# Fast evaluation of genus 2 modular polynomials via theta functions

Jean Kieffer (CNRS Nancy)

Leuven Isogeny Days 5, September 12, 2024

## Classical modular polynomials

Fix $\ell \geq 1$ prime. The classical modular polynomial of level $\ell$ is

$$\Phi_\ell \in \mathbb{Z}[X, Y].$$

If $k$ is a field of char. $\neq \ell$, and $E, E'$ are elliptic curves over $k$, then

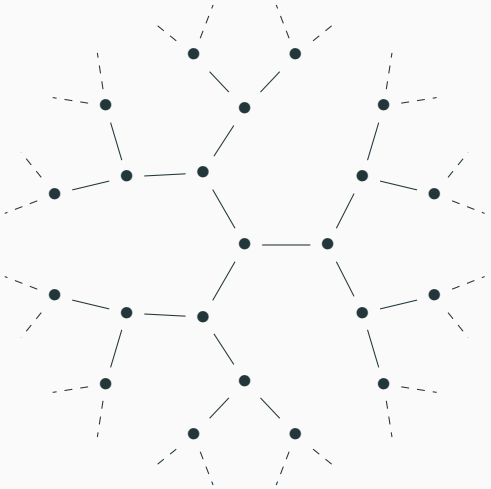
$$\Phi_\ell(j(E), j(E')) = 0 \iff E \text{ and } E' \text{ are } \ell\text{-isogenous over } \overline{k}.$$

**Example**

$$\begin{aligned}\Phi_2(X, Y) = {} & X^3 + Y^3 - X^2Y^2 + 1488X^2Y + 1488XY^2 - 162000X^2 - 162000Y^2 \\ & + 40773375XY + 8748000000X + 8748000000Y - 157464000000000.\end{aligned}$$

# Navigating isogeny graphs

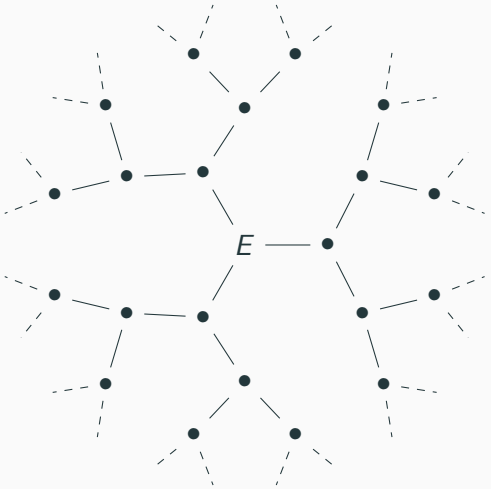
Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

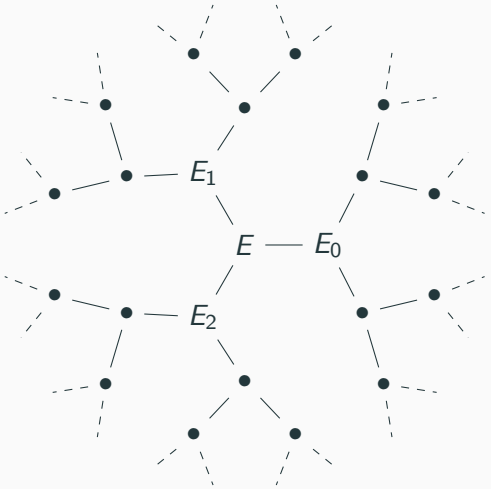
- Starting point: $E$



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

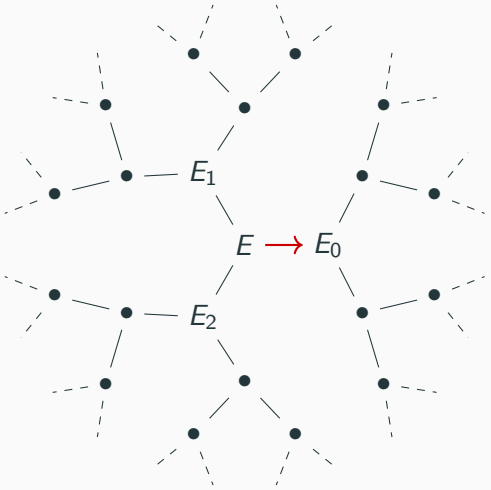
- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

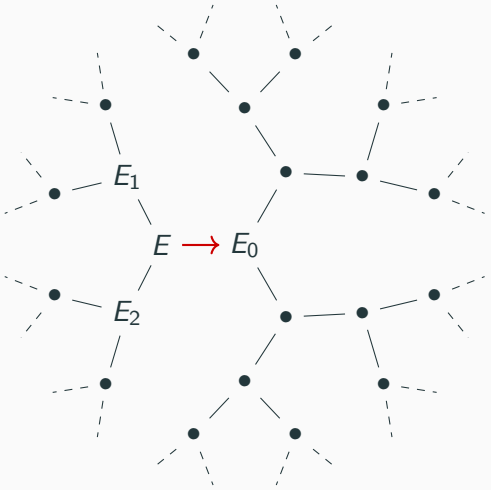
- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots
- Pick path to $E_0$, say



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

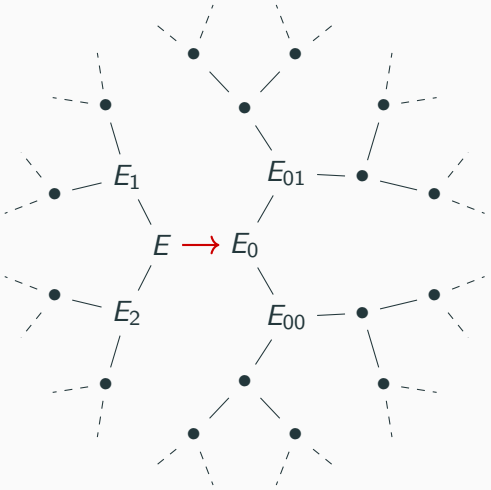
- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots
- Pick path to $E_0$, say



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

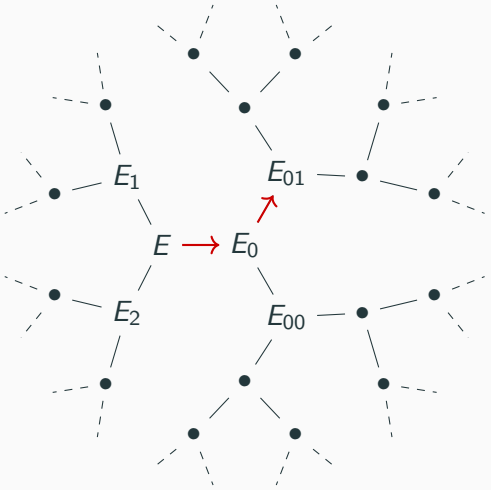
- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots
- Pick path to $E_0$, say
- Solve $\Phi_2(j(E_0), Y)/(Y - j(E)) = 0$: find 2 roots $j(E_{00})$, $j(E_{01})$



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

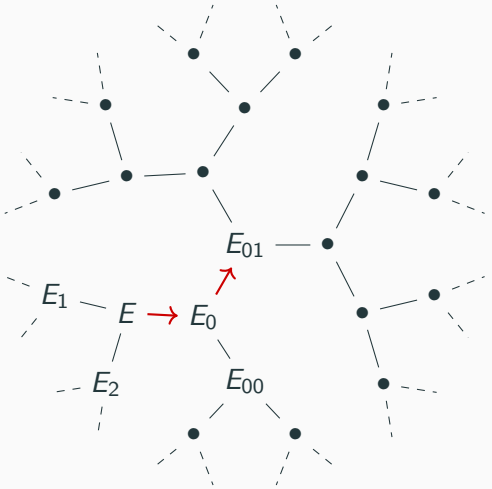
- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots
- Pick path to $E_0$, say
- Solve $\Phi_2(j(E_0), Y)/(Y - j(E)) = 0$: find 2 roots $j(E_{00})$, $j(E_{01})$
- Pick path to $E_{01}$, say



# Navigating isogeny graphs

Supersingular isogeny graph over $\mathbb{F}_{p^2}$, $\ell = 2$:

- Starting point: $E$
- Solve $\Phi_2(j(E), Y) = 0$ in $\mathbb{F}_{p^2}$: find 3 roots
- Pick path to $E_0$, say
- Solve $\Phi_2(j(E_0), Y)/(Y - j(E)) = 0$: find 2 roots $j(E_{00})$, $j(E_{01})$
- Pick path to $E_{01}$, say
- Continue!



# Remarks on modular polynomials

- As opposed to Vélu's formulas, no kernel information as input.
- Efficient algorithm in $O(\ell^2)$ if the kernel/image of isogenies are unknown.
- Rich literature on computing modular polynomials in relation with point counting. See Sabrina and Damien's ANTS paper [KR24].

**What about higher dimensions?**

# Genus 2 modular polynomials: setup

To generalize $\Phi_\ell$, we need:

- A family of abelian varieties: for instance p.p. abelian surfaces, either $\mathrm{Jac}(C)$ where $C$ has genus 2 or $E_1 \times E_2$.
- Isogenies between them: for instance $(\ell, \ell)$-isogenies where $\ell$ is a fixed prime. This means $\ker(\varphi) \subset A[\ell]$ is an isotropic $(\mathbb{Z}/\ell\mathbb{Z})^2$.
- New invariants to replace the $j$-invariant: for instance the Igusa invariants $j_1, j_2, j_3$. (Not defined for $E_1 \times E_2$.)

# Genus 2 modular polynomials: properties

Given PPASs $A$ and $A'$ over a field $k$ with Igusa invariants $(j_1, j_2, j_3)$ and $(j_1', j_2', j_3')$, we want some algebraic equation which is satisfied by these invariants exactly when $A$ and $A'$ are $(\ell, \ell)$-isogenous.

We actually need three equations, one for each invariant. Write them in the form:

$$\Psi_{\ell,1}(j_1, j_2, j_3, j_1') = 0, \qquad \text{i.e. } j_1' \text{ is a root of } \Psi_{\ell,1}(j_1, j_2, j_3, X)$$

$$j_2' = \frac{\Psi_{\ell,2}}{\partial_X \Psi_{\ell,1}}(j_1, j_2, j_3, j_1'),$$

$$j_3' = \frac{\Psi_{\ell,3}}{\partial_X \Psi_{\ell,2}}(j_1, j_2, j_3, j_1').$$

Assuming only $A$ is known, we solve for $j_1'$, then determine $j_2'$ and $j_3'$.

# Genus 2 modular polynomials: definition

**Definition/Proposition**

The genus 2 modular polynomials (of Siegel type, in Igusa invariants, of level $\ell$) are the unique set of three rational fractions

$$\Psi_{\ell,1}, \Psi_{\ell,2}, \Psi_{\ell,3} \in \mathbb{Q}(J_1, J_2, J_3)[X]$$

satisfying the property from the previous slide. See e.g. [BL09].

In principle, everything we can do with classical modular polynomials is also possible with this generalized version.

(There isn't enough space to write down $\Psi_{2,1}$ on this slide, unfortunately...)

# Genus 2 modular polynomials: remarks

**Major drawback:** genus 2 modular polynomials are huge.

- Degree in each of the 4 variables is $O(\ell^3)$
- Size of coefficients is $O(\ell^3 \log \ell)$, so total size $O(\ell^{15} \log \ell)$ [K22].

$\Psi_{2,1}$ is 280 kB, $\Psi_{3,1}$ is 68 MB.

Cannot reasonably hope to write them down for $\ell > 7$.

# Genus 2 modular polynomials: remarks

**Major drawback:** genus 2 modular polynomials are huge.

- Degree in each of the 4 variables is $O(\ell^3)$
- Size of coefficients is $O(\ell^3 \log \ell)$, so total size $O(\ell^{15} \log \ell)$ [K22].

$\Psi_{2,1}$ is 280 kB, $\Psi_{3,1}$ is 68 MB.

Cannot reasonably hope to write them down for $\ell > 7$.

**More reasonable task**

Given $j_1, j_2, j_3 \in k$, evaluate the polynomials $\Psi_{\ell,k}(j_1, j_2, j_3, X)$ for $1 \leq k \leq 3$.

- This is what we need to navigate isogeny graphs.
- Smaller output: if $j_1, j_2, j_3 \in \mathbb{Q}$, output size is $\ell^6(\log \ell + \text{size of } j_1, j_2, j_3)$.
  If $j_1, j_2, j_3 \in \mathbb{F}_q$, output size is $\ell^3 \log q$.

# Main result

**Theorem (K. '24?)**

Given primes $p, \ell$ and a generic tuple $(j_1, j_2, j_3) \in \mathbb{F}_p^3$, one can evaluate $\Psi_{\ell,k}(j_1, j_2, j_3, X) \in \mathbb{F}_p[X]$ for $1 \leq k \leq 3$ in time $\widetilde{O}(\ell^6 \log p)$.

- Not quasi-linear time, but still the most efficient way to navigate genus 2 isogeny graphs without torsion information.
- The algorithm also works over $\mathbb{Q}$ (in quasi-linear time!) and other number fields/finite fields.

## Related example

Taken from [vBCCK23].

Over $\mathbb{Q}$, consider the genus 2 curves

$$C_1 : y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$
$$C_2 : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862.$$

## Related example

Taken from [vBCCK23].

Over $\mathbb{Q}$, consider the genus 2 curves

$$C_1 : y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45.$$
$$C_2 : y^2 + xy = -x^5 + 2573x^4 + 92187x^3 + 2161654285x^2 + 406259311249x + 93951289752862.$$

**Fact**

There exists a $(31, 31)$-isogeny $\varphi : \mathrm{Jac}(C_1) \to \mathrm{Jac}(C_2)$ defined over $\mathbb{Q}$.

The algorithm we used to construct $C_2$ directly computes rational roots of modular polynomials over $\mathbb{Q}$ in time $\widetilde{O}(\ell^3)$. Time: roughly 1h.

# The evaluation algorithm: preliminaries

We describe the algorithm for elliptic curves, as in [Eng09].

**Reminders on elliptic curves over $\mathbb{C}$:**

- They are complex tori of the form $E(\tau) = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ where $\tau \in \mathcal{H}_1$ (i.e. $\tau \in \mathbb{C}$ and $\mathrm{Im}(\tau) > 0$).
- The period $\tau$ is unique up to the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}_1$.
- The $j$-invariant of $E(\tau)$ is given by an analytic function $j : \mathcal{H}_1 \to \mathbb{C}$.
- Given a prime $\ell > 1$ and $\tau \in \mathcal{H}_1$, one can easily enumerate the elliptic curves that are $\ell$-isogenous to $E(\tau)$: they correspond to sublattices of index $\ell$ in $\mathbb{Z} + \tau\mathbb{Z}$.

# The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.
4. Compute $j(\tau'_1), \ldots, j(\tau'_{\ell+1})$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.
4. Compute $j(\tau'_1), \ldots, j(\tau'_{\ell+1})$.
5. Compute $\Phi_\ell(\widetilde{j}, X) = \Phi_\ell(j(\tau), X) = \prod_{k=1}^{\ell+1}(X - j(\tau'_k))$ in $\mathbb{C}[X]$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.
4. Compute $j(\tau'_1), \ldots, j(\tau'_{\ell+1})$.
5. Compute $\Phi_\ell(\widetilde{j}, X) = \Phi_\ell(j(\tau), X) = \prod_{k=1}^{\ell+1}(X - j(\tau'_k))$ in $\mathbb{C}[X]$.
6. Recognize each coefficient of $\Phi_\ell(\widetilde{j}, X)$ as an integer.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.
4. Compute $j(\tau'_1), \ldots, j(\tau'_{\ell+1})$.
5. Compute $\Phi_\ell(\widetilde{j}, X) = \Phi_\ell(j(\tau), X) = \prod_{k=1}^{\ell+1}(X - j(\tau'_k))$ in $\mathbb{C}[X]$.
6. Recognize each coefficient of $\Phi_\ell(\widetilde{j}, X)$ as an integer.
7. Output the reduced polynomial modulo $p$.

## The evaluation algorithm: outline

Given $j(E) \in \mathbb{F}_p$, we evaluate $\Phi_\ell(j(E), X)$ as follows.

1. Lift $j(E)$ to $\widetilde{j} \in \mathbb{Z}$. We will evaluate $\Phi_\ell(\widetilde{j}, X)$, then reduce it mod $p$.
2. Compute $\tau \in \mathcal{H}_1$ such that $j(\tau) = \widetilde{j}$.
3. Enumerate periods $\tau'_1, \ldots, \tau'_{\ell+1}$ of all elliptic curves that are $\ell$-isogenous to $E(\tau)$.
4. Compute $j(\tau'_1), \ldots, j(\tau'_{\ell+1})$.
5. Compute $\Phi_\ell(\widetilde{j}, X) = \Phi_\ell(j(\tau), X) = \prod_{k=1}^{\ell+1}(X - j(\tau'_k))$ in $\mathbb{C}[X]$.
6. Recognize each coefficient of $\Phi_\ell(\widetilde{j}, X)$ as an integer.
7. Output the reduced polynomial modulo $p$.

In steps 2 to 5, we use interval arithmetic and a high precision $N = \Theta(\ell \log \ell + \ell \log p)$ digits to get a unique and provably correct result in step 6.

**We must compute periods and $j$-invariants in quasi-linear time in $N$.**

## Evaluating the $j$-invariant

To efficiently evaluate $j(\tau)$, we write it in terms of theta functions.
Set $q = \exp(\pi i \tau)$, and

$$\theta_{00}(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2},$$
$$\theta_{01}(\tau) = \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2},$$
$$\theta_{10}(\tau) = \sum_{n \in \mathbb{Z}} q^{(n+\frac{1}{2})^2}.$$

These series converge fast. Sum enough terms, then

$$j(\tau) = 32 \frac{(\theta_{00}^8 + \theta_{01}^8 + \theta_{10}^8)^3}{(\theta_{00}\theta_{01}\theta_{10})^8}.$$

**Still not quasi-linear in the required precision...**

# Evaluating theta functions

**Theorem (Elkies, K., in preparation)**

Given $N \geq 0$, and given $\tau \in \mathcal{H}_1$ that is suitably reduced, one can evaluate $\theta_{00}(\tau)$, $\theta_{01}(\tau)$, $\theta_{10}(\tau)$ to precision $N$ in quasi-linear time $O(\mathcal{M}(N) \log N)$, uniformly in $\tau$.

- Implemented in [FLINT] 3.1: `https://flintlib.org/doc/acb_theta.html`. (A new, faster version is in preparation.)
- Applies to theta functions in any genus $g$, still in quasi-linear time.
- Earlier works [Dup11], [LT14] are specific to small $g$, tricky to run in interval arithmetic, and less efficient.
- When evaluating $\Phi_\ell$, we add a (negligible) reduction step to move $\tau'_1, \dots, \tau'_{\ell+1}$ to the fundamental domain under $\mathrm{SL}_2(\mathbb{Z})$.

## Genus 2 translation

To evaluate $\Psi_{\ell,k}(j_1, j_2, j_3, X)$ for $1 \leq k \leq 3$ instead of $\Phi_\ell(j(E), X)$:

- Same general approach (complex uniformization and interval arithmetic)
- Replace $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathcal{H}_1$ by $\mathrm{Sp}_4(\mathbb{Z})$ acting on $\mathcal{H}_2$: period matrices
- Use genus 2 theta functions
- Extra step to handle the denominator of modular equations $\Psi_{\ell,k}$ and make sure we recognize integers.

One project I have: break the genus 2 point-counting records, SEA-style.

## Genus 2 translation

To evaluate $\Psi_{\ell,k}(j_1, j_2, j_3, X)$ for $1 \leq k \leq 3$ instead of $\Phi_\ell(j(E), X)$:

- Same general approach (complex uniformization and interval arithmetic)
- Replace $\mathrm{SL}_2(\mathbb{Z})$ acting on $\mathcal{H}_1$ by $\mathrm{Sp}_4(\mathbb{Z})$ acting on $\mathcal{H}_2$: period matrices
- Use genus 2 theta functions
- Extra step to handle the denominator of modular equations $\Psi_{\ell,k}$ and make sure we recognize integers.

One project I have: break the genus 2 point-counting records, SEA-style.

**Thank you!**

# References


[vBCCK23] R. van Bommel, S. Chidambaram, E. Costa, and J. Kieffer, *Computing isogeny classes of typical principally polarized abelian surfaces over the rationals*, LuCaNT 2023

[BL09] R. Bröker and K. Lauter, *Modular polynomials for genus 2*, LMS J. Comput. Math 12 (326–339), 2009.

[Dup11] R. Dupont, *Fast evaluation of modular functions using Newton iterations and the AGM*, Math. Comp. 80, 1823–1847, 2011.

[Eng09] A. Enge, *Computing modular polynomials in quasi-linear time*, Math. Comp. 78, 1809–1824, 2009.

[FLINT] The FLINT team, *FLINT: Fast Library for Number Theory*, version 3.1.0, 2023.

[K22] J. Kieffer, *Degree and height estimates for modular equations on PEL Shimura Varieties*, J. London Math. Soc. (2) 105, 1314–1361, 2022.

[KR24] S. Kunzweiler and D. Robert, *Computing modular polynomials by deformation*, ANTS 2024

[LT14] H. Labrande and E. Thomé, *Computing theta functions in quasi-linear time in genus 2 and above*, ANTS 2016

(K. '24?) J. Kieffer, *Evaluating modular equations for abelian surfaces*, 2022.