Counting ℓ-isogenies with different modular polynomials

Based on joint work with Thomas den Hollander,
Marc Houben, Sören Kleine, Marzio Mula & Daniel Slamanig

Sebastian A. Spindler • October 7th, 2025

Research Institute
Cyber Defence
University of the Bundeswehr Munich

The **classical modular polynomial** $\Phi_\ell \in \mathbb{Z}[J_0, J_1]$ is mainly known by the following property:

$$\Phi_\ell(j_0, j_1) = 0 \iff j_0 \text{ and } j_1 \text{ are } \ell\text{-isogenous}$$

- Where does this polynomial come from?
- Why does the above hold?
- Are there other polynomials <u>like</u> this?

Agenda

- A brief intro to modular curves
- The classical modular polynomial
- The resultant technique
- Other modular polynomials
  - The canonical modular polynomial
  - The Atkin modular polynomial
  - The Weber modular polynomial
- A cryptographic application: Isogeny proofs of knowledge

- Elliptic curves over $\mathbb{C}$ correspond to quotients $\mathbb{C}/\Lambda$ by two-dimensional lattices $\Lambda \subseteq \mathbb{C}$ via the isomorphism

$$\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C}),\ z \mapsto [\wp(z;\Lambda) : \wp'(z;\Lambda) : 1]$$

- Any such lattice Λ can be rotated and stretched* into a lattice of the form

$$\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$$

for an element $\tau \in \mathbb{H}$ in the **upper half-plane**

$$\mathbb{H} = \{\tau \in \mathbb{C} :\ \mathrm{Im}(\tau) > 0\}$$

- We write $E_{\Lambda_\tau} =: E_\tau$ and $j(E_\tau) =: j(\tau)$

*These operations preserve the isomorphism class of E_Λ

The $\mathrm{SL}_2(\mathbb{Z})$-action and the j-invariant

- The group $\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2} \colon ad - bc = 1 \right\}$ acts on $\mathbb{H}$ via **Möbius transformations**

  $$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\tau) = \tfrac{a\tau+b}{c\tau+d}, \quad \text{and we have } \ j\left(\tfrac{a\tau+b}{c\tau+d}\right) = j(\tau),$$

  so $j(\tau)$ induces a function on the set of orbits

  $$j(\tau)\colon\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$$

- Compactifying $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ yields the **modular curve** $X(1)$, and $j(\tau)$ defines a rational function on this projective curve; in fact:

Theorem

The modular curve $X(1)$ has genus 0, i.e. $X(1) \cong \mathbf{P}^1(\mathbb{C})$, with rational function field

$$\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$$

Interjection: Congruence subgroups

- Let $N \in \mathbb{N}$. The kernel of the surjective entry-wise reduction

$$\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N)$$

  is the N-th **principal congruence subgroup** $\Gamma(N)$ of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \colon \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod N \}$$

- Any subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{N}$ is called a **congruence subgroup** of $\mathrm{SL}_2(\mathbb{Z})$
- The minimal $N \in \mathbb{N}$ with $\Gamma(N) \subseteq \Gamma$ is called the **level** of Γ

New modular curves

- For any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ we can consider a *suitable* compactification of the set of orbits

$$\Gamma \backslash \mathbb{H}$$

to obtain* the modular curve $X(\Gamma)$

- We already saw an example: $X(\Gamma(1)) = X(\mathrm{SL}_2(\mathbb{Z})) = X(1)$
- Further we will be interested in

$$X_0(N) := X(\Gamma_0(N))$$

for the level N congruence subgroup

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \colon \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N \right\}$$

* $X(\Gamma)$ can alternatively be defined via an extended action of Γ

- For any N-torsion basis $E_\tau[N] = \langle P, Q \rangle$ and $\left(\begin{smallmatrix} a & b \\ Nc' & d \end{smallmatrix}\right) \in \Gamma_0(N)$ we have
$$\begin{pmatrix} a & b \\ Nc' & d \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} aP + bQ \\ dQ \end{pmatrix}$$
- Varying over all possible bases and identifying orbits according to the above law, one deduces* that elements of
$$\Gamma_0(N) \backslash \mathbb{H}$$
correspond to isomorphism classes of elliptic curves together with a cyclic N-order subgroup $\langle Q \rangle$, i.e. with a cyclic N-isogeny
- For simplicity: Focus on $N = \ell$ a prime from now on

*Using the surjectivity of $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N)$

Understanding $X_0(\ell)$

- Forgetting the ℓ-isogeny, i.e. bunching together orbits according to the full $\mathrm{SL}_2(\mathbb{Z})$-action, induces a degree $\ell + 1$ map

$$X_0(\ell) \to X(1)$$

corresponding to the degree $\ell + 1$ function field extension

$$\mathbb{C}(j(\tau)) = \mathbb{C}(X(1)) \hookrightarrow \mathbb{C}(X_0(\ell))$$

- Further

$$\tau \mapsto j(\ell\tau)$$

induces a rational function on $X_0(\ell)$, corresponding to the target j-invariant of the ℓ-isogeny; in fact:

Theorem

$$\mathbb{C}(X_0(\ell)) = \mathbb{C}(j(\tau), j(\ell\tau))$$

- In terms of isogenies: ℓ-isogenies are (generically) determined by their starting and target j-invariant

The classical modular polynomial

- The minimal polynomial of $j(\ell\tau)$ over $\mathbb{C}(j(\tau)) = \mathbb{C}(X(1))$ is called the **classical modular polynomial**

$$\Phi_\ell(j(\tau), J) \in \mathbb{Z}[j(\tau)][J]$$

- As a bivariate polynomial $\Phi_\ell(J_0, J_1) \in \mathbb{Z}[J_0, J_1]$, it is symmetric and in each variable of degree

$$\deg_{J_i} \Phi_\ell(J_0, J_1) = \ell + 1 = [\mathbb{C}(X_0(\ell)) : \mathbb{C}(X(1))]$$

- The roots of $\Phi_\ell(j(\tau), J)$ are given by

$$a_i^*(j(\ell\tau)) = j(\ell a_i(\tau)) \quad (i = 0, \ldots, \ell)$$

for a representative set $\{a_0, \ldots, a_\ell\}$ of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$; as this gives the j-invariants ℓ-isogenous to $j(\tau)$, one immediately obtains

Theorem

Let ℓ be a prime and $j_0, j_1 \in \mathbb{C}$. Then

$$\#\{\ell\text{-isogenies } j_0 \to j_1\} = \text{Multiplicity of } j_1 \text{ as a root of } \Phi_\ell(j_0, J)$$

Why does it work in positive characteristic?

It is also well-known that this extends to positive characteristic:

Theorem

Let $p \neq \ell$ be primes and $j_0, j_1 \in \overline{\mathbb{F}_p}$. Then

$$\#\{\ell\text{-isogenies } j_0 \to j_1\} = \text{Multiplicity of } j_1 \text{ as a root of } \Phi_\ell(j_0, J)$$

Why? It's complicated:

- *Algebraic* theory of modular functions does not directly extend to positive characteristic
- Igusa developed *geometric* theory of modular functions in arbitrary characteristic …
- … and proved the existence of a model of the level ℓ modular function field that behaves well under reduction modulo p

In this talk: Take understanding of classical modular polynomial over arbitrary fields as base point

Other modular polynomials

Why are we interested in other modular polynomials?

- Additional *level structure* obtained from congruence subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ allows for compacter representation of isogenies
- Certain level structures can be used to remove ‘redundant’ information

The **resultant** $\mathrm{res}_Y(g,h) \in R$ of two polynomials $g, h \in R[Y]$ is usually known for the following property, given $R = K$ is a field:

$$\mathrm{res}_Y(g,h) = 0 \iff g \text{ and } h \text{ share a common root in } \overline{K}$$

Via an arithmetic approach to subresultants, this can be extended:

Theorem

Let $g \in K[Y]$ and $h \in K[J][Y]$ be non-zero polynomials, and let $u \in K$ such that $\deg_Y h(u,Y) = \deg_Y h$. Further let

$$m = \#\{\!\{\text{Roots } x \in \overline{K} \text{ of } g \text{ such that } h(u,x) = 0\}\!\}$$

Then $\mathrm{res}_Y(g,h) \in K[J]$ has a root of multiplicity at least m at u.*

*Modulo technicalities in small characteristics

The resultant technique – Our strategy

How to approach other modular polynomials:

1. Find modular function(s) and corresponding polynomial over $\mathbb{C}$
2. Check if this modular polynomial has integer coefficients
3. Use modular theory to understand relation to ℓ-isogenies over $\mathbb{C}$
4. Translate this into a suitable resultant equation, relating the obtained polynomial back to the classical modular polynomial
5. Profit*!

*Modulo understanding of classical modular polynomial

- If $X_0(\ell)$ has genus 0, then
$$X_0(\ell) \cong \mathbf{P}^1(\mathbb{C}) \text{ and } \mathbb{C}(X_0(\ell)) = \mathbb{C}(f_\ell(\tau)),$$
so we obtain a 1-parameter parametrization of ℓ-isogenies
- This happens if and only if $\ell - 1$ divides 12, i.e. for
$$\ell \in \{2, 3, 5, 7, 13\}$$
- In this case one can generate $\mathbb{C}(X_0(\ell))$ over $\mathbb{C}$ by the modular function
$$f_\ell(\tau) := \ell^s \cdot \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s}$$
where $s = 12/(\ell - 1)$ and $\eta(\tau)$ is the Dedekind η function

THE CANONICAL MODULAR POLYNOMIAL – DEFINITION II

- The minimal polynomial of $f_\ell(\tau)$ over $\mathbb{C}(j(\tau)) = \mathbb{C}(X(1))$ is called the **canonical modular polynomial**

$$\Phi_\ell^c(T, j(\tau)) \in \mathbb{Z}[j(\tau)][T]$$

- As a bivariate polynomial $\Phi_\ell^c(T, j) \in \mathbb{Z}[T, j]$, we find

$$\begin{tikzcd} & \mathbb{C}(j(\tau), f_\ell(\tau)) \arrow[dr, equal, "1"] & \\ \mathbb{C}(j(\tau)) \arrow[ur, hook, "\ell+1"] & & \mathbb{C}(f_\ell(\tau)) \end{tikzcd}$$

$$\deg_T \Phi_\ell^c(T, j) = \ell + 1 \qquad \qquad \deg_j \Phi_\ell^c(T, j) = 1$$

Interjection: The Fricke involution

- We have an involution ω_ℓ on $X_0(\ell)$ induced by the Möbius transformation via the matrix

$$\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}, \text{ i.e. } \tau \mapsto \frac{-1}{\ell\tau}$$

- On $j(\tau)$ and $j(\ell\tau)$ we have

$$\omega_\ell^*(j(\tau)) = j \circ \omega_\ell(\tau) = j(\ell\tau) \text{ and } \omega_\ell^*(j(\ell\tau)) = j(\tau)$$

- Thus, in terms of ℓ-isogenies, ω_ℓ corresponds to taking the dual
- On $f_\ell(\tau)$ we have

$$\omega_\ell^*(f_\ell(\tau)) = f_\ell \circ \omega_\ell(\tau) = f_\ell\left(-\tfrac{1}{\ell\tau}\right) = \ell^s / f_\ell(\tau)$$

for $\ell \in \{2, 3, 5, 7, 13\}$, with $s = 12/(\ell - 1)$

- From the action of ω_ℓ on $f_\ell(\tau)$, one obtains for the ℓ-isogeny $j_0 \to j_1$ parametrized by $f_\ell(\tau_0)$:

$$\Phi_\ell^c(f_\ell(\tau_0), j_0) = 0 \text{ and } \Phi_\ell^c(\ell^s/f_\ell(\tau_0), j_1) = 0$$

- Thus

$$\Phi_\ell^c(T, j_0) \text{ and } \Phi_\ell^c(\ell^s/T, j_1)$$

  share common roots according to ℓ-isogenies between j_0 and j_1

Proposition

$$\mathrm{res}_T(\Phi_\ell^c(T, J_0), \Phi_\ell^c(\ell^s/T, J_1) \cdot T^{\ell+1}/\ell^s) = \pm \ell^{s\cdot\ell} \cdot \Phi_\ell(J_0, J_1)$$

THEOREM

Let $\ell \in \{2, 3, 5, 7, 13\}$, $s = 12/(\ell - 1)$, $p \neq \ell$ *and* $j_0, j_1 \in \overline{\mathbb{F}_p}$. *Then*

$$\#\{\ell\text{-isogenies } j_0 \to j_1\} = \#\left\{\!\!\left\{ \begin{array}{c} \text{Roots } f \text{ of } \Phi_\ell^c(T, j_0) \\ \text{such that} \\ \Phi_\ell^c(\ell^s/f, j_1) = 0 \end{array} \right\}\!\!\right\}$$

REMARK

Away from the problematic points ($j_0 = 0$ and $j_0 = 1728$), one can explicitly associate to a root f of $\Phi_\ell^c(T, j_0)$ an ℓ-isogeny kernel polynomial via a 'generic' formula

- When the quotient*

$$X_0^+(\ell) := X_0(\ell)/\langle\omega_\ell\rangle$$

has genus 0, we still get a 1-parameter parametrization of ℓ-isogenies up to dualization

- This happens for the **supersingular primes**

$$\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 59, 71\}$$

- In this case one can compute a *nice* ω_ℓ-invariant function

$$g_\ell(\tau)$$

on $X_0(\ell)$ generating the subfield $\mathbb{C}(X_0^+(\ell)) \subseteq \mathbb{C}(X_0(\ell))$ over $\mathbb{C}$

*This is not a *modular* curve anymore

- The minimal polynomial of $g_\ell(\tau)$ over $\mathbb{C}(j(\tau)) = \mathbb{C}(X(1))$ is called the **Atkin modular polynomial**

$$\Phi_\ell^A(Y, j(\tau)) \in \mathbb{Z}[j(\tau)][Y]$$

- As a bivariate polynomial $\Phi_\ell^A(Y, j) \in \mathbb{Z}[Y, j]$, we find

$$\begin{tikzcd}
 & \mathbb{C}(j(\tau), g_\ell(\tau)) & \\
\mathbb{C}(j(\tau)) \arrow[ur, hook, "\ell + 1"] & & \mathbb{C}(g_\ell(\tau)) \arrow[ul, hook', "2"']
\end{tikzcd}$$

$$\deg_Y \Phi_\ell^A(Y, j) = \ell + 1 \qquad \deg_j \Phi_\ell^A(Y, j) = 2$$

- Since $g_\ell(\tau)$ is ω_ℓ-invariant, one obtains for the pair of dual ℓ-isogenies $j_0 \longleftrightarrow j_1$ parametrized by $g_\ell(\tau_0)$:

$$\Phi_\ell^A(g_\ell(\tau_0), j_0) = 0 \text{ and } \Phi_\ell^A(g_\ell(\tau_0), j_1) = 0$$

- Hence

$$\Phi_\ell^A(Y, j_0) \text{ and } \Phi_\ell^A(Y, j_1)$$

share common roots according to the (dual pairs of) ℓ-isogenies between j_0 and j_1

PROPOSITION

$$\mathrm{res}_Y\left(\Phi_\ell^A(Y, J_0), \frac{\Phi_\ell^A(Y, J_1) - \Phi_\ell^A(Y, J_0)}{J_1 - J_0}\right) = \Phi_\ell(J_0, J_1)$$

The Atkin multiplicity theorem

Theorem

Let $\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}$, $p \neq \ell$ and define

$$\delta_\ell(Y, J_0, J_1) := \frac{\Phi_\ell^A(Y, J_1) - \Phi_\ell^A(Y, J_0)}{J_1 - J_0}$$

For any $j_0, j_1 \in \overline{\mathbb{F}_p}$ we then have

$$\#\{\ell\text{-isogenies } j_0 \to j_1\} = \# \left\{\!\!\left\{ \begin{array}{c} \text{Roots } g \text{ of } \Phi_\ell^A(Y, j_0) \\ \text{such that} \\ \delta_\ell(g, j_0, j_1) = 0 \end{array} \right\}\!\!\right\}$$

Remark

Away from the problematic points ($j_0 = 0$, $j_0 = 1728$, and non-equivalent dual loops) one can explicitly associate to a root g of $\Phi_\ell^A(Y, j_0)$ an ℓ-isogeny kernel polynomial via a 'generic' formula*

---

*Modulo computational limitations

- There is a modular curve $X(W)$ of level 48 and genus 0
- Explicitly, a generator of $\mathbb{C}(X(W))$ is given by

$$\mathfrak{f}(\tau) = \frac{\eta(\tau)^2}{\eta\left(\frac{\tau}{2}\right)\eta(2\tau)},$$

with a degree 72 cover $X(W) \to X(1)$ given by the polynomial

$$\Psi^W(F, j) = (F^{24} - 16)^3 - j \cdot F^{24},$$

i.e.

$$j = \frac{(F^{24} - 16)^3}{F^{24}} =: \mathcal{J}(F)$$

- For $\ell \geq 5$* we can take the pullback

$$\begin{tikzcd}
 & X(W \cap \Gamma_0(\ell)) \arrow[dl] \arrow[dr] \arrow[dd, phantom, "\lrcorner" rotate=-45] & \\
X(W) \arrow[dr, "\mathcal{J}"'] & & X_0(\ell) \arrow[dl, "\pi"] \\
 & X(1) &
\end{tikzcd}$$

to work similarly to the classical modular polynomial: Explicitly, we have

$$\mathbb{C}(X(W \cap \Gamma_0(\ell))) = \mathbb{C}(\mathfrak{f}(\tau), \mathfrak{f}(\ell\tau))$$

*The levels 48 of W and ℓ of $\Gamma_0(\ell)$ need to be coprime

- Let $\ell \geq 5$. The minimal polynomial of $\mathfrak{f}(\ell\tau)$ over $\mathbb{C}(X(W)) = \mathbb{C}(\mathfrak{f}(\tau))$ is called the **Weber modular polynomial**

$$\Phi_\ell^W(F, \mathfrak{f}(\tau)) \in \mathbb{Z}[\mathfrak{f}(\tau)][F]$$

- As a bivariate polynomial $\Phi_\ell^W(F_0, F_1) \in \mathbb{Z}[F_0, F_1]$, it behaves just like the classical modular polynomial:
    - Φ_ℓ^W is symmetric
    - Φ_ℓ^W has degree $\ell + 1$ in each variable
- Notably, Φ_ℓ^W is much sparser and much smaller than Φ_ℓ

- We expect Φ_ℓ^W to behave 'like Φ_ℓ for the lifted $\mathfrak{f}$-invariants'
- Explicitly,

$$\Phi_\ell^W(F_0, F_1) \text{ and } \Phi_\ell(\mathcal{J}(F_0), \mathcal{J}(F_1))$$

should be closely related

PROPOSITION

$$\operatorname{res}_{F_1}(\Phi_\ell^W(F_0, F_1), \Psi^W(F_1, J_1)) = \operatorname{res}_{J_0}(\Phi_\ell(J_0, J_1), \Psi^W(F_0, J_0))$$

Rephrased as a 'usable' equation:

PROPOSITION

$$\operatorname{res}_{F_1}(\Phi_\ell^W(F_0, F_1), \Psi^W(F_1, J_1)) = F_0^{24\cdot(\ell+1)}\Phi_\ell(\mathcal{J}(F_0), J_1)$$

THEOREM

Let $\ell \geq 5$ be a prime, $p \neq \ell$, $j_0, j_1 \in \overline{\mathbb{F}_p}$, and fix a Weber lift $\mathfrak{f}_0 \in \overline{\mathbb{F}_p}$ of j_0, i.e.

$$\Psi^W(\mathfrak{f}_0, j_0) = 0$$

Then

$$\#\{\ell\text{-isogenies } \mathcal{J}(\mathfrak{f}_0) = j_0 \to j_1\} = \#\left\{\!\!\left\{ \begin{array}{c} \text{Roots } \mathfrak{f}_1 \text{ of } \Phi_\ell^W(\mathfrak{f}_0, F) \\ \text{such that} \\ \Psi^W(\mathfrak{f}_1, j_1) = 0 \end{array} \right\}\!\!\right\}$$

How to encode isogeny paths I

A path in the supersingular ℓ-isogeny graph is now encoded as follows:

- Classically, via a chain $(j_0, j_1, \dots, j_k)$ of j-invariants such that

$$j_0 \xrightarrow{\Phi_\ell(j_0,j_1)=0} j_1 \xrightarrow{\Phi_\ell(j_1,j_2)=0} j_2 \xrightarrow{\qquad\qquad} \dots$$

- Canonically, via a chain of invariants $(f_0, \dots, f_{k-1})$ such that

$$\begin{tikzcd}
& f_0 \arrow[dl, "\Phi_\ell^c(f_0{,}j_0)=0"] \arrow[dr, "\Phi_\ell^c(\ell^s/f_0{,}j_1)=0"] & & f_1 \arrow[dl, "\Phi_\ell^c(f_1{,}j_1)=0"] \arrow[dr, "\Phi_\ell^c(\ell^s/f_1{,}j_2)=0"] & & \dots \arrow[dl] \arrow[dr] & \\
j_0 & & j_1 & & j_2 & & \dots
\end{tikzcd}$$

How to encode isogeny paths II

- Atkin-ly, via a chain of invariants $(g_0, \dots, g_{k-1})$ such that

$$\begin{tikzcd}[column sep=small]
 & g_0 \arrow[dl] \arrow[dr] \arrow[d, phantom, "\substack{\Phi_\ell^A(g_0,j)\\=\\(j-j_0)(j-j_1)}"] & & g_1 \arrow[dl] \arrow[dr] \arrow[d, phantom, "\substack{\Phi_\ell^A(g_1,j)\\=\\(j-j_1)(j-j_2)}"] & & \dots \arrow[dl] \arrow[dr] & \\
j_0 & {} & j_1 & {} & j_2 & & \dots
\end{tikzcd}$$

- Weber-ly, via a lifted chain of invariants $(\mathfrak{f}_0, \dots, \mathfrak{f}_k)$ such that

$$\begin{tikzcd}
\mathfrak{f}_0 \arrow[r, "\Phi_\ell^W(\mathfrak{f}_0{,}\mathfrak{f}_1)=0"] \arrow[d, "\Psi^W(\mathfrak{f}_0{,}j_0)=0"] & \mathfrak{f}_1 \arrow[r, "\Phi_\ell^W(\mathfrak{f}_1{,}\mathfrak{f}_2)=0"] \arrow[d, "\Psi^W(\mathfrak{f}_1{,}j_1)=0"] & \dots \arrow[r, "\Phi_\ell^W(\mathfrak{f}_{k-1}{,}\mathfrak{f}_k)=0"] & \mathfrak{f}_k \arrow[d, "\Psi^W(\mathfrak{f}_k{,}j_k)=0"'] \\
j_0 & j_1 & \dots & j_k
\end{tikzcd}$$

Isogeny PoK: The R1CS-SNARK pipeline

How to obtain a proof of knowledge?

1. Phrase the above equations (stepwise) into a rank-1 constraint system
$$Az \bullet Bz = Cz$$
over a field $\mathbb{F}$
2. Plug this into a R1CS-compatible zk-SNARK, e.g. Aurora or Ligero
3. Profit? Over which field are we working?

Importantly:

Proposition

For $j_0 \in \mathbb{F}_{p^2}$ supersingular, the polynomials
$$\Phi_\ell(j_0, J), \;\; \Phi_\ell^c(T, j_0), \;\; \Phi_\ell^A(Y, j_0), \;\; \Psi^W(F, j_0)$$
all split over $\mathbb{F}_{p^2}$.

Benchmarks for $\ell = 2$

	Φ_2 [CLL23]	Φ_2^c [dH+25]	Φ_2^A (WIP)
Prover time (ms)	934	669	418
Verifier time (ms)	99	74	49
Proof size (kB)	194	178	156

Table: Benchmarks for $\ell = 2$, Aurora

	Φ_2 [CLL23]	Φ_2^c [dH+25]	Φ_2^A (WIP)
Prover time (ms)	587	420	263
Verifier time (ms)	847	634	423
Proof size (kB)	1849	1599	1306

Table: Benchmarks for $\ell = 2$, Ligero

Open questions

- Are these modular polynomials optimal for the proof of knowledge approach?
- Comparison to the radical isogeny formulas for $\ell > 2$
- Can the isogeny characterization of Φ_ℓ over arbitrary fields be proven in a more ‘approachable’ way?
  - Simplifying Igusa’s proof would already be a good starting point

Thank you for your attention!

[CLL23] K. Cong, Y.-F. Lai, and S. Levin. "Efficient Isogeny Proofs Using Generic Techniques". In: *ACNS 2023.*

[Col22] L. Colò. "Oriented supersingular elliptic curves and class group actions". PhD thesis. Aix-Marseille Université, 2022.

[dH+25] T. den Hollander, S. Kleine, M. Mula, D. Slamanig, and S. A. Spindler. "More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials". In: *CRYPTO 2025.*

[DS05] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics 228. Springer, NY, 2005.

[Ler97] R. Lercier. "Algorithmique des courbes elliptiques dans les corps finis". PhD thesis. Ecole Polytechnique, 1997.

Bonus: Weierstrass $\wp$-functions & Eisenstein series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$$

$$\wp'(z;\Lambda) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3}$$

$$G_{2k}(\Lambda) = \sum_{w\in\Lambda\setminus\{0\}} w^{-2k}$$

$g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$

Then

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

and for any curve given by an equation of this form, a suitable Λ exists

Bonus: The orbits of $\Gamma_0(N)$

Proposition ([DS05, Theorem 1.5.1])

For $N \in \mathbb{N}$ we have a bijection

$$\Gamma_0(N)\backslash\mathbb{H} \to S_0(N)$$

induced by

$$\tau \mapsto [E_\tau, \langle \tfrac{1}{N} + \Lambda_\tau \rangle]$$

Bonus: The Dedekind η function

The Dedekind η function is given by

$$\eta(\tau) = e^{\frac{\pi i \tau}{12}} \cdot \prod_{n=1}^{\infty} \left(1 - e^{2n\pi i \tau}\right),$$

and it satisfies

$$\eta(\tau + 1) = e^{\frac{\pi i}{12}} \cdot \eta(\tau) \text{ and } \eta\left(-\tfrac{1}{\tau}\right) = \sqrt{-i\tau} \cdot \eta(\tau)$$

Bonus: The canonical-Atkin transfer

- For $\ell \in \{2, 3, 5, 7, 13\}$ both $X_0(\ell)$ and $X_0^+(\ell)$ have genus 0
- How are $f_\ell(\tau)$ and $g_\ell(\tau)$ related?
- We have $g_\ell(\tau) \in \mathbb{C}(X_0(\ell)) = \mathbb{C}(f_\ell(\tau))$
- Can we find the rational expression explicitly?

Theorem

Let $\ell \in \{2, 3, 5, 7, 13\}$ *and* $s = 12/(\ell - 1)$. *Then*

$$g_\ell(\tau) = \frac{f_\ell(\tau)^2 + 2s \cdot f_\ell(\tau) + \ell^s}{f_\ell(\tau)}$$