite (Faltings).
- Mordell–Weil rank
- Endomorphism algebra $\mathsf{End}(A) \otimes \mathbb{Q}$

A natural way to represent an isogeny classes, is by its irreducible isogeny graph.

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 subgroups.

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
  $\Rightarrow$ the isogeny class of an abelian variety is finite (Faltings).
- Mordell–Weil rank
- Endomorphism algebra $\mathsf{End}(A) \otimes \mathbb{Q}$

A natural way to represent an isogeny classes, is by its irreducible isogeny graph.

What shape can these take?

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.

Abelian surfaces

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

www.LMFDB.org has genus 2 curves with small minimal absolute discriminant.

These are grouped by isogeny class of their Jacobian.

However, the isogeny classes are known to not be complete.

Problem

Given an abelian surface A, compute its isogeny class.

Abelian surfaces

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

`www.LMFDB.org` has genus 2 curves with small minimal absolute discriminant.

These are grouped by isogeny class of their Jacobian.

However, the isogeny classes are known to not be complete.

Problem

Given a principally polarized abelian surface, compute all other principally polarized abelian surfaces in its isogeny class.

Generic approach

Problem

Given a principally polarized abelian surface, compute all other principally polarized abelian surfaces in its isogeny class.

1. List irreducible isogeny types.
2. List the possible degrees for each type.
3. Search for all isogenies of a given type and degree.
4. Reapply as needed.

Irreducible isogeny types

Irreducible isogeny types depend on $\dim A$ and $\mathsf{End}(A)^\dagger$.

There is a bijection

$$\left\{ \varphi : A \to B \colon \begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \wr\downarrow \lambda_A & & \wr\downarrow \lambda_B \\ A^\vee & \xleftarrow[\varphi^\vee]{} & B^\vee \end{array} \quad \#\ker\varphi < \infty \right\} \longleftrightarrow \left\{ (\mu, K) \colon \begin{array}{l} \mu \in \mathsf{End}(A)^\dagger, \mu > 0 \\ K \subseteq A[\mu] \ \text{ maximal isotropic} \end{array} \right\}$$

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

$$\varphi : (A, \lambda_A) \to (A/K, \lambda_{A/K}) \longleftarrow\!\shortmid (\mu, K)$$

Irreducible isogeny types

Irreducible isogeny types depend on $\dim A$ and $\mathsf{End}(A)^\dagger$.

There is a bijection

$$\left\{ \varphi : A \to B : \begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \wr\downarrow{\scriptstyle \lambda_A} & & \wr\downarrow{\scriptstyle \lambda_B} \\ A^\vee & \xleftarrow[\varphi^\vee]{} & B^\vee \end{array} \quad \#\ker\varphi < \infty \right\} \longleftrightarrow \left\{ (\mu, K) : \begin{array}{l} \mu \in \mathsf{End}(A)^\dagger, \mu > 0 \\ K \subseteq A[\mu] \ \text{ maximal isotropic} \end{array} \right\}$$

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

$$\varphi : (A, \lambda_A) \to (A/K, \lambda_{A/K}) \longleftarrow\!\shortmid (\mu, K)$$

Elliptic curves/$\mathbb{Q}$: $\mathsf{End}(A) = \mathsf{End}(A)^\dagger = \mathbb{Z}$

Sufficient to consider $\mu = \ell$ a prime, i.e., $\mathbb{Z}/\ell\mathbb{Z} \simeq K \subset A[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$.

Irreducible isogeny types

Irreducible isogeny types depend on $\dim A$ and $\mathsf{End}(A)^\dagger$.

There is a bijection

$$\left\{ \varphi : A \to B : \begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \wr\downarrow \lambda_A & & \wr\downarrow \lambda_B \\ A^\vee & \xleftarrow[\varphi^\vee]{} & B^\vee \end{array} \quad \#\ker\varphi < \infty \right\} \longleftrightarrow \left\{ (\mu, K) : \begin{array}{l} \mu \in \mathsf{End}(A)^\dagger, \mu > 0 \\ K \subseteq A[\mu] \text{ maximal isotropic} \end{array} \right\}$$

Elliptic curves/$\mathbb{Q}$: $\mathsf{End}(A) = \mathsf{End}(A)^\dagger = \mathbb{Z}$
Sufficient to consider $\mu = \ell$ a prime, i.e., $\mathbb{Z}/\ell\mathbb{Z} \simeq K \subset A[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$.
For higher dimension: If $\mathsf{End}(A)^\dagger = \mathbb{Z}$, sufficient to consider $\mu \in \{\ell, \ell^2\}$.

van Bommel's trick

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

If $\mathsf{End}(A)^\dagger = \mathbb{Z}$, sufficient to consider $\mu \in \{\ell, \ell^2\}$.

Lemma

$K \subset A[\ell^e]$ maximal isotropic $\implies pK \cap A[\ell^{e-2}] \subset A[\ell^{e-2}]$ maximal isotropic.

van Bommel's trick

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

If $\mathsf{End}(A)^\dagger = \mathbb{Z}$, sufficient to consider $\mu \in \{\ell, \ell^2\}$.

Lemma

$K \subset A[\ell^e]$ maximal isotropic $\implies pK \cap A[\ell^{e-2}] \subset A[\ell^{e-2}]$ maximal isotropic.

If $\mathsf{End}(A)^\dagger = \mathbb{Z}$, then an isogeny $\varphi : A \to B$ can always be factored as

$$A \xrightarrow{\alpha \in \mathsf{End}(A)} A \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} A_n = B,$$

where $\deg \varphi_i \in \{\ell_i^{\dim A}, \ell_i^{2 \dim A}\}$ for ℓ_i prime.

Irreducible isogeny types

If $\mathsf{End}(A)^\dagger = \mathbb{Z}$, then an isogeny $\varphi : A \to B$ can always be factored as

$$A \xrightarrow{\alpha \in \mathsf{End}(A)} A \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} A_n = B,$$

where $\deg \varphi_i \in \{\ell_i^{\dim A}, \ell_i^{2\dim A}\}$ for ℓ_i prime.

Furthermore, if $\dim A = 2$, we can assure that $K_i = \ker \varphi_i$ is:

- 1-step: maximal isotropic subgroup of $A[\ell_i]$, or
- 2-step: maximal isotropic subgroup of $A[\ell_i^2]$ and $K_i \simeq (\mathbb{Z}/\ell_i\mathbb{Z})^2 \times \mathbb{Z}/\ell_i^2\mathbb{Z}$.

Generic approach

Problem

Given a principally polarized abelian surface, compute all other principally polarized abelian surfaces in its isogeny class.

1. List irreducible isogeny types.
   These depend on the dimension of A and $\mathsf{End}(A)^\dagger$.
   $E/\mathbb{Q}$: 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. List the possible degrees for each type.
3. Search for all isogenies of a given type and degree.
4. Reapply as needed.

Possible degrees

Theorem (Mazur)

Let ℓ be a prime such that exists an isogeny $\varphi : E \to E'$ with kernel of order ℓ. Then $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$

Possible degrees

Theorem (Mazur)

Let ℓ be a prime such that exists an isogeny $\varphi : E \to E'$ with kernel of order ℓ. Then $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$

No effective global results are known for surfaces.

The best known results are unpractical and “depend” on A (Lombardo, Zywina).

Possible degrees

Theorem (Mazur)

Let ℓ be a prime such that exists an isogeny $\varphi : E \to E'$ with kernel of order ℓ. Then $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$

No effective global results are known for surfaces.

The best known results are unpractical and "depend" on A (Lombardo, Zywina).

For $\mathsf{End}(A^{\mathsf{al}}) = \mathbb{Z}$ we can instead do one surface at a time (Dieulefait).

Algorithm (Dieulefait)[1]

Input: Conductor of A and a finite set list of L-polynomials
Output: Finite superset of primes ℓ with reducible mod-ℓ Galois representation.

In particular, the primes ℓ for which 1-step or 2-step ℓ-isogenies are possible.

Possible degrees

No effective global results are known for surfaces.

The best known results are unpractical and “depend” on A (Lombardo, Zywina).

For $\mathsf{End}(A^{\mathsf{al}}) = \mathbb{Z}$ we can instead do one surface at a time (Dieulefait).

Algorithm (Dieulefait)[1]

Input: Conductor of A and a finite set list of L-polynomials
Output: Finite superset of primes ℓ with reducible mod-ℓ Galois representation.

In particular, the primes ℓ for which 1-step or 2-step ℓ-isogenies are possible.

$\mathsf{End}(A^{\mathsf{al}}) = \mathbb{Z}$ + principally polarized $\implies A = \mathsf{Jac}(\text{genus 2 curve})$
This restrict us to typical genus 2 curves.

Possible degrees

For $\mathsf{End}(A^{\mathsf{al}}) = \mathbb{Z}$ we can instead do one surface at a time (Dieulefait).

Algorithm (Dieulefait)[1]

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

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

In particular, the primes ℓ for which 1-step or 2-step ℓ-isogenies are possible.

$\mathsf{End}(A^{\mathsf{al}}) = \mathbb{Z}$ + principally polarized $\Longrightarrow A = \mathsf{Jac}(\text{genus 2 curve})$
This restrict us to typical genus 2 curves.

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)

Generic approach

Problem

Given a principally polarized abelian variety A compute its isogeny class.

1. List irreducible isogeny types
   These depend on the dimension of A and $\mathsf{End}(A)^\dagger$.
   $E/\mathbb{Q}$: 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. List the possible degrees for each type.
   $E/\mathbb{Q}$: $\ell \leq 19$ or $\ell \in \{37, 43, 67, 163\}$.
   Typical surface: Algorithmically produce finite list of possible ℓ for A.
3. Search for all isogenies of a given type and degree.
4. Reapply as needed.

Searching for isogenies

For elliptic curves one may use modular polynomials $\phi_\ell(x, y) \in \mathbb{Z}[x, y]$. Defined by

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

The size grows as $\widetilde{O}(\ell^3)$

- $\ell = 17$: 23 KB, 8 pages 📜
- $\ell = 163$: 28 MB, 5000+ pages 📚

Modular polynomials for surfaces are impractical!
More variables $\phi_\ell(x_1, x_2, x_3, y) \in \mathbb{Z}[x_1, x_2, x_3, y]$.
Size grows as $\widetilde{O}(\ell^{15})$.

- $\ell = 2$: 1.4 MB 💾
- $\ell = 3$: 400 MB 💿

We will instead use complex analytic methods.

Geometric invariants

$E : y^2 = x^3 - 27c_4x - 54c_6$

We may define the j-invariant in two ways:

- Algebraically: $j(E) = 1728\frac{c_4^3}{c_4^3 - c_6^2}$
- Modularly: $j(E) = j(\tau) = 1728\frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2}$, where $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}),\ \operatorname{im}\tau > 0$

Geometric invariants

$E : y^2 = x^3 - 27c_4x - 54c_6$

We may define the j-invariant in two ways:

- Algebraically: $j(E) = 1728\frac{c_4^3}{c_4^3 - c_6^2}$
- Modularly: $j(E) = j(\tau) = 1728\frac{E_4(\tau)^3}{E_4(\tau)^3 - E_6(\tau)^2}$, where $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}),\ \operatorname{im}\tau > 0$

$C : y^2 = f(x), \quad f \in \mathbb{Z}[x]$ and $\deg f \in \{5, 6\}$

One of the possible analogues of c_4, c_6 are the Igusa–Clebsch invariants

$$(I_2, I_4, I_6, I_{10}) \in \mathbb{P}(2, 4, 6, 10)$$

These can also be associated to Siegel modular forms via

$$\mathrm{Jac}(C)(\mathbb{C}) \simeq \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2), \text{ with } \tau \in \mathbb{H}_2.$$

Precisely, there exists $\lambda \in \mathbb{C}^\times$ such that $\lambda^k I_k(\tau) = I_k(C) \in \mathbb{Z}$

Geometric invariants

$C : y^2 = f(x), \quad f \in \mathbb{Z}[x]$ and $\deg f \in \{5, 6\}$

One of the possible analogues of c_4, c_6 are the Igusa–Clebsch invariants

$$(I_2, I_4, I_6, I_{10}) \in \mathbb{P}(2, 4, 6, 10)$$

These can also be associated to Siegel modular forms via

$$\mathrm{Jac}(C)(\mathbb{C}) \simeq \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2), \text{ with } \tau \in \mathbb{H}_2.$$

Precisely, there exists $\lambda \in \mathbb{C}^\times$ such that $\lambda^k I_k(\tau) = I_k(C) \in \mathbb{Z}$

Unfortunately, I_2 and I_6 are only quotients of modular forms.

We opt instead for the modular forms M_k of weight $k \in \{4, 6, 10, 12\}$, such that

$$M_4 = 2^{-2} I_4 \qquad M_6 = 2^{-3}(I_2 I_4 - 3 I_6)$$

$$M_{10} = -2^{-12} I_{10} \qquad M_{12} = 2^{-15} I_2 I_{10}$$

Choice of generators

$$\mathrm{Jac}(y^2 = f(x))(\mathbb{C}) \simeq \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2), \text{ with } \tau \in \mathbb{H}_2.$$

We opt for modular invariants M_k of weight $k \in \{4, 6, 10, 12\}$, such that

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

These have integral Fourier coefficients (and we can also represent $E \times E'$).

Theorem

$(M_4, M_6, M_{10}, M_{12})$ generate the graded $\mathbb{C}$-algebra of Siegel modular forms of $\mathbb{H}_2$.

Theorem (Igusa)

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

Kieffer's trick

Theorem (Igusa)

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

Theorem (Kieffer 2022)

Assume that there exists $\lambda \in \mathbb{C}^\times$ such that $\lambda^k M_k(\tau) \in \mathbb{Z}$.
If f is a Siegel modular form of even weight k with integer Fourier coefficients,

$$\prod_{\gamma} \left(X - (12\lambda \ell^{c_\gamma})^k f(\gamma\tau) \right)$$

has **integer** coefficients, where γ loops over specific coset representatives for the Hecke operator $T(\ell)$ (resp. $T_1(\ell^2)$) and $0 \leq c_\gamma \leq 2$ (resp. 3).

$$\left\{ \mathbb{C}^2 / \left(\mathbb{Z}^2 + \gamma\tau\mathbb{Z}^2 \right) \right\}_\gamma = \left\{ \text{surfaces 1-step (resp. 2-step) isogenous to } \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2) \right\}$$

Kieffer's trick

Theorem (Kieffer 2022)

Assume that there exists $\lambda \in \mathbb{C}^\times$ such that $\lambda^k M_k(\tau) \in \mathbb{Z}$.
If f is a Siegel modular form of even weight k with integer Fourier coefficients,

$$\prod_\gamma \left(X - (12\lambda\ell^{c_\gamma})^k f(\gamma\tau)\right)$$

has **integer** coefficients, where γ loops over specific coset representatives for the Hecke operator $T(\ell)$ (resp. $T_1(\ell^2)$) and $0 \leq c_\gamma \leq 2$ (resp. 3).

$$\left\{\mathbb{C}^2/\left(\mathbb{Z}^2 + \gamma\tau\mathbb{Z}^2\right)\right\}_\gamma = \left\{\text{surfaces 1-step (resp. 2-step) isogenous to } \mathbb{C}^2/(\mathbb{Z}^2 + \tau\mathbb{Z}^2)\right\}$$

In other words, if we start with a $\lambda^k M_k(\tau) \in \mathbb{Z}$, then

$$(12\lambda\ell^{c_\gamma})^k M_k(\gamma\tau_C)$$

can be grouped in Galois orbits of algebraic **integers**.

Complex analytic approach

Given $(m_4, m_6, m_{10}, m_{12}) \in \mathbb{P}(4, 6, 10, 12)(\mathbb{Z})$ and ℓ.
Compute complex balls that provably contain:

1. $\tau \in \mathbb{H}_2$
2. $\lambda \in \mathbb{C}^\times$ such that $\lambda^k M_k(\tau) = m_k$
3. For each coset coset representative γ of the Hecke operator $T(\ell)$ (or $T_1(\ell^2)$)

$$(12\lambda\ell^{c_\gamma})^k M_k(\gamma\tau).$$

Keep the γ's such that the computed balls for $\left(12\lambda\ell^{c_\gamma}\right)^k M_k(\gamma\tau)$ contain an integer.

Complex approach

For $\ell = 31$ and $C\colon y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45$ there is only one γ such that the ball $\left(12\lambda\ell^{c_\gamma}\right)^4 M_4(\gamma\tau) \cap \mathbb{Z} \neq \emptyset$, and

$$\begin{aligned}
\left(12\lambda\ell^{c_\gamma}\right)^4 M_4(\gamma\tau) &= \alpha^2 \cdot 318972640 \pm 7.8 \times 10^{-47} \\
\left(12\lambda\ell^{c_\gamma}\right)^6 M_6(\gamma\tau) &= \alpha^3 \cdot 1225361851336 \pm 5.5 \times 10^{-39} \\
\left(12\lambda\ell^{c_\gamma}\right)^{10} M_{10}(\gamma\tau) &= \alpha^5 \cdot 10241530643525839 \pm 1.6 \times 10^{-29} \\
\left(12\lambda\ell^{c_\gamma}\right)^{12} M_{12}(\gamma\tau) &= -\alpha^6 \cdot 307105165233242232724 \pm 4.6 \times 10^{-22}
\end{aligned}$$

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

Complex approach

For $\ell = 31$ and $C\colon y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45$ there is only one γ such that the ball $\left(12\lambda\ell^{c_\gamma}\right)^4 M_4(\gamma\tau) \cap \mathbb{Z} \neq \emptyset$, and

$$\begin{aligned}
\left(12\lambda\ell^{c_\gamma}\right)^4 M_4(\gamma\tau) &= \alpha^2 \cdot 318972640 \pm 7.8 \times 10^{-47} \\
\left(12\lambda\ell^{c_\gamma}\right)^6 M_6(\gamma\tau) &= \alpha^3 \cdot 1225361851336 \pm 5.5 \times 10^{-39} \\
\left(12\lambda\ell^{c_\gamma}\right)^{10} M_{10}(\gamma\tau) &= \alpha^5 \cdot 10241530643525839 \pm 1.6 \times 10^{-29} \\
\left(12\lambda\ell^{c_\gamma}\right)^{12} M_{12}(\gamma\tau) &= -\alpha^6 \cdot 307105165233242232724 \pm 4.6 \times 10^{-22}
\end{aligned}$$

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

We can confirm that these are indeed integers by certifying the vanishing of

$$\prod_\gamma \left(\left(12\lambda\ell^{c_\gamma}\right)^k M_k(\gamma\tau) - m'_k \right) \in \mathbb{Z}.$$

by recomputing the relevant $\left(12\lambda\ell^{c_\gamma}\right)^k M_k(\gamma\tau)$ at higher precision.

Reconstructing curves

Given $(m'_4, m'_6, m'_{10}, m'_{12}) = (318972640, 1225361851336, 10241530643525839, \ldots)$
we want to find a curve C' isogenous to C over $\mathbb{Q}$.

By applying Mestre's algorithm we obtain

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

a quadratic twist by -83761 of the desired curve

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

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

Reconstructing curves

Given $(m'_4, m'_6, m'_{10}, m'_{12}) = (318972640, 1225361851336, 10241530643525839, \ldots)$
we want to find a curve C' isogenous to C over $\mathbb{Q}$.

By applying Mestre's algorithm we obtain

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

a quadratic twist by -83761 of the desired curve

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

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

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 create a certificate for the isogeny (6.5 hours and 3 MB).

Reconstructing curves

Given $(m'_4, m'_6, m'_{10}, m'_{12}) = (318972640, 1225361851336, 10241530643525839, \ldots)$
we want to find a curve C' isogenous to C over $\mathbb{Q}$.

By applying Mestre's algorithm we obtain

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

a quadratic twist by -83761 of the desired curve

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

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

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 create a certificate for the isogeny (6.5 hours and 3 MB).

We would like be able to also obtain a certificate for the completeness of the

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

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

Only 2 523 new curves are explained by Richelot isogenies.

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

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

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

Only 2 523 new curves are explained by Richelot isogenies.

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

Chidambaram's observation

A 2-step isogeny of degree 4 always implies an existence of a second one.
This explains the 6913 $\triangle$ and the 756 $\bowtie$ we found.

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

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

Only 2 523 new curves are explained by Richelot isogenies.

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

Chidambaram's observation

A 2-step isogeny of degree 4 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, 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.

Upcoming to LMFDB

There is a new set of 5 235 806 curves soon to be added to LMFDB.

Of these, 1 823 592 are typical, split amongst 1 538 149 isogeny classes.

We found $687\,763+\varepsilon$ new curves (in 97 days).

Of those 289 553 could be obtained via Richelot isogenies.

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

$$\left\{2^2, 3^2, 2^4, 5^2, 7^2, 3^4, 13^2, 17^2, 5^4, 31^2, 7^4, 11^4, 13^4\right\}.$$

Upcoming to LMFDB

There is a new set of 5 235 806 curves soon to be added to LMFDB.

Of these, 1 823 592 are typical, split amongst 1 538 149 isogeny classes.

We found $687\,763+\varepsilon$ new curves (in 97 days).

Of those 289 553 could be obtained via Richelot isogenies.

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

$$\left\{2^2, 3^2, 2^4, 5^2, 7^2, 3^4, 13^2, 17^2, 5^4, 31^2, 7^4, 11^4, 13^4\right\}.$$

Some observations per size:

- 2: 75% degree 2^2, 22% degree 3^4, and then 3^2, 5^4, 5^2, 7^4, 7^2, ...
- 3: 99.2% are $\triangle$ made up by degree 2^4 isogenies.
- 4: 97.8% are $\succ\!\!-$ made up by degree 2^2 isogenies.
- 5: 99.8% are $\bowtie$ made up by degree 2^4 isogenies.
- 6: 75% + 15% are graphs made up by degree 2^2 isogenies.

Life, the universe, and everything

42 Richelot isogenous curves with conductor $497051100 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 17^2$