# On the Use of Atkin and Weber Modular Polynomials in Isogeny Proofs of Knowledge

Thomas den Hollander[*] Marzio Mula[†] Daniel Slamanig[‡]
Sebastian A. Spindler[§]

Research Institute CODE, Universität der Bundeswehr München

**Abstract**

Zero-knowledge proofs of knowledge of isogenies constitute a key building block in the design of isogeny-based signature schemes and have numerous other practical applications. A recent line of work investigated such proofs based on generic proof systems, e.g., zk-SNARKs, along with a suitable arithmetization and in particular rank-1 constraint systems (R1CS). Cong, Lai and Levin (ACNS'23) considered proving the knowledge of an isogeny of degree $2^k$ between supersingular elliptic curves via modular polynomial relations. Recently, den Hollander et al. (CRYPTO'25) have shown that the use of canonical modular polynomials instead of the classical ones allows to improve on the number of constraints for the same types of isogenies, and further allows to extend this approach to isogenies of higher (though limited) degrees. Another recent work by Levin and Pedersen (ASIACRYPT'25) showed that switching from modular polynomials to radical isogeny formulas also leads to significant improvements (at least for the case of the prime $\ell = 2$).

A natural question that remained open is whether sticking with the modular polynomial-based approach, but switching to other candidates of modular polynomials, and in particular Atkin and Weber polynomials, is possible and gives improvements and flexibility. In this paper we show that the use of the Atkin modular polynomials enables the use of degrees not covered by existing works and improves the number of constraints for $\ell > 2$ by up to 27%, while the Weber polynomials allow up to 39% sparser constraint systems than the current state of the art. As in our prior work on canonical modular polynomials, the adaption of well-known results to the Atkin and Weber modular polynomials also requires some technical work, especially when going to positive characteristic. To this end we expand and optimize our previous resultant-based methodology, resulting in much simpler proofs for our multiplicity theorems.

## 1 Introduction

The use of zero-knowledge proofs of knowledge of a secret isogeny has various applications, ranging from the design of digital signatures [GPS17, BKV19, DKL+20, BBC+25], over the generation of supersingular elliptic curves of unknown endomorphism ring [BCC+23], to various applications in the design of cryptographic protocols and real world deployments (cf. [dHKM+25] for a discussion). Most of these works construct dedicated zero-knowledge proofs via sigma protocols, typically having a small challenge space and thus require a significant number or parallel repetitions (cf. [BDGP23] for a rather recent survey). An alternative approach is to not design a sigma protocol for a certain hard relation, but to rely on alternative possibly more generic proof systems along with suitable representations of isogenies.

In [CSRT22] the authors for the first time deviated from the aforementioned strategy and proposed the use of succinct non-interactive arguments (SNARGs) for isogeny proofs. In particular, they suggested to use a sumcheck protocol based on modular polynomial relations in the 2-isogeny graph. However, due to their focus on verifiable delay functions (VDFs), they did not require knowledge soundness nor the zero-knowledge property, and a practical assessment was left open.

[*]thomasdh@unibw.de [†]marzio.mula@unibw.de [‡]daniel.slamanig@unibw.de [§]s.spindler@unibw.de

This article is the full version (including minor corrections) of the article published as part of the PQCrypto 2026 conference proceedings, which can be found at https://doi.org/10.1007/978-3-032-22698-3_2.

Cong, Lai and Levin [CLL23] then deepened the study of proving modular polynomial relations. Instead of using any tailored (or ad-hoc) proof system, the authors express modular polynomial relations, and in particular the knowledge of an isogeny of degree $2^k$ between supersingular elliptic curves, as a rank-1 constraint system (R1CS). This allows them to rely on existing zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) that support R1CS arithmetization such as Aurora [BCR+19], Ligero [AHIV17] or Limbo [DOT21]. The authors managed to construct a proof system for a NIST-level I instance that runs in just above a second, which for use-cases such as the generation of supersingular elliptic curves of unknown endomorphism ring [BCC+23] significantly improved over the state of the art. These developments in turn motivated further efforts to optimize R1CS constraints, with two concurrent lines of work pursuing different reduction strategies.

In [dHKM+25], the authors propose replacing the classical modular polynomials with canonical modular polynomials, achieving a further decrease in the number of constraints for the same classes of isogenies. They additionally construct constraint systems for higher-degree $\ell$-isogenies with $\ell \in \{3, 5, 7, 13\}$. An alternative direction is taken in [LP25], which replaces the modular polynomial representation altogether by the recently introduced radical isogeny formulas [CD20, CDV20, CDHV22] for $\ell = 2$. These formulas have a particularly simple form and require no auxiliary conditions to prevent backtracking, yielding once again a more efficient proof system.

For completeness, we also note the approach of [MNV24], which arithmetizes isogeny walks via Vélu's formulas and employs the Nova folding scheme [KST22] to recursively aggregate proofs. However, their construction rests on discrete-logarithm assumptions. Adapting it to the post-quantum setting, e.g., relying on [BC25], would require additional lattice-based assumptions for isogeny proofs of knowledge, where such a mix of assumptions seems undesirable.

Given that the use of (canonical) modular polynomials seems to provide the most general setting that does not impose any particular restrictions, a natural question is whether other classes of modular polynomials allow to further improve the arithmetization via R1CS in terms of the constraint system and to extend the list of supported primes $\ell$.

## 1.1 Technical Overview & Our Contributions

We focus on $\ell^n$-isogenies between supersingular elliptic curves over $\mathbb{F}_{p^2}$, represented as sequences of $\ell$-isogenies between $j$-invariants $j_0 \to j_1 \to \cdots \to j_n$.

The reason why R1CS can be effectively used to prove knowledge of $\ell^n$-isogenies is that they can be expressed as 'chains' of solutions of suitable equations: For example, Cong, Lai and Levin [CLL23] use the classical modular polynomial, leveraging the well-known fact that two elliptic curves are $\ell$-isogenous (over a fixed algebraic closure) if and only if their $j$-invariants are roots of the classical modular polynomial $\Phi_\ell$. In this way, one can view an $\ell^n$-isogeny as a chain of solutions $\{(j_i, j_{i+1})\}_{i=0}^{n-1}$ of the equation $\Phi_\ell(J_0, J_1) = 0$.

A natural question is whether other equations can be used to concretely improve the resulting R1CS, especially when working with a slightly larger prime $\ell$ – a question that is affirmatively answered in [dHKM+25], by showing that the use of canonical modular polynomials leads to a 48% improvement over [CLL23].

In this work, we follow a similar footprint as [CLL23, dHKM+25]: We select and study suitable modular equations to encode $\ell^n$-isogenies, optimize them for R1CS, and evaluate the performance of the resulting zk-SNARK. Our goal is to extend the picture of [CLL23, dHKM+25] by considering two more families of modular polynomials.

**Atkin and Weber modular polynomials.** We study Atkin modular polynomials, denoted as $\Phi_\ell^A(Y, J)$, and Weber modular polynomials, denoted as $\Phi_\ell^W(F_0, F_1)$. For both families we provide new proofs for some of their basic features, building on our previous results on canonical modular polynomials in [dHKM+25] and combining resultant theory with tools from the theory of modular functions. In particular, with the Atkin Multiplicity Theorem we illustrate how, for $\ell \leq 31$ or $\ell \in \{41, 47, 59, 71\}$, the $\ell^n$-isogeny relation can be expressed as a chain of solutions $\{(t_i^+, j_i, j_{i+1})\}_{i=0}^{n-1}$ of the system

$$\Phi_\ell^A(Y, J_0) = 0 = \frac{\Phi_\ell^A(Y, J_1) - \Phi_\ell^A(Y, J_0)}{J_1 - J_0},$$

while the Weber Multiplicity Theorem proves that, for $\ell \geq 5$, an $\ell^n$-isogeny can be expressed as a chain of solutions $\{(\mathfrak{f}_i, \mathfrak{f}_{i+1})\}_{i=0}^{n-1}$ of the equation

$$\Phi_\ell^W(F_0, F_1) = 0,$$

with the further constraint that $(\mathfrak{f}_1, j_1)$ and $(\mathfrak{f}_n, j_n)$ satisfy the equation $(F^{24} - 16)^3 - F^{24} \cdot J = 0$. We also confirm that in both cases the chains of solutions always lie in $\mathbb{F}_{p^2}$ when describing a chain of supersingular $j$-invariants. Throughout the paper, we highlight how the modular equations we encounter, as well as the restrictions we impose on the choice of $\ell$, relate to the properties of certain complex modular function fields.

To verify the computational claims on which some of our proofs rely, we provide SageMath scripts in an accompanying GitHub repository[1].

**Automated R1CS optimization.** We generalize some of the optimizations described in our previous work [dHKM+25] and present an algorithm that can perform these and more in a systematic way (cf. Section 5.3). We provide a framework in Rust which is used to describe, optimize and measure the number of constraints, variables and non-zero entries in the R1CS constraint matrices[2]. We expect this framework to be useful for describing and comparing constraint systems consistently, especially in the context of isogeny walks.

# 2 Preliminaries

## 2.1 Resultants

Let $R$ be an integral domain and let $g, h \in R[X]$ be non-zero polynomials. The *resultant* of $g$ and $h$ is an important algebraic tool to detect common divisors between these two polynomials. We state its necessary properties here and give the theoretical background in Appendix A, where we expand upon the results of [dHKM+25, §2.2].

**Proposition 1** ([dHKM+25, Proposition 1])**.** Let $g, h \in R[X]$ be non-zero polynomials, and let $\varphi\colon R \to S$ be a ring homomorphism, extended to a ring homomorphism $\varphi\colon R[X] \to S[X]$ via coefficient-wise application. If $\varphi$ preserves the degrees of $g$ and $h$, then we have

$$\varphi(\mathrm{res}(g, h)) = \mathrm{res}(\varphi(g), \varphi(h)).$$

**Proposition 2.** Let $g, g_1, g_2, h \in R[X]$ be non-zero polynomials over an integral domain $R$, and write $d = \deg(g)$ and $e = \deg(h)$. Then

$$\mathrm{res}(h, g) = (-1)^{d \cdot e} \cdot \mathrm{res}(g, h) \quad \text{and} \quad \mathrm{res}(g_1 g_2, h) = \mathrm{res}(g_1, h) \cdot \mathrm{res}(g_2, h).$$

*Proof.* Lemma 32 and Proposition 36. □

Using the above multiplicativity of the resultant, we can extend our previous resultant technique [dHKM+25, Proposition 2] to also account for roots with higher multiplicity. Additional, this multiplicativity also yields a convenient evaluation property.

**Proposition 3** ([Bos18, Corollary 4.4.9])**.** Let $g, h \in R[X]$ be non-zero polynomials over an integral domain $R$, and suppose that we can factor $g = c \prod_{j=1}^{n} (X - \alpha_i)$ with $c, \alpha_1, \ldots, \alpha_n \in R$. Then

$$\mathrm{res}(g, h) = c^{\deg(h)} \cdot \prod_{i=1}^{n} h(\alpha_i).$$

In particular, $\mathrm{res}(g, h) = 0$ if and only if $g$ and $h$ share a common divisor of positive degree.

*Proof.* Corollary 37. □

[1] https://github.com/QuSAC/IsogenyPoKviaVariousModPolys

[2] https://github.com/QuSAC/isogeny-walk-constraint-counter

**Theorem 4.** *Let $K$ be a field, let $g \in K[X]$ and $h \in K[u, X]$ be non-zero polynomials, and let $u_0 \in K$ such that $\deg_X h(u_0, X) = \deg_X h$. Further write*

$$m = \#\left\{\!\!\left\{ \text{Roots } x \in \overline{K} \text{ of } g \text{ such that } h(u_0, x) = 0 \right\}\!\!\right\}$$

*where the double bracket notation indicates a multiset, i.e. we count each root of $g$ with its multiplicity. Then*

$$\frac{\partial^k}{\partial u^k}\bigg|_{u=u_0} \operatorname{res}_X(g, h) = 0 \text{ for } k \in \{0, \ldots, m-1\}.$$

*Proof.* Theorem 39. □

## 2.2 Elliptic curves

We assume some familiarity with isogenies of elliptic curves and refer to [Sil09] for the main definitions. Throughout, we work over perfect fields $K$ of characteristic $\operatorname{char}(K) \neq \ell$ and consider isogenies of $\ell$-power degree defined over the algebraic closure $\overline{K}$, which are hence always separable. We identify elliptic curves up to isomorphism over $\overline{K}$ – labelling them by their $j$-invariant – and we regard two isogenies as equivalent if they differ by post-composition with an isomorphism. This lets us view an $\ell^n$-isogeny as a chain of $\ell$-isogenies between $j$-invariants, i.e., an *isogeny walk*. When we refer to the *number of non-equivalent $\ell$-isogenies $j_0 \to j_1$*, we are talking about the number of equivalence classes of $\ell$-isogenies from a fixed curve $E_0$ over $\overline{K}$ of $j$-invariant $j_0$ that map to some elliptic curve $E_1$ over $\overline{K}$ of $j$-invariant $j_1$; note that this number does not depend on the choice of representatives.

## 2.3 Modular Curves

We briefly recall the definitions of $X_0(N)$ and $X_0^+(N)$ following [DS05, Chapters 1-2], [Cox13, §11.B], [Elk98, §3], and [CN79, §4].

For any $N \in \mathbb{N}$, we denote by $\Gamma(N)$ the *principal congruence subgroup of level $N$*, i.e. the subgroup of the *modular group* $\mathrm{SL}_2(\mathbb{Z})$ given by

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

A *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that there is an $N \in \mathbb{N}$ with $\Gamma(N) \subseteq \Gamma$, and the minimal such $N$ is called the *level* of $\Gamma$. According to the following result, which covers general properties of the principal congruence subgroups, this minimality can be understood equivalently in terms of size or in terms of divisibility.

**Proposition 5.** For $N \in \mathbb{N}$ the reduction homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N)$ is surjective. In particular, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = \#\mathrm{SL}_2(\mathbb{Z}/N)$. Moreover, for any $M, N \in \mathbb{N}$ we have

$$\Gamma(M) \cap \Gamma(N) = \Gamma(\operatorname{lcm}(M, N)) \quad \text{and} \quad \Gamma(M) \cdot \Gamma(N) = \Gamma(\gcd(M, N)).$$

*Proof.* The fact that the reduction is surjective is well-known (see, for example, [DS05, Exercise 1.2.2]), and the identity $\Gamma(M) \cap \Gamma(N) = \Gamma(\operatorname{lcm}(M, N))$ is immediate from the definitions. Moreover, since $\Gamma(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a normal subgroup, we see that $\Gamma(M) \cdot \Gamma(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that clearly lies inside $\Gamma(\gcd(M, N))$, and by the second group isomorphism theorem and the above identity we have an isomorphism

$$\Gamma(M)/\Gamma(\operatorname{lcm}(M, N)) \cong (\Gamma(M) \cdot \Gamma(N))/\Gamma(N). \tag{1}$$

Now we note that the Chinese remainder theorem gives us a ring isomorphism

$$\mathbb{Z}/\gcd(M, N) \times \mathbb{Z}/\operatorname{lcm}(M, N) \cong \mathbb{Z}/M \times \mathbb{Z}/N$$

via reordering of the prime power factors, and this has two consequences: First, this translates to an isomorphism of the unit groups

$$(\mathbb{Z}/\gcd(M, N))^\times \times (\mathbb{Z}/\operatorname{lcm}(M, N))^\times \cong (\mathbb{Z}/M)^\times \times (\mathbb{Z}/N)^\times.$$

Second, taking matrix rings and then unit groups results in a second group isomorphism

$$\mathrm{GL}_2(\mathbb{Z}/\gcd(M,N)) \times \mathrm{GL}_2(\mathbb{Z}/\operatorname{lcm}(M,N)) \cong \mathrm{GL}_2(\mathbb{Z}/M) \times \mathrm{GL}_2(\mathbb{Z}/N).$$

Due to the short exact sequence

$$0 \to \mathrm{SL}_2(R) \hookrightarrow \mathrm{GL}_2(R) \xrightarrow{\det} R^\times \to 0$$

for any commutative ring $R$, we therefore obtain

$$\#\mathrm{SL}_2(\mathbb{Z}/\gcd(M,N)) \cdot \#\mathrm{SL}_2(\mathbb{Z}/\operatorname{lcm}(M,N)) = \#\mathrm{SL}_2(\mathbb{Z}/M) \cdot \#\mathrm{SL}_2(\mathbb{Z}/N).$$

Finally, rephrasing the above equation in view of the surjectivity of the $\mathrm{SL}_2(\mathbb{Z})$ reduction maps yields

$$\begin{aligned}
[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\gcd(M,N))] &= \#\mathrm{SL}_2(\mathbb{Z}/\gcd(M,N)) \\
&= \frac{\#\mathrm{SL}_2(\mathbb{Z}/M)}{\#\mathrm{SL}_2(\mathbb{Z}/\operatorname{lcm}(M,N))} \cdot \#\mathrm{SL}_2(\mathbb{Z}/N) \\
&= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M)]}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\operatorname{lcm}(M,N))]} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] \\
&= \frac{1}{[\Gamma(M) : \Gamma(\operatorname{lcm}(M,N))]} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] \\
&= \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma(M) \cdot \Gamma(N) : \Gamma(N)]} = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M) \cdot \Gamma(N)]
\end{aligned}$$

where the penultimate step follows from Equation (1). Thus

$$[\Gamma(\gcd(M,N)) : \Gamma(M) \cdot \Gamma(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(M) \cdot \Gamma(N)]}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(\gcd(M,N))]} = 1,$$

i.e. $\Gamma(M) \cdot \Gamma(N) = \Gamma(\gcd(M,N))$ as desired. □

An important example of a level $N$ congruence subgroup is the group

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

The group $\mathrm{SL}_2(\mathbb{Z})$ acts (from the left) on the complex upper half plane $\mathfrak{H}$ via Möbius transformations, which are defined as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d} \quad \text{for } \tau \in \mathfrak{H}.$$

We denote by $Y(1)$ the quotient space $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$, i.e. the set of orbits of $\mathfrak{H}$ under $\mathrm{SL}_2(\mathbb{Z})$. Importantly, the $j$-invariant $j(\tau)\colon \mathfrak{H} \to \mathbb{C}$ is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ and thus induces a function $Y(1) \to \mathbb{C}$. With this, one can prove that $Y(1)$ is in bijection with the *moduli space* of complex elliptic curves up to isomorphism. The compactification of $Y(1)$ is

$$X(1) = Y(1) \cup \mathrm{SL}_2(\mathbb{Z})\backslash(\mathbb{Q} \cup \{\infty\}).$$

Similarly, we denote by $Y_0(N)$ the quotient space $\Gamma_0(N)\backslash\mathfrak{H}$, i.e. the set of orbits of $\mathfrak{H}$ under $\Gamma_0(N)$. One can prove that $Y_0(N)$ is in bijection with the moduli space of $N$-isogenies, that is the set of equivalence classes of pairs $(E, C)$, where $E$ is a complex elliptic curve, $C$ is a cyclic subgroup of $E$ of order $N$, and two pairs $(E, C)$ and $(E', C')$ are equivalent if and only if there is an isomorphism $\varphi\colon E \to E'$ such that $\varphi(C) = C'$. The compactification of $Y_0(N)$ is

$$X_0(N) = Y_0(N) \cup \Gamma_0(N)\backslash(\mathbb{Q} \cup \{\infty\}).$$

Quotients of $\mathfrak{H}$ by subgroups of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some $N$, and their compactifications, are called *modular curves*. In particular, $X(1)$ and $X_0(N)$ are modular curves.

To see how $X_0^+(N)$ is constructed, we consider the *Fricke involution* $\omega_N$ – a special case of an *Atkin–Lehner involution* – given as the Möbius transformation by the matrix

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Importantly, due to the following result this is an involution on $X_0(N)$:

**Lemma 6** ([Mor95, Proposition 2.2]). We have $w_N \Gamma_0(N) w_N^{-1} = \Gamma_0(N)$.

In terms of isogenies, the Fricke involution corresponds to dualization since $j \circ \omega_N(\tau) = j(N\tau)$. Now $X_0^+(N)$ is obtained by quotienting $X_0(N)$ by the Fricke involution $\omega_N$. Equivalently,

$$X_0^+(N) = (\Gamma_0(N) \cup w_N \Gamma_0(N)) \backslash (\mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}),$$

where the above quotient makes sense since, more generally, matrices with positive determinant act on $\mathfrak{H} \cup \mathbb{Q}\{\infty\}$ via Möbius transformations. We stress, however, that this is not a modular curve since $w_n \notin \mathrm{SL}_2(\mathbb{Z})$.

A *modular function* for a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a function $t \colon \mathfrak{H} \cup \{\infty\} \to \mathbb{C}$ which is invariant under $\Gamma$, meromorphic on $\mathfrak{H}$, and meromorphic at the cusps – i.e., for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the Fourier expansion of $t(\gamma\tau)$ has the form $\sum_{n=-m}^{\infty} a(n) e^{2\pi i n \tau}$. Equivalently, a modular function is a rational function on the modular curve $X(\Gamma)$. As for $X_0^+(N)$, we define modular functions as modular functions on $X_0(N)$ that are invariant under the Atkin–Lehner involution $\omega_N$. Note that these correspond to rational functions on $X_0^+(N)$ via precomposition with the quotient map $X_0(N) \to X_0^+(N)$. Hence, for all the curves $X$ we consider, we can canonically identify the field $\mathbb{C}(X)$ of modular functions on $X$ with the function field of $X$ as an algebraic curve – this connection will be crucial for our approach, as it allows us to understand these curves equivalently through their modular functions due to the correspondence between algebraic curves and function fields (cf. [DS05, Theorems 7.2.5-6]). We can give explicit generators for the function fields we will consider:

**Theorem 7.** *Let $N \in \mathbb{N}$. Then*

$$\mathbb{C}(X_0(N)) = \mathbb{C}(j(\tau), j(N\tau)) \text{ and } \mathbb{C}(X_0^+(N)) = \mathbb{C}(j(\tau) + j(N\tau), j(\tau) \cdot j(N\tau)).$$

*In particular, for $N = 1$ we have $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$.*

*Proof.* The first equation is proven in [Mil17, Theorem 6.1]. Further $\omega_N$ swaps $j(\tau)$ and $j(N\tau)$ as $j(\tau)$ is invariant under $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, so $j(\tau) + j(N\tau)$ and $j(\tau) \cdot j(N\tau)$ are invariant under $\omega_N$ and clearly generate a degree 2 subfield of $\mathbb{C}(X_0(N))$ for $N > 1$; as the quotient map $X_0(N) \to X_0^+(N)$ has degree 2 since $\omega_N$ is a non-trivial involution (unless $N = 1$), we obtain the second claim. □

Finally, we recall that the *classical modular polynomial* $\Phi_N(J)$ is defined as the minimal polynomial of $j(N\tau) \in \mathbb{C}(X_0(N))$ over $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$. Explicitly, given representatives $a_0, \ldots, a_k$ of the cosets $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N)$, it can be factored as

$$\Phi_N(J) = \prod_{i=0}^{k} (J - j(N a_i(\tau))). \tag{2}$$

As $\Phi_N(J)$ turns out to have coefficients in $\mathbb{Z}[j(\tau)]$, we can equivalently consider it as a bivariate polynomial $\Phi_N(J_0, J_1) \in \mathbb{Z}[J_0, J_1]$.

For $N = \ell$ prime we see that $j(\ell a_i(\tau))$, $i = 0, \ldots, \ell$, give the $j$-invariants that are $\ell$-isogenous to $j(\tau)$, i.e. for a curve $E_\tau$ of $j$-invariant $j(\tau)$ they give the $j$-invariants of the quotients of $E_\tau$ by order $\ell$ subgroups. This leads to the following result over $\mathbb{C}$, which was extended to positive characteristic by Igusa [Igu59]:

**Classical Multiplicity Theorem.** *Let $\ell$ be a prime and let $K$ be a perfect field with $\mathrm{char}(K) \neq \ell$. Then, for any $j_0, j_1 \in K$, the number of non-equivalent $\ell$-isogenies $j_0 \to j_1$ coincides with the multiplicity of $j_1$ as a root of $\Phi_\ell(j_0, J_1)$.*

# 3 Atkin Modular Polynomials

In this section we focus on the so-called *supersingular primes*, which are the primes $\ell \in \mathbb{N}$ such that $X_0^+(\ell)$ has genus 0. The list of supersingular primes, denoted by $\mathcal{L}$, contains in particular those for which $X_0(\ell)$ has genus 0 or 1 – this follows from the Riemann-Hurwitz formula (see e.g. [Ogg74, Proposition 1]). The complete list, which also includes some primes for which $X_0(\ell)$ has genus greater than 1, was determined by Lehner and Newman [LN64, Theorems 8 and 9]:

$$\mathcal{L} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}.$$

The reason why the genus 0 case is particularly relevant for our application boils down to the existence of a *Hauptmodul* for $X_0^+(\ell)$. We will now recall what this means exactly: Let $X$ be a modular curve, or the quotient of a modular curve by some Atkin–Lehner involution. When $X$ has genus 0, its function field $\mathbb{C}(X)$ is generated by a (unique up to translation) modular function with a unique simple pole of residue 1 at $\infty$. Such a function is called a *Hauptmodul*, and it can be shifted to obtain a (unique) *normalized Hauptmodul*, i.e., a Hauptmodul whose $q$-expansion has constant term 0. A classic example is $X(1)$, for which a (non-normalized) Hauptmodul is the $j$-invariant modular function $j(\tau)$. Another relevant example is $X_0(\ell)$, which has genus 0 if and only if $\ell \in \{2, 3, 5, 7, 13\}$; in this case, a Hauptmodul is

$$t_\ell(\tau) := \left(\frac{\eta(\tau)}{\eta(\ell\tau)}\right)^{2s} \tag{3}$$

where $s = 12/(\ell-1)$ and $\eta(\tau) = e^{\frac{\pi i \tau}{12}} \cdot \prod_{n=1}^{\infty}(1 - e^{2n\pi i\tau})$ is the Dedekind eta function. In particular, for each such $\ell$, the $j$-invariant $j(\tau)$ can be expressed as a rational function of $t_\ell(\tau)$. If we view $X_0(\ell)$ as a moduli space, this means that $t_\ell(\tau)$ parametrizes $\ell$-isogenies and, consequently, one can project $X_0(\ell)$ onto $X(1)$ by mapping each value of $t_\ell(\tau)$ to the $j$-invariant of the domain of the corresponding isogeny. Notably, the Fricke involution identifies an isogeny with its dual. Therefore we do not expect an analogue projection to map a Hauptmodul $t_\ell^+(\tau)$ for $X_0^+(\ell)$ to the $j$-invariant. Indeed, due to $j(\ell\tau) \neq j(\tau)$, $j(\tau)$ does not descend to a function on $X_0^+(\ell)$. Nevertheless, as we will see, $t_\ell^+(\tau)$ identifies a *pair* of $j$-invariants – which are the domains/codomains of the dual pair of isogenies represented by $t_\ell^+(\tau)$.

**Finding the normalized Hauptmodul for $X_0^+(\ell)$.** We will now describe how to obtain explicit generators $t_\ell^+(\tau)$ of $\mathbb{C}(X_0^+(\ell))$ for $\ell \in \mathcal{L}$. When $X_0(\ell)$ has genus 0, a Hauptmodul for $X_0^+(\ell)$ is easily derived from a Hauptmodul of $X_0(\ell)$.

**Proposition 8.** Suppose that $X_0(\ell)$ has genus 0 and let $t_\ell(\tau)$ be as in Equation (3). Then

$$t_\ell^+(\tau) = t_\ell(\tau) + 2s + \ell^s / t_\ell(\tau)$$

is the normalized Hauptmodul for $X_0^+(\ell)$.

*Proof.* By Theorem 7 $\mathbb{C}(X_0(\ell))$ is a degree 2 field extension of $\mathbb{C}(X_0^+(\ell))$ since $j(\tau)$ is not invariant under $\omega_\ell$. Moreover, as an immediate consequence of the properties of $\eta$ [Mü95, Lemma 5.5], we have

$$t_\ell\left(-\frac{1}{\ell\tau}\right) = \frac{\ell^s}{t_\ell(\tau)}, \tag{4}$$

which shows that $t_\ell^+ \circ \omega_\ell(\tau) = t_\ell^+(\tau)$ and therefore $\mathbb{C}(t_\ell^+(\tau)) \subseteq \mathbb{C}(X_0^+(\ell))$. Since

$$t_\ell(\tau)^2 - t_\ell(\tau)(t_\ell^+(\tau) - 2s) + \ell^s = 0,$$

we have that $\mathbb{C}(X_0(\ell))$ is a degree 2 extension of $\mathbb{C}(t_\ell^+(\tau))$, which implies that $t_\ell^+(\tau)$ generates $\mathbb{C}(X_0^+(\ell))$. To conclude, we need to show that $t_\ell^+(\tau)$ is normalized and has a unique pole of order 1 at $\infty$, but this follows immediately from the $q$-expansion

$$t_\ell^+(\tau) = q^{-1} + \textstyle\sum_{n\geq 1} a_n q^n$$

of $t_\ell^+(\tau)$, which can be verified via direct computation using low precision (see also the SageMath script `qExpansions.sage`). □

A harder task is giving explicit formulas for the supersingular primes such that $X_0(\ell)$ has genus $> 0$, i.e. for $\ell \in \mathcal{L} \setminus \{2, 3, 5, 7, 13\}$. A first approach, conjectured in [CN79] and proved in [Bor92, Theorem 1.1], is to use suitable *Thompson series*, whose $q$-expansions are determined by the so-called *head characters* of the *Monster group* (the largest sporadic simple group). Another approach is to use a technique developed by Atkin called *blanchiment*, consisting in combining powers of functions of the form

$$\frac{\sum_{m,n} q^{am^2+bmn+cn^2}}{\eta(\tau)\eta(\ell\tau)}$$

for suitable integers $a, b, c$ to obtain generators of $X_0^+(\ell)$ with small order at $\infty$ (see [Ler97, §3.3.2] and [Mor95, §2.3.1]). A third approach, explored in [CHY07, Table 1], uses combinations of generalized Dedekind eta functions.

For our purposes, it will be sufficient to refer to the former construction. The corresponding $q$-expansions have been pre-computed up to the first hundreds of coefficients by G. C. Greubel on `https://oeis.org/` as the McKay–Thompson series of the class $\ell$A for the Monster group.

**The Atkin modular polynomial.** Fixing $\ell \in \mathcal{L}$, we can now consider the minimal polynomial $\Phi_\ell^A(Y)$ of the normalized Hauptmodul $t_\ell^+(\tau) \in \mathbb{C}(X_0^+(\ell))$ over the field $\mathbb{C}(j(\tau)) = \mathbb{C}(X(1))$, which is called the $\ell^{th}$ *Atkin modular polynomial* as (a variation of) it was originally considered by Atkin [Atk91, §2.2] for the optimization of Schoof's point counting algorithm [Sch85]. Following the presentation of Lercier [Ler97, §3.3.2] and Morain [Mor95, §2.3], we can give its construction more explicitly: The finitely many cosets of $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$ are represented by the matrices

$$a_n = \begin{pmatrix} 0 & -1 \\ 1 & n \end{pmatrix},\ 0 \le n < \ell, \quad \text{and} \quad a_\ell = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and, as $t_\ell^+(\tau)$ generates $\mathbb{C}(X_0(\ell))$ over $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ by Theorem 7, the Atkin modular polynomial is given by

$$\Phi_\ell^A(Y) = \prod_{n=0}^{\ell} \left(Y - t_\ell^+(a_n(\tau))\right) = \left(Y - t_\ell^+(\tau)\right) \prod_{n=0}^{\ell-1} \left(Y - t_\ell^+\left(\frac{-1}{\tau + n}\right)\right).$$

Note that, due to the fact that $t_\ell^+(\tau)$ is a modular function for $\Gamma_0(\ell)$, one can choose any representatives $a_0, \ldots, a_\ell$ of this collection of cosets to factor $\Phi_\ell^A(Y)$.

Moving from the modular interpretation to a more explicit approach, we first describe, for the supersingular primes $\ell \in \mathcal{L}$, the form of the Atkin modular polynomial in more detail. Via direct inspection we can see that $\Phi_\ell^A(Y)$ has coefficients in $\mathbb{Z}[j(\tau)]$, and can thus be considered as a bivariate polynomial $\Phi_\ell^A(Y, j) \in \mathbb{Z}[Y, j]$, which we list in the script `AtkinModularPolys.sage`. These polynomials were computed by Kohel[3]; however, the exact polynomials $\Xi_\ell(Y, j)$ given by Kohel, which are also integrated into SageMath as a database, are not exactly the minimal polynomials of the respective normalized Hauptmoduln. In fact, they are related to the above minimal polynomials via

$$\Xi_\ell(Y, j) = \begin{cases} \Phi_\ell^A(Y, j), & \ell \le 19 \\ \Phi_\ell^A(Y - 1, j), & \ell \ge 23 \end{cases}.$$

For uniformity we stick to our original definition $\Phi_\ell^A(Y, j)$, but we note that all our results, being invariant with respect to integer shifts of the variable $Y$, also apply to the polynomials in Kohel's database.

**Proposition 9.** Let $\ell \in \mathcal{L}$. Then the $\ell^{th}$ Atkin modular polynomial $\Phi_\ell^A(Y, j)$ is of the form

$$\Phi_\ell^A(Y, j) = j^2 - j \cdot \left(Y^\ell + \sum_{i=0}^{\ell-1} a_i Y^i\right) + Y^{\ell+1} + \sum_{i=0}^{\ell} b_i Y^i$$

with integer coefficients $a_i, b_i \in \mathbb{Z}$.

We note that we can also see $\deg_j \Phi_\ell^A(Y, j) = 2$ from the fact that $\mathbb{C}(X_0^+(\ell)) \subseteq \mathbb{C}(X_0(\ell))$ is a degree 2 field extension. With this we can understand the modular picture better:

**Corollary 10.** Let $\ell \in \mathcal{L}$. Then

$$\Phi_\ell^A(t_\ell^+(\tau), j) = (j - j(\tau)) \cdot (j - j(\ell\tau)).$$

*Proof.* By Proposition 9 we know that $\Phi_\ell^A(t_\ell^+(\tau), j)$ is monic of degree 2 in $j$, and by definition it has $j(\tau)$ as a root. Moreover, applying (the action of) $\omega_\ell$ to the expression $\Phi_\ell^A(t_\ell^+(\tau), j(\tau)) = 0$ yields $\Phi_\ell^A(t_\ell^+(\tau), j(\ell\tau)) = 0$ due to the $\omega_\ell$-invariance of $t_\ell^+(\tau)$. Thus $\Phi_\ell^A(t_\ell^+(\tau), j)$ has the two distinct roots $j(\tau)$ and $j(\ell\tau)$, as claimed. □

[3] `https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/atkin_polynomials.html`

To capture the above factorization arithmetically, we will also need the difference quotient polynomial

$$\delta_\ell(Y, J_0, J_1) := \frac{\Phi_\ell^A(Y, J_1) - \Phi_\ell^A(Y, J_0)}{J_1 - J_0} = J_0 + J_1 - \left( Y^\ell + \sum_{i=0}^{\ell-1} a_i Y^i \right).$$

**Corollary 11.** Let $K$ be a field and $j_0, j_1, j_2 \in K$ with $j_1 \neq j_2$. Then, for each $\ell \in \mathcal{L}$,

$$\gcd(\Phi_\ell^A(Y, j_0), \delta_\ell(Y, j_0, j_1), \delta_\ell(Y, j_0, j_2)) = 1.$$

*Proof.* For any $t^+ \in \overline{K}$ the polynomial $\Phi_\ell^A(t^+, j) \in \overline{K}[j]$ can have at most two (not necessarily distinct) roots by Proposition 9; hence, if $t^+$ is a root of $\Phi_\ell^A(Y, j_0)$, then either $j_0$ is a double root of $\Phi_\ell^A(t^+, j)$ or there is a unique $j_1 \in \overline{K}$ with $j_1 \neq j_0$ such that $\Phi_\ell^A(t^+, j_1) = 0$. Stated equivalently, there is a unique $j_1 \in \overline{K}$ such that $t^+$ is a common root of $\Phi_\ell^A(Y, j_0)$ and $\delta_\ell(Y, j_0, j_1)$. □

## 3.1 The Atkin Multiplicity Theorem

Motivated by Corollary 10, we relate the Atkin modular polynomial to the classical modular polynomial via resultant theory.

**Proposition 12.** For any $\ell \in \mathcal{L}$ we have

$$\mathrm{res}_Y(\Phi_\ell^A(Y, J_0), \delta_\ell(Y, J_0, J_1)) = \Phi_\ell(J_0, J_1)$$

where the resultant is computed over the coefficient ring $R = \mathbb{Z}[J_0, J_1]$ of bivariate polynomials.

*Proof.* This can be verified via direct computation (cf. the SageMath script `AtkinModularPolys.sage`). However, as this computation is somewhat expensive, we also give a modular proof : Since $j(\tau)$ is transcendental, we have a ring embedding

$$\varphi\colon \mathbb{Z}[J_0, J_1] \hookrightarrow \mathbb{C}(j(\tau))[J_1],\ J_0 \mapsto j(\tau),$$

and in view of Proposition 1 we get

$$\varphi(\mathrm{res}_Y(\Phi_\ell^A(Y, J_0), \delta_\ell(Y, J_0, J_1))) = \mathrm{res}_Y(\Phi_\ell^A(Y, j(\tau)), \delta_\ell(Y, j(\tau), J_1)).$$

Moreover, $\varphi$ clearly maps the right-hand side of the claimed equation to $\Phi_\ell(j(\tau), J_1)$, and due to the injectivity of $\varphi$ it suffices that this polynomial is equal to the right-hand resultant above.

Now let $a_0, \ldots, a_\ell \in \mathrm{SL}_2(\mathbb{Z})$ be representatives of the left cosets $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$, so that

$$\Phi_\ell^A(Y, j(\tau)) = \prod_{n=0}^{\ell} \big(Y - t_\ell^+(a_n(\tau))\big).$$

In view of Corollary 10, Proposition 3 then yields

$$\begin{aligned}
\mathrm{res}_Y(\Phi_\ell^A(Y, j(\tau)), \delta_\ell(Y, j(\tau), J_1)) &= \prod_{n=0}^{\ell} \delta_\ell(t_\ell^+(a_n(\tau)), j(\tau), J_1) \\
&= \prod_{n=0}^{\ell} \frac{\Phi_\ell^A(t_\ell^+(a_n(\tau)), J_1) - \Phi_\ell^A(t_\ell^+(a_n(\tau)), j(\tau))}{J_1 - j(\tau)} \\
&= \prod_{n=0}^{\ell} \frac{(J_1 - j(a_n(\tau))) \cdot (J_1 - j(\ell a_n(\tau)))}{J_1 - j(\tau)} \\
&= \prod_{n=0}^{\ell} (J_1 - j(\ell a_n(\tau))) = \Phi_\ell(j(\tau), J_1)
\end{aligned}$$

where we applied the $\mathrm{SL}_2(\mathbb{Z})$-invariance of $j(\tau)$ in the penultimate step and Equation (2) in the last step. □

**Remark 1.** Using the invariance $\mathrm{res}_Y(f,g) = \mathrm{res}_Y(f, g-f)$ of the resultant together with the multiplicativity from Proposition 2, one can show that the equation of Proposition 12 is equivalent to

$$\mathrm{res}_Y(\Phi_\ell^A(Y,J_0), \Phi_\ell^A(Y,J_1)) = (J_1 - J_0)^{\ell+1} \cdot \Phi_\ell(J_0,J_1);$$

see also [Haj23, p. 8] for this latter equation, up to a sign error for $\ell = 2$. This highlights why we need to consider the difference quotient as our second equation: If we want to detect loops, i.e. evaluate $J_0$ and $J_1$ at the same $j$-invariant $j_0$, then we need to check whether $\Phi_\ell^A(t^+, j)$ has a double root at $j_0$ for some $t^+$. However, this will not be possible just using the polynomial $\Phi_\ell^A(Y, j_0)$ twice, but we instead also need to consider its $j$-derivative; to elegantly capture this case and the case of two distinct $j$-invariants in the same equation, we thus opt for the difference quotient.

In view of our general result on derivatives of resultants, we can use the above equation to prove a crucial relation between the Atkin modular polynomial and $\ell$-isogenies. We note that a partial version of this result also appears in [Haj23, Proposition 2.9] purely in the language of modular curves.

**Atkin Multiplicity Theorem.** *Let $\ell \in \mathcal{L}$, let $K$ be a field of characteristic $\mathrm{char}(K) \notin [\ell] = \{1, \dots, \ell\}$ and let $j_0, j_1 \in K$. Then the number of (non-equivalent) $\ell$-isogenies $j_0 \to j_1$ is equal to the cardinality of the multiset*

$$\left\{\!\!\left\{ \text{Roots } t^+ \in \overline{K} \text{ of } \Phi_\ell^A(Y,j_0) \text{ such that } \delta_\ell(t^+, j_0, j_1) = 0 \right\}\!\!\right\}.$$

*In particular, $j_0$ and $j_1$ are $\ell$-isogenous if and only if there exists $t^+ \in \overline{K}$ such that*

$$\Phi_\ell^A(t^+, j_0) = 0 = \delta_\ell(t^+, j_0, j_1). \tag{AM}$$

*Proof.* To simplify notation we may assume that $K$ is algebraically closed. For any $j_0, j_1 \in K$ we now write $\chi_\ell(j_0,j_1)$ for the number of roots of $\Phi_\ell^A(Y,j_0)$ (counted with multiplicity) that are roots of $\delta_\ell(Y,j_0,j_1)$, and we write $\nu_\ell(j_0,j_1)$ for the number of non-equivalent $\ell$-isogenies from $j_0$ to $j_1$. Hence our goal is to show that $\chi_\ell(j_0,j_1) = \nu_\ell(j_0,j_1)$; however, it suffices to prove the inequality

$$\chi_\ell(j_0,j_1) \leq \nu_\ell(j_0,j_1) \tag{5}$$

for all $j_0, j_1 \in K$ since summing both quantities over all possible $j_1$ for a fixed $j_0 \in K$ then yields

$$\ell + 1 = \deg_Y(\Phi_\ell^A(Y,j_0)) = \sum_{j_1 \in K} \chi_\ell(j_0,j_1) \leq \sum_{j_1 \in K} \nu_\ell(j_0,j_1) = \ell + 1$$

in view of the Classical Multiplicity Theorem and Corollary 11, so all inequalities will have to be equalities.

To prove the inequality (5) we can use our previous results: Indeed, as $\delta_\ell(Y,J_0,J_1)$ has leading $Y$-coefficient $-1$, Propositions 1 and 12 yield the identity

$$\mathrm{res}_Y(\Phi_\ell^A(Y,j_0), \delta_\ell(Y,j_0,J_1)) = \Phi_\ell(j_0,J_1)$$

in the polynomial ring $K[J_1]$, and applying Theorem 4 to the $K$-linear evaluation $J_1 \mapsto j_1$ shows that for any $k \in \{0, \dots, \chi_\ell(j_0,j_1) - 1\}$ the $k^{th}$ $J_1$-derivative of this resultant vanishes at $J_1 = j_1$. Due to our assumption $\mathrm{char}(K) \notin [\ell]$, this means that $\Phi_\ell(j_0,J_1)$ has a root of multiplicity at least $\chi_\ell(j_0,j_1)$ at $J_1 = j_1$, and inequality (5) follows. □

## 3.2 Atkin Root Computation

Similarly to [dHKM+25, §3], the Atkin Multiplicity Theorem leads us to the question of how to compute the additional invariants $t_1^+, \dots, t_k^+ \in \overline{\mathbb{F}_p}$ for a path

$$j_0 \xrightarrow{t_1^+} j_1 \xrightarrow{t_2^+} \dots \xrightarrow{t_{k-1}^+} j_{k-1} \xrightarrow{t_k^+} j_k$$

of $j$-invariants; to this end we derive a low-degree equation for $t_i^+$ over $\mathbb{F}_p(j_{i-1}, j_i)$.

**Corollary 13.** Let $\ell \in \mathcal{L}$, let $j_0, j_1 \in \overline{\mathbb{F}_p}$ for a prime $p > \ell$, and consider the gcd-polynomial

$$\Lambda_\ell(j_0, j_1) := \gcd(\Phi_\ell^A(Y, j_0), \delta_\ell(Y, j_0, j_1)) \in \mathbb{F}_p(j_0, j_1)[Y].$$

Writing $\nu_\ell(j, j')$ for the number of non-equivalent $\ell$-isogenies $j \to j'$, we then have

$$\deg \Lambda_\ell(j_0, j_1) \leq \min\{\nu_\ell(j_0, j_1), \nu_\ell(j_1, j_0)\}.$$

Moreover:

(a) $\deg \Lambda_\ell(j_0, j_1) \geq 1$ if and only if $j_0$ and $j_1$ are $\ell$-isogenous.

(b) If $j_0$ is ordinary or $p > 4\ell^3$, then $\deg \Lambda_\ell(j_0, j_1) \leq 2$.

*Proof.* From the Atkin Multiplicity Theorem we directly see that $\deg \Lambda_\ell(j_0, j_1)$ is bounded above by $\nu_\ell(j_0, j_1)$ since $\Lambda_\ell(j_0, j_1)$ is a divisor of $\Phi_\ell^A(Y, j_0)$ such that each of its roots is also a root of $\delta_\ell(Y, j_0, j_1)$. Moreover, $\Lambda_\ell$ is symmetric in $(j_0, j_1)$. Indeed, for $j_0 \neq j_1$ we have

$$\begin{aligned}\Lambda_\ell(j_0, j_1) &= \gcd(\Phi_\ell^A(Y, j_0), (j_1 - j_0)\delta_\ell(Y, j_0, j_1)) \\ &= \gcd(\Phi_\ell^A(Y, j_0), \Phi_\ell^A(Y, j_1) - \Phi_\ell^A(Y, j_0)) = \gcd(\Phi_\ell^A(Y, j_0), \Phi_\ell^A(Y, j_1)),\end{aligned}$$

which clearly is symmetric in $(j_0, j_1)$. Together with the prior analysis we therefore obtain the general upper bound on the degree of $\Lambda_\ell(j_0, j_1)$. Furthermore, claim (a) follows immediately from the Atkin Multiplicity Theorem. Finally, suppose that $j_0$ is ordinary or that $p > 4\ell^3$. Then there are at most two non-equivalent $\ell$-isogenies $j_0 \to j_1$ or at most two non-equivalent $\ell$-isogenies $j_1 \to j_0$: In the supersingular case with $p > 4\ell^3$ this follows from [BS25, Corollary 16] for $j_0 \neq 0$ and from [LOX20, Theorem 2(2)] for $j_0 = 0$, and in the ordinary case this follows from the structure of ordinary isogeny volcanoes (cf. [BS25, Corollary 27]), using throughout the asymmetry [BS25, Proposition 4] of isogeny graphs. Therefore our general degree bound yields claim (b). □

Contrary to [dHKM+25, Corollary 2], the inequality in Corollary 13 is generally not an equality, as the following example shows:

**Example 1.** For $\ell = 3$, $p = 13$ and $j_0 = 5$ we have $\Phi_\ell^A(Y, j_0) = (Y - 5)^2 \cdot (Y - 9)^2$ and $\delta_\ell(Y, j_0, j_0) = -(Y - 5) \cdot (Y - 9) \cdot (Y - 12)$. Therefore there are four non-equivalent $\ell$-isogenies $j_0 \to j_0$, double the degree of $\Lambda_\ell(j_0, j_0) = (Y - 5) \cdot (Y - 9)$.

The issue in the above example is that, in contrast to the canonical modular polynomial $\Phi_\ell^c$, the Atkin modular polynomial $\Phi_\ell^A$ can have roots of higher multiplicity even away from the special $j$-invariants 0 and 1728. On the modular side, these additional multi-roots come from the ramification of the quotient map $X_0(\ell) \to X_0^+(\ell)$ at degree $\ell$ endomorphisms that are not equivalent to their dual. This also motivates the following result, which we include for completeness, even though we do not need it in the sequel. We relay its rather long and technical proof to the end of Appendix A.

**Lemma 14.** Let $\ell \in \mathcal{L}$ and let $K$ be a field of characteristic $\mathrm{char}(K) \neq \ell$. Furthermore let $j_0 \in K$ such that $j_0 \notin \{0, 1728\}$ and suppose that $t^+ \in K$ is a double root of $\Phi_\ell^A(Y, j_0)$. Then the following holds:

(a) $t^+$ is not a root of $\Phi_\ell^A(Y, j_1)$ for any $j_1 \in K$ with $j_1 \neq j_0$.

(b) $t^+$ is not a triple root of $\Phi_\ell^A(Y, j_0)$, i.e. its multiplicity as a root is exactly 2.

Additionally, as for the canonical modular polynomial (cf. [dHKM+25, Lemma 3]), the polynomials $\Phi_\ell^A(Y, 0)$ and $\Phi_\ell^A(Y, 1728)$ have specific factorizations:

**Lemma 15.** Let $\ell \in \mathcal{L}$. Then there are integers $t_0^+, t_{1728}^+ \in \mathbb{Z}$ as well as monic non-constant irreducible polynomials $h_0$ and $h_{1728}$ in $\mathbb{Z}[Y]$ such that

$$\Phi_\ell^A(Y, 0) = (Y - t_0^+)^{e_0} \cdot h_0^3 \text{ and } \Phi_\ell^A(Y, 1728) = (Y - t_{1728}^+)^{e_{1728}} \cdot h_{1728}^2,$$

where

$$e_0 = \begin{cases} 1, & \ell = 3 \\ 2, & \ell \equiv 1 \bmod 3 \\ 0, & \ell \equiv 2 \bmod 3 \end{cases} \text{ and } e_{1728} = \begin{cases} 1, & \ell = 2 \\ 2, & \ell \equiv 1 \bmod 4 \\ 0, & \ell \equiv 3 \bmod 4 \end{cases}.$$

Moreover, the following holds for a field $K$ and $j^* \in \{0, 1728\} \subseteq K$:

(a) $\Phi_\ell^A(t_{j^*}^+, j) = (j - j^*)^2$.

(b) If $\mathrm{char}(K) \notin \{2, 3, \ell\}$, then $t_{j^*}^+ \in K$ is not a root of $h_{j^*}$.

(c) If $\mathrm{char}(K) \notin [4\ell]$, then $h_{j^*}$ does not have a double root in $\overline{K}$.

*Proof.* In the SageMath script `AtkinModularPolys.sage` we confirm the factorizations of $\Phi_\ell^A(Y, 0)$ and $\Phi_\ell^A(Y, 1728)$, as well as the additional claims (a) and (b) by evaluation, where we check for claim (b) that $h_{j^*}(t_{j^*}^+)$ only has prime factors in $\{2, 3, \ell\}$. Finally, for claim (c) one confirms computationally that the discriminant $\mathrm{res}(h_{j^*}, \frac{\partial}{\partial Y} h_{j^*})$ of $h_{j^*}$ only has prime divisors in $[4\ell]$; then, as applying $\mathbb{Z} \to K$ coefficient-wise preserves the degrees of $h_{j^*}$ and its derivative, we deduce the claim with Propositions 1 and 3. □

**Remark 2.** Lemma 15(c) can be seen as the analogue of Lemma 14(a) for the special $j$-invariants: Indeed, for $\mathrm{char}(K) \notin [4\ell]$ the loops at $j^* \in \{0, 1728\} \subseteq K$ are exactly given by the root $t_{j^*}^+$ according to the Atkin Multiplicity Theorem and [BS25, Lemma 29]. Therefore any root of $h_{j^*}$ will encode an $\ell$-isogeny to a different $j$-invariant, and the exponents 3 resp. 2 correctly account for the asymmetry in isogeny graphs (cf. [BS25, Proposition 4]); if the target $j$-invariant does not lie in $\{0, 1728\}$, one could thus immediately obtain the claim from Lemma 14(a).

**Remark 3.** To get a gcd-polynomial for which the degree coincides with the minimal number of $\ell$-isogenies between the two $j$-invariants, one can instead consider

$$\begin{cases} \gcd(\Phi_\ell^A(Y, j_0), \Phi_\ell^A(Y, j_1)), & \text{if } j_0 \neq j_1 \\ \gcd(\Phi_\ell^A(Y, j_0), \delta_\ell(Y, j_0, j_0)^2), & \text{if } j_0 = j_1. \end{cases}$$

to account for the reduction of root multiplicities caused by the derivative.

### 3.3 The (Supersingular) Splitting Behavior of $\Phi_\ell^A(Y, j_0)$

To apply the Atkin modular polynomials for a R1CS-based proof of knowledge, we also need to understand the splitting behavior of $\Phi_\ell^A(Y, j_0) \in \mathbb{F}_{p^2}[Y]$ for a supersingular $j$-invariant $j_0 \in \mathbb{F}_{p^2}$. For the small primes $\ell \in \{2, 3, 5, 7, 13\}$ for which $X_0(\ell)$ has genus 0 and for which we understand the splitting behavior of the canonical modular polynomial[4] $\Phi_\ell^c(T, j_0)$ due to Theorem 42, we can transfer Proposition 8 to the case of positive characteristic.

**Proposition 16.** Let $\ell \in \{2, 3, 5, 7, 13\}$, let $K$ be an algebraically closed field with $\mathrm{char}(K) \neq \ell$, write $s = 12/(\ell - 1)$ as before and define on $K^\times$ the rational map

$$\epsilon_\ell \colon K^\times \to K,\ f \mapsto f + 2s + \ell^s / f.$$

Then $\epsilon_\ell$ is invariant with respect to the involution $\iota_\ell \colon K^\times \to K^\times,\ f \mapsto \ell^s / f$ and induces a bijection

$$\overline{\epsilon}_\ell \colon K^\times / \iota_\ell \xrightarrow{\sim} K.$$

Furthermore this rational map $\epsilon_\ell$ satisfies

$$\Phi_\ell^A(\epsilon_\ell(T), j) = (j - \mathcal{J}_\ell(T)) \cdot (j - \mathcal{J}_\ell(\ell^s / T)) \tag{6}$$

where $\mathcal{J}_\ell(T) = \Phi_\ell^c(T, 0)/T$ represents the $j$-invariant in terms of $T$. Thus, for $\overline{\epsilon}_\ell(\{f, \ell^s/f\}) = \epsilon_\ell(f)$, the roots of $\Phi_\ell^A(\epsilon_\ell(f), j)$ are precisely $\{\mathcal{J}_\ell(f), \mathcal{J}_\ell(\ell^s/f)\}$.

*Proof.* It is immediate that $\epsilon_\ell$ is invariant under the involution $\iota_\ell$. Furthermore, for any $a \in K$ we have $\epsilon_\ell(f) = a$ if and only if $f$ satisfies the polynomial equation $T^2 + (2s - a)T + \ell^s = 0$, and from the constant term we deduce that this polynomial factors as $(T - f)(T - \ell^s/f)$ for some $f \in K^\times$ since $K$ is algebraically closed. Altogether, $\epsilon_\ell$ indeed induces the claimed bijection.

[4] We recall the theory of canonical modular polynomials in Appendix B.

Finally, to verify Equation (6), we consider the ring homomorphism

$$\varphi\colon \mathbb{Q}(T)[j] \to \mathbb{C}(t_\ell(\tau))[j],\ T \mapsto t_\ell(\tau),$$

which is an embedding since $t_\ell(\tau)$ is transcendental. In view of Proposition 8 and Corollary 10 we now obtain

$$\begin{aligned}\varphi(\Phi_\ell^A(\epsilon_\ell(T), j)) &= \Phi_\ell^A(\epsilon_\ell(\varphi(T)), j) = \Phi_\ell^A(\epsilon_\ell(t_\ell(\tau)), j)\\ &= \Phi_\ell^A(t_\ell^+(\tau), j) = (j - j(\tau)) \cdot (j - j(\ell\tau))\\ &= (j - \mathcal{J}_\ell(t_\ell(\tau))) \cdot (j - \mathcal{J}_\ell(\ell^s/t_\ell(\tau)))\\ &= \varphi((j - \mathcal{J}_\ell(T)) \cdot (j - \mathcal{J}_\ell(\ell^s/T))),\end{aligned}$$

and the injectivity of $\varphi$ yields the remaining claims. □

With the help of the rational maps $\epsilon_\ell$ and the theory of canonical modular polynomials we can directly derive the following splitting theorem for the Atkin modular polynomials at supersingular $j$-invariants for $\ell \in \{2, 3, 5, 7, 13\}$:

**Corollary 17.** Let $\ell \in \{2, 3, 5, 7, 13\}$, let $p \neq \ell$ be a prime and let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular $j$-invariant. Then $\Phi_\ell^A(Y, j_0)$ splits over $\mathbb{F}_{p^2}$.

*Proof.* Let $t^+ \in \overline{\mathbb{F}_p}$ be a root of $\Phi_\ell^A(Y, j_0)$. By Proposition 16 we then find an element $f \in \overline{\mathbb{F}_p}^\times$ such that $\epsilon_\ell(f) = t^+$ as well as $j_0 \in \{\mathcal{J}_\ell(f), \mathcal{J}_\ell(\ell^s/f)\}$. Switching $f$ for $\ell^s/f$ if necessary, we may assume $j_0 = \mathcal{J}_\ell(f)$, i.e. $\Phi_\ell^c(f, j_0) = 0$. But then Theorem 42 yields $f \in \mathbb{F}_{p^2}$, and we obtain $t^+ = \epsilon_\ell(f) \in \mathbb{F}_{p^2}$. □

To analyze the splitting behavior of the Atkin modular polynomials for all $\ell \in \mathcal{L}$, one would hope to directly adapt the techniques of [dHKM+25, §3.3] (cf. the Canonical Reconstruction Theorem) to arrive at an analogous *Atkin Reconstruction Theorem*. However, this approach runs into multiple computational issues since the Hauptmodul does not determine the $j$-invariant uniquely anymore[5]. For this reason we will turn to a graph-theoretic approach to prove the splitting theorem for supersingular $j$-invariants. First we handle the special $j$-invariants 0 and 1728 separately:

**Proposition 18.** Let $\ell \in \mathcal{L}$, let $p \neq \ell$ be a prime and let $j^* \in \{0, 1728\} \subseteq \mathbb{F}_{p^2}$ be supersingular. Then $\Phi_\ell^A(Y, j^*)$ splits over $\mathbb{F}_{p^2}$.

*Proof.* In the script `AtkinModularPolys.sage` we confirm that the claim holds for $p \leq 4\ell^2$, so we may assume $p > 4\ell^2$. Moreover, in view of Corollary 17 we may assume $\ell > 3$. Now let $t^+ \in \overline{\mathbb{F}_p}$ be a root of $\Phi_\ell^A(Y, j^*)$, and let $j_1 \in \overline{\mathbb{F}_p}$ be the unique $j$-invariant satisfying $\delta_\ell(t^+, j^*, j_1) = 0$ (cf. Corollary 11). Then $j_1$ is $\ell$-isogenous to $j^*$ by the Atkin Multiplicity Theorem, so $j_1 \in \mathbb{F}_{p^2}$ is a supersingular $j$-invariant. Noting that for $j^* = 0$ (resp. $j^* = 1728$) we necessarily have $p \equiv 2 \bmod 3$ (resp. $p \equiv 3 \bmod 4$), we can now use the explicit knowledge of the neighborhood of $j^*$ in the supersingular $\ell$-isogeny graph as discussed in [LOX20]:

- For $j_1 \notin \{0, 1728\}$ there is exactly one $\ell$-isogeny $j_1 \to j^*$ (up to equivalence) by [LOX20, Theorem 2].
- If $\{j^*, j_1\} = \{0, 1728\}$, then there are exactly two non-equivalent $\ell$-isogenies $1728 \to 0$ by [LOX20, Theorem 2].
- If $j^* = j_1$, then there are at most two non-equivalent $\ell$-isogenies $j^* \to j_1$ by [LOX20, Theorem 1].

By Corollary 13 the gcd-polynomial $\Lambda_\ell(j^*, j_1) \in \mathbb{F}_p(j^*, j_1)[Y]$ thus is either a linear polynomial over $\mathbb{F}_{p^2}$ or a polynomial of degree at most two over $\mathbb{F}_p$, so $\Lambda_\ell(j^*, j_1)(t^+) = 0$ gives $t^+ \in \mathbb{F}_{p^2}$. □

[5] Through extensive computations via interpolation one can still obtain formulas for the associated kernel polynomials. We provide these *conjectured* Atkin kernel polynomial formulas, together with a more detailed explanation of their computation, in our GitHub repository for SageMath scripts (`https://github.com/QuSAC/IsogenyPoKviaVariousModPolys/`).

For sufficiently large prime characteristics we can now easily obtain the desired splitting behavior via analysis of the supersingular $\ell$-isogeny graph:

**Theorem 19.** *Let $\ell \in \mathcal{L}$, let $p > 4\ell^4$ be a prime and let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular $j$-invariant. Then $\Phi_\ell^A(Y, j_0)$ splits over $\mathbb{F}_{p^2}$.*

*Proof.* Due to Proposition 1 we may assume $j_0 \notin \{0, 1728\}$. Hence [BS25, Corollaries 16 & 18] show that there is at most one double edge, and otherwise only simple edges, at the vertex $j_0$ in the supersingular $\ell$-isogeny graph. Thus Corollary 13 shows that $\Phi_\ell^A(Y, j_0)$ splits completely over $\mathbb{F}_{p^2}$ except possibly for a single irreducible factor of degree 2. However, via direct inspection one sees that the discriminant of $\Phi_\ell^A(Y, j_0)$ is a square in $\mathbb{F}_{p^2}$ (for $\ell = 2$ due to the fact that $j_0 - 1728 \in \mathbb{F}_{p^2}$ is a square, see [dHKM+25, Corollary 3]), so it cannot have this single irreducible factor of degree 2 by [Gow90, Theorem 1.8], and we obtain our claim. □

**Remark 4.** Due to the fact that $X_0(\ell)$ parametrizes $\ell$-isogenies, which can always be defined over $\mathbb{F}_{p^2}$ for supersingular curves after an appropriate choice of models for the elliptic curves (cf. [AAM19, Theorem 6]), it is certain that the above splitting claim also holds for all smaller characteristics $\ell \neq p < 4\ell^4$ (see also [Col22, Theorem 5.36]); checking this claim manually, however, is computationally infeasible. Alternatively, one could prove it by computing a model for $X_0(\ell)$, explicitly realizing the quotient map $X_0(\ell) \to X_0^+(\ell)$ as a rational map and explicitly associating to a kernel polynomial of an $\ell$-isogeny the correct point on $X_0(\ell)$. As we will only be interested in sufficiently large characteristics for our application due to attacks on path-finding in the supersingular $\ell$-isogeny graph, we omit these computations here. Moreover, as previously mentioned, there are also multiple hurdles when trying to adapt the reconstruction approach pursued in [dHKM+25, §3.3]; this adaption would be very similar to the alternative approach sketched above.

# 4 Weber Modular Polynomials

In [Web98, §125–144] Weber defined a modular function of level 48 – denoted by $\mathfrak{f}$ – for a suitable modular group $\Gamma_W$ of index 72 in $\mathrm{SL}_2(\mathbb{Z})$. His main goal was to study the Hilbert class field, i.e., the maximal unramified abelian extension of imaginary quadratic number fields (see [Bir69] and [Cox13, §12.B]). He noted that, for any CM (i.e., imaginary quadratic) point $\tau$, the element $\mathfrak{f}(\tau)$ generated a small-degree extension of the Hilbert class field of $\mathbb{Q}(\tau)$. Moreover, the minimal polynomial of $\mathfrak{f}(\tau)$ was more compact than that of $j(\tau)$. This feature was further explored in several other works [YZ97, BLS12, LY19, HS22], which assess how 'optimal' the logarithmic height of $\mathfrak{f}(\tau)$ is at CM points.

The intuition that modular equations are in general more compact for $\mathfrak{f}(\tau)$ than they are for $j(\tau)$ led Bröker, Lauter, and Sutherland [BLS12] to construct, for every $\ell \geq 5$, the *Weber modular polynomial* $\Phi_\ell^W(F_0, F_1)$. As we will see in this section, $\Phi_\ell^W$ captures the $\ell$-isogeny relation in the same way as the classical modular polynomials. More precisely, we will prove that a chain of $\ell$-isogenies over a finite field can be viewed as a chain of consecutive roots of $\Phi_\ell^W(F_0, F_1)$. This is already illustrated in [CRSEL+25], leveraging the observation that $\mathfrak{f}$ parametrizes elliptic curves with a level 48 structure. In this way, isogenies between $\mathfrak{f}$-invariants can be interpreted as isogenies between the corresponding $j$-invariants that respect this level structure.

A further reason to consider $\Phi_\ell^W$ in our work is that it enjoys a (heuristically) 72 times smaller logarithmic height and a sparser structure than $\Phi_\ell$. More precisely, the coefficient of $F_0^a F_1^b$ in $\Phi_\ell^W(F_0, F_1)$ can be nonzero only when $\ell a + b \equiv \ell + 1 \bmod 24$ [BLS12, §7.3].

**The Weber modular curve.** We start by introducing the Weber modular function(s):

**Definition 1.** The *Weber modular function* $\mathfrak{f}(\tau)$ is defined by

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

For reference we also define the other Weber modular functions[6]

$$\mathfrak{f}_+(\tau) := \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)} \quad \text{and} \quad \mathfrak{f}_-(\tau) := \frac{\sqrt{2}\eta(2\tau)}{\eta(\tau)}.$$

[6] Historically these functions are denoted $\mathfrak{f}_1(\tau)$ and $\mathfrak{f}_2(\tau)$, respectively, but we switch the notation to avoid confusion with the later notation for roots of the Weber modular polynomial.

These functions satisfy the following cover equations over $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$:

**Lemma 20** ([Cox13, Theorem 12.17 & Corollary 12.19])**.** We have

$$(\mathfrak{f}(\tau)^{24} - 16)^3 - \mathfrak{f}(\tau)^{24} j(\tau) = 0 = (\mathfrak{f}_\pm(\tau)^{24} + 16)^3 - \mathfrak{f}_\pm(\tau)^{24} j(\tau).$$

Furthermore we have

$$\mathfrak{f}(\tau+2) = e^{-2\pi \mathrm{i}/24}\mathfrak{f}(\tau), \quad \mathfrak{f}\left(-\tfrac{1}{\tau}\right) = \mathfrak{f}(\tau) \text{ and } \mathfrak{f}_\pm\left(\tfrac{-1}{\tau}\right) = \mathfrak{f}_\mp(\tau).$$

Throughout this section we will highlight multiple reasons for why we start from the function $\mathfrak{f}(\tau)$ instead of the functions $\mathfrak{f}_\pm(\tau)$; for now, let us describe its corresponding modular curve in more detail:

**Proposition 21.** The invariance subgroup

$$\Gamma_W = \{M \in \mathrm{SL}_2(\mathbb{Z}) \colon \mathfrak{f}(M\tau) = \mathfrak{f}(\tau)\}$$

of the Weber modular function $\mathfrak{f}(\tau)$ is a level 48 congruence subgroup generated by $\Gamma(48)$ and the five matrices

$$\begin{pmatrix} 10 & 103 \\ 13 & 134 \end{pmatrix}, \begin{pmatrix} 13 & 72 \\ 24 & 133 \end{pmatrix}, \begin{pmatrix} -77 & -90 \\ 6 & 7 \end{pmatrix}, \begin{pmatrix} -25 & 14 \\ -34 & 19 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

We refer to $X(\Gamma_W)$ as the *Weber modular curve*.

*Proof.* The fact that $\Gamma_W$ contains $\Gamma(48)$ follows from Lemma 20, though it can also be verified through computation by checking that a (finite) family of generators of $\Gamma(48)$, which can be computed using SageMath, keeps $\mathfrak{f}(\tau)$ invariant. Furthermore one computationally checks that the five matrices given above keep $\mathfrak{f}(\tau)$ invariant as well, e.g. by comparing $q$-expansions. Therefore $\Gamma_W$ at least contains the group $\Gamma'$ we claim it to be equal to, and $\Gamma'$ has index 72 in $\mathrm{SL}_2(\mathbb{Z})$ due to Proposition 5 since the five matrices above generate an index 72 subgroup of $\mathrm{SL}_2(\mathbb{Z}/48)$.

Finally, the equation

$$\Psi^W(F, j) := (F^{24} - 16)^3 - F^{24} \cdot j \in \mathbb{Z}[F, j]$$

is irreducible over $\mathbb{C}(j)$: If we could factor $\Psi^W(F, j) = g \cdot h$ with $g, h \in \mathbb{C}[j][F]$, then we would necessarily have $\deg_j(g) + \deg_j(h) = 1$, i.e. $\Psi^W(F, j) = (a \cdot j + b) \cdot h$ where $a, b, h \in \mathbb{C}[F]$. However, as $(F^{24} - 16)^3$ and $F^{24}$ are coprime in $\mathbb{C}[F]$, this forces $h$ to be a unit. Therefore $\Psi^W(F, j)$ is irreducible as a polynomial over $\mathbb{C}[j]$, and with Gauss's lemma we conclude that it is also irreducible over $\mathbb{C}(j)$. As $j(\tau)$ is transcendental over $\mathbb{C}$, Lemma 20 thus shows that $\Psi^W(F, j(\tau))$ is the minimal polynomial of $\mathfrak{f}(\tau)$ over $\mathbb{C}(j(\tau))$, i.e. $\mathbb{C}(j(\tau)) \subseteq \mathbb{C}(\mathfrak{f}(\tau))$ is a field extension of degree $72 = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_W]$ due to [Col22, Proposition 1.33]. In conclusion, $\Gamma' \subseteq \Gamma_W$ both are index 72 subgroups of $\mathrm{SL}_2(\mathbb{Z})$, and the claim $\Gamma_W = \Gamma'$ follows. □

**Remark 5.** [LMF25, Modular curve 48.72.0.d.1] gives $\mathrm{GL}_2(\mathbb{Z}/48)$ generators of a curve isomorphic to the Weber modular curve $X(\Gamma_W)$. By computing enough words of determinant 1 in these generators and constructively lifting along the reduction $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/48)$, one then obtains a congruence subgroup of level 48 and index 72 in $\mathrm{SL}_2(\mathbb{Z})$. This, however, is not the group $\Gamma_W$; in fact, it is the invariance subgroup of $\mathfrak{f}_-(\tau)$, but from this one can derive the subgroup $\Gamma_W$ via the matrix $S = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$. Indeed, $S^{-1} \cdot \Gamma_W \cdot S$ is the invariance subgroup of $\mathfrak{f}_-(\tau)$ by [Ler97, Proposition 7] since $\mathfrak{f}(S\tau)/\mathfrak{f}_-(\tau)$ is a constant function due to the transformation properties given in [Cox13, Corollary 12.19]. This also shows that (the invariance subgroup of) $\mathfrak{f}_-(\tau)$ has level 48 and not 24 as claimed in [Col22, Proposition 3.57][7], which can also be verified by checking that $\mathfrak{f}_-(\tau)$ is *not* invariant with respect to the matrix $\left(\begin{smallmatrix} 25 & 24 \\ -24 & -23 \end{smallmatrix}\right) \in \Gamma(24)$.

**The Weber modular polynomial.** The following result is the crucial reason why we can use the Weber function $\mathfrak{f}(\tau)$ 'like' the $j$-invariant $j(\tau)$ to construct a modular polynomial for $\ell$-isogenies.

[7] The issue is that $\mathfrak{f}_+(\tau) = \mathfrak{f}_-(S\tau)$ is not invariant under shifts of the argument by multiples of 24.

**Corollary 22.** Let $N \in \mathbb{N}$ with $\gcd(N, 48) = 1$. Then the Weber subgroup $\Gamma_W$ satisfies

$$\Gamma_W \cdot \Gamma_0(N) = \mathrm{SL}_2(\mathbb{Z}),$$

and the inclusion $\Gamma_W \subseteq \mathrm{SL}_2(\mathbb{Z})$ thus induces a bijection

$$\Gamma_W / (\Gamma_W \cap \Gamma_0(N)) \simeq \mathrm{SL}_2(\mathbb{Z}) / \Gamma_0(N).$$

*Proof.* Due to $\Gamma(48) \subseteq \Gamma_W$ and $\Gamma(N) \subseteq \Gamma_0(N)$ we have

$$\mathrm{SL}_2(\mathbb{Z}) \supseteq \Gamma_W \cdot \Gamma_0(N) \supseteq \Gamma(48) \cdot \Gamma(N) = \mathrm{SL}_2(\mathbb{Z})$$

by Proposition 5 since $\gcd(48, N) = 1$. □

Geometrically, the above result states that the modular curve $X(\Gamma_W \cap \Gamma_0(N))$ is the pullback of the two covers $\mathcal{W}\colon X(\Gamma_W) \to X(1)$ and $X_0(N) \to X(1)$, the latter being given by taking the domain $j$-invariant of the isogeny. Equivalently, the function field of the curve $X(\Gamma_W \cap \Gamma_0(N))$ is generated by $\mathfrak{f}(\tau)$ and $j(N\tau)$, noting that $j(\tau)$ is also contained in $\mathbb{C}(\mathfrak{f}(\tau))$.

The following description of the function field grounds the Weber modular polynomial as the analogue of the classical modular polynomial:

**Theorem 23.** *Let $N \in \mathbb{N}$ with $\gcd(N, 48) = 1$. Then we have*

$$\mathbb{C}(X(\Gamma_W \cap \Gamma_0(N))) = \mathbb{C}(\mathfrak{f}(\tau), \mathfrak{f}(N\tau)).$$

*Proof.* This follows analogously to Theorem 7 (see again [Mil17, Theorem 6.1]); note that this uses the fact that $\mathfrak{f}(N\tau) = \omega_N^* \mathfrak{f}(\tau)$ since $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma_W$. □

We now define, for $N \in \mathbb{N}$ coprime to 48, the $N$-th *Weber modular polynomial* $\Phi_N^W(F) \in \mathbb{C}(\mathfrak{f}(\tau))[F]$ to be the minimal polynomial of $\mathfrak{f}(N\tau)$ over $\mathbb{C}(\mathfrak{f}(\tau))$. We collect its properties, noting that the proofs are analogous to the classical case:

**Theorem 24.** *Let $N \in \mathbb{N}$ with $\gcd(N, 48) = 1$. Then the Weber modular polynomial $\Phi_N^W(F)$ has coefficients in $\mathbb{Z}[\mathfrak{f}(\tau)]$ and satisfies*

$$\Phi_N^W(F) = \prod_{i=0}^{k} (F - \mathfrak{f}(Na_i(\tau)))$$

*for any matrices $a_0, \ldots, a_k \in \Gamma_W$ representing the cosets $\Gamma_W / (\Gamma_W \cap \Gamma_0(N))$. Moreover, viewed as a bivariate polynomial $\Phi_N^W(F_0, F_1) \in \mathbb{Z}[F_0, F_1]$, it satisfies the following:*

(a) $\deg_{F_1} \Phi_N^W(F_0, F_1) = \deg_{J_1} \Phi_N(J_0, J_1)$.

(b) *If $N > 1$, then $\Phi_N^W(F_0, F_1) = \Phi_N^W(F_1, F_0)$.*

*Proof.* Due to [Col22, Proposition 1.33] and Corollary 22 we have

$$\deg_F \Phi_N^W(F) = [\Gamma_W : \Gamma_W \cap \Gamma_0(N)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = \deg_J \Phi_N(J),$$

and the product formula for $\Phi_N(F)$ follows directly from the fact that this product is $\Gamma_W$-invariant, monic of the correct degree and has $\mathfrak{f}(N\tau)$ as a root. The fact that $\Phi_N^W(F)$ has coefficients in $\mathbb{Z}[j(\tau)]$ follows via analysis of the $q$-expansion of $\mathfrak{f}(\tau)$ analogously to [Lan87, §5.2] and [Cox13, Theorem 11.18(i)][8], and the symmetry follows from the fact that $\mathfrak{f}(N\tau) = \omega_N^* \mathfrak{f}(\tau)$ due to $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma_W$ (see also [Lan87, Theorem 5.2.3]). □

**Remark 6.** The above highlights the first advantage of the Weber modular function $\mathfrak{f}(\tau)$ over $\mathfrak{f}_\pm(\tau)$: Since $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma_W$, which would not hold for the invariance subgroups of $\mathfrak{f}_\pm(\tau)$ by Lemma 20, we can simply compute $\omega_N^* \mathfrak{f}(\tau)$ as $\mathfrak{f}(N\tau)$.

[8] For our purposes it will be enough to know this for a few small prime degrees $N = \ell$; for $\ell < 5000$ these polynomials can be found on Sutherland's website `https://math.mit.edu/~drew/WeberModPolys.html`.

## 4.1 The Weber Multiplicity Theorem

To simplify formulas, we restrict to primes $N = \ell$ with $\gcd(N, 48) = 1$, i.e. $\ell \geq 5$, from now on. We again use resultant theory to relate the Weber modular polynomial to the classical modular polynomial; our motivation comes from Corollary 22 and Theorem 24, which indicate that $\Phi_\ell^W$ plays the role of the classical modular polynomial for $\mathfrak{f}$-invariants above the $j$-invariants.

**Proposition 25** (Weber resultant equation)**.** Let $\ell \geq 5$ be a prime. Then we have

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

or, equivalently,

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

where $\mathcal{W}(F) = \frac{\left(F^{24}-16\right)^3}{F^{24}}$ defines the cover $\mathcal{W}\colon X(\Gamma_W) \to X(1)$.

*Proof.* Let us first confirm the equivalence of the two equations by proving the equality

$$\operatorname{res}_{J_0}\Big(\Phi_\ell(J_0, J_1), \Psi^W(F_0, J_0)\Big) \overset{!}{=} F_0^{24\cdot(\ell+1)}\Phi_\ell(\mathcal{W}(F_0), J_1).$$

For this we view the polynomials on the left as elements in $\mathbb{Q}(F_0, J_1)[J_0]$ to write

$$\Psi^W(F_0, J_0) = -F_0^{24} \cdot (J_0 - \mathcal{W}(F_0)).$$

Thus Propositions 2 and 3 yield

$$\begin{aligned}
&\operatorname{res}_{J_0}\Big(\Phi_\ell(J_0, J_1), \Psi^W(F_0, J_0)\Big) \\
&\quad= \operatorname{res}_{J_0}\Big(\Psi^W(F_0, J_0), \Phi_\ell(J_0, J_1)\Big) \\
&\quad= \operatorname{res}_{J_0}\Big(-F_0^{24}, \Phi_\ell(J_0, J_1)\Big) \cdot \operatorname{res}_{J_0}(J_0 - \mathcal{W}(F_0), \Phi_\ell(J_0, J_1)) \\
&\quad= (-F_0^{24})^{\deg_{J_0}\Phi_\ell(J_0,J_1)} \cdot \Phi_\ell(\mathcal{W}(F_0), J_1) \\
&\quad= F_0^{24\cdot(\ell+1)}\Phi_\ell(\mathcal{W}(F_0), J_1).
\end{aligned}$$

Hence the two equations are equivalent, and we can prove the second equation instead. As $\mathfrak{f}(\tau)$ is transcendental over $\mathbb{C}$, we have a ring embedding

$$\varphi\colon \mathbb{Z}[F_0, J_1] \hookrightarrow \mathbb{C}(\mathfrak{f}(\tau))[J_1],\ F_0 \mapsto \mathfrak{f}(\tau),$$

and in view of Proposition 1 we get

$$\varphi\Big(\operatorname{res}_{F_1}(\Phi_\ell^W(F_0, F_1), \Psi^W(F_1, J_1))\Big) = \operatorname{res}_{F_1}\Big(\Phi_\ell^W(\mathfrak{f}(\tau), F_1), \Psi^W(F_1, J_1)\Big).$$

Moreover, as we have $\mathcal{W}(\mathfrak{f}(\tau)) = j(\tau)$, $\varphi$ maps the right side of our claimed equation to

$$\varphi\Big(F_0^{24\cdot(\ell+1)} \cdot \Phi_\ell(\mathcal{W}(F_0), J_1)\Big) = \mathfrak{f}(\tau)^{24\cdot(\ell+1)} \cdot \Phi_\ell(j(\tau), J_1),$$

and due to the injectivity of $\varphi$ it suffices to show that the above two expressions on the right coincide.

Now let $a_0, \ldots, a_\ell \in \Gamma_W$ be representatives of the left cosets $\Gamma_W/(\Gamma_W \cap \Gamma_0(\ell))$, so that, as explained in Theorem 24,

$$\Phi_\ell^W(\mathfrak{f}(\tau), F_1) = \prod_{i=0}^{\ell}(F_1 - \mathfrak{f}(\ell a_i(\tau))). \tag{7}$$

Working over the field extension $\mathbb{C}(\mathfrak{f}(\tau))(\mathfrak{f}(\ell a_i(\tau)) \mid i = 0, \ldots, \ell)$ of $\mathbb{C}(\mathfrak{f}(\tau))$, Proposition 3 therefore gives

$$\begin{aligned}
\operatorname{res}_{F_1}\Big(\Phi_\ell^W(\mathfrak{f}(\tau), F_1), \Psi^W(F_1, J_1)\Big) &= \prod_{i=0}^{\ell}\Psi^W(\mathfrak{f}(\ell a_i(\tau)), J_1) \\
&= \prod_{i=0}^{\ell}\Big((\mathfrak{f}(\ell a_i(\tau))^{24} - 16)^3 - \mathfrak{f}(\ell a_i(\tau))^{24} \cdot J_1\Big).
\end{aligned}$$

Crucially, due to Corollary 22 the representatives $a_0, \dots, a_\ell$ also represent the cosets $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$, and hence

$$\Phi_\ell(j(\tau), J_1) = \prod_{i=0}^{\ell} (J_1 - j(\ell a_i(\tau))).$$

In view of $\mathcal{W}(\mathfrak{f}(\ell a_i(\tau))) = j(\ell a_i(\tau))$, we obtain two polynomials of degree $\ell+1$ in $J_1$ with the roots $j(\ell a_i(\tau))$, $i = 0, \dots, \ell$, so these polynomials coincide up to their leading coefficients. Finally, $\Phi_\ell(j(\tau), J_1)$ is clearly monic in $J_1$, whereas the leading coefficient of the above resultant is

$$\prod_{i=0}^{\ell} \left(-\mathfrak{f}(\ell a_i(\tau))^{24}\right) = \Phi_\ell^W(\mathfrak{f}(\tau), 0)^{24}$$

due to the factorization equation (7). In view of the injectivity of $\varphi$, we have altogether thus proved

$$\mathrm{res}_{F_1}(\Phi_\ell^W(F_0, F_1), \Psi^W(F_1, J_1)) = \Phi_\ell^W(F_0, 0)^{24} \cdot \Phi_\ell(\mathcal{W}(F_0), J_1) \tag{8}$$

so far. Finally, suppose for a proof by contradiction that

$$\Phi_\ell^W(F_0, 0) \neq F_0^{\ell+1}.$$

Since $\Phi_\ell^W(F_0, 0)$ is monic of degree $\ell+1$, this means that we can find an $\mathfrak{f} \in \mathbb{C}^\times$ with $\Phi_\ell^W(\mathfrak{f}, 0) = 0$. Now Equation (8) yields

$$\mathrm{res}_{F_1}(\Phi_\ell^W(\mathfrak{f}, F_1), \Psi^W(F_1, J_1)) = 0$$

in view of Proposition 1, using that $\Phi_\ell^W(F_0, F_1)$ is monic in $F_1$. As $\Phi_\ell^W(\mathfrak{f}, F_1)$ has at most $\ell+1$ distinct roots and $\Psi^W(f, J_1)$ has at most one root for any $f \in \mathbb{C}$, we can find a $j \in \mathbb{C}$ such that $\Phi_\ell^W(\mathfrak{f}, F_1)$ and $\Psi^W(F_1, j)$ do not have any common roots. Therefore, as $\Psi^W(F_1, J_1)$ is monic in $F_1$, Propositions 1 and 3 result in the contradiction

$$0 = \mathrm{res}_{F_1}(\Phi_\ell^W(\mathfrak{f}, F_1), \Psi^W(F_1, J_1))(J_1 = j) = \mathrm{res}_{F_1}(\Phi_\ell^W(\mathfrak{f}, F_1), \Psi^W(F_1, j)) \neq 0.$$

We conclude that $\Phi_\ell^W(F_0, 0) = F_0^{\ell+1}$, and Equation (8) finally takes the correct form. □

Using only resultants and the definition of the Weber modular polynomial, we have determined its constant term in the above proof. We highlight this result, also in the language of the Weber $\mathfrak{f}$-function:

**Corollary 26.** Let $\ell \geq 5$ be a prime. Then

$$\Phi_\ell^W(F_0, 0) = F_0^{\ell+1}.$$

Equivalently, for representatives $a_0, \dots, a_\ell$ of the cosets $\Gamma_W/(\Gamma_W \cap \Gamma_0(\ell))$ we have

$$\prod_{i=0}^{\ell} \mathfrak{f}(\ell a_i(\tau)) = \mathfrak{f}(\tau)^{\ell+1}.$$

With our tool for derivatives of resultants, we can now connect the Weber modular polynomial to $\ell$-isogenies:

**Weber Multiplicity Theorem.** *Let $\ell \geq 5$ be a prime, let $K$ be a field with $\mathrm{char}(K) \notin [\ell]$ and let $\mathfrak{f}_0, j_1 \in K$. Then the number of (non-equivalent) $\ell$-isogenies $j_0 := \mathcal{W}(\mathfrak{f}_0) \to j_1$ is equal to the cardinality of the multiset*

$$\left\{\!\!\left\{ \text{Roots } \mathfrak{f}_1 \in \overline{K}^\times \text{ of } \Phi_\ell^W(\mathfrak{f}_0, F_1) \text{ such that } \Psi^W(\mathfrak{f}_1, j_1) = 0 \right\}\!\!\right\}.$$

*In particular, $j_0$ and $j_1$ are $\ell$-isogenous if and only if there exists an $\mathfrak{f}$-invariant above $j_1$ that is $\ell$-isogenous to $\mathfrak{f}_0$, i.e. an $\mathfrak{f}_1 \in \overline{K}^\times$ such that*

$$\mathcal{W}(\mathfrak{f}_1) = \frac{\left(\mathfrak{f}_1^{24} - 16\right)^3}{\mathfrak{f}_1^{24}} = j_1 \quad \text{and} \quad \Phi_\ell^W(\mathfrak{f}_0, \mathfrak{f}_1) = 0. \tag{WM}$$

*Proof.* As both $\Psi^W(F_0, J_0)$ and $\Phi_\ell^W(F_0, F_1)$ are monic in $F_0$, Propositions 1 and 25 yield

$$\mathrm{res}_{F_1}(\Phi_\ell^W(\mathfrak{f}_0, F_1), \Psi^W(F_1, J_1)) = \mathfrak{f}_0^{24\cdot(\ell+1)}\Phi_\ell(\mathcal{W}(\mathfrak{f}_0), J_1).$$

Applying Theorem 4 to the $K$-linear evaluation $J_1 \mapsto j_1$ thus shows that, due to $\mathfrak{f}_0 \neq 0$, the multiplicity of $j_1$ as a root of $\Phi_\ell(j_0, J_1)$ is an upper bound for the number of roots of $\Phi_\ell^W(\mathfrak{f}_0, F_1)$, counted with multiplicity, that also solve $\Psi^W(F_1, j_1) = 0$. Since both $\Phi_\ell^W(\mathfrak{f}_0, F_1)$ and $\Phi_\ell(j_0, J_1)$ have degree $\ell + 1$, we hence obtain the claim as in the proof of the Atkin Multiplicity Theorem. □

**Remark 7.** Note that the above result extends to any congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of level $N$ with Hauptmodul $f(\tau)$ and any $\ell \in \mathbb{N}$ such that $\gcd(\ell, N) = 1$, as long as one only considers cyclic $\ell$-isogenies and the minimal polynomials $\Phi_\ell^\Gamma(f(\tau), F_1) \in \mathbb{C}(f(\tau))[F_1]$ and $\Psi^\Gamma(F, j(\tau)) \in \mathbb{C}(j(\tau))[F]$ have coefficients in $\mathbb{Z}[f(\tau)]$ and $\mathbb{Z}[j(\tau)]$, respectively. However, there are some additional technicalities when $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ does not lie in the subgroup $\Gamma$; see also [Brö06, §6.8].

## 4.2 Weber Root Computation

As in Section 3.2 we take the greatest common divisor of our two equations to find a low-degree equation with which we can lift Weber invariants.

**Corollary 27.** Let $\ell \geq 5$ be a prime, let $\mathfrak{f}_0, j_1 \in \overline{\mathbb{F}_p}$ for a prime $p > \ell$, and consider the gcd-polynomial

$$\Omega_\ell(\mathfrak{f}_0, j_1) \coloneqq \gcd(\Phi_\ell^W(\mathfrak{f}_0, F), \Psi^W(F, j_1)) \in \mathbb{F}_p(\mathfrak{f}_0, j_1)[F].$$

Writing $\nu_\ell(j, j')$ for the number of non-equivalent $\ell$-isogenies $j \to j'$, we then have

$$\deg \Omega_\ell(\mathfrak{f}_0, j_1) \leq \nu_\ell(\mathcal{W}(\mathfrak{f}_0), j_1).$$

Moreover:

(a) $\deg \Omega_\ell(\mathfrak{f}_0, j_1) \geq 1$ if and only if $\mathcal{W}(\mathfrak{f}_0)$ and $j_1$ are $\ell$-isogenous.

(b) If $\mathcal{W}(\mathfrak{f}_0)$ is ordinary or $p > 4\ell^3$, then $\deg \Omega_\ell(\mathfrak{f}_0, j_1) \leq 3$, where the case $\deg \Omega_\ell(\mathfrak{f}_0, j_1) = 3$ can only occur if $\mathcal{W}(\mathfrak{f}_0) = 0$.

*Proof.* As in the proof of Corollary 13, the general inequality and claim (a) follow directly from the Weber Multiplicity Theorem. Moreover, claim (b) follows from [BS25, Corollary 16], [LOX20, Theorem 2(2)] and the structure of ordinary isogeny volcanoes (cf. [BS25, Corollary 27]). □

In contrast to the Atkin modular polynomial, we can get a degree 3 equation even above the bound $p > 4\ell^3$:

**Example 2.** For $p = 509$ and $\ell = 5$ we have $\Phi_5(0, J) = (J - 151)^3 \cdot (J - 191)^3$, $\Psi^W(116, 0) = 0$ and $\Omega_5(116, 191) = F^3 - 118F^2 + 188F + 207$.

Moreover, the modular polynomial can again have multi-roots away from (lifts of) the special $j$-invariants 0 and 1728:

**Example 3.** For $p = 41$ and $\ell = 11$ we have $\Psi^W(8, j) = 4 \cdot (j - 32)$ and $\Phi_{11}^W(8, F)$ has a root of multiplicity 2 at $F = -10$.

As the $\mathfrak{f}$-invariants encode $j$-invariants with additional level structure, the number and occurrence of multi-roots of $\Phi_\ell^W(\mathfrak{f}_0, F_1)$ is limited by the behavior of $\Phi_\ell(\mathcal{W}(\mathfrak{f}_0), J_1)$. Any analysis beyond that is specific to the primes $\ell$ and $p$, but at least we can characterize when $\Psi^W$ has roots of higher multiplicity.

**Proposition 28.** We have

$$\mathrm{disc}_F(\Psi^W(F, j)) = \mathrm{res}_F(\Psi^W(F, j), \tfrac{\partial}{\partial F}\Psi^W(F, j)) = -2^{540} \cdot 3^{72} \cdot (j - 1728)^{24} \cdot j^{48}.$$

In particular, for $j_0 \in \overline{\mathbb{F}_p}$ with $p \geq 5$:

$$\Psi^W(F, j_0) \text{ has multi-roots } \iff j_0 \in \{0, 1728\}.$$

Moreover,

$$\Psi^W(F,0) = (F^6 - 2F^3 + 2)^3 \cdot (F^6 - 2)^3 \cdot (F^6 + 2)^3 \cdot (F^6 + 2F^3 + 2)^3$$

and

$$\Psi^W(F,1728) = (F^8 - 4) \cdot (F^8 - 2F^4 + 4) \cdot (F^8 + 2F^4 + 4) \cdot (F^8 + 2)^2 \cdot (F^{16} - 2F^8 + 4)^2.$$

*Proof.* The claimed discriminant formula is a straightforward resultant computation. Furthermore, as $\Psi^W(F,j)$ is monic in $F$, Proposition 1 shows that we can compute

$$\mathrm{disc}_F(\Psi^W(F,j_0)) = -2^{540} \cdot 3^{72} \cdot (j_0 - 1728)^{24} \cdot j_0^{48}$$

via evaluation of the above formula, and the claim on multi-roots follows from Proposition 3. Finally, the two specific factorizations are also verified easily. □

### 4.3 The (Supersingular) Splitting Behavior of $\Psi^W(F, j_0)$

Since we want to investigate the use of the Weber modular polynomials for R1CS-based proofs of knowledge, we need to study the splitting behavior of $\Psi^W(F, j_0) \in \mathbb{F}_{p^2}[F]$ for a supersingular $j$-invariant $j_0 \in \mathbb{F}_{p^2}$. While [CRSEL+25, §3.5] discusses how to efficiently lift $j_0$ to an $\mathfrak{f}$-invariant, the following theoretical result will be sufficient for us:

**Theorem 29** ([Col22, Theorem 5.38])**.** *Let $p$ be a prime and let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular $j$-invariant. Then $\Psi^W(F, j_0)$ splits over $\mathbb{F}_{p^2}$.*

**Remark 8.** The discussion in [Col22, p. 111] highlights the main reason for the choice of the Weber modular function $\mathfrak{f}(\tau)$ over the other two functions $\mathfrak{f}_\pm(\tau)$: Because of Lemma 20 the 72 roots of $\Phi^{W,j}(F, j(\tau))$ are given by

$$\left\{ e^{2\pi \mathrm{i} \cdot k/24} \mathfrak{f}(\tau), e^{2\pi \mathrm{i} \cdot k/24} e^{\pm 2\pi \mathrm{i}/16} \mathfrak{f}_\pm(\tau) \mid k \in \{0, \ldots, 23\} \right\},$$

i.e. the functions $\mathfrak{f}_\pm(\tau)$ are first shifted by primitive $16^{th}$ roots of unity. Due to this relation and the above result their minimal equation $(F^{24} + 16)^3 - F^{24} j_0$ has a root over $\mathbb{F}_{p^2}$ if and only if $\mathbb{F}_{p^2}$ contains a primitive $16^{th}$ root of unity, which happens if and only if $p \equiv \pm 1 \bmod 8$. In fact, for $p \equiv \pm 3 \bmod 8$ the equation has to split into irreducible quadratic factors since $\mathbb{F}_{p^4}$ contains a primitive $16^{th}$ root of unity.

## 5 Optimizing R1CS-based Isogeny Proofs of Knowledge

### 5.1 Atkin Modular Polynomials

We will now arithmetize the Atkin modular polynomials by converting them into an R1CS. It will be crucial for efficiency that $\Phi_\ell^A(Y, j)$ only has one term linear in $j$ as well as the term $j^2$. Interestingly, we can define four different arithmetization strategies, each with a different domain where it is optimal.

**Lemma 30.** The equations $\Phi_\ell^A(Y, j_0) = \delta_\ell(Y, j_0, j_1) = 0$ can be arithmetized using the following number of constraints:

| $\ell$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 41 | 47 | 59 | 71 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Constraints over $\mathbb{F}_{p^2}$ | 2 | 3 | 5 | 6 | 8 | 9 | 10 | 11 | 11 | 13 | 14 | 16 | 17 | 20 | 23 |
| Constraints over $\mathbb{F}_p$ | 5 | 8 | 12 | 13 | 17 | 20 | 23 | 25 | 24 | 29 | 31 | 36 | 36 | 43 | 48 |

*Proof.* We describe 4 different approaches, all linear in $\ell$, with a decreasing factor at the cost of an increased constant term.

$1^{st}$ *approach.* The first approach is to compute all powers of $Y$ up to $Y^\ell$, in $\ell - 1$ constraints. We can check $\delta_\ell(Y, j_0, j_1) = 0$ with a linear combination without any additional constraints. To compute $\Phi_\ell^A(Y, j_0)$, we can use the fact that

$$\begin{aligned}\Phi_\ell^A(Y, j_0) &= (j_0 - Y)\left(j_0 - \sum_{i=0}^{\ell} a_i Y^i + Y\right) + \sum_{i=0}^{\ell+1} b_i Y^i - \sum_{i=1}^{\ell+1} a_{i-1} Y^i + Y^2 \\ &= -(j_0 - Y)(j_1 - Y) + \sum_{i=1}^{\ell} (b_i - a_{i-1}) Y^i + Y^2 + b_0\end{aligned}$$

where the second equality follows from $\delta_\ell(Y, j_0, j_1) = 0$. Note that the term $Y^{\ell+1}$ term disappears from the sum. The result is a linear combination and a single additional product, using $\ell$ constraints in total for each step.

Working over $\mathbb{F}_p$, we can make use of the fact that even powers can be created using a square, and odd powers can be created through

$$Y^{2a+1} = \frac{1}{2}\left(\left(Y^a + Y^{a+1}\right)^2 - Y^{2a} - Y^{2a+2}\right).$$

Since computing $Y^{2a+1}$ requires knowledge of $Y^{2a+2}$, this approach cannot be used for the highest power if it is odd. This means that over $\mathbb{F}_p$, $\ell = 2$ requires $2\ell + 1$ constraints, while for $\ell \geq 3$, we use $2\ell + 2$ constraints instead, 2 for $\ell - 2$ squares and 3 to compute $Y^\ell$ and $\Phi_\ell^A(Y, j_0)$.

$2^{nd}$ *approach.* Alternatively, the equations from Lemma 15 can be used to arithmetize these constraints more efficiently, by requiring fewer powers of $Y$. In particular,

$$\Phi_\ell^A(Y, j) = j^2 - 1728j + (1 - 1728^{-1}j)\Phi_\ell^A(Y, 0) + 1728^{-1}j\Phi_\ell^A(Y, 1728)$$

and

$$\delta_\ell(Y, j_0, j_1) = j_0 + j_1 - 1728 - 1728^{-1}\Phi_\ell^A(Y, 0) + 1728^{-1}\Phi_\ell^A(Y, 1728).$$

This gives rise to the following equivalent system:

$$\begin{aligned}\begin{bmatrix}0\\0\end{bmatrix} &= \begin{bmatrix}1 & -j_0\\0 & 1\end{bmatrix}\begin{bmatrix}j_0^2 - 1728j_0 & 1 - 1728^{-1}j_0 & 1728^{-1}j_0\\ j_0 + j_1 - 1728 & -1728^{-1} & 1728^{-1}\end{bmatrix}\begin{bmatrix}1\\ \Phi_\ell^A(Y,0)\\ \Phi_\ell^A(Y,1728)\end{bmatrix} \\ &= \begin{bmatrix}-j_0 j_1 & 1 & 0\\ j_0 + j_1 - 1728 & -1728^{-1} & 1728^{-1}\end{bmatrix}\begin{bmatrix}1\\ \Phi_\ell^A(Y,0)\\ \Phi_\ell^A(Y,1728)\end{bmatrix}.\end{aligned}$$

To see that this is true, note that $\left[\begin{smallmatrix}1 & -j_0\\0 & 1\end{smallmatrix}\right]$ is well-defined and invertible.

For arithmetization over $\mathbb{F}_{p^2}$, first compute powers of $Y$ to $\frac{\ell+1}{2}$ (assume $\ell > 2$) in $\frac{\ell-1}{2}$ constraints. We can now use Lemma 15 to compute $\Phi_\ell^A(Y, 1728)$ using a single square. $\Phi_\ell^A(Y, 0)$ can also be created using a square and taking a linear combination, using

$$\sum_{i=0}^{\ell+1} c_i Y^i \quad = \quad \left(\sum_{i=0}^{\frac{\ell+1}{2}} d_i Y^i\right)^2 + \sum_{i=0}^{\frac{\ell+1}{2}-1} e_i Y^i \quad = \quad \sum_{k=0}^{\ell+1}\left(\sum_{i=\max\left(0, k-\frac{\ell+1}{2}\right)}^{\min\left(k, \frac{\ell+1}{2}\right)} d_i d_{k-i}\right) Y^k + \sum_{i=0}^{\frac{\ell+1}{2}-1} e_i Y^i. \quad (9)$$

Here the coefficients $d_0, \ldots, d_{\frac{\ell+1}{2}}$ can be used to create all powers $i \geq \frac{\ell+1}{2}$ with the right coefficient $c_i$, while $e_0, \ldots, e_{\frac{\ell-1}{2}}$ is used to fix the lower values.

Finally, for the first constraint we need to compute the product $j_0 j_1$ while the second constraint can be checked for free in a linear combination when computing $\Phi_\ell^A(Y, 1728)$. In total, this method requires $\frac{\ell+1}{2} + 2$ constraints.

Over $\mathbb{F}_p$, if $\ell \equiv 3 \bmod 4$, the powers $Y^2, \ldots Y^{\frac{\ell+1}{2}}$ can be computed as squares, after which two squares and a product are needed to check the constraints, for $\ell + 6$ constraints in total. For $\ell \equiv 1 \bmod 4$, we need one additional constraint, since computing $Y^{\frac{\ell+1}{2}}$ now requires a product instead of a square, for $\ell + 7$ constraints in total.

$3^{rd}$ *approach.* Continuing, by building the powers up to just $Y^{\lceil \frac{\ell+1}{3} \rceil}$, we need $\left\lceil \frac{\ell+1}{3} \right\rceil - 1$ constraints. If $\ell \equiv 3 \bmod 4$, two squarings are sufficient to compute $\Phi_\ell^A(Y, 1728)$ through the technique of Eq. (9) and then using Lemma 15. If $\ell \equiv 1 \bmod 4$, the method from Eq. (9) cannot be used and a product is necessary instead. The term $\Phi_\ell^A(Y, 0)$ can be computed with a product and a square through Lemma 15, after which another product computes $j_0 j_1$. This process requires $\left\lceil \frac{\ell+1}{3} \right\rceil + 4$ constraints.

Over $\mathbb{F}_p$, if $\ell \equiv 11 \bmod 12$, a square can be used for $Y^{\lceil \frac{\ell+1}{3} \rceil}$, and two squares can be used to build $\Phi_\ell^A(Y, 1728)$, for a total of $2\left\lceil \frac{\ell+1}{3} \right\rceil + 10$ constraints. If $\ell \equiv 5 \bmod 12$ or $\ell \equiv 7 \bmod 12$, we require $2\left\lceil \frac{\ell+1}{3} \right\rceil + 11$ constraints instead, and for other $\ell$, we need $2\left\lceil \frac{\ell+1}{3} \right\rceil + 12$ constraints.

$4^{th}$ *approach.* Finally, we may construct powers up to $Y^{\lceil \frac{\ell+1}{4} \rceil}$. If $\ell \equiv 2 \bmod 3$, we can compute $h_0$ as a square and $\Phi_\ell^A(Y, 0)$ using a square and a product. Otherwise, if $\ell \equiv 1 \bmod 3$, either $h_0$ or $(Y - t_0^+)h_0$ has an even degree, we can use Eq. (9) to build one using a square and use a product for the other. Again a square and a product suffices for $\Phi_\ell^A(Y, 0)$. If $\ell \equiv 3 \bmod 4$, $(Y - t_{1728}^+)^{e_{1728}/2} \cdot h_{1728}$ may be constructed using a square, or using a product if $\ell \equiv 1 \bmod 4$. Like before, we need one additional square for $\Phi_\ell^A(Y, 1728)$ and one product for $j_0 j_1$. This requires $\left\lceil \frac{\ell+1}{4} \right\rceil + 5$ constraints if $\ell \equiv 2 \bmod 3$ and $\left\lceil \frac{\ell+1}{4} \right\rceil + 6$ constraints otherwise.

Over $\mathbb{F}_p$, if $\ell \equiv 7 \bmod 8$, a square can be used for all powers of $Y$ as well as for $(Y - t_{1728}^+)^{e_{1728}/2} \cdot h_{1728}$, and so $2\left\lceil \frac{\ell+1}{4} \right\rceil + 15$ constraints are necessary. If $\ell \equiv 3 \bmod 8$ or $\ell \equiv 5 \bmod 8$, one square becomes a product for $2\left\lceil \frac{\ell+1}{4} \right\rceil + 16$ constraints in total. If $\ell \equiv 1 \bmod 8$, another square becomes a product for $2\left\lceil \frac{\ell+1}{4} \right\rceil + 17$ constraints in total. □

## 5.2 Weber Modular Polynomials

Unlike the Atkin modular polynomials, the Weber modular polynomials do not have a general structure that is easily exploitable to obtain an optimized constraint system. For smaller $\ell$ however, the Weber polynomials are very sparse, leading to similarly sparse constraint matrices. We will therefore focus on these cases.

**Theorem 31.** *A path of length k built from the Weber modular polynomial $\Phi_\ell^W(X, Y)$ for $\ell \in \{5, 7, 11\}$ can be arithmetized in $5k + 3$, $8k + 3$ and $10k + 4$ constraints over $\mathbb{F}_{p^2}$ and $12k + 4$, $19k + 6$ and $24k + 9$ over $\mathbb{F}_p$, respectively.*

*Proof.* We consider $\ell \in \{5, 7, 11\}$ separately:

$\ell = 5$: The Weber modular polynomial for $\ell = 5$ is

$$\Phi_5^W(X, Y) = X^6 + Y^6 - X^5Y^5 + 4XY.$$

Squaring each input twice and then taking a product, we obtain powers $X^2$, $Y^2$, $X^4$, $Y^4$, $X^5$ and $Y^5$ in $2k + 2$ squarings and $1k + 1$ multiplications. We can compute

$$XY = \frac{1}{2}\Big((X + Y)^2 - X^2 - Y^2\Big)$$

using one squaring (or use a product over $\mathbb{F}_{p^2}$) and finish by encoding the polynomial as

$$\Phi_5^W(X, Y) = -(X - Y^5)(Y - X^5) + 5XY = 0.$$

This gives a total of $5k + 3$ constraints over $\mathbb{F}_{p^2}$ and $12k + 7$ over $\mathbb{F}_p$.

$\ell = 7$: The Weber modular polynomial for $\ell = 7$ is

$$\Phi_7^W(X, Y) = X^8 + Y^8 - X^7Y^7 + 7X^4Y^4 - 8XY,$$

and can be arithmetized as follows. First, we build the powers $X^2$, $X^4$ and $X^8$ in $3k + 3$ squarings. We then compute $XY$ and $X^2Y^2$, $X^3Y^3$, $X^4Y^4$ and $X^7Y^7$ in $2k$ squares and $2k$ products. In the last product, the constraint can be tested for free. This takes $8k + 3$ constraints over $\mathbb{F}_{p^2}$ and $19k + 6$ over $\mathbb{F}_p$.

$\underline{\ell = 11}$: Finally, the Weber modular polynomial $\Phi_{11}^W(X, Y)$ is given by

$$X^{12} + Y^{12} - X^{11}Y^{11} + 11X^9Y^9 - 44X^7Y^7 + 88X^5Y^5 - 88X^3Y^3 + 32XY.$$

We first square three times to obtain $X^2$, $X^4$ and $X^8$. From this, $X^{12}$ can be obtained using a product. We do the same for the cross terms, building first $XY$ and then $X^2Y^2$, $X^4Y^4$ and $X^8Y^8$. We can now finish by using two constraints: First we compute $X^2Y^2(X^8Y^8 + 44X^4Y^4)$ and finally we test that

$$0 \quad = \quad X^{12} \; + \; Y^{12} \; + \; 32XY \; + \; XY\Big(-\Big(X^{10}Y^{10} + 44X^6Y^6\Big) + 11X^8Y^8 + 88X^4Y^4 - 88X^2Y^2\Big).$$

This takes $10k + 4$ constraints over $\mathbb{F}_{p^2}$ and $24k + 9$ constraints over $\mathbb{F}_p$. □

### 5.3 Automatic R1CS Non-Zero Entry Optimization

We have created a Rust library[9] to describe the constraint systems provided in this paper and count the number of constraints, variables and non-zero entries. Such a systematic approach is beneficial due the many subtle embedding choices that impact the final R1CS. For example, variables over $\mathbb{F}_{p^2}$ may be embedded into a R1CS using two elements of $\mathbb{F}_p$. A square over $\mathbb{F}_{p^2}$ may then be represented in two constraints, and a product in three. The variable $x \in \mathbb{F}_{p^2}$ itself may be represented as $(a, b)$, with $x = a + b\alpha$ and $\alpha^2$ a non-square residue in $\mathbb{F}_p$, but also as $(a, a + b)$, which in most cases results in sparser constraint matrices.

This optimization is one of the optimizations described in [dHKM+25, §4]. Another is a change of variables: If multiple variables appear often in the same linear combination in the constraint system, it may be beneficial to redefine one of the variables in terms of this linear combination. The representation $(a, a + b)$ may in fact be described as a special case of variable redefinition over the resulting R1CS over $\mathbb{F}_p$, after transforming squares and products over $\mathbb{F}_{p^2}$ into constraints over $\mathbb{F}_p$. Our library captures and generalizes these optimizations.

Formally, a constraint system $(A, B, C)$ can be transformed into an equivalent system $(AV, BV, CV)$ for an invertible matrix $V$. After this, a valid assignment $\vec{a}$ may be transformed into $V^{-1}\vec{a}$, since

$$A\vec{a} \circ B\vec{a} - C\vec{a} = AV(V^{-1}\vec{a}) \circ BV(V^{-1}\vec{a}) - CV(V^{-1}\vec{a}).$$

Minimizing the number of non-zero entries then involves finding an invertible $W = V^T$ such that $W\begin{pmatrix} A^T & B^T & C^T \end{pmatrix}$ has the most zeros.

Instead of considering the full system, we can exploit the repetitive nature of the isogeny path and optimize each step individually, where we should take care to handle repeated variables correctly. To be precise, there are three categories of variables: A single variable representing '1', 'step' variables such as the roots $t_i^+$ that appear only in one step, and 'curve' variables such as the $j$-invariants that appear in two consecutive steps. These should be treated as follows:

- We should always keep the variable representing '1' intact, i.e. the left column and top row of $W$ should consist of a 1 followed by zeros.
- Curve variables may be substituted, but only for linear combinations of '1' and of other variables of the same curve. For example, $j_i \to j_i + 100$ is allowed, while $j_i \to j_i + 100j_{i+1}$ is not, since this would now require us to compensate for $100j_{i+1}$ at index $i - 1$.
- Variables at steps may be substituted for linear combinations of any other variable used in the step. For example, the root $t_i^+$ of $\Phi_\ell^A(Y, j_i)$ and $\Phi_\ell^A(Y, j_{i+1})$ may be substituted for $t_i^+ + j_i + 3j_{i+1} + 50$.

Constructing the matrix $W$ then consists of invertible column operations under the above restrictions. We use two approaches to this problem: First, an exact approach, based on the combinatorial search method from [EM98]. As it finds $W$ in the case where it is unrestricted, we call this algorithm three times on a transformed problem, corresponding to only the step variables, the curve variables and the variable 1, respectively. Since the exact algorithm is too inefficient for large instances, there we use a heuristic approach, where we use pairwise linear combinations of columns to incrementally make the constraint matrices sparser[10].

[9] Available at `https://github.com/QuSAC/isogeny-walk-constraint-counter`.

[10] For more detail on both approaches, see the `Readme.md` file of the Rust library.

# 6 Evaluation

Figure 1 shows the number of constraints required to express an isogeny walk using the different arithmetizations, normalized by dividing by $\log_2(\ell)$ to give the number of constraints per $\lambda$ that is needed for a $k$-step walk such that $\ell^k \geq 2^\lambda$.

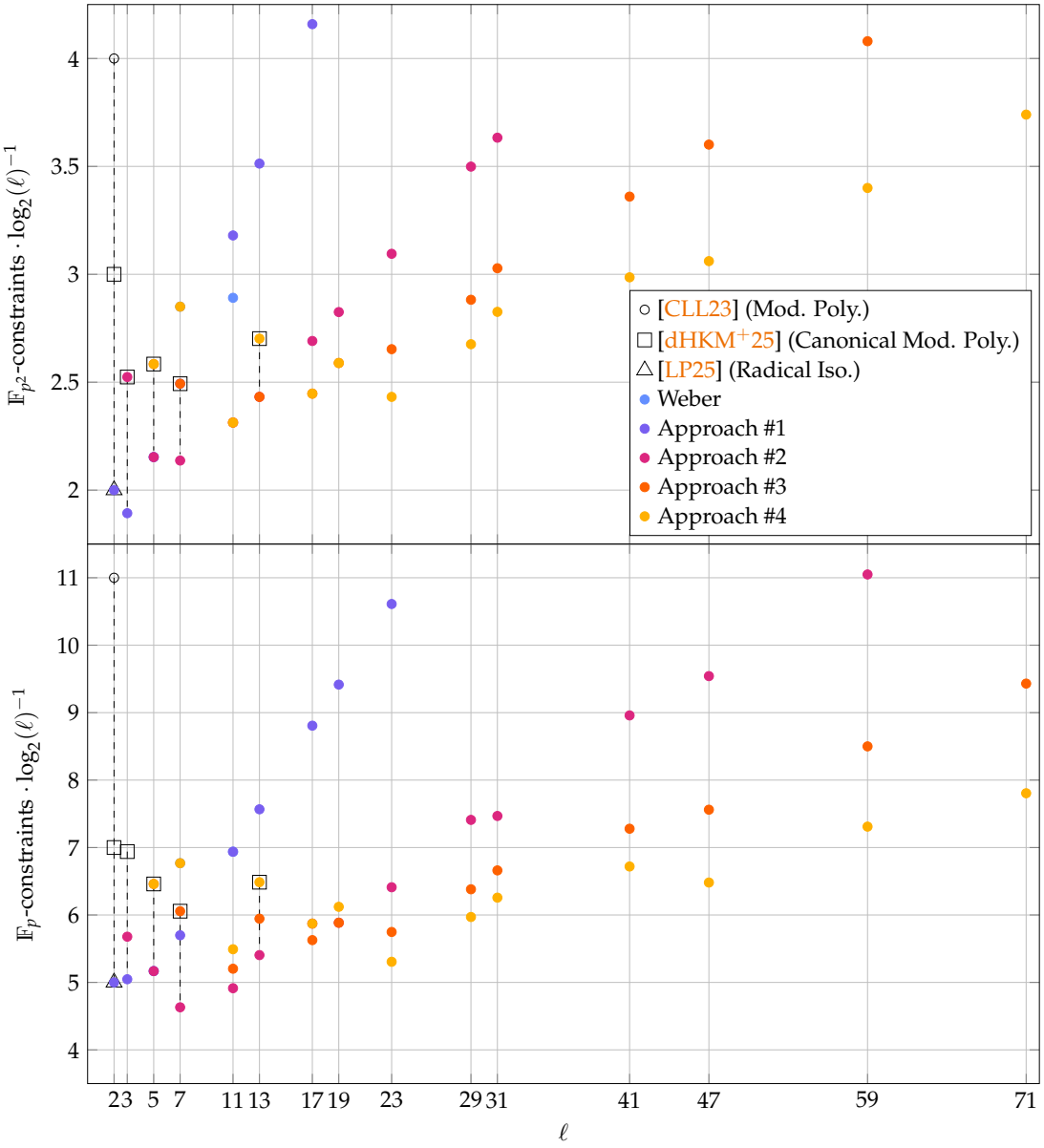



Figure 1: A comparison of the number of constraints for an isogeny of degree $\ell^k$ between [CLL23], [dHKM+25], [LP25], and this work, with $k$ such that $\ell^k \geq 2^\lambda$. The result is divided by $\lambda$. The top plot shows the results for $\mathbb{F}_{p^2}$, and the bottom for $\mathbb{F}_p$.

Table 1 shows the number of necessary constraints in table form, whereas Table 2 shows the number of non-zero entries in the constraint matrices. Because the constraint-minimizing approach may not necessarily be optimal in terms of the non-zero entries, the approach that optimizes the latter is also specified.

We can see that switching to the Atkin and Weber polynomials has a threefold benefit. Firstly, the use of the Atkin polynomials allows for more isogeny degrees $\ell$ than previous approaches, while the Weber modular polynomials even give, in theory, an approach that works for every prime degree $\ell \geq 5$ and that should be more practical than using the classical modular polynomial.

| $\ell$ | $\mathbb{F}_{p^2}$ | | | | | $\mathbb{F}_p$ | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Classical | Canonical | Radical | Atkin | Weber | Classical | Canonical | Radical | Atkin | Weber |
| 2 | $4\lambda+2$ | $3\lambda$ | $2\lambda+2$ | $2\lambda$ (1) | | $11\lambda+7$ | $7\lambda$ | $5\lambda+5$ | $5\lambda$ (1) | |
| 3 | | 2.52$\lambda$ | | 1.89$\lambda$ (1) | | | 6.94$\lambda$ | | 5.05$\lambda$ (1) | |
| 5 | | 2.58$\lambda$ | | 2.15$\lambda$ (1) | $2.15\lambda+3$ | | 6.46$\lambda$ | | 5.17$\lambda$ (2) | $5.17\lambda+7$ |
| 7 | | 2.49$\lambda$ | | 2.14$\lambda$ (2) | $2.85\lambda+3$ | | 6.06$\lambda$ | | 4.63$\lambda$ (2) | $6.77\lambda+6$ |
| 11 | | | | 2.31$\lambda$ (4) | $2.89\lambda+4$ | | | | 4.91$\lambda$ (2) | $6.94\lambda+9$ |
| 13 | | 2.70$\lambda$ | | 2.43$\lambda$ (3) | | | 6.49$\lambda$ | | 5.41$\lambda$ (2) | |
| 17 | | | | 2.45$\lambda$ (4) | | | | | 5.63$\lambda$ (3) | |
| 19 | | | | 2.59$\lambda$ (4) | | | | | 5.89$\lambda$ (3) | |
| 23 | | | | 2.43$\lambda$ (4) | | | | | 5.31$\lambda$ (4) | |
| 29 | | | | 2.68$\lambda$ (4) | | | | | 5.97$\lambda$ (4) | |
| 31 | | | | 2.83$\lambda$ (4) | | | | | 6.26$\lambda$ (4) | |
| 41 | | | | 2.99$\lambda$ (4) | | | | | 6.72$\lambda$ (4) | |
| 47 | | | | 3.06$\lambda$ (4) | | | | | 6.48$\lambda$ (4) | |
| 59 | | | | 3.40$\lambda$ (4) | | | | | 7.31$\lambda$ (4) | |
| 71 | | | | 3.74$\lambda$ (4) | | | | | 7.81$\lambda$ (4) | |

Table 1: The number of constraints required to arithmetize a walk for security level $\lambda$, i.e. a walk such that $\ell^k > 2^\lambda$. We compare the classical [CLL23], canonical [dHKM+25] and radical [LP25] approach to ours. In our approach, the number of variables is always equal to the number of constraints, plus one additional variable in $\mathbb{F}_{p^2}$ or two in $\mathbb{F}_p$. The number in brackets indicates which approach is used.

| $\ell$ | $\mathbb{F}_{p^2}$ | | | | | $\mathbb{F}_p$ | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Classical | Canonical | Radical | Atkin | Weber | Classical | Canonical | Radical | Atkin | Weber |
| 2 | $21\lambda+6$ | $13\lambda$ | $10\lambda+10$ | $12\lambda$ | | $79\lambda+23$ | $41\lambda$ | $36\lambda+36$ | $46\lambda$ | |
| 3 | | 11.36$\lambda$ | | 10.10$\lambda$ | | | 41.01$\lambda$ | | 37.86$\lambda$ | |
| 5 | | 12.06$\lambda$ | | 11.20$\lambda$ | $7.32\lambda+9$ | | 41.78$\lambda$ | | 42.21$\lambda$ | $31.01\lambda+31$ |
| 7 | | 12.47$\lambda$ | | 15.67$\lambda$ | $9.26\lambda+9$ | | 43.81$\lambda$ | | 45.95$\lambda$ | $31.70\lambda+28$ |
| 11 | | | | 11.85$\lambda$ | $10.41\lambda+12$ | | | | 45.95$\lambda$ | $35.27\lambda+40$ |
| 13 | | 15.13$\lambda$ | | 14.59$\lambda$ | | | 52.43$\lambda$ | | 55.67$\lambda$ | |
| 17 | | | | 13.21$\lambda$ | | | | | 52.85$\lambda$ | |
| 19 | | | | 17.19$\lambda$ | | | | | 57.68$\lambda$ | |
| 23 | | | | 16.14$\lambda$ | | | | | 48.41$\lambda$ | |
| 29 | | | | 17.09$\lambda$ | | | | | 53.93$\lambda$ | |
| 31 | | | | 22.00$\lambda$ | | | | | 66.81$\lambda$ | |
| 41 | | | | 19.60$\lambda$ | | | | | 62.34$\lambda$ | |
| 47 | | | | 23.24$\lambda$ | | | | | 69.67$\lambda$ | |
| 59 | | | | 26.01$\lambda$ | | | | | 78.88$\lambda$ | |
| 71 | | | | 30.08$\lambda$ | | | | | 90.25$\lambda$ | |

Table 2: The number of non-zero entries required to arithmetize a walk for security level $\lambda$, i.e. a walk such that $\ell^k > 2^\lambda$. We compare the classical [CLL23], canonical [dHKM+25] and radical [LP25] approach to ours. We use the same approach for the Atkin polynomials as in Table 1. There are three cases where another approach is optimal over $\mathbb{F}_p$: Approach 3 uses 48.37$\lambda$ non-zero entries and 5.95$\lambda$ constraints for $\ell = 13$, and approach 4 uses 43.06$\lambda$ non-zero entries and 5.87$\lambda$ constraints for $\ell = 17$ and 53.44$\lambda$ non-zero entries with 6.12$\lambda$ constraints for $\ell = 19$.

Secondly, the Atkin modular polynomials provide more efficient constraint systems for all $\ell$ for which previous approaches *do* exist, even though for $\ell = 2$ it is asymptotically on par with the radical isogeny approach pursued in [LP25]. The biggest improvement is for $\ell = 3$ over $\mathbb{F}_p$, with a 27% reduction in the number of constraints. Our arithmetizations for $\ell = 3$ over $\mathbb{F}_{p^2}$ and for $\ell \in \{7, 11\}$ over $\mathbb{F}_p$ achieve a lower normalized constraint count than any existing approach and degree, reducing the number of constraints by 5% over the previous best.

The third improvement comes from the use of the Weber polynomials. These allow us to lower the number of non-zero entries by up to 39% in the case of $\ell = 5$ over $\mathbb{F}_{p^2}$. This approach also improves the normalized number of non-zero entries by 27% compared to the radical approach, which was the previous best.

We also note that, while the Weber modular polynomials are competitive in the number of constraints for $\ell = 5$, for increasing $\ell$ this number seems to grow much faster than for the Atkin modular polynomials. Conceptually, this comes from the fact that, being of degree $\ell + 1$ in both of its variables, the Weber modular polynomial has asymptotically $O(\ell)$ times as many monomial terms as the Atkin modular polynomial, even though it is noticeably sparser than the classical modular polynomial. For this reason we expect the Weber modular polynomial to not outperform the Atkin modular polynomial for larger $\ell$.

| | | Aurora | | | Ligero | | |
|---|---|---|---|---|---|---|---|
| | | Classical | Canonical | Ours | Classical | Canonical | Ours |
| $\mathbb{F}_{p^2}$ | Proof time (ms) | 934 | 669 | 418 | 587 | 420 | 263 |
| | Verif. time (ms) | 99 | 74 | 49 | 847 | 634 | 423 |
| | Proof size (kB) | 194 | 178 | 156 | 1849 | 1599 | 1306 |
| $\mathbb{F}_p$ | Proof time (ms) | 1216 | 727 | 495 | 427 | 255 | 174 |
| | Verif. time (ms) | 98 | 62 | 44 | 493 | 313 | 224 |
| | Proof size (kB) | 166 | 147 | 134 | 1733 | 1381 | 1167 |

Table 3: An evaluation of our results compared to the classical [CLL23] and canonical approach [dHKM+25] for walks with $\ell = 2$. The results from $\mathbb{F}_{p^2}$ correspond to the identification protocol with parameter set p434, with path length $k = 216$ and security level $\lambda = 128$, while $\mathbb{F}_p$ corresponds to p441+. The timings and proof sizes are projected based on the number of constraints, from timings in [CLL23] and the methodology of [dHKM+25]. We expect our results for $\ell = 2$ to be on par with [LP25].

All results that perform optimally according to one metric or more can be found in Appendix C. The provided Rust code produces all results.

To give an indication of practical measurements, Table 3 contains the projected prover and verifier time as well as the proof size for a 2-isogeny walk in comparison to prior work.

**Comparison with the radical isogeny formulas.** Let us conclude our evaluation with a more detailed comparison to the radical isogeny approach of [LP25]. A direct translation between the two underlying relations is not as straightforward as one might hope for two reasons. The first is related to the non-backtracking property, and we will discuss the resulting differences during our numerical evaluation below. The second issue is more subtle: Since the model $y^2 = x^3 + Ax^2 + Cx$ in the radical isogeny formulation determines the next 2-isogeny in the $j$-invariant formulation by factoring out the kernel point $(0, 0)$, one cannot publish the coefficients $(A_0, C_0)$ for the appropriate Montgomery model of the starting $j$-invariant $j_0$ without leaking part of the secret.

This leakage can be circumvented in two ways: In the first fix the prover can extend the secret path by an additional step $j_{-1} \to j_0$ such that the two steps $j_{-1} \to j_0 \to j_1$ compose to a cyclic isogeny[11]. Afterwards, the prover computes a Montgomery model $E_{-1} : y^2 = x^3 + A_{-1}x^2 + C_{-1}x$ of $j$-invariant $j_{-1}$ such that the point $(0, 0)$ defines the 2-isogeny giving the chosen step $j_{-1} \to j_0$. With this setup and their secret knowledge, the prover can then compute the radical isogeny path of Montgomery models $E_{-1} \to E_0 \to \cdots \to E_k$ such that $j(E_i) = j_i$, and this will translate to a proof of the $j$-invariant path $j_0 \to \cdots \to j_k$ that does not leak the secret path. For this reason the measurements of the radical isogeny approach provided in Tables 1 and 2 are for proving a radical isogeny path that has one additional step compared to the modular polynomial approaches. We also note that the pre-computation of the additional step $j_{-1} \to j_0$ and the path of Montgomery models is comparable to the pre-computation of the additional roots needed for the translation to our modular polynomial approaches (cf. Sections 3.2, 4.2 and [dHKM+25, §3.2]).

As an alternative solution to the the leakage issue, the prover can publish only the $j$-invariant $j_0$ of the starting curve, and then prove knowledge of an appropriate secret Montgomery model $y^2 = x^3 + A_0x^2 + C_0x$ that is non-singular and of the correct $j$-invariant $j_0$ (in addition to computing and proving the corresponding radical isogeny path of Montgomery models). This solution comes at a larger R1CS overhead than the first fix, requiring an additional 7 constraints and 25 non-zero entries over $\mathbb{F}_{p^2}$ (resp. 18 constraints and 96 non-zero entries over $\mathbb{F}_p$).

Comparing the measurements in Table 1, we see that we achieve the same asymptotic number of constraints for $\ell = 2$ as the radical isogeny formulas. As hinted at earlier, however, our approach does not automatically guarantee that the proven path does not include backtracking edges, whereas the radical isogeny formulas guarantee this property by construction. For our approach, prevention of such backtracking walks can be added at the cost of $\log_\ell(2) \cdot \lambda$ constraints both over $\mathbb{F}_{p^2}$ and over $\mathbb{F}_p$ using the technique of [dHKM+25, §4.4][12]. As the non-backtracking property is desirable in practice due to better mixing properties [ABLS07, BCC+23] and the resulting cyclicity of the composed secret $\ell^k$-isogeny [CFL+19, Corollary 4.5], this additional cost makes our approach slightly less practical than the approach of [LP25], at least for $\ell = 2$.

[11] This is necessary to ensure the applicability of the radical isogeny formulas.

[12] For the same costs, one can alternatively check that any two consecutive roots $t_i^+$ and $t_{i+1}^+$ are distinct. In contrast to the check via $j$-invariants, this allows for paths using parallel double edges, which might be undesirable in practice [LB20, §7].

While radical isogeny formulas are available for primes $\ell \leq 37$ [CDHV22] and conjectured for all odd primes [Dec24], their use for proving knowledge of odd degree isogenies has not been thoroughly explored in the literature yet. We expect them to also be very competitive with our approach for these larger degrees, though for a fair comparison one would need to analyze how much the equation systems coming from these formulas can be optimized.

**Acknowledgements.** We would like to thank Marc Houben for pointing us to the Weber modular polynomials and for several valuable insights. We also thank Eugenio Paracucchi for a helpful preliminary discussion, Shai Levin and Robi Pedersen for helpful discussions on their radical isogeny proof of knowledge, and the anonymous reviewers for their feedback.

# References

[AAM19] Gora Adj, Omran Ahmadi, and Alfred Menezes. On isogeny graphs of supersingular elliptic curves over finite fields. *Finite Fields and Their Applications*, 55:268–283, 2019. 14

[ABLS07] Noga Alon, Itai Benjamini, Eyal Lubetzky, and Sasha Sodin. Non-backtracking random walks mix faster. *Communications in Contemporary Mathematics*, 09(04):585–603, 2007. 26

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017: 24th Conference on Computer and Communications Security*, pages 2087–2104, Dallas, TX, USA, October 31 – November 2, 2017. ACM Press. 2

[Atk91] Arthur Oliver Lonsdale Atkin. The number of points on an elliptic curve modulo a prime, 1991. Email on the Number Theory Mailing List. 8

[BBC+25] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM: Simple and compact identification and signatures from large prime degree isogenies. In Tibor Jager and Jiaxin Pan, editors, *PKC 2025: 28th International Conference on Theory and Practice of Public Key Cryptography, Part III*, volume 15676 of *Lecture Notes in Computer Science*, pages 300–332, Røros, Norway, May 12–15, 2025. Springer, Cham, Switzerland. 1

[BC25] Dan Boneh and Binyi Chen. LatticeFold+: Faster, simpler, shorter lattice-based folding for succinct proof systems. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part VII*, volume 16006 of *Lecture Notes in Computer Science*, pages 327–361, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland. 2

[BCC+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023, Part II*, volume 14005 of *Lecture Notes in Computer Science*, pages 405–437, Lyon, France, April 23–27, 2023. Springer, Cham, Switzerland. 1, 2, 26

[BCR+19] Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, and Nicholas P. Ward. Aurora: Transparent succinct arguments for R1CS. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019, Part I*, volume 11476 of *Lecture Notes in Computer Science*, pages 103–128, Darmstadt, Germany, May 19–23, 2019. Springer, Cham, Switzerland. 2

[BDGP23] Ward Beullens, Luca De Feo, Steven D. Galbraith, and Christophe Petit. Proving knowledge of isogenies: a survey. *Designs, Codes and Cryptography*, 91(11):3425–3456, 2023. 1

[Bir69] Bryan John Birch. Weber's class invariants. *Mathematika*, 16(2):283–294, 1969. 14

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247, Kobe, Japan, December 8–12, 2019. Springer, Cham, Switzerland. 1

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, April 2012. 14

[Bor92] Richard E. Borcherds. Monstrous moonshine and monstrous lie superalgebras. *Inventiones mathematicae*, 109(1):405–444, 1992. 7

[Bos18] Siegfried Bosch. *Algebra. From the Viewpoint of Galois Theory*. Birkhäuser Advanced Texts Basler Lehrbücher. Birkhäuser Cham, 2018. 3, 32, 33, 34

[Brö06] Reinier Bröker. *Constructing elliptic curves of prescribed order*. PhD thesis, Leiden University, 2006. 19

[BS25] Sebastiano Boscardin and Sebastian A. Spindler. Exploring Kaneko's bound: On multiedges, loops and the diameter of the supersingular $\ell$-isogeny graph. Cryptology ePrint Archive, Paper 2025/1361, 2025. 11, 12, 14, 19, 35

[CD20] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 111–129, Paris, France, April 15–17, 2020. Springer, Cham, Switzerland. 2

[CDHV22] Wouter Castryck, Thomas Decru, Marc Houben, and Frederik Vercauteren. Horizontal racewalking using radical isogenies. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022, Part II*, volume 13792 of *Lecture Notes in Computer Science*, pages 67–96, Taipei, Taiwan, December 5–9, 2022. Springer, Cham, Switzerland. 2, 27

[CDV20] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland. 2

[CFL+19] Annamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskás. Ramanujan graphs in cryptography. In Jennifer S. Balakrishnan, Amanda Folsom, Matilde Lalín, and Michelle Manes, editors, *Research Directions in Number Theory. Women in Numbers IV*, volume 19 of *Association for Women in Mathematics Series*, pages 1–40. Springer Cham, 2019. 26

[CHY07] Hung-Jen Chiang-Hsieh and Yifan Yang. Determination of hauptmoduls and construction of abelian extensions of quadratic number fields. *Canadian Mathematical Bulletin*, 50(3):334—346, 2007. 8

[CLL23] Kelong Cong, Yi-Fu Lai, and Shai Levin. Efficient isogeny proofs using generic techniques. In Mehdi Tibouchi and Xiaofeng Wang, editors, *ACNS 2023: 21st International Conference on Applied Cryptography and Network Security, Part II*, volume 13906 of *Lecture Notes in Computer Science*, pages 248–275, Kyoto, Japan, June 19–22, 2023. Springer, Cham, Switzerland. 2, 24, 25, 26, 39

[CN79] J. H. Conway and S. P. Norton. Monstrous moonshine. *Bulletin of the London Mathematical Society*, 11(3):308–339, 1979. 4, 7

[Col22] Leonardo Colò. *Oriented supersingular elliptic curves and class group actions*. PhD thesis, Aix-Marseille Université, 2022. `https://leonardocolo.com/documents/thesis/PhD_Thesis.pdf`. 14, 15, 16, 20

[Cox13] David A. Cox. *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. John Wiley & Sons, 2nd edition, 2013. 4, 14, 15, 16

[CRSEL+25] Maria Corte-Real Santos, Jonathan Komada Eriksen, Antonin Leroux, Michael Meyer, and Lorenz Panny. Evaluation of modular polynomials from supersingular elliptic curves. Cryptology ePrint Archive, Paper 2025/1154, 2025. 14, 20

[CSRT22] Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. Verifiable isogeny walks: Towards an isogeny-based postquantum VDF. In Riham AlTawy and Andreas Hülsing, editors, *SAC 2021: 28th Annual International Workshop on Selected Areas in Cryptography*, volume 13203 of *Lecture Notes in Computer Science*, pages 441–460, Virtual Event, September 29 – October 1, 2022. Springer, Cham, Switzerland. 1

[Dec24] Thomas Decru. Radical $\sqrt[N]{\text{élu}}$ isogeny formulae. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024, Part V*, volume 14924 of *Lecture Notes in Computer Science*, pages 107–128, Santa Barbara, CA, USA, August 18–22, 2024. Springer, Cham, Switzerland. 27

[dHKM+24] Thomas den Hollander, Sören Kleine, Marzio Mula, Daniel Slamanig, and Sebastian A. Spindler. More efficient isogeny proofs of knowledge via canonical modular polynomials. Cryptology ePrint Archive, Paper 2024/1738, 2024. Full ePrint version. 32

[dHKM+25] Thomas den Hollander, Sören Kleine, Marzio Mula, Daniel Slamanig, and Sebastian A. Spindler. More efficient isogeny proofs of knowledge via canonical modular polynomials. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025, Part I*, volume 16000 of *Lecture Notes in Computer Science*, pages 131–166, Santa Barbara, CA, USA, August 17–21, 2025. Springer, Cham, Switzerland. 1, 2, 3, 10, 11, 13, 14, 23, 24, 25, 26, 32, 36, 37, 39

[DKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 64–93, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland. 1

[DOT21] Cyprien Delpech de Saint Guilhem, Emmanuela Orsini, and Titouan Tanguy. Limbo: Efficient zero-knowledge MPCitH-based arguments. In Giovanni Vigna and Elaine Shi, editors, *ACM CCS 2021: 28th Conference on Computer and Communications Security*, pages 3022–3036, Virtual Event, Republic of Korea, November 15–19, 2021. ACM Press. 2

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer New York, NY, 2005. 4, 6

[Elk98] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998. 4

[EM98] S. Egner and T. Minkwitz. Sparsification of rectangular matrices. *Journal of Symbolic Computation*, 26(2):135–149, 1998. 23

[Gow90] Roderick Gow. Some properties and uses of the discriminant of a polynomial. In Ray Ryan, Ted Hurley, and Phil Rippon, editors, *Irish Mathematical Society Bulletin*, volume 24, pages 12–19. Irish Mathematical Society, March 1990. 14

[GPS17] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume

10624 of *Lecture Notes in Computer Science*, pages 3–33, Hong Kong, China, December 3–7, 2017. Springer, Cham, Switzerland. 1

[Haj23] Nadir Hajouji. Supersingular isogeny graphs from algebraic modular curves. arXiV:2303.09096v3 [math.NT], 2023. 10

[HS22] Marc Houben and Marco Streng. Generalized class polynomials. *Research in Number Theory*, 8(4):103, November 2022. 14

[Igu59] Jun-Ichi Igusa. Fibre systems of Jacobian varieties: (III. Fibre systems of elliptic curves). *American Journal of Mathematics*, 81(2):453–476, 1959. 6

[KST22] Abhiram Kothapalli, Srinath Setty, and Ioanna Tzialla. Nova: Recursive zero-knowledge arguments from folding schemes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022, Part IV*, volume 13510 of *Lecture Notes in Computer Science*, pages 359–388, Santa Barbara, CA, USA, August 15–18, 2022. Springer, Cham, Switzerland. 2

[Lan87] Serge Lang. *Elliptic Functions*. Springer New York, New York, NY, 1987. 16

[LB20] Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphisms. In *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Series*, pages 7–22. Mathematical Sciences Publishers, 2020. 26

[Ler97] Reynald Lercier. *Algorithmique des courbes elliptiques dans les corps finis*. PhD thesis, Ecole Polytechnique, June 1997. https://univ-rennes.hal.science/tel-01101949. 8, 15

[LMF25] The LMFDB Collaboration. The L-functions and modular forms database (beta version). https://beta.lmfdb.xyz, 2025. 15

[LN64] J. Lehner and M. Newman. Weierstrass points of $\gamma_0(n)$. *Annals of Mathematics*, 79(2):360–368, 1964. 6

[LOX20] Songsong Li, Yi Ouyang, and Zheng Xu. Neighborhood of the supersingular elliptic curve isogeny graph at $j = 0$ and 1728. *Finite Fields and Their Applications*, 61:101600, 2020. 11, 13, 19

[LP25] Shai Levin and Robi Pedersen. Faster proofs and VRFs from isogenies. In Goichiro Hanaoka and Bo-Yin Yang, editors, *Advances in Cryptology – ASIACRYPT 2025, Part IV*, volume 16248 of *Lecture Notes in Computer Science*, pages 307–340, Melbourne, VIC, Australia, December 8–12, 2025. Springer, Singapore, Singapore. 2, 24, 25, 26, 39

[LY19] Yingkun Li and Tonghai Yang. On a conjecture of Yui and Zagier. *Algebra & Number Theory*, 2019. 14

[Mil17] James Stuart Milne. Modular functions and modular forms (elliptic modular curves). https://www.jmilne.org/math/CourseNotes/MF.pdf, 2017. v1.31. 6, 16

[MNV24] Krystal Maughan, Joseph P. Near, and Christelle Vincent. Foldable, recursive proofs of isogeny computation with reduced time complexity. In Marek Osinski, Brian La Cour, and Lia Yeh, editors, *IEEE International Conference on Quantum Computing and Engineering, QCE 2024, Montreal, QC, Canada, September 15-20, 2024*, pages 1304–1308. IEEE, 2024. 2

[Mor95] François Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques. *Journal de Théorie des Nombres de Bordeaux*, 7(1):255–282, 1995. 6, 8

[Mü95] Volker Müller. *Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei*. PhD thesis, Universität des Saarlandes, 1995. https://publikationen.sulb.uni-saarland.de/handle/20.500.11880/25777. 7, 37

[Ogg74] Andrew P. Ogg. Hyperelliptic modular curves. *Bulletin de la Société Mathématique de France*, 102:449–462, 1974. 6

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Mathematics of Computation*, 44(170):483–494, April 1985. 8

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* Springer New York, NY, 2nd edition, 2009. 4

[Tsu13] Kiminori Tsukazaki. *Explicit isogenies of elliptic curves*. PhD thesis, University of Warwick, July 2013. http://webcat.warwick.ac.uk/record=b2688905~S1.

[vzGG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 3rd edition, 2013. 32

[Web98] Heinrich Weber. *Lehrbuch der Algebra*, volume 3. F. Vieweg und Sohn, Braunschweig, 2nd edition, 1898. Dritter Band: Elliptische Funktionen und algebraische Zahlen. 14

[YZ97] Noriko Yui and Don Zagier. On the singular values of Weber modular functions. *Math. Comput.*, 66(220):1645–1662, October 1997. 14

# A Accounting for Multi-Roots with Resultants

In the following we discuss the theory of *resultants*, with the explicit goal to build on and strengthen [dHKM+25, Proposition 2]. We briefly recall the fundamental notions, but refer to [dHKM+24, Appendix B] as well as to [Bos18, §4.4] and [vzGG13, §6.3] for further information on resultants.

Throughout this section we fix $R$ to be a commutative (as well as unital and associative) ring. For $n \in \mathbb{N}_0$ we consider the free $R$-module

$$\mathcal{P}_n := \{s \in R[X] \colon \deg(s) < n\}$$

of rank $n$, equipped with the *descending monomial basis* $(X^{n-1}, X^{n-2}, \dots, X, 1)$.

**Definition 2.** Let $g, h \in R[X]$ be non-zero polynomials of respective degrees $d, e \in \mathbb{N}_0$ and define the $R$-linear map

$$\sigma \colon \mathcal{P}_e \times \mathcal{P}_d \to \mathcal{P}_{d+e},\ (s,t) \mapsto s \cdot g + t \cdot h.$$

We call the representation matrix of $\sigma$ with respect to the descending monomial bases of each $\mathcal{P}_n$ the *Sylvester matrix* $\mathrm{Syl}(g,h)$ of $g$ and $h$. Further, the *resultant* $\mathrm{res}(g,h)$ of $g$ and $h$ is defined as

$$\mathrm{res}(g,h) := \det \mathrm{Syl}(g,h) \in R.$$

For emphasis we sometimes indicate the variable $X$ with respect to which the resultant is taken in the index of res – for example, we would write $\mathrm{res}_X(g,h)$ above.

The following symmetry of the resultant is immediate via column permutations:

**Lemma 32.** Let $g, h \in R[X]$ be non-zero polynomials of degrees $d, e \in \mathbb{N}_0$. Then

$$\mathrm{res}(h,g) = (-1)^{d \cdot e} \cdot \mathrm{res}(g,h)$$

Additionally, the resultant satisfies a compatibility result that will frequently prove useful:

**Proposition 33** ([dHKM+24, Lemma 16])**.** Let $g, h \in R[X]$ be non-zero polynomials, and let $\varphi \colon R \to S$ be a ring homomorphism, extended to a ring homomorphism $\varphi \colon R[X] \to S[X]$ via coefficient-wise application. If $\varphi$ preserves the degrees of $g$ and $h$, then we have

$$\varphi(\mathrm{Syl}(g,h)) = \mathrm{Syl}(\varphi(g), \varphi(h)),$$

where on the left-hand side $\varphi$ is applied entry-wise. In particular, in this situation we have

$$\varphi(\mathrm{res}(g,h)) = \mathrm{res}(\varphi(g), \varphi(h)).$$

*Proof.* This follows from the definitions and the fact that the determinant is compatible with ring homomorphisms as it is defined as a multivariate polynomial in the entries of the matrix. □

The following technical result is from [dHKM+25, §2.2]; our main goal in this section is to strengthen it for our purposes.

**Proposition 34** ([dHKM+25, Proposition 2])**.** Let $R = K[u]$ be a polynomial ring over a field $K$ and fix an element $u_0 \in K$. Additionally let $g, h \in R[X]$ be non-zero polynomials and extend the $K$-linear evaluation homomorphism $\varphi \colon R \to K$ given by $u \mapsto u_0$ to a ring homomorphism $\varphi \colon R[X] \to K[X]$ via coefficient-wise application. Further suppose that $\varphi$ preserves the $X$-degrees of $g$ and $h$, and write

$$m := \deg \gcd(\varphi(g), \varphi(h)).$$

Then

$$\frac{\partial^k}{\partial u^k}\bigg|_{u=u_0} \mathrm{res}_X(g,h) = 0 \ \text{ for } k \in \{0, \dots, m-1\}.$$

To work towards our goal we will require an alternative characterization of resultants over fields:

**Lemma 35** ([Bos18, Lemma 4.4.5]). Let $K$ be a field and let $g, h \in K[X]$ be non-zero polynomials of degrees $d, e \in \mathbb{N}_0$, respectively. Further let $b_0 \in K$ denote the leading coefficient of $h$, and consider the linear endomorphism $\sigma' \colon \mathcal{P}_{d+e} \to \mathcal{P}_{d+e}$ uniquely defined by the images

$$(hX^{d-1}, \dots, hX, h, X^{e-1}, \dots, X, 1) \mapsto (hX^{d-1}, \dots, hX, h, gX^{e-1}, \dots, gX, g)$$

Then we have

$$\operatorname{res}(h, g) = b_0^d \cdot \det(\sigma').$$

*Proof.* The polynomial $hX^i$ has degree $e + i$, so the polynomials $(hX^{d-1}, \dots, hX, h, X^{e-1}, \dots, X, 1)$ have pairwise distinct degrees and hence define a $K$-basis of $\mathcal{P}_{d+e}$. Furthermore the defining linear map $\sigma$ of $\operatorname{res}(h, g)$ can be expressed as $\sigma = \sigma' \circ \varphi$ with the $K$-linear isomorphism

$$\varphi \colon \mathcal{P}_d \times \mathcal{P}_e \to \mathcal{P}_{d+e},\ (s, t) \mapsto s \cdot h + t$$

that maps the descending monomial bases to the above basis.

Following the definition of the Sylvester matrix and the resultant as its determinant, we thus have to consider the representation matrix (and its determinant) of this $K$-linear isomorphism with respect to the descending monomial bases. This representation matrix is lower triangular with $b_0$ in the first $d$ diagonal entries and 1 in the last $e$ diagonal entries, so its determinant is $b_0^d$ and we obtain the desired description of $\operatorname{res}(h, g)$. □

The above characterization now allows us to deduce multiplicativity of the resultant in each component, at least when working over an integral domain:

**Proposition 36.** Let $R$ be an integral domain. For any non-zero polynomials $g_1, g_2, h \in R[X]$ we then have

$$\operatorname{res}(g_1 g_2, h) = \operatorname{res}(g_1, h) \cdot \operatorname{res}(g_2, h) \quad \text{and} \quad \operatorname{res}(h, g_1 g_2) = \operatorname{res}(h, g_1) \cdot \operatorname{res}(h, g_2).$$

*Proof.* Due to Proposition 33 (applied to the embedding of $R$ into its field of fractions) we may assume that $R = K$ is a field. Now let us write $\deg(g_i) = d_i$, $d = d_1 + d_2$ and $\deg(h) = e$. We first prove the second equation: Consider the linear endomorphisms $\sigma_1'$, $\sigma_2'$ and $\sigma_{12}'$ of Lemma 35 for the polynomials $g_1$, $g_2$ and $g_1 \cdot g_2$. Then the determinant of $\sigma_i'$ coincides with the determinant of the linear map $\mathcal{P}_{d+e} \to \mathcal{P}_{d+e}$ given by

$$(hX^{d-1}, \dots, hX, h, X^{e-1}, \dots, X, 1) \mapsto (hX^{d-1}, \dots, hX, h, g_i X^{e-1}, \dots, g_i X, g_i)$$

for $i \in \{1, 2\}$. Indeed, this endomorphism's representation matrix (with respect to the basis used for the definition above) is a block diagonal matrix consisting of an identity matrix of size $d - d_i$ and the representation matrix of $\sigma_i'$ (again taken with respect to the basis from Lemma 35). As the above linear maps for $i \in \{1, 2\}$ clearly compose to $\sigma_{12}'$, we can hence apply the multiplicativity of the determinant and the formula of Lemma 35 (with $b_0 \in R$ the leading coefficient of $h$) to deduce

$$\operatorname{res}(h, g_1) \cdot \operatorname{res}(h, g_2) = b_0^{d_1} \det(\sigma_1') \cdot b_0^{d_2} \det(\sigma_2') = b_0^{d_1 + d_2} \det(\sigma_{12}') = \operatorname{res}(h, g).$$

Lastly we apply Lemma 32 to obtain the other multiplicativity

$$\begin{aligned} \operatorname{res}(g_1, h) \cdot \operatorname{res}(g_2, h) &= (-1)^{d_1 e + d_2 e} \operatorname{res}(h, g_1) \operatorname{res}(h, g_2) \\ &= (-1)^{(d_1 + d_2) e} \operatorname{res}(h, g_1 g_2) \\ &= (-1)^{(d_1 + d_2) e} (-1)^{de} \operatorname{res}(g_1 g_2, h) = \operatorname{res}(g_1 g_2, h) \end{aligned}$$

as claimed. □

The restriction to integral domains for the above multiplicity result might at first seem unnatural, but it is necessary even when two polynomials do not multiply to zero:

**Example 4.** Consider the coefficient ring $R = \mathbb{Z}/4\mathbb{Z}$ and the two non-zero polynomials $g = 2X + 1$ and $h = 2$ in $R[X]$. Then $g^2 = 1$, so $\operatorname{Syl}(g^2, h)$ is an empty matrix and we obtain $\operatorname{res}(g^2, h) = 1$. However $\operatorname{Syl}(g, h)$ has the single entry 2, i.e. $\operatorname{res}(g, h) = 2$ and thus $\operatorname{res}(g, h)^2 = 0 \neq 1 = \operatorname{res}(g^2, h)$.

The multiplicativity of the resultant also gives a useful evaluation law:

**Corollary 37** ([Bos18, Corollary 4.4.9])**.** Let $g, h \in R[X]$ be non-zero polynomials over an integral domain $R$, and suppose that we can factor $g = c\prod_{j=1}^{n}(X - \alpha_i)$ with $c, \alpha_1, \ldots, \alpha_n \in R$. Then

$$\operatorname{res}(g,h) = c^{\deg(h)} \cdot \prod_{i=1}^{n} h(\alpha_i).$$

In particular, $\operatorname{res}(g,h) = 0$ if and only if $g$ and $h$ share a common divisor of positive degree.

*Proof.* By factoring $h$ over an extension of $R$, e.g. over the algebraic closure of its fraction field, and applying Proposition 33 as well as Proposition 36, the claim immediately reduces to the linear factor case $g = (X - \alpha)$, $h = (X - \beta)$. Here we get

$$\operatorname{Syl}(g,h) = \begin{pmatrix} 1 & 1 \\ -\alpha & -\beta \end{pmatrix},$$

so $\operatorname{res}(g,h) = -\beta + \alpha = h(\alpha)$ as desired. □

As the final preparatory step, we extract one part of the upcoming proof that immediately follows from the product rule:

**Lemma 38.** Let $R = A[u]$ be a polynomial ring, let $s, t \in R$, let $u_0 \in A$ and let $m, n \in \mathbb{N}_0$ such that

$$\left.\frac{\partial^i}{\partial u^i}\right|_{u=u_0} s = 0 \text{ for } i \in \{0, \ldots, m-1\} \quad \text{and} \quad \left.\frac{\partial^l}{\partial u^l}\right|_{u=u_0} t = 0 \text{ for } l \in \{0, \ldots, n-1\}.$$

Then

$$\left.\frac{\partial^k}{\partial u^k}\right|_{u=u_0} (s \cdot t) = 0 \text{ for all } k \in \{0, \ldots, m+n-1\}.$$

Thus we arrive at a strengthened version of Proposition 34 that is able to account for different root multiplicities:

**Theorem 39.** *Let $K$ be a field, let $g \in K[X]$ and $h \in K[u, X]$ be non-zero polynomials, and let $u_0 \in K$ such that $\deg_X h(u_0, X) = \deg_X h$. Further write*

$$m = \#\{\!\{\text{Roots } x \in \overline{K} \text{ of } g \text{ such that } h(u_0, x) = 0\}\!\}$$

*where the double bracket notation indicates a multiset, i.e. we count each root of $g$ with its multiplicity. Then*

$$\left.\frac{\partial^k}{\partial u^k}\right|_{u=u_0} \operatorname{res}_X(g,h) = 0 \text{ for } k \in \{0, \ldots, m-1\}.$$

*Proof.* In view of Proposition 33 (applied to an embedding of $K$ into an algebraic closure) we may assume that $K$ is algebraically closed. Now let $\xi_1, \ldots, \xi_n \in K$ denote the distinct roots of $g$ that are also roots of $h(u_0, X)$, and let $e_1, \ldots, e_n$ denote their multiplicities as roots of $g$. Then we define for any $i \in [m]$ the polynomial

$$g_i \coloneqq \prod_{k : e_k \geq i} (X - \xi_k) \in K[X];$$

each of these polynomials divides $h(u_0, X)$, so $\deg \gcd(g_i, h(u_0, X)) = \deg(g_i)$, and Proposition 34 thus gives

$$\left.\frac{\partial^k}{\partial u^k}\right|_{u=u_0} \operatorname{res}_X(g_i, h) = 0 \text{ for } k \in \{0, \ldots, \deg(g_i) - 1\}. \tag{10}$$

Furthermore

$$g_1 \cdots g_m = (X - \xi_1)^{e_1} \cdots (X - \xi_n)^{e_n}$$

is a divisor of $g$ in $K[X]$, so we find a polynomial $g_0 \in K[X]$ such that $g = g_0 \cdots g_m$, and with Proposition 36 we obtain

$$\operatorname{res}_X(g,h) = \operatorname{res}_X(g_0,h) \cdot \operatorname{res}_X(g_1,h) \cdots \operatorname{res}_X(g_m,h).$$

Now iteratively applying Lemma 38 to the above decomposition with Equation (10) and

$$\deg(g_1) + \cdots + \deg(g_m) = e_1 + \cdots + e_n = m$$

yields the claim. □

*The proof of Lemma 14.* We close out this section by providing a proof of Lemma 14. First let us introduce additional notation: We write

$$\Delta_\ell(Y, j) \coloneqq \delta_\ell(Y, j, j) = \frac{\partial}{\partial j}\Phi_\ell^A(Y, j)$$

for the $j$-derivative of $\Phi_\ell^A(Y, j)$ and

$$\vartheta_\ell^{(1)}(Y, j) \coloneqq \frac{\partial}{\partial Y}\Phi_\ell^A(Y, j) \text{ and } \vartheta_\ell^{(2)}(Y, j) \coloneqq \frac{\partial^2}{\partial Y^2}\Phi_\ell^A(Y, j)$$

for the first two $Y$-derivatives of $\Phi_\ell^A(Y, j)$. For ease of reference we state the result again:

**Lemma 14.** Let $\ell \in \mathcal{L}$ and let $K$ be a field of characteristic $\operatorname{char}(K) \neq \ell$. Furthermore let $j_0 \in K$ such that $j_0 \notin \{0, 1728\}$ and suppose that $t^+ \in K$ is a double root of $\Phi_\ell^A(Y, j_0)$. Then the following holds:

(a) $t^+$ is not a root of $\Phi_\ell^A(Y, j_1)$ for any $j_1 \in K$ with $j_1 \neq j_0$.

(b) $t^+$ is not a triple root of $\Phi_\ell^A(Y, j_0)$, i.e. its multiplicity as a root is exactly 2.

*Proof.* The necessary computations for the following proof are provided in the SageMath script `MultiRootProof.sage`.

To prove claim (a), assume for a contradiction that there is some $j_1 \in K$ with $j_1 \neq j_0$ such that $\Phi_\ell^A(t^+, j_1) = 0$. Then the two roots of the degree two polynomial $\Phi_\ell^A(t^+, j)$ are distinct and thus simple, so $\Phi_\ell^A(t^+, j)$ and $\Delta_\ell(t^+, j)$ do not share a common root. Hence the two polynomials $\Phi_\ell^A(t^+, j)$ and $\Phi_\ell^A(t^+, j) - \Delta_\ell(t^+, j)$ also have no root in common, so Proposition 33 and Corollary 37 show that

$$\operatorname{res}_j(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \Delta_\ell(Y, j)) \in \mathbb{Z}[Y]$$

does not vanish when evaluated at $t^+$ (after reduction modulo $\operatorname{char}(K)$).

However, by assumption $\Phi_\ell^A(Y, j_0)$ is divisible by $(Y - t^+)^2$, which forces its $Y$-derivative $\vartheta_\ell^{(1)}(Y, j_0)$ to be divisible by $(Y - t^+)$. Put differently, the two polynomials $\Phi_\ell^A(t^+, j)$ and $\Phi_\ell^A(t^+, j) - \vartheta_\ell^{(1)}(t^+, j)$ share the common root $j_0$, so Proposition 33 and Corollary 37 imply that

$$\operatorname{res}_j(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \vartheta_\ell^{(1)}(Y, j)) \in \mathbb{Z}[Y]$$

vanishes at $t^+$ (after reduction modulo $\operatorname{char}(K)$). Now writing

$$\operatorname{res}_j(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \Delta_\ell(Y, j)) = -g_\Delta \cdot h \text{ and } \operatorname{res}_j(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \vartheta_\ell^{(1)}(Y, j)) = -\ell \cdot g_\vartheta \cdot h$$

with monic polynomials $g_\Delta, g_\vartheta, h \in \mathbb{Z}[Y]$ such that $h$ is of maximal degree, the above shows that $g_\vartheta$ vanishes at $t^+$ (after reduction modulo $\operatorname{char}(K)$). Thus $g_\vartheta$ and $g_\vartheta - \vartheta_\ell^{(1)}(Y, j_0)$ share the common root $t^+$, so Proposition 33 and Corollary 37 yield[13]

$$0 = \operatorname{res}_Y(g_\vartheta, g_\vartheta - \vartheta_\ell^{(1)}(Y, j_0)) = n_\ell \cdot j_0^{m_0} \cdot (j_0 - 1728)^{m_{1728}}$$

for exponents $m_0, m_{1728} \in \mathbb{N}$ and some integer $n_\ell \in \mathbb{N}$.

Due to our assumption $j_0 \notin \{0, 1728\}$ we deduce that the characteristic $\operatorname{char}(K)$ is a prime divisor of $n_\ell$, and this reduces us to a finite list of remaining cases. Indeed, as $t^+$ is still a root of $g_\vartheta \in K[Y]$, we can now iterate over all prime divisors $p$ of $n_\ell$ and verify that for all roots $t'$ of $g_\vartheta \in \mathbb{F}_p[Y]$ we have the divisibility

$$\gcd(\Phi_\ell^A(t', j), \vartheta_\ell^{(1)}(t', j)) \mid j^2 \cdot (j - 1728)^2$$

to arrive at a contradiction to the assumption $j_0 \notin \{0, 1728\}$ since $\Phi_\ell^A(t^+, j_0) = 0 = \vartheta_\ell^{(1)}(t^+, j_0)$.

[13] We cannot directly compare $\operatorname{res}_Y(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \Delta_\ell(Y, j))$ and $\operatorname{res}_Y(\Phi_\ell^A(Y, j), \Phi_\ell^A(Y, j) - \vartheta_\ell^{(1)}(Y, j))$ as the former could evaluate to 0 at $j_0$ even if $t^+$ is not a common root of $\Phi_\ell^A(Y, j_0)$ and $\Delta_\ell(Y, j_0)$. With an additional resultant computation, the above indirectly shows that this could only happen for sufficiently small characteristics (see also [BS25, Proposition 19]).

To prove claim (b), assume to the contrary that $t^+$ is a triple root of $\Phi_\ell^A(Y, j_0)$. By part (a) we know that $j_0$ then is a double root of $\Phi_\ell^A(t^+, j)$, so the four polynomials

$$\Phi_\ell^A(Y,j),\ \vartheta_\ell^{(1)}(Y,j),\ \vartheta_\ell^{(2)}(Y,j),\ \Delta_\ell(Y,j)$$

all evaluate to 0 at $(t^+, j_0)$. Proposition 33 and Corollary 37 thus yield six polynomials in $\mathbb{Z}[Y]$ with a root at $t^+$ (after reduction modulo $\mathrm{char}(K)$) by taking the $j$-resultants[14] of any two distinct polynomials in the list

$$\Phi_\ell^A(Y,j),\ \Phi_\ell^A(Y,j) - \vartheta_\ell^{(1)}(Y,j),\ \Phi_\ell^A(Y,j) - \vartheta_\ell^{(2)}(Y,j),\ \Phi_\ell^A(Y,j) - \Delta_\ell(Y,j).$$

From part (a) we moreover know that $t^+$ is not a root of $\Phi_\ell^A(Y,0) \in K[Y]$ or $\Phi_\ell^A(Y,1728) \in K[Y]$, so we can divide out any common factor of $\Phi_\ell^A(Y,0)$ or $\Phi_\ell^A(Y,1728)$ with each of the above six resultant polynomials to obtain new polynomials $r_0, \ldots, r_5 \in \mathbb{Z}[Y]$ whose reductions modulo $\mathrm{char}(K)$ still all have the common root $t^+$. For any $i, k \in \{0, \ldots, 5\}$ we therefore obtain

$$\mathrm{res}_Y(r_i, r_k) \equiv 0 \mod \mathrm{char}(K)$$

with Proposition 33 and Corollary 37 as long as the leading coefficients of $r_i$ and $r_k$ are not divisible by $\mathrm{char}(K)$. Putting this issue aside for a second, we deduce that $\mathrm{char}(K)$ is a prime factor of the nonzero integer

$$a_\ell := \gcd(\{\mathrm{res}_Y(r_i, r_k) \mid 0 \le i < k \le 5\}).$$

Now we can verify that the leading coefficients of $r_0, \ldots, r_5$ all divide the integer $a_\ell$; therefore $\mathrm{char}(K)$ always divides $a_\ell$, and this again reduces us to a finite list of cases. Indeed, for each such prime $p = \mathrm{char}(K) \neq \ell$ we still know that $t^+$ is a root of

$$\gcd(r_0, \ldots, r_5) \in \mathbb{F}_p[Y],$$

and for each root $t'$ of this greatest common divisor we can check[15] that for all roots $j' \notin \{0, 1728\}$ of $\Phi_\ell^A(t', j)$ the power $(Y - t')^3$ does not divide $\Phi_\ell^A(Y, j')$. □

# B An Overview of Canonical Modular Polynomials

In this section we give a brief overview of the theory of the canonical modular polynomials $\Phi_\ell^c(T, j)$, which was investigated in [dHKM+25, §3]. As the applications found in the cited paper are restricted to the primes $\ell \in \{2, 3, 5, 7, 13\}$ for which the modular curve $X_0(\ell)$ has genus 0, we will restrict this overview to these primes.

In the following we always write $s = 12/(\ell - 1)$ for a previously fixed prime $\ell \in \{2, 3, 5, 7, 13\}$. We first recall the structure of $\Phi_\ell^c(T, j)$:

**Lemma 40** ([dHKM+25, Lemma 1])**.** Let $\ell \in \{2, 3, 5, 7, 13\}$. Then the $\ell^{th}$ canonical modular polynomial $\Phi_\ell^c(T, j)$ is of the form

$$\Phi_\ell^c(T,j) = T^{\ell+1} + \sum_{i=1}^{\ell} c_i T^i + \ell^s - T \cdot j = \Phi_\ell^c(T,0) - T \cdot j$$

for some integer coefficients $c_i \in \mathbb{Z}$. In particular, the rational function

$$\Theta_\ell^c(T,j) := \Phi_\ell^c(\ell^s/T, j) \cdot T^{\ell+1}/\ell^s = T^{\ell+1} + \sum_{i=1}^{\ell} c_i \ell^{s\cdot(i-1)} T^{\ell+1-i} + \ell^{s\cdot\ell} - T^\ell \cdot j$$

is a polynomial with integer coefficients. Writing $\mathcal{J}_\ell(T) := \Phi_\ell^c(T,0)/T$, we furthermore have that for any $f \in K^\times$ and $j_0 \in K$:

$$j_0 = \mathcal{J}_\ell(f) \text{ if and only if } \Phi_\ell^c(f, j_0) = 0.$$

[14] One can adapt this first step to work with the $Y$-resultants having $j_0$ as a common root instead, also conceptually simplifying the next step; however, due to linearly growing $Y$-degree the necessary computations get noticeably more expensive.
[15] A posteriori this check will only be necessary for $p = 2$, where we cannot detect the root multiplicity via derivatives.

The main tool to relate the canonical modular polynomial to the classical modular polynomial is the following resultant equation:

**Proposition 41.** For any $\ell \in \{2,3,5,7,13\}$ we have

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

where the resultant is computed over the coefficient ring $R=\mathbb{Z}[J_0,J_1]$ of bivariate polynomials.

*Proof.* In view of Lemma 32, this follows from the resultant equation in [dHKM+25, Proposition 3]. Using the modular interpretation, we also given an alternative proof of this equation at the end of this section. □

We obtain the following connection between the roots of the canonical modular polynomial and the number of non-equivalent $\ell$-isogenies between two $j$-invariants:

**Canonical Multiplicity Theorem.** *Let $\ell \in \{2,3,5,7,13\}$, let $K$ be a field with $\mathrm{char}(K) \notin [\ell]$ and let $j_0, j_1 \in K$. Then the number of (non-equivalent) $\ell$-isogenies $j_0 \to j_1$ is equal to the cardinality of the multiset*

$$\left\{\!\!\left\{ \text{Roots } f \in \overline{K}^\times \text{ of } \Phi_\ell^c(T,j_0) \text{ such that } \Phi_\ell^c(\ell^s/f, j_1) = 0 \right\}\!\!\right\}.$$

*In particular, $j_0$ and $j_1$ are $\ell$-isogenous if and only if there exists an $f \in \overline{K}^\times$ such that*

$$\Phi_\ell^c(f,j_0) = 0 = \Phi_\ell^c(\ell^s/f, j_1). \tag{CM}$$

**Remark 9.** The above result can be found as [dHKM+25, Multiplicity Theorem]; in that article, however, the proof required a careful analysis of the different root multiplicities since we had not yet uncovered Theorem 4 as a strengthening of Proposition 34. We note here that, with this strengthening, one can give a simplified proof of the Canonical Multiplicity Theorem that is completely analogous to the proof of the Atkin Multiplicity Theorem of Section 3.1.

In fact, the above connection can be made more explicit by systematically associating to a root of the system (CM) a kernel polynomial describing the associated isogeny; this was done in [dHKM+25, Reconstruction Theorem], which we restate here:

**Canonical Reconstruction Theorem.** *Let $\ell \in \{2,3,5,7,13\}$, let $K$ be a field such that its characteristic satisfies $\mathrm{char}(K) \notin \{2,3,\ell\}$, let $j_0 \in K \setminus \{0,1728\}$ be a $j$-invariant and let $f \in \overline{K}^\times$ be a root of $\Phi_\ell^c(T,j_0)$. Define the parameters*

$$A = -3j_0(j_0-1728) \quad \text{and} \quad B = -2j_0(j_0-1728)^2$$

*and the elliptic curve*

$$E\colon y^2 = x^3 + Ax + B.$$

*Then $j(E) = j_0$, and we can associate to $f$ a kernel polynomial $\phi_\ell(f)$ of degree $\left\lceil \frac{\ell-1}{2} \right\rceil$ that defines over $K(f)$ an $\ell$-isogeny from $E$ to a curve with $j$-invariant $\mathcal{J}_\ell(\ell^s/f)$. Moreover, $f$ can be expressed as a $K$-rational function in the coefficients $1 = s_0, s_1, \ldots, s_n$ of $\phi_\ell(f)$, i.e.*

$$K(f) = K(s_1,\ldots,s_n).$$

In particular, this theorem can be used to understand the splitting behavior of $\Phi_\ell^c(T,j_0)$ for a supersingular $j$-invariant $j_0$:

**Theorem 42** ([dHKM+25, Theorem 2]). *Let $\ell \in \{2,3,5,7,13\}$, let $p \neq \ell$ be a prime and let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular $j$-invariant. Then $\Phi_\ell^c(T,j_0)$ splits over $\mathbb{F}_{p^2}$.*

For completeness we close out this section by providing a modular proof of the resultant equation for the canonical modular polynomial, akin to Propositions 12 and 25. To this end we first recall the modular interpretation in more detail: $\Phi_\ell^c(T,j(\tau))$ is the minimal polynomial of

$$f_\ell(\tau) = \ell^s \cdot \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s} = \ell^s/t_\ell(\tau) = \omega_\ell^* t_\ell(\tau)$$

over $\mathbb{C}(j(\tau)) = \mathbb{C}(X(1))$, where the last equality is proven in [Mü95, Lemma 5.5].

Furthermore, for representatives $a_0, \ldots, a_\ell \in \mathrm{SL}_2(\mathbb{Z})$ of the cosets $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$ it is given by

$$\Phi_\ell^c(T, j(\tau)) = \prod_{n=0}^{\ell} (T - f_\ell(a_n(\tau))). \tag{11}$$

Due to being the minimal polynomial of $f_\ell(\tau)$, it satisfies[16]

$$\Phi_\ell^c(f_\ell(\tau), j(\tau)) = 0 = \Phi_\ell^c(\ell^s / f_\ell(\tau), j(\ell\tau)),$$

where we obtain the second equation by applying the (action of the) Fricke involution $\omega_\ell$ to the first equation. In particular, the rational function $\mathcal{J}_\ell$ satisfies $\mathcal{J}_\ell(f_\ell(\tau)) = j(\tau)$ and $\mathcal{J}_\ell(\ell^s/f_\ell(\tau)) = j(\ell\tau)$.

*Modular proof of Proposition 41.* As $j(\tau)$ is transcendental over $\mathbb{C}$, we have a ring embedding

$$\varphi\colon \mathbb{Z}[J_0, J_1] \hookrightarrow \mathbb{C}(j(\tau))[J_1],\ J_0 \mapsto j(\tau),$$

and in view of Proposition 33 we get

$$\varphi(\mathrm{res}_T(\Phi_\ell^c(T, J_0), \Theta_\ell^c(T, J_1))) = \mathrm{res}_T(\Phi_\ell^c(T, j(\tau)), \Theta_\ell^c(T, J_1)).$$

Moreover, clearly $\varphi$ maps the right side of our claimed equation to

$$\varphi\Big((-1)^{\ell+1} \cdot \ell^{s\cdot\ell} \cdot \Phi_\ell(J_0, J_1)\Big) = (-1)^{\ell+1} \cdot \ell^{s\cdot\ell} \cdot \Phi_\ell(j(\tau), J_1),$$

and due to the injectivity of $\varphi$ it suffices to show that the above two expressions coincide.

Now let $a_0, \ldots, a_\ell \in \mathrm{SL}_2(\mathbb{Z})$ be representatives of the left cosets $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(\ell)$. As the Fricke involution acts on $f_\ell(\tau)$ via $\omega_\ell^* f_\ell(\tau) = \ell^s/f_\ell(\tau)$, Equation (11) and Proposition 37 then give

$$\begin{aligned}\mathrm{res}_T(\Phi_\ell^c(T, j(\tau)), \Theta_\ell^c(T, J_1)) &= \prod_{n=0}^{\ell} \Theta_\ell^c(f_\ell(a_n(\tau)), J_1) \\ &= \prod_{n=0}^{\ell} \Big(f_\ell(a_n(\tau))^{\ell+1}/\ell^s \cdot \Phi_\ell^c(\ell^s/f_\ell(a_n(\tau)), J_1)\Big).\end{aligned}$$

Furthermore, due to Equation (2) we have

$$\Phi_\ell(j(\tau), J_1) = \prod_{n=0}^{\ell} (J_1 - j(\ell a_n(\tau))),$$

so the two polynomials above are of degree $\ell + 1$ in $J_1$ with the roots $j(\ell a_n(\tau))$, $n = 0, \ldots, \ell$, and we deduce that they coincide up to their leading coefficient. Here we see that $\Phi_\ell(j(\tau), J_1)$ is monic, whereas the leading coefficient of the resultant is

$$\begin{aligned}\prod_{n=0}^{\ell} f_\ell(a_n(\tau))^{\ell+1}/\ell^s \cdot (-\ell^s/f_\ell(a_n(\tau))) &= (-1)^{(\ell+1)^2} \prod_{n=0}^{\ell} (-f_\ell(a_n(\tau)))^\ell \\ &= (-1)^{\ell+1} \cdot \Phi_\ell^c(0, j(\tau))^\ell = (-1)^{\ell+1}(\ell^s)^\ell\end{aligned}$$

due to the factorization equation (11) and Lemma 40. In view of the injectivity of $\varphi$, the claimed equation follows. □

# C All Results for the Atkin and Weber Arithmetizations

In the table below we present the results for the Atkin and Weber modular polynomials, for all $\ell$ under consideration and all our approaches to arithmetization. We omit results that are surpassed on all metrics. For comparison, we add the results that are the previous state of the art. The best results in a column for an $\ell$ and field are underlined.

[16] This is the modular background underlying the Canonical Multiplicity Theorem.

| New? | Approach | $\ell$ | Field | Constraints | Variables | Non-zero entries |
|---|---|---|---|---|---|---|
| [CLL23] | Classical | 2 | $\mathbb{F}_{p^2}$ | $4k+2$ | $4k+3$ | $21k+6$ |
| [dHKM+25] | Canonical | 2 | $\mathbb{F}_{p^2}$ | $3k$ | $3k+1$ | $13k$ |
| [LP25] | Radical | 2 | $\mathbb{F}_{p^2}$ | $2k$ | $2k+2$ | $10k$ |
| New | Atkins 1 | 2 | $\mathbb{F}_{p^2}$ | $2k$ | $2k+1$ | $12k$ |
| [dHKM+25] | Canonical | 3 | $\mathbb{F}_{p^2}$ | $4k$ | $4k+1$ | $18k$ |
| New | Atkins 1 | 3 | $\mathbb{F}_{p^2}$ | $3k$ | $3k+1$ | $16k$ |
| [dHKM+25] | Canonical | 5 | $\mathbb{F}_{p^2}$ | $6k$ | $6k+1$ | $28k$ |
| New | Atkins 1 | 5 | $\mathbb{F}_{p^2}$ | $5k$ | $5k+1$ | $26k$ |
| New | Weber | 5 | $\mathbb{F}_{p^2}$ | $5k+3$ | $5k+4$ | $17k+9$ |
| [dHKM+25] | Canonical | 7 | $\mathbb{F}_{p^2}$ | $7k$ | $7k+1$ | $35k$ |
| New | Atkins 2 | 7 | $\mathbb{F}_{p^2}$ | $6k$ | $6k+1$ | $44k$ |
| New | Weber | 7 | $\mathbb{F}_{p^2}$ | $8k+3$ | $8k+4$ | $26k+9$ |
| New | Atkins 4 | 11 | $\mathbb{F}_{p^2}$ | $8k$ | $8k+1$ | $41k$ |
| New | Weber | 11 | $\mathbb{F}_{p^2}$ | $10k+4$ | $10k+5$ | $36k+12$ |
| [dHKM+25] | Canonical | 13 | $\mathbb{F}_{p^2}$ | $10k$ | $10k+1$ | $56k$ |
| New | Atkins 3 | 13 | $\mathbb{F}_{p^2}$ | $9k$ | $9k+1$ | $54k$ |
| New | Atkins 4 | 17 | $\mathbb{F}_{p^2}$ | $10k$ | $10k+1$ | $54k$ |
| New | Atkins 4 | 19 | $\mathbb{F}_{p^2}$ | $11k$ | $11k+1$ | $73k$ |
| New | Atkins 4 | 23 | $\mathbb{F}_{p^2}$ | $11k$ | $11k+1$ | $73k$ |
| New | Atkins 4 | 29 | $\mathbb{F}_{p^2}$ | $13k$ | $13k+1$ | $83k$ |
| New | Atkins 4 | 31 | $\mathbb{F}_{p^2}$ | $14k$ | $14k+1$ | $109k$ |
| New | Atkins 4 | 41 | $\mathbb{F}_{p^2}$ | $16k$ | $16k+1$ | $105k$ |
| New | Atkins 4 | 47 | $\mathbb{F}_{p^2}$ | $17k$ | $17k+1$ | $129k$ |
| New | Atkins 4 | 59 | $\mathbb{F}_{p^2}$ | $20k$ | $20k+1$ | $153k$ |
| New | Atkins 4 | 71 | $\mathbb{F}_{p^2}$ | $23k$ | $23k+1$ | $185k$ |
| [CLL23] | Classical | 2 | $\mathbb{F}_p$ | $11k+5$ | $11k+7$ | $79k+23$ |
| [dHKM+25] | Canonical | 2 | $\mathbb{F}_p$ | $7k$ | $7k+2$ | $41k$ |
| [LP25] | Radical | 2 | $\mathbb{F}_p$ | $5k$ | $5k+4$ | $36k$ |
| New | Atkins 1 | 2 | $\mathbb{F}_p$ | $5k$ | $5k+2$ | $46k$ |
| [dHKM+25] | Canonical | 3 | $\mathbb{F}_p$ | $11k$ | $11k+2$ | $65k$ |
| New | Atkins 1 | 3 | $\mathbb{F}_p$ | $8k$ | $8k+2$ | $60k$ |
| [dHKM+25] | Canonical | 5 | $\mathbb{F}_p$ | $15k$ | $15k+2$ | $97k$ |
| New | Atkins 2 | 5 | $\mathbb{F}_p$ | $12k$ | $12k+2$ | $98k$ |
| New | Weber | 5 | $\mathbb{F}_p$ | $12k+7$ | $12k+9$ | $72k+31$ |
| [dHKM+25] | Canonical | 7 | $\mathbb{F}_p$ | $17k$ | $17k+2$ | $123k$ |
| New | Atkins 2 | 7 | $\mathbb{F}_p$ | $13k$ | $13k+2$ | $129k$ |
| New | Atkins 3 | 7 | $\mathbb{F}_p$ | $17k$ | $17k+2$ | $118k$ |
| New | Weber | 7 | $\mathbb{F}_p$ | $19k+6$ | $19k+8$ | $89k+28$ |
| New | Atkins 2 | 11 | $\mathbb{F}_p$ | $17k$ | $17k+2$ | $189k$ |
| New | Atkins 3 | 11 | $\mathbb{F}_p$ | $18k$ | $18k+2$ | $157k$ |
| New | Atkins 4 | 11 | $\mathbb{F}_p$ | $19k$ | $19k+2$ | $128k$ |
| New | Weber | 11 | $\mathbb{F}_p$ | $24k+9$ | $24k+11$ | $122k+40$ |
| [dHKM+25] | Canonical | 13 | $\mathbb{F}_p$ | $24k$ | $24k+2$ | $194k$ |
| New | Atkins 2 | 13 | $\mathbb{F}_p$ | $20k$ | $20k+2$ | $206k$ |
| New | Atkins 3 | 13 | $\mathbb{F}_p$ | $22k$ | $22k+2$ | $179k$ |
| New | Atkins 3 | 17 | $\mathbb{F}_p$ | $23k$ | $23k+2$ | $216k$ |
| New | Atkins 4 | 17 | $\mathbb{F}_p$ | $24k$ | $24k+2$ | $176k$ |
| New | Atkins 3 | 19 | $\mathbb{F}_p$ | $25k$ | $25k+2$ | $245k$ |
| New | Atkins 4 | 19 | $\mathbb{F}_p$ | $26k$ | $26k+2$ | $227k$ |
| New | Atkins 4 | 23 | $\mathbb{F}_p$ | $24k$ | $24k+2$ | $219k$ |
| New | Atkins 4 | 29 | $\mathbb{F}_p$ | $29k$ | $29k+2$ | $262k$ |
| New | Atkins 4 | 31 | $\mathbb{F}_p$ | $31k$ | $31k+2$ | $331k$ |
| New | Atkins 4 | 41 | $\mathbb{F}_p$ | $36k$ | $36k+2$ | $334k$ |
| New | Atkins 4 | 47 | $\mathbb{F}_p$ | $36k$ | $36k+2$ | $387k$ |
| New | Atkins 4 | 59 | $\mathbb{F}_p$ | $43k$ | $43k+2$ | $464k$ |
| New | Atkins 4 | 71 | $\mathbb{F}_p$ | $48k$ | $48k+2$ | $555k$ |