

Algorithmic aspects of abelian surfaces through Riemann theta functions

Jean Kieffer

RT2N conference, CIRM Luminy, September 2026



Abelian varieties

Let k be a field.

An **abelian variety** A/k is a smooth, projective variety equipped with an abelian group law $+$. Let g be its dimension.

If $g = 1$, then A is an **elliptic curve**. Any elliptic curve E/k has a **Weierstrass model**:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \text{in } \mathbb{P}_k^2,$$

where $\Delta(a_1, \dots, a_6) \neq 0$ and $0_E = (0 : 1 : 0)$. Given P, Q on E , there are algebraic formulas to compute $P + Q$.

If $g = 2$, then A is an **abelian surface**.

Isogenies

- $A(k)$ and $A(\bar{k})$ are abelian groups.

Isogenies

- $A(k)$ and $A(\bar{k})$ are abelian groups.
- We can consider **morphisms** $\phi : A \rightarrow A'$. Over k , respecting the group law.

Isogenies

- $A(k)$ and $A(\bar{k})$ are abelian groups.
- We can consider **morphisms** $\phi : A \rightarrow A'$. Over k , respecting the group law.
- A morphism $\phi : A \rightarrow A'$ is an **isogeny** if $\ker \phi$ is finite, ϕ is dominant, and $\dim A = \dim A'$. (Any two properties imply the third).

Isogenies

- $A(k)$ and $A(\bar{k})$ are abelian groups.
- We can consider **morphisms** $\phi : A \rightarrow A'$. Over k , respecting the group law.
- A morphism $\phi : A \rightarrow A'$ is an **isogeny** if $\ker \phi$ is finite, ϕ is dominant, and $\dim A = \dim A'$. (Any two properties imply the third).
- An isogeny ϕ as a **degree** $\deg(\phi) \in \mathbb{Z}_{\geq 1}$. If $\text{char}(k) \nmid \deg(\phi)$, we identify

$$\ker(\phi) = \{P \in A(\bar{k}) : \phi(P) = 0_{A'}\}$$

and we have $\deg(\phi) = \# \ker(\phi)$.

Isogenies

- $A(k)$ and $A(\bar{k})$ are abelian groups.
- We can consider **morphisms** $\phi : A \rightarrow A'$. Over k , respecting the group law.
- A morphism $\phi : A \rightarrow A'$ is an **isogeny** if $\ker \phi$ is finite, ϕ is dominant, and $\dim A = \dim A'$. (Any two properties imply the third).
- An isogeny ϕ as a **degree** $\deg(\phi) \in \mathbb{Z}_{\geq 1}$. If $\text{char}(k) \nmid \deg(\phi)$, we identify

$$\ker(\phi) = \{P \in A(\bar{k}) : \phi(P) = 0_{A'}\}$$

and we have $\deg(\phi) = \# \ker(\phi)$.

Example

$$\begin{aligned} \phi : (E : y^2 = x^3 + x^2 + 2x + 1) &\rightarrow (E' : y^2 = x^3 + x^2 - 18x - 43) \\ (x, y) &\mapsto \left(\frac{x^3 + 4x + 4}{x^2}, y \frac{x^3 - 4x - 8}{x^3} \right) \end{aligned}$$

is an isogeny of degree 3 over $k = \mathbb{Q}$.

Isogeny theorems

Theorem (Mazur 1978)

Let ℓ be a prime, and assume there exists an isogeny $\phi : E \rightarrow E'$ between elliptic curves over $\mathbb{Q}$ of degree ℓ . Then $\ell \leq 163$.

Given $E/\mathbb{Q}$, the **isogeny class** of E is

$$\text{Isog}(E) := \{E'/\mathbb{Q} \text{ up to isomorphism: } E' \text{ is isogenous to } E\}.$$

Theorem (Kenku 1982)

For any elliptic curve $E/\mathbb{Q}$, we have $\#\text{Isog}(E) \leq 8$.

Are there similar uniform bounds for isogenies between abelian surfaces over $\mathbb{Q}$? This question is wide open.

A computational approach

Elliptic curves and abelian varieties are amenable to computation.

1. What can we compute?
2. How can we compute it? Study algorithms.
3. Can these computations prove new theorems, or suggest conjectures?

The L -functions and Modular Forms Database

From lmfdb.org/EllipticCurve/Q/?sort_order=class_size&sort_dir=op:

→ Elliptic curves over $\mathbb{Q}$ → Search resultsCitation · Feedback · Hide Menu

Elliptic curve search results

Introduction

Overview Random

Universe Knowledge

L-functions

Rational All

Modular forms

Classical Maass

Hilbert Bianchi

Varieties

Elliptic curves

over $\mathbb{Q}$

over number fields

Genus 2 curves

Higher genus families

Abelian varieties over $\mathbb{F}_q$

Belyi maps

Fields

Number fields

p -adic fields

Refine search

Advanced search options

Conductor

Discriminant

j -invariant

Rank

Bad p

include

Curves per isogeny class

Complex multiplication

Torsion

Sort order

Select

▼ isogeny class size

columns to display

Search again

Random curve

Diagram search

Learn more

Source and acknowledgments

Completeness of the data

Reliability of the data

Elliptic curve labels

Congruent number curves

Stein-Watkins dataset

BHKSSW dataset

Results (1-50 of 3824372 matches)

Next

Download

displayed columns for

all

results to

Text

Label	Class size	Torsion	CM	Weierstrass equation
705600.bwu8	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 + 896097300x + 467734632946000$
705600.bwu7	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 + 148161300x - 523061966000$
705600.bwu6	8	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 755006700x - 4683053774000$
705600.bwu5	8	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 5327294700x + 146321329714000$
705600.bwu4	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 10633406700x - 421926912974000$
705600.bwu3	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 84178094700x + 9613604548114000$
705600.bwu2	8	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 84707294700x + 9489188569714000$
705600.bwu1	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 - 1355316494700x + 607308275951314000$
705600.bwt8	8	$\mathbb{Z}/2\mathbb{Z}$		$y^2 = x^3 + 24681300x + 25128866000$

Abelian varieties in cryptography

E.g. $k = \mathbb{F}_p$, $p \simeq 2^{256}$.

1. **Elliptic curve cryptography** (ECC). The typical hard problem is DLOG: given $P, nP \in E(k)$, compute n (e.g. Diffie–Hellman, ECDSA). $\#E(k)$ must be (close to) prime.
Abelian surfaces can be used as well (HECC).
2. **Isogeny-based cryptography** is a fast-growing, post-quantum alternative. The typical hard problem is: given E, E' , find an isogeny between them (e.g. CSIDH, SQIsign, MIKE).

Algorithms are used both in constructive and destructive approaches.

Often a source of mathematical questions: what are the most efficient formulas to add points on elliptic curves?

Representing abelian varieties

Throughout, we will assume that A is **principally polarized (pp)**: A carries an ample line bundle $\mathcal{L}$ that is in a sense “simplest possible”. Elliptic curves carry a canonical such $\mathcal{L}$.

Then $\mathcal{L}^{\otimes 3}$ induces an embedding $A \hookrightarrow \mathbb{P}^{3g-1}$.

If in addition $\dim A = 2$, then we have even better models:

- Generically, A is the **Jacobian of a genus 2 curve**:

$$\mathcal{C} : y^2 + h(x)y = f(x), \quad \deg(h) \leq 3, \deg(f) \leq 6.$$

- Otherwise $A \simeq E_1 \times E_2$ over k or a quadratic extension.

Two computational problems

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

Isogeny class

Given a p.p.a.v. A over a number field k , compute

$$\text{Isog}(A) := \{\text{p.p.a.v. } A'/k \text{ up to isomorphism} : A' \text{ is isogenous to } A\}.$$

We know $\text{Isog}(A)$ is finite by Faltings' theorem (1983).

Both problems are considered solved for elliptic curves. My goal is to present recent progress in the $g = 2$ case, using **Riemann theta functions** as a key tool.

1. Complex theory: theta functions and isogenies.
2. Point counting.
3. Isogeny classes.

**Complex theory:
theta functions and isogenies**

The Siegel moduli space

Let $g \geq 1$. The **Siegel upper half-space** is

$$\mathcal{H}_g = \{ \tau \in \text{Mat}_{g \times g}(\mathbb{C}) : \tau^T = \tau, \text{Im}(\tau) > 0 \}.$$

Any g -dimensional p.p.a.v. $A/\mathbb{C}$ is isomorphic to

$$A(\tau) = \mathbb{C}^g / \mathbb{Z}^g + \tau \mathbb{Z}^g$$

for some (small) **period matrix** $\tau \in \mathcal{H}_g$. This τ is unique up to the action of $\text{Sp}_{2g}(\mathbb{Z})$:

$$\gamma \tau = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix} \tau := (a_\gamma \tau + b_\gamma)(c_\gamma \tau + d_\gamma)^{-1}.$$

Some representatives for τ are better than others. We'll say that $\tau \in \mathcal{H}_g$ is **reduced** if τ is sufficiently close to the usual fundamental domain for $\text{Sp}_{2g}(\mathbb{Z}) \curvearrowright \mathcal{H}_g$.

Riemann theta functions

Let $a, b \in \{0, 1\}^g$. The **Riemann theta functions** (rather theta constants, of level 4) are

$$\theta_{a,b}(\tau) = \sum_{n \in \mathbb{Z}^g + \frac{a}{2}} \exp(\pi i(n^T \tau n + n^T b)).$$

The values $\theta_{a,b}(\tau)$ as a, b vary allow us to write down a projective model for $A(\tau)$.

Consequently, algebraic invariants of A should have an expression in terms of $\theta_{a,b}$.

Example: $g = 1$

$E_4(\tau) = \frac{1}{2}(\theta_{00}^8 + \theta_{01}^8 + \theta_{10}^8)$ and $\Delta(\tau) = (\frac{1}{2}\theta_{00}\theta_{01}\theta_{10})^8$, then $j(\tau) = E_4^3(\tau)/\Delta(\tau)$.

Igusa invariants

When $g = 2$, there are functions $m_i : \mathcal{H}_2 \rightarrow \mathbb{C}$ for $i \in \{4, 6, 10, 12\}$ such that

- Each m_i is a polynomial in $\theta_{a,b}$.
- m_i is a **Siegel modular form** of weight $\det^i$: $m(\gamma\tau) = \det(c_\gamma\tau + d_\gamma)^i m_i(\tau)$, with integral Fourier expansion.
- $(m_4(\tau) : m_6(\tau) : m_{10}(\tau) : m_{12}(\tau)) \in \mathbb{P}^{4,6,10,12}(\mathbb{C})$ determines the isomorphism class of $A(\tau)$.

The Siegel moduli space $\mathcal{A}_2(\mathbb{C}) = \mathrm{Sp}_4(\mathbb{Z}) \backslash \mathcal{H}_2$ is birational to $\mathbb{P}^3$. The **Igusa invariants** j_1, j_2, j_3 can be constructed from the m_i 's, e.g. $j_1 = m_4 m_6 / m_{10}$.

Let $\mathcal{C}$ be a genus 2 curve. Then there are polynomials $M_i(\mathcal{C})$ in the coefficients of $\mathcal{C}$ such that $(M_4(\mathcal{C}) : \cdots : M_{12}(\mathcal{C})) = (m_4(\tau) : \cdots : m_{12}(\tau))$ whenever $\mathrm{Jac}(\mathcal{C}) \simeq A(\tau)$.

Conversely, **Mestre's algorithm** (1991) reconstructs $\mathcal{C}$ from its invariants.

(ℓ, ℓ) -isogenies over $\mathbb{C}$

Let A, A' be p.p. abelian surfaces (over k) and ℓ a prime $\neq \text{char}(k)$.

Then $A[\ell](\bar{k}) \simeq (\mathbb{Z}/\ell\mathbb{Z})^4$. We say $\phi : A \rightarrow A'$ is an (ℓ, ℓ) -isogeny if $\ker(\phi) \subset A[\ell]$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ and **isotropic** for the Weil pairing induced by the polarization.

Prototypical example over $k = \mathbb{C}$

$$\begin{array}{ccccc} \mathbb{C}^2/\mathbb{Z}^2 + \tau\mathbb{Z}^2 = & A(\tau) & \rightarrow & A(\tau/\ell) & = \mathbb{C}^2/\mathbb{Z}^2 + \frac{\tau}{\ell}\mathbb{Z}^2 \\ & z & \mapsto & z. & \end{array}$$

Note: $\tau/\ell = \gamma\tau$ where $\gamma = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ell & \\ & & & \ell \end{pmatrix} \in \text{GSp}_4(\mathbb{Q})^+$.

Lemma

Let ℓ be a prime, and write $\Gamma = \mathrm{Sp}_4(\mathbb{Z})$. Then

$$S_\ell := \Gamma \backslash \Gamma \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ell & \\ & & & \ell \end{pmatrix} \Gamma$$

has an explicit set of representatives consisting of $\ell^3 + \ell^2 + \ell + 1$ upper-triangular matrices in $\mathrm{GSp}_4(\mathbb{Q})^+$, of determinant ℓ^2 .

Let $\tau \in \mathcal{H}_2$. Then the quotients $A(\tau)/K$, as K runs through isotropic $(\mathbb{Z}/\ell\mathbb{Z})^2$ subgroups of $A[\ell]$, are the abelian surfaces $A(\gamma\tau)$ for $\gamma \in S_\ell$.

For $\tau \in \mathcal{H}_2$, let

$$F_\ell(\tau, Y) = \prod_{\gamma \in S_\ell} (Y - j_1(\gamma\tau)).$$

The coefficients of F_ℓ are weight 0 Siegel modular functions, so they are rational functions in j_1, j_2, j_3 . We obtain the first **Siegel modular polynomial**

$$\Psi_{\ell,1} \in \mathbb{Q}(X_1, X_2, X_3)[Y].$$

One also defines $\Psi_{\ell,i}$ for $i \in \{2, 3\}$ so that $j_i(A') = \Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), j_1(A'))$. Together they define a birational model for $X_0(\ell)$.

Ball arithmetic

To use this complex theory in algorithms, we have to manipulate complex numbers in a mathematically sound way. But we only have finitely many bits at our disposal.

- Use **ball arithmetic**: $z \in \mathbb{C}$ is encoded as $(z_{\text{mid}}, \varepsilon)$, both exact dyadic, such that $|z - z_{\text{mid}}| \leq \varepsilon$. We say z is given at **precision N** if $\varepsilon \leq 2^{-N}$.
- Operations (sum, products, exponential, ...) are mathematically meaningful.
- Work with polynomial and matrices using error bounds on every coefficient.

For instance it's easy to verify that $z \neq 0$ (compute z at high enough precision), but verifying that $z = 0$ is harder.

Theorem (The AGM method; Dupont 2006)

Given a genus 2 curve $\mathcal{C}/k$ where $k \subset \mathbb{C}$ is a number field, one can compute a reduced period matrix $\tau \in \mathcal{H}_2$ of $\text{Jac}(\mathcal{C})$ at precision N in time $O_{\mathcal{C}}(N(\log N)^2)$.

This is **quasi-linear time** in N .

An alternative approach would be to write down hyperelliptic integrals. In principle, they can be evaluated in quasi-linear time as holonomic functions.

Evaluating theta functions: summation

Conversely, we'll need to **evaluate theta functions** at some precision N to get algebraic data from periods. Recall:

$$\theta_{0,0}(\tau) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i (n^T \tau n)).$$

Let's compute a partial sum. For a given n :

$$|\exp(\pi i (n^T \tau n))| = \exp(-\|n\|_\tau^2)$$

where $\|\cdot\|_\tau$ is the Euclidean norm attached to $\pi \operatorname{Im}(\tau)$.

So we need to compute a partial sum with $O_g(N^{g/2})$ terms, assuming τ is reduced. This summation algorithm runs in time $O_g(N^{1+g/2} \log N)$.

Evaluating theta functions: fast algorithm

Theorem (Elkies, K. 2026+)

Given $g \geq 1$, a reduced point $\tau \in \mathcal{H}_g$ and a binary precision N , one can compute $(\theta_{a,b}(\tau))_{a,b}$ at precision N in time $O_g(N(\log N)^2)$.

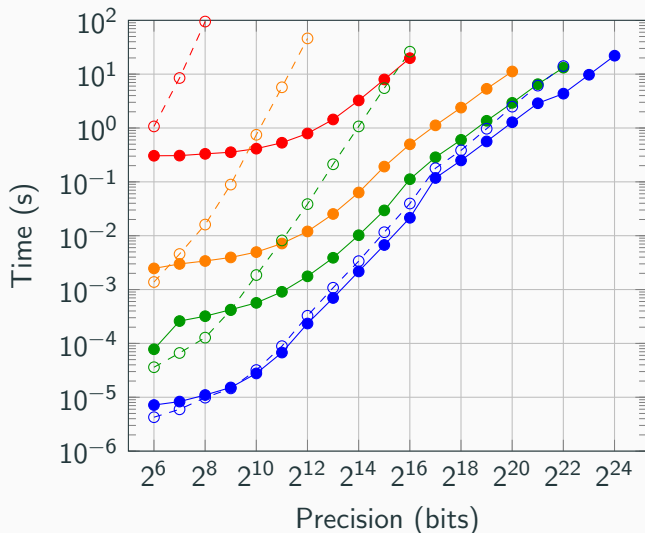
- Fast evaluation algorithms for $\theta_{a,b}$ were previously known for small g , but were heuristic (unless $g \leq 2$) and slower in practice.
- Generalizes to arbitrary theta values $\theta_{a,b}(z, \tau)$.
- Implemented in FLINT: https://flintlib.org/doc/acb_theta.html.

Performance comparison in FLINT: fast algorithm vs. summation

$\theta_{0,0}(\tau)$ for a typical
reduced τ

$g = 1, 2, 4, 8$

Dashed line is
summation, solid line is
the fast algorithm.



Point counting

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

- Schoof's algorithm (1985): $\tilde{O}(\log^5 p)$ if $g = 1$. Uses $A[\ell]$.

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

- Schoof's algorithm (1985): $\tilde{O}(\log^5 p)$ if $g = 1$. Uses $A[\ell]$.
- Pila (1990): Polytime algorithm for any fixed g .

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

- Schoof's algorithm (1985): $\tilde{O}(\log^5 p)$ if $g = 1$. Uses $A[\ell]$.
- Pila (1990): Polytime algorithm for any fixed g .
- The Schoof–Elkies–Atkin or SEA algorithm (1990's): $\tilde{O}(\log^4 p)$ for $g = 1$. Uses ℓ -isogenies.

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

- Schoof's algorithm (1985): $\tilde{O}(\log^5 p)$ if $g = 1$. Uses $A[\ell]$.
- Pila (1990): Polytime algorithm for any fixed g .
- The Schoof–Elkies–Atkin or SEA algorithm (1990's): $\tilde{O}(\log^4 p)$ for $g = 1$. Uses ℓ -isogenies.
- Gaudry–Schost (2012) use the Schoof–Pila approach for $g = 2$: $\tilde{O}(\log^8 p)$.

The problem

Point counting

Given a p.p.a.v. A over a finite field k , compute $\#A(k)$.

We'll take $k = \mathbb{F}_q$ of “large” characteristic p . We want polynomial-time algorithms in $\log(q)$; listing all the points on A is exponential time. Let $g = \dim A$.

- Schoof's algorithm (1985): $\tilde{O}(\log^5 p)$ if $g = 1$. Uses $A[\ell]$.
- Pila (1990): Polytime algorithm for any fixed g .
- The Schoof–Elkies–Atkin or SEA algorithm (1990's): $\tilde{O}(\log^4 p)$ for $g = 1$. Uses ℓ -isogenies.
- Gaudry–Schost (2012) use the Schoof–Pila approach for $g = 2$: $\tilde{O}(\log^8 p)$.

I'll explain how to apply the SEA strategy in the $g = 2$ case.

The characteristic polynomial of Frobenius

Let $\ell \neq p$ be a small prime. Choosing a (symplectic) basis of $A[\ell](\overline{\mathbb{F}}_q)$, the Frobenius endomorphism Frob_q of A acts as

$$\rho_\ell(\text{Frob}_q) \in \text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

The characteristic polynomial of Frobenius

Let $\ell \neq p$ be a small prime. Choosing a (symplectic) basis of $A[\ell](\overline{\mathbb{F}}_q)$, the **Frobenius endomorphism** Frob_q of A acts as

$$\rho_\ell(\text{Frob}_q) \in \text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

Theorem (RH for abelian varieties; Weil 1949)

There is a polynomial $R \in \mathbb{Z}[X]$, monic of degree $2g$, such that for all $\ell \neq p$:

$$\text{charpoly}(\rho_\ell(\text{Frob}_q)) = R \bmod \ell.$$

The complex roots of R have absolute value $q^{1/2}$, and $\#A(\mathbb{F}_q) = R(1)$.

Schoof's algorithm computes R .

Schoof's algorithm

Schoof's algorithm

Consider $O(\log q)$ small primes $\ell_1, \dots, \ell_r$. For each i , compute $\text{charpoly}(\rho_{\ell}(\text{Frob}_q))$ in $(\mathbb{Z}/\ell\mathbb{Z})[X]$ in polynomial time in ℓ and $\log(q)$. Recover $R \in \mathbb{Z}[X]$ using the Chinese remainder theorem.

How is $\text{charpoly}(\rho_{\ell}(\text{Frob}_q))$ computed? Choose a suitable coordinate x in some projective model of A . There is a polynomial D_{ℓ} of degree $O(\ell^{2g})$ such that

$$A[\ell] = \{P \in A(\overline{\mathbb{F}}_q) : D_{\ell}(x(P)) = 0\}.$$

Computing $\rho_{\ell}(\text{Frob}_q)$ essentially amounts to computing $X^q \bmod D_{\ell}$. This can be done in time $\tilde{O}(\ell^{2g} \log(q)^2)$ using fast exponentiation.

For $g = 2$, the cost of computing D_{ℓ} (bivariate resultants) actually dominates.

The SEA approach

Elkies's method (1990's) is to replace $A[\ell]$ by the kernel of an isogeny.

Now fix $g = 2$. Assume that:

- There exists an (ℓ, ℓ) -isogeny $\phi : A \rightarrow A'$ defined over $\mathbb{F}_q$. This means $\rho_\ell(\text{Frob}_q)$ stabilizes 2-dimensional isotropic subspace; we say ℓ is Elkies for A .
- We can compute $\ker(\phi)$ as the zero locus of a polynomial D_ϕ .

Then we can compute $R' = \text{charpoly}(\text{Frob}_q|_{\ker \phi})$, and

$$\text{charpoly}(\rho_\ell(\text{Frob}_q)) = R'(X) \cdot q^2 R'(q/X).$$

Computing R' is cheaper, because $\deg D_\phi = O(\ell^2)$ instead of $O(\ell^4)$.

Computing the codomain

Assume ℓ is Elkies. We first look for A' using Siegel modular polynomials:

1. Evaluate $\Psi_{\ell,k}(j_1(A), j_2(A), j_3(A), Y) \in \mathbb{F}_q[Y]$ for $1 \leq k \leq 3$;
2. Find a root of $\Psi_{\ell,1}$ in $\mathbb{F}_q$ (Cantor–Zassenhaus), giving the Igusa invariants of A' ;
3. Recover A' as a Jacobian using Mestre's algorithm.

So we'll need to **evaluate Siegel modular polynomials** at A . How much does this cost?

Computing the codomain

Assume ℓ is Elkies. We first look for A' using Siegel modular polynomials:

1. Evaluate $\Psi_{\ell,k}(j_1(A), j_2(A), j_3(A), Y) \in \mathbb{F}_q[Y]$ for $1 \leq k \leq 3$;
2. Find a root of $\Psi_{\ell,1}$ in $\mathbb{F}_q$ (Cantor–Zassenhaus), giving the Igusa invariants of A' ;
3. Recover A' as a Jacobian using Mestre's algorithm.

So we'll need to **evaluate Siegel modular polynomials** at A . How much does this cost?

If $g = 1$, Cohen (1984) proved that $\Phi_\ell(X, Y)$ has height $\sim 6\ell \log \ell$, hence total size $O(\ell^3 \log \ell)$. Moreover Φ_ℓ can be computed in quasi-linear time: we're fine.

Computing the codomain

Assume ℓ is Elkies. We first look for A' using Siegel modular polynomials:

1. Evaluate $\Psi_{\ell,k}(j_1(A), j_2(A), j_3(A), Y) \in \mathbb{F}_q[Y]$ for $1 \leq k \leq 3$;
2. Find a root of $\Psi_{\ell,1}$ in $\mathbb{F}_q$ (Cantor–Zassenhaus), giving the Igusa invariants of A' ;
3. Recover A' as a Jacobian using Mestre's algorithm.

So we'll need to **evaluate Siegel modular polynomials** at A . How much does this cost?

If $g = 1$, Cohen (1984) proved that $\Phi_\ell(X, Y)$ has height $\sim 6\ell \log \ell$, hence total size $O(\ell^3 \log \ell)$. Moreover Φ_ℓ can be computed in quasi-linear time: we're fine.

Theorem (K. 2022)

$\Psi_{\ell,i}$ has degree $O(\ell^3)$ in each variable and height $O(\ell^3 \log \ell)$.

The expected total size is $\Theta(\ell^{15} \log \ell)$. Writing them down is utterly impractical.

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

1. **Lift** the genus 2 curve $\mathcal{C}$ such that $A = \text{Jac}(\mathcal{C})$ to $\tilde{\mathcal{C}}$ over a number field k ;

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

1. **Lift** the genus 2 curve $\mathcal{C}$ such that $A = \text{Jac}(\mathcal{C})$ to $\tilde{\mathcal{C}}$ over a number field k ;
2. Compute a period matrix τ of $\tilde{\mathcal{C}}$ to a **high numerical precision N** ;

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

1. **Lift** the genus 2 curve $\mathcal{C}$ such that $A = \text{Jac}(\mathcal{C})$ to $\tilde{\mathcal{C}}$ over a number field k ;
2. Compute a period matrix τ of $\tilde{\mathcal{C}}$ to a **high numerical precision N** ;
3. Evaluate $\theta_{a,b}(\gamma\tau)$ for all $\gamma \in S_\ell$ at precision N , as well as partial derivatives;

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

1. **Lift** the genus 2 curve $\mathcal{C}$ such that $A = \text{Jac}(\mathcal{C})$ to $\tilde{\mathcal{C}}$ over a number field k ;
2. Compute a period matrix τ of $\tilde{\mathcal{C}}$ to a **high numerical precision N** ;
3. Evaluate $\theta_{a,b}(\gamma\tau)$ for all $\gamma \in S_\ell$ at precision N , as well as partial derivatives;
4. Evaluate $\Psi_{\ell,i}$ in $\mathbb{C}[X]$ as a product over γ ;

Evaluation of modular polynomials

Instead we evaluate $\Psi_{\ell,i}(j_1(A), j_2(A), j_3(A), X)$ as follows:

1. **Lift** the genus 2 curve $\mathcal{C}$ such that $A = \text{Jac}(\mathcal{C})$ to $\tilde{\mathcal{C}}$ over a number field k ;
2. Compute a period matrix τ of $\tilde{\mathcal{C}}$ to a **high numerical precision N** ;
3. Evaluate $\theta_{a,b}(\gamma\tau)$ for all $\gamma \in S_\ell$ at precision N , as well as partial derivatives;
4. Evaluate $\Psi_{\ell,i}$ in $\mathbb{C}[X]$ as a product over γ ;
5. Recognize the result in $k[X]$, and **reduce** back to $\mathbb{F}_q$.

If $q = p$ is prime (so $k = \mathbb{Q}$), this runs in time $\tilde{O}(\ell^6 \cdot h(\tilde{\mathcal{C}}))$.

Isogenies from modular polynomials

Theorem (K., Page, Robert 2025)

There is an algorithm which, on the input of:

- two generic genus 2 curves $\mathcal{C}, \mathcal{C}'$ over a field k such that $A = \text{Jac}(\mathcal{C})$ and $A' = \text{Jac}(\mathcal{C}')$ are (ℓ, ℓ) -isogenous,
- and the 6×3 matrix of partial derivatives of Siegel modular polynomials w.r.t. $j_1(A), \dots, j_3(A')$ evaluated at (A, A') ,

computes an explicit model for an (ℓ, ℓ) -isogeny $\varphi : A \rightarrow A'$ in time $\tilde{O}(\ell)$.

This generalizes results of Elkies (1998) in the $g = 1$ case. Partial derivatives of $\Psi_{\ell,i}$ can also be evaluated numerically.

The distribution of Elkies primes

To state a complexity result, we need to study how Elkies primes are distributed.

We can prove an **average statement over reductions** of a fixed A , generalizing results of Shparlinski–Sutherland (2015) in the $g = 1$ case.

The distribution of Elkies primes

To state a complexity result, we need to study how Elkies primes are distributed.

We can prove an **average statement over reductions** of a fixed A , generalizing results of Shparlinski–Sutherland (2015) in the $g = 1$ case.

Fix A a p.p. abelian surface over $\mathbb{Q}$ such that $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Let $P \geq 1$.

Say that a prime $p \in [P, 2P]$ of good reduction is **deficient** if the proportion of primes $\ell \leq 100 \log P$ that are Elkies for A_p is less than $1/4$.

Theorem (Benoist, K. 2025)

As $P \rightarrow \infty$, the proportion of primes $p \in [P, 2P]$ that are deficient tends to zero.

In fact the proportion of Elkies primes as p varies in $[P, 2P]$ converges weakly to a Gaussian distribution centered in $3/8$ with standard deviation $\propto \sqrt{P/\log P}$.

Analogous statements holds in the RM case, and over number fields.

Expectation

Let $\mathcal{C}$ be a genus 2 curve over $\mathbb{Q}$, let $A = \text{Jac}(\mathcal{C})$, and let $H = h(\mathcal{C})$. Assume $\text{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Choose $q \geq 1$ and an integer $n = \Theta(H \log q)$. Then, given distinct primes $p_1, \dots, p_n$ of good reduction such that $\log(p_i) = O(\log q)$, one can compute $\#A_{p_i}(\mathbb{F}_{p_i})$ for each $1 \leq i \leq n$ in expected average time $\tilde{O}(\log^6 q)$.

Further directions

- Implementation (also in the RM case).
- Distribution of Elkies primes on average over all p.p.a.v.'s over a fixed $\mathbb{F}_q$ (joint with A. Benoist and F. Baril Boudreau).
- Full proof of complexity statement?
- Can we take advantage of rational $(\mathbb{Z}/\ell\mathbb{Z})$ subgroups in $A[\ell]$?

Isogeny classes

Main theorem

Isogeny class

Given a p.p.a.v. A over a number field k , compute

$$\text{Isog}(A) := \{\text{p.p.a.v. } A'/k \text{ up to isomorphism} : A' \text{ is isogenous to } A\}.$$

Main theorem

Isogeny class

Given a p.p.a.v. A over a number field k , compute

$$\text{Isog}(A) := \{\text{p.p.a.v. } A'/k \text{ up to isomorphism} : A' \text{ is isogenous to } A\}.$$

We say A that is **typical** if $\text{End}_{\bar{k}}(A) = \mathbb{Z}$.

Theorem (van Bommel, Chidambaram, Costa, K. 2023)

There is an algorithm which, given a genus 2 curve $\mathcal{C}/\mathbb{Q}$ such that $A = \text{Jac}(\mathcal{C})$ is typical, computes $\text{Isog}(A)$.

We computed the isogeny classes of all Jacobians of genus 2 curves in the LMFDB that are typical.

Some extreme examples

Let

$$\mathcal{C}_1 : y^2 + (x^3 + x^2 + x + 1)y = -x^3 - x^2$$

$$\mathcal{C}_2 : y^2 + y = x^5 - 363x^4 - 2517x^3 + 151106x^2 + 487525x - 16355862$$

$$\mathcal{C}_3 : y^2 + (x + 1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45$$

$$\mathcal{C}_4 : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 \\ + 406259311249x + 93951289752862$$

$$\mathcal{C}_5 : y^2 = (x + 4)(x + 11)(4x - 1)(12x + 13)(15x - 4).$$

Then

- $\text{Isog}(\text{Jac}(\mathcal{C}_1)) = \{\text{Jac}(\mathcal{C}_1), \text{Jac}(\mathcal{C}_2)\}$, linked by an isogeny of degree 13^4 .
- $\text{Isog}(\text{Jac}(\mathcal{C}_3)) = \{\text{Jac}(\mathcal{C}_3), \text{Jac}(\mathcal{C}_4)\}$, linked by an isogeny of degree 31^2 .
- $\# \text{Isog}(\text{Jac}(\mathcal{C}_5)) = 42$.

Indecomposable isogenies

Call an isogeny $\phi : A \rightarrow A'$ between p.p.a.v.'s over k **indecomposable** if there is no decomposition $\phi = \psi' \circ \psi$, where $\psi : A \rightarrow B$ and $\psi' : B \rightarrow A'$ are isogenies over k of degree > 1 , and B is principally polarized.

Lemma

Let $\phi : A \rightarrow A'$ be an indecomposable isogeny between typical p.p. abelian surfaces. Then there exists a prime ℓ such that either:

- ϕ is an (ℓ, ℓ) -isogeny: $\ker(\phi) \subset A[\ell](\bar{k})$ is an isotropic $(\mathbb{Z}/\ell\mathbb{Z})^2$.*
- $\ker(\phi) \subset A[\ell^2](\bar{k})$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2 \times \mathbb{Z}/\ell^2\mathbb{Z}$, and $[\ell] \ker(\phi) \perp (\ker \phi \cap A[\ell])$ inside $A[\ell]$.*

We will compute the codomains of all indecomposable isogenies from A and repeat.

We have the **mod- ℓ Galois representation**

$$\rho_\ell : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

If an isogeny ϕ as in the previous slide exists, then ρ_ℓ is **reducible**.

A consequence of Serre's open image theorem (1986)

If A is typical, then ρ_ℓ is irreducible for all but finitely many primes ℓ .

Dieulefait (2002) describes an algorithm to find a finite set containing all reducible primes for a given A .

Computing isogenies of a fixed degree

I'll focus on (ℓ, ℓ) -isogenies from now on. The algorithm is the same for the other indecomposable type, *mutatis mutandis*.

Easier, finite problem

Given a typical p.p. abelian surface $A/\mathbb{Q}$ and a prime ℓ , compute the codomains of all (ℓ, ℓ) -isogenies from A defined over $\mathbb{Q}$.

We could use Siegel modular polynomials, but it would hardly be practical for the degree 13^4 or 31^2 examples.

Computing isogenies of a fixed degree

I'll focus on (ℓ, ℓ) -isogenies from now on. The algorithm is the same for the other indecomposable type, *mutatis mutandis*.

Easier, finite problem

Given a typical p.p. abelian surface $A/\mathbb{Q}$ and a prime ℓ , compute the codomains of all (ℓ, ℓ) -isogenies from A defined over $\mathbb{Q}$.

We could use Siegel modular polynomials, but it would hardly be practical for the degree 13^4 or 31^2 examples.

Idea (that doesn't quite work)

When computing $\Psi_{\ell,1}(j_1(A), j_2(A), j_3(A), Y)$ using the analytic method, we compute the Igusa invariants of (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{C}$. Couldn't we directly detect which are rational numbers and which are not?

Integral rescaling

Let $\mathcal{C}/\mathbb{Q}$ be a genus 2 curve with **integral coefficients** such that $A = \text{Jac}(\mathcal{C})$, and let $\tau \in \mathcal{H}_2$ be a period matrix of A . Recall:

$$(M_4(\mathcal{C}) : \cdots : M_{12}(\mathcal{C})) = (m_4(\tau) : \cdots : m_6(\tau)) \in \mathbb{P}^{4,6,10,12}(\mathbb{C}).$$

Key lemma: integral rescaling

Let $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(\mathcal{C}) \in \mathbb{Z}$ for $i \in \{4, 6, 10, 12\}$. Then for each $i \in \{4, 6, 10, 12\}$, the quantities

$$N(i, \gamma) := (12\lambda\ell^2 \det(d_\gamma)^{-1})^i m_i(\gamma\tau) \quad \text{for } \gamma \in S_\ell$$

form a $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -stable collection of **algebraic integers**.

Algorithm and certification

Input: Invariants $M_4(\mathcal{C}), \dots, M_{12}(\mathcal{C}) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

Algorithm and certification

Input: Invariants $M_4(\mathcal{C}), \dots, M_{12}(\mathcal{C}) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:

Algorithm and certification

Input: Invariants $M_4(\mathcal{C}), \dots, M_{12}(\mathcal{C}) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:
 - $\tau \in \mathcal{H}_2$

Algorithm and certification

Input: Invariants $M_4(C), \dots, M_{12}(C) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:
 - $\tau \in \mathcal{H}_2$
 - $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(C)$ for $i \in \{4, 6, 10, 12\}$

Algorithm and certification

Input: Invariants $M_4(C), \dots, M_{12}(C) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:

- $\tau \in \mathcal{H}_2$
- $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(C)$ for $i \in \{4, 6, 10, 12\}$
- $N(i, \gamma)$, for each $i \in \{4, 6, 10, 12\}$ and $\gamma \in S_\ell$.

Algorithm and certification

Input: Invariants $M_4(C), \dots, M_{12}(C) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:
 - $\tau \in \mathcal{H}_2$
 - $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(C)$ for $i \in \{4, 6, 10, 12\}$
 - $N(i, \gamma)$, for each $i \in \{4, 6, 10, 12\}$ and $\gamma \in S_\ell$.
2. Keep the γ_0 's such that $N(i, \gamma_0)$ contains an **integer** a_i for each $i \in \{4, 6, 10, 12\}$.
If there are none, stop. Otherwise the a_i 's are putative invariants for $A(\gamma_0\tau)$.

Algorithm and certification

Input: Invariants $M_4(C), \dots, M_{12}(C) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:
 - $\tau \in \mathcal{H}_2$
 - $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(C)$ for $i \in \{4, 6, 10, 12\}$
 - $N(i, \gamma)$, for each $i \in \{4, 6, 10, 12\}$ and $\gamma \in S_\ell$.
2. Keep the γ_0 's such that $N(i, \gamma_0)$ contains an **integer** a_i for each $i \in \{4, 6, 10, 12\}$.
If there are none, stop. Otherwise the a_i 's are putative invariants for $A(\gamma_0\tau)$.
3. Recompute τ, λ and $N(i, \gamma_0)$ at **high precision** (but not $N(i, \gamma)$ for other γ 's).

Algorithm and certification

Input: Invariants $M_4(C), \dots, M_{12}(C) \in \mathbb{Z}$, a prime ℓ .

Output: Invariants of all (ℓ, ℓ) -isogenous abelian surfaces over $\mathbb{Q}$.

1. At **low precision**, compute complex balls that provably contain:
 - $\tau \in \mathcal{H}_2$
 - $\lambda \in \mathbb{C}^\times$ such that $\lambda^i m_i(\tau) = M_i(C)$ for $i \in \{4, 6, 10, 12\}$
 - $N(i, \gamma)$, for each $i \in \{4, 6, 10, 12\}$ and $\gamma \in S_\ell$.
2. Keep the γ_0 's such that $N(i, \gamma_0)$ contains an **integer** a_i for each $i \in \{4, 6, 10, 12\}$.
If there are none, stop. Otherwise the a_i 's are putative invariants for $A(\gamma_0\tau)$.
3. Recompute τ, λ and $N(i, \gamma_0)$ at **high precision** (but not $N(i, \gamma)$ for other γ 's).
4. Confirm that $N(i, \gamma_0) = a_i$: the product

$$\prod_{\gamma \in S_\ell} (N(i, \gamma) - a_i) \in \mathbb{Z}$$

is sufficiently close to 0, hence equal to 0.

Example: $\ell = 31$

Let $\ell = 31$ and

$$\mathcal{C}_3 : y^2 + (x + 1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$

Working at precision $N = 300$, there is a single $\gamma_0 \in S_\ell$ that we keep in step 2.

Putting $\alpha = 2^2 \cdot 3^2 \cdot 31$, we have

$$|N(4, \gamma_0) - \alpha^2 \cdot 318972640| \leq 7.8 \times 10^{-47},$$

$$|N(6, \gamma_0) - \alpha^3 \cdot 1225361851336| \leq 5.5 \times 10^{-39},$$

$$|N(10, \gamma_0) - \alpha^5 \cdot 10241530643525839| \leq 1.6 \times 10^{-29},$$

$$|N(12, \gamma_0) - \alpha^6 \cdot 307105165233242232724| \leq 4.6 \times 10^{-22}.$$

We certify these equalities by working at precision $N = 4\,128\,800$.

Finally we reconstruct A' using Mestre's algorithm. We might be off by a quadratic twist, but twisting back to find $\mathcal{C}_4$ is not difficult.

Further directions

- Compute the isogenies as rational maps.
- Typical genus 2 Jacobians over **number fields** (Hugo Nartz).
- Any p.p. abelian surface over $\mathbb{Q}$. Different approaches are called for depending on the type of (geometric) endomorphism algebra.
- Any p.p. abelian surface over a number field?
- Remove the p.p. assumption?
- Abelian threefolds?