Cyclic isogeny walks on genus-zero modular curves

Aleksei Udovenko[a]

SnT, University of Luxembourg, Esch-sur-Alzette, Luxembourg

Abstract. Isogeny-based cryptography implementations have to navigate a large space of options for representing elliptic curves and isogenies and for the corresponding arithmetic. This work collects, completes, and organizes the set of algebraic maps and relations available when working with genus-zero modular curves $X_0(N)$, which parametrize cyclic N-isogenies of elliptic curves and can be represented by a single field element. This abstract notion covers many single-parameter curve models, such as Montgomery, Edwards, Jacobi quartic, Hessian curve, Deuring normal form. Such single-parameter models for the same modular curve are related by degree-1 rational maps, which limits the remaining options for improving the expressions. This representation is universal in the sense that it can be obtained from any other algebraic parametrization of such isogenies, or simply from the j-invariants through which the isogeny passes, away from singularities. We show how to derive rational maps for computing such lifting from the j-line to $X_0(N)$.

Our main technical contribution is the definition, analysis, and computation of non-backtracking modular polynomials over these curves obtained using an extended method of Elkies. In addition to characterizing cyclic extensions of isogenies, they have many other useful properties, such as having lower degree and being sparser than other typical modular polynomials, smoother walk models (being better at distinguishing different isogenies), carrying additional isogeny of different degree along the walk. We also propose radical representations of the same relation, which sheds new light on a few existing radical isogeny formulas.

We illustrate the use of the framework by achieving more compact R1CS encodings for isogeny proofs of knowledge.

Keywords: Isogenies · Elliptic curves · Modular polynomials · Modular curves · Parametrization · R1CS

1 Introduction

Isogenies of elliptic curves (and higher-dimensional abelian varieties) play a significant role in the post-quantum branch of cryptography. Their rich mathematical structure inspires many constructions and applications, such as signatures [AAA+25], key exchange [CLM+18], verifiable secret sharing [ABCP23b], distributed key generation [ABCP23a], etc.

Isogenies are *homomorphisms* between elliptic curve groups, which are infinite objects when considered over the algebraic closure of the field. Yet, the sole *relation* on pairs of curves of being related by a degree-ℓ isogeny already encompasses a lot of useful cryptographic structure. For example, two elliptic curves are related by a cyclic degree-2

E-mail: aleksei@affine.group (Aleksei Udovenko)

[a]The work is funded by the Luxembourg National Research Fund's (FNR) project PQSeal (CORE/24/IS/18978392).

This work is licensed under a "CC BY 4.0" license.

Date of this document: 2026-10-21.

isogeny if and only if their j-invariants (j_1, j_2) form a zero of the level-2 classical modular polynomial $\Phi_2 \in \mathbb{Z}[X, Y]$:

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

Such polynomials exist for any degree $\ell > 1$ and are such that $\Phi_\ell(j_1, j_2) = 0$ if and only if there exist two ℓ-isogenous elliptic curves with j-invariants j_1, j_2. Evidently, Φ_2 is not a particularly compact polynomial and there are other ways to represent essentially the same relation, by using alternative modular polynomials [dHKM+25, dHMSS26], radical isogeny formulas [CDV20], or more traditional methods based on arithmetic of specific curve models, such as Montgomery curves. These methods work over alternative parametrizations of elliptic curves instead of working directly with j-invariants.

Modular curves are mathematical objects parametrizing isogenies and related structures. Usually, they are defined analytically, as quotients of an (extended) complex upper half-plane by the action of certain subgroups of the group $\mathrm{SL}_2(\mathbb{Z})$. For the purpose of this work, we will only rely on the *algebraic* role of modular curves in parametrizing cyclic isogenies and ignore their analytical nature and definitions; we will use however the standard names for modular curves such as $X_0(N), X_1(N), X(N)$. In fact, everything in this work can be derived "from scratch" using simple algebraic methods, which we will outline in Section 2.

The *abstract* nature of modular curves leads to simple classification of many single-parameter curve models. Each class, indexed by the respective modular curve, shares the same various relations (such as modular polynomials), up to a Möbius transformation (a fractional linear change of variable). In particular, in this classification, the Legendre curve $y^2 = x(x-1)(x-\lambda)$ and the Montgomery curve $y^2 = x^3 + Ax^2 + x$ both define an $X_0(4) \simeq X(2)$ structure via the variable change $\lambda = \frac{A+2}{4}$. Even though these two curves generally have different j-invariants (i.e., are not isomorphic), they describe the same cyclic 4-isogeny, and this governs the shapes of the isogeny relations and some arithmetic.

Our contribution

We propose an algebraic framework for genus-zero modular curves, which is a collection of rational maps and relations available for these models, arranged by types: coverings, duality operators, modular polynomials, lifting maps, rotations.

Single-parameter models of low-degree isogenies are universal (can be extracted from any N-isogeny data) and cover many practical representations, such as the Montgomery model (possibly with additional level structure such as 3-isogeny data). In the supersingular case, all these $X_0(N)$-parameters are also defined over $\mathbb{F}_{p^2}$, which is crucial for all cryptographic applications. Finally, such models are defined only up to a degree-1 rational map of the form $x \mapsto \frac{ax+b}{cx+d}$; this leaves almost no room for further improvement of the formulas without introducing more variables per an isogeny step.

Our main contribution is a systematic study of non-backtracking modular polynomials, arising in the construction of modular towers by Elkies [Elk97]. Our study includes: definition, computation, formulations (including fiber product $\mathbf{R}(x) = \mathbf{L}(y)$, duality-radical $\mathbf{w}(x^\ell) = \mathbf{w}(y)^\ell$), analysis of their properties. In particular, chaining some of our modular polynomials yields smooth models for 2- and 3-isogeny walks. This means in particular that our parametrizations are in bijection with cyclic isogenies, up to pre- or post-composition with an isomorphism. This contrasts to classic modular polynomials, where potential multiple edges $\Phi_N(j_1, j_2) = 0$ correspond to the same pair (j_1, j_2). Our most compact 2-isogeny modular polynomial is

$$\Phi_{16,2}(x, y) = y^2 - 2x^2y + 1, \tag{1}$$

which is probably the one most useful for applications. It is quite surprising that such an equation is in a way equivalent to the clumsy $\Phi_2(x, y)$ mentioned in the introduction. It is also arguably the most compact expression possible, since an equation with fewer monomials or lower degrees would not imply the necessary structure.

Our main goal is to provide a handbook with a collection of maps and relations. Most of these can be (and usually are) derived by hand from the chosen elliptic curve model, division polynomials, etc.; our framework only simplifies access and provides a clear picture on what information is available. Therefore, for applications, we focus on non-backtracking polynomials which are not so well-known. Their main utility is in compact algebraic parametrizations of isogeny walks. We consider an application to isogeny proofs of knowledge using generic proof systems [CLL23] and compare to the state-of-the-art.

Related work Maier systematized [Mai09] genus-zero modular curves $X_0(N)$ and coverings between them. General modular picture and many relevant maps are described for example in Tsukazaki's [Tsu13] or Colò's thesis [Col22]. Various modular polynomials were studied and computed in several works [ES10, BLS12], but most of them allow backtracking. A very recent work [dHKM+25] studies so-called canonical modular polynomials $\Phi^c_\ell(X, j)$, which in fact relate a j-invariant and a modular parameter $X_0(\ell)$ of a prime level ℓ. These polynomials essentially represent the coverings in our framework. Several works [FJP14, OT20] used the maps $A \mapsto 2\frac{A-6}{A+2}, A \mapsto -2\frac{A+6}{A-2}$ for optimization of isogeny walks in SIDH/CSIDH [CLM+18] without explicitly noting their link with parametrization of 4-isogenies by the Montgomery A-coefficients. Based on these results, [MN23] derived an equation relating the two Montgomery A-coefficients on a 2-isogeny path, which is essentially the modular polynomial of level 2 on $X_0(4)$ in terms of this paper: $\Phi_{4,2}(B, -A) = A^2 + 12A - 4B^2A - 8B^2 + 36$. An equivalent expression of (1) was described by León and Muñoz in [LM25], together with relevant lifting maps, yet its generic meaning was not derived. In fact, an equivalent expression $y^2 = \frac{x^2+1}{2x}$ appears already in [GSR03, Sec.5] used for constructing an asymptotically optimal finite field tower, inspired by the Elkies work. We also mention radical isogeny expressions [CDV20, Dec24] which also have connections to our framework (this question was also theoretically studied in [Pri24]). Various connections between $X_0(N)$ and usual curve models were mentioned in a few works, e.g. [Mai09, Col22, OM22, BRS25].

Notation The letter $\mathbb{F}$ denotes a field (typically, the field of rational numbers $\mathbb{Q}$ or a finite field $\mathbb{F}_q$ of characteristic p), and $\overline{\mathbb{F}}$ denotes its algebraic closure. For an integer $n \geq 2$, we use ζ_n to denote a primitive n-th root of unity. For a fractional map f, $\mathrm{num}(f)$ and $\mathrm{denom}(f)$ are its numerator and denominator respectively (up to any scalar multiple). For a polynomial $f(x) \in \mathbb{Q}[x]$, we denote by $\mathrm{prim}(f)$ its unique up to sign scalar multiple $g(x) = c \cdot f(x) = \sum_{i=0}^{n} g_i x^i \in \mathbb{Z}[x]$, $c \in \mathbb{Q} \setminus \{0\}$, such that $\gcd(g_0, \ldots, g_n) = 1$ in $\mathbb{Z}$. We call an integer polynomial $f(x)$ primitive if $f = \mathrm{prim}(f)$. Usually, we will work with the affine line $\mathbb{A}^1(\mathbb{F}) = \mathbb{F}$; the extension to the projective line $\mathbb{P}^1(\mathbb{F}) \simeq \mathbb{F} \cup \{\infty\}$ is understood but is not relevant since it only adds degenerate cases (cusps), as will be discussed. For an integer N, the radical $\mathrm{rad}(N)$ is its squarefree part: $\mathrm{rad}(N) = \prod_{\text{prime } p|N} p$.

2 Framework

In this section, we describe a framework for working with modular curves. It consists in organization of different maps (covers and inverses of their pairs, duality and rotation automorphisms) and relations (novel modular polynomials for isogeny degrees dividing level of the curve), as well as a methodology for computing the missing parts (namely, the inverses of covers, modular polynomials). We also explicitly show a radical structure of

some covers which yields rotation maps and radical expression of the respective modular polynomials.

2.1 Isogenies of elliptic curves

Over complex numbers, any elliptic curve is isomorphic to a complex torus $\mathbb{C}/\Lambda$ for some complex lattice Λ. Unfortunately, such isomorphisms are not available when working with elliptic curves over finite fields, which is the case of cryptographic applications. In this work, we focus on elliptic curves defined over finite fields and isogenies between such curves. An isogeny $\phi : E_1 \to E_2 \simeq E_1/H$ between two elliptic curves E_1, E_2 is a surjective homomorphism of the algebraic groups with a finite kernel H. We will be mostly interested in *cyclic* isogenies, i.e. those whose kernel is a cyclic subgroup.

In fact, we will mostly ignore the *group* structure of elliptic curves and the *mapping* (homomorphism) nature of isogenies, and focus on the *relation* of elliptic curves being N-isogenous. In addition, by an "elliptic curve" we will understand its isomorphism class, identified by the j-invariant. This relation can be described algebraically by *classical modular polynomials* $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$, which are symmetric polynomials of degree $\psi(N)$ in each variable, where $\psi(N) = N \cdot \prod_{\text{prime } \ell | N} \left(1 + \ell^{-1}\right)$ is the Dedekind psi function. In particular, $\psi(\ell^e) = (\ell + 1)\ell^{e-1}$ for any prime ℓ and $e \geq 1$.

Definition 1 (N-isogenous j-invariants)**.** For $N \geq 2$ coprime to the field characteristic p, we say that elements $j, j' \in \mathbb{F}$ are N-isogenous if $\Phi_N(j, j') = 0$.

Definition 2 (N-isogeny graph)**.** The N-isogeny graph (V, E_N) is a directed multigraph defined by the vertex set $V = \overline{\mathbb{F}}$ and the edge set

$$E_N = \left\{ (j, j') \in \overline{\mathbb{F}}^2 \mid \Phi_N(j, j') = 0 \right\},$$

where the number of edges $j \to j'$ is given by the multiplicity of $\Phi_N(j, j') = \Phi_N|_j(j')$ as a univariate polynomial in j' (see e.g. [Gal12, §25.2]).

Let $N = d_1 \times d_2 \times \ldots \times d_n$ for integers $d_i > 1$ in a fixed order. Then, any cyclic N-isogeny can be uniquely decomposed as a sequence of n isogenies of degrees $d_1, \ldots, d_n$ respectively. This naturally transfers to the correspondence of an edge in the graph (V, E_N) to a set of paths in the merged graph $(V, E_{d_1} \cup \ldots \cup E_{d_n})$.

An elliptic curve is called *supersingular*, if the trace of the Frobenius endomorphism is a multiple of the characteristic p. Supersingular isogeny graphs (when $p \nmid N$) are connected and isolated from ordinary curves, and their j-invariants can be defined over $\mathbb{F}_{p^2}$.

2.2 Modular curves

Usually, modular curves are defined as quotients of the complex upper half-plane by the action of certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$. However, they can also be defined purely algebraically. For a complete formal treatment, we refer to the standard literature [Igu59a, Igu59b], [DR73, Ch. IV-V], [KM85, Chs. 3,5,8], [Mil17]. For this work, $X_0(N)$ will be the most relevant modular curve; $X(N)$ and $X_1(N)$ are only needed to make references to the literature and to explain rotation automorphisms / radical formulas.

Definition 3. Fix an integer $N \geq 1$ and a field $\mathbb{F} \in \{\mathbb{Q}, \mathbb{F}_q\}$ of characteristic coprime to N or zero. The open modular curves $Y_0(N)$, $Y_1(N)$, $Y(N)$ are algebraic curves over $\mathbb{F}$ ($\mathbb{F}(\zeta_N)$ for $Y(N)$) whose geometric points parametrize (up to isomorphism) elliptic curves E together with:

- $Y_0(N)$: a cyclic subgroup of order N on E;

- $Y_1(N)$: a point of order N on E;
- $Y(N)$: a basis (P, Q) of $E[N]$ with a fixed Weil pairing $e_N(P, Q) = \zeta_N \in \overline{\mathbb{F}}$.

Proposition 1 ([DR73, Ch. IV], [KM85, Chs. 5,8]). *The described modular curves have smooth compactifications denoted by $X_0(N)$, $X_1(N)$, $X(N)$, respectively. The finitely many points in $X_0(N) \setminus Y_0(N)$ (resp. $X_1(N) \setminus Y_1(N)$ and $X(N) \setminus Y(N)$) are called* cusps.

Proposition 2 ([Mil17, Thm.6.1,§6-7]). *The classical modular equation $\Phi_N(j, j') = 0$ can be viewed as a singular plane model of $X_0(N)$.*

We remark that the reduction from $\mathbb{Q}$ ($\mathbb{Q}[\zeta_N]$ for $X(N)$) to positive characteristic $p \nmid N$ for these curves is formally stated in [Mil17, Thm.8.6,Thm.8.8], [DS05, Thm.8.6.1], [Igu59b].

The *cusps* are not parametrizing isogeny structures of elliptic curves but rather of the degenerate curve with $j = \infty$. In our models in Section 4, the cusps added are $\infty \in \mathbb{P}^1(\mathbb{F})$ for $X(1) \simeq X_1(1) \simeq X_0(1)$ (the j-line) and all its preimages under modular covers from other modular curves (i.e., natural projections forgetting the additional parametrized structure). The modular covers will map ∞ to itself, thus ∞ will be a cusp on all considered modular curves. This allows to work with the affine models without losing useful information. The other cusps can be easily computed (in the forms of cusp polynomials) to test validity of inputs in the implementations when necessary.

Proposition 3 ([FK90]). *The modular curves $X_0(N)$, $X_1(N)$, $X(N)$ have genus zero if and only if*

- *$X_0(N)$: $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$;*
- *$X_1(N)$: $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$;*
- *$X(N)$: $N \in \{1, 2, 3, 4, 5\}$;*

For the listed values of N, the respective modular curves over $\overline{\mathbb{F}}$ can be parametrized by $\overline{\mathbb{F}}$ (excluding the cusp at ∞). Such a parameter is often denoted by t_N, and in complex analysis is called a *Hauptmodul*. Since $\mathbb{P}^1(\mathbb{F})$ is smooth, such a model does not have singularities. In particular, it naturally distinguishes multiple N-isogenies between the same pair of j-invariants, however, only up to pre- and post-isomorphism. Furthermore, isogeny relations between successive parameters (needed to describe longer isogeny walks) may still have singularities.

Remark 1. There is a subtle difference between counting multiplicities as in Definition 2 and via $X_0(N)$. Both consider endpoints up to isomorphisms, but the former counts distinct cyclic subgroups on *one fixed* starting elliptic curve. For example, we have a double 2-isogeny edge from $j = 1728$ to $j = 287496$, but a single 2-isogeny edge in the other direction. On $X_0(2)$, we will see only one point for each direction, because the two cyclic subgroups on $j = 1728$ are related by an automorphism on that curve. The multiplicities can be extracted by evaluating the ramification index of the covers (see next sections).

Since $X_0(N)$ parametrizes a cyclic isogeny kernel, it also must parametrize all "intermediate" j-invariants and isogenies. Note that the model $\Phi_N(j_0, j_1) = 0$ may sometimes fail to do so due to singularities such as distinct N-isogenies between same j-invariants j_0, j_1, especially for large N.

Proposition 4. *An element $t_N \in X_0(N)$ parametrizes a sequence $\mathcal{J}_N(t_N) = (j_d)_{d|N}$ of j-invariants, $\mathcal{J}_N : X_0(N) \to X(1)^{\sigma_0(N)}$ with σ_0 being the number of positive divisors of N, such that $\Phi_\ell(j_d, j_{d\ell}) = 0$ for all $\ell \mid N$ and all $d \mid N/\ell$. In particular, the N-isogeny parametrized by t_N connects j_1 and j_N.*

Remark 2. Assuming t_N parametrizes an isogeny $\phi : E \to E/\langle P \rangle$ for some $P \in E[N]$, we have $j_1 = j(E), j_N = j(E/\langle P \rangle)$, and, more generally, $j_{N/d} = j(E/\langle [d]P \rangle)$. Note however that $X_0(N)$ only parametrizes such points P up to a constant multiple, since only the kernel subgroup is determined, in contrast to $X_1(N)$ which also fixes the point itself.

Concrete models for genus-zero $X_0(N)$ together with the maps $\mathcal{J}_N$ are well summarized in a work of Maier [Mai09], while being derived in parts long time ago [Kle78, Gie79, FK90]. We will use slight variations of these maps and models of curves $X_0(N)$, equivalent up to linear variable changes.

Example 1. For a prime ℓ, an element $t_{\ell^e} \in X_0(\ell^e)$ describes a path of length e in the ℓ-isogeny graph:

$$\mathcal{J}_{\ell^e}(t_{\ell^e}) = (j_1, j_\ell, j_{\ell^2}, \ldots, j_{\ell^e}), \quad \Phi_\ell(j_{\ell^i}, j_{\ell^{i+1}}) = 0 \quad \forall i \in \{0, \ldots, e-1\}\,.$$

Despite Φ_ℓ being symmetric, the parametrized paths are directed and non-backtracking in the sense of the parametrized isogenies being cyclic. Equivalently, the parametrization is ordered and the direction is simply a compact way to capture the order.

Example 2. For a composite $N = \ell_1^{e_1} \ldots \ell_k^{e_k}$, ℓ_i primes, an element $t_N \in X_0(N)$ describes a k-dimensional grid of j-invariants, where each prime ℓ_i defines a "direction" in which e_i steps are done. However, for genus-zero $X_0(N)$, we will only encounter $k \leq 2$, i.e., at most two distinct prime degrees.

In this work we focus on the abstract isogeny relation. However, since $X_0(N)$ parametrizes actual isogenies themselves, these parameters can be used to evaluate the isogeny mappings. General approach for this is described in [Tsu13] and [Gal12, §25.2]. The former is implemented in SageMath[1] [Sag26]. Furthermore, most of our concrete models are based on Montgomery curves (whenever $4|N$), and one can almost directly reuse known arithmetic and implementations (e.g. [Ren18]).

Relation to standard curve models While we will focus on abstract viewpoint of modular curves parametrizing isogeny structures, they are often realized by elliptic curve models used in practice. Concretely, if an elliptic curve family E_t with a parameter t has $j(E_t) \in \mathcal{J}_N(\sigma(t))$ in $\mathbb{F}(t)$ for some N, a rational model of $X_0(N)$, and a Möbius transformation $\sigma(t) = \frac{at+b}{ct+d}, ad - bc \neq 0$, then t parametrizes precisely $X_0(N)$ with E_t being one of the curves involved in the isogeny.

2.3 Coverings from $X_0(N)$ to $X_0(N/\ell)$

The modular curves $X_0(N)$ form a hierarchical structure, meaning that parameters for $X_0(N/\ell)$ structures (for $\ell|N$) included in the parametrized structure by $X_0(N)$ can be computed by rational maps. It is sufficient to know projection maps from $X_0(N)$ to $X_0(N/\ell)$ for all prime divisors ℓ of N, and any deeper projection can be constructed as their composition. For each such ℓ, we need to define two covers, which we will call *left* and *right* covers.

Proposition 5 (See e.g. [DI95, §7.3])**.** *For any $N > 1$, and $\ell|N$, there exist two rational projections (see Figure 1)*

$$\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell} : X_0(N) \to X_0(N/\ell)$$

such that $\mathbf{L}_{N,\ell}(t_N)$ parametrizes $(j_d)_{d|(N/\ell)}$ and $\mathbf{R}_{N,\ell}(t_N)$ parametrizes $(j_{\ell d})_{d|(N/\ell)}$, where t_N parametrizes $(j_d)_{d|N}$.

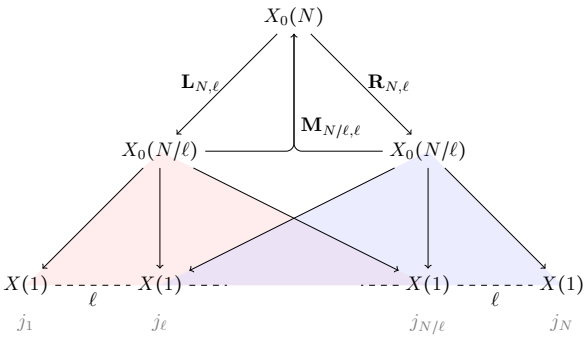

Figure 1: The two ℓ-coverings $\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell}$ from $X_0(N)$ and their inverse $\mathbf{M}_{N/\ell,\ell}$.

Since j_1, j_N from $\mathcal{J}_N(t)$ can still be recovered from $\mathbf{L}_{N,\ell}(t)$ and $\mathbf{R}_{N,\ell}(t)$, and they satisfy $\Phi_N(j_1, j_N) = 0$ which is a model for $X_0(N)$ by Proposition 2, we obtain the following.

Lemma 1. *The pair of covers* $(\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell})$ *is birational onto its image.*

We will typically use prime ℓ but the proposition equally applies to arbitrary $\ell | N$. Since any such substructure is identified by how many ℓ-isogenies are dropped in the beginning and in the end of the parametrized ℓ-isogeny paths, for each prime ℓ, any composition of such projection maps is identified by how many $\mathbf{L}$ and $\mathbf{R}$ steps it includes, and is independent of their order.

Proposition 6. *Compatible projection maps commute: for any* N *and* ℓ, ℓ' *such that* $(\ell \cdot \ell') | N$,

$$\begin{aligned}
\mathbf{L}_{N/\ell,\ell'} \circ \mathbf{R}_{N,\ell} &= \mathbf{R}_{N/\ell',\ell} \circ \mathbf{L}_{N,\ell'}, \\
\mathbf{L}_{N/\ell,\ell'} \circ \mathbf{L}_{N,\ell} &= \mathbf{L}_{N/\ell',\ell} \circ \mathbf{L}_{N,\ell'} &&= \mathbf{L}_{N,\ell\cdot\ell'}, \\
\mathbf{R}_{N/\ell,\ell'} \circ \mathbf{R}_{N,\ell} &= \mathbf{R}_{N/\ell',\ell} \circ \mathbf{R}_{N,\ell'} &&= \mathbf{R}_{N,\ell\cdot\ell'}.
\end{aligned}$$

For genus zero modular curves $X_0(N)$, all the projection maps were explicitly listed by Maier [Mai09], although most of them were already known before [Kle78, Gie79, FK90]. We will always assume that ∞ is a cusp on all genus-zero $X_0(N)$ and that the covers map cusps to cusps, and non-cusps to non-cusps.

Remark 3. We remark that coverings can be computed from scratch via rational parametrization of the corresponding modular polynomials (first, Φ_ℓ, and then ours $\Phi_{N,\ell}$, defined in Subsection 3.1). Thus, everything described in Section 2 can be easily computed from classical modular polynomials $\Phi_\ell(X, Y)$ for $\ell = 2, 3, 5, 7, 13$.

Reduction from $\mathbb{Q}$ The covers can be defined over $\mathbb{Q}$ and then reduced modulo any prime. Since $X_0(N)$ has a good reduction modulo any prime $p \nmid N$ (geometrically), it is left to check the reduction of the rational parametrization itself, for which it is sufficient to check that the degree of any cover $X_0(N) \to X(1)$ or $X_0(N) \to X_0(M)$, $M | N$, is preserved (when using an established model for $X(1)$ or $X_0(M)$ modulo p). The following lemma gives a simple criterion to check this. In all cases in this work, the parametrizations will have good reductions for all $p \nmid N$.

Lemma 2. *Let* $\pi : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ *be given by* $x \mapsto \frac{f(x)}{g(x)}$ *with* $f, g \in \mathbb{Z}[x]$. *If* $p \nmid f_d \cdot g_d \cdot \mathrm{Res}_x(f, g)$, *where* f_d *and* g_d *are respectively the leading coefficients of* f *and* g, *then the reduction of* π *modulo* p *preserves its degree.*

[1] See source code sage/src/sage/schemes/elliptic_curves /isogeny_small_degree.py.

2.4 Dual isogenies

Dual isogenies can be simply and abstractly expressed in terms of $X_0(N)$ parameters. The dual isogeny simply has all isogeny directions reversed, at every level of the hierarchy of covers. This corresponds to the change of the parametrized sequence from $(j_d)_{d|N}$ to $(j_{N/d})_{d|N}$. In other words, j_1 is swapped with j_N, j_ℓ is swapped with $j_{N/\ell}$, etc. However, one can also apply the duality map only to any subset of involved primes. Let $N = \ell^k M$ where prime $\ell \nmid M$. Then, the ℓ-duality map changes the parametrized sequence from $(j_{\ell^i d})_{0\le i\le k, d|M}$ to $(j_{\ell^{k-i} d})_{0\le i\le k, d|M}$.

For genus-zero modular curves, the corresponding involutions $X_0(N) \to X_0(N)$ can be expressed as degree-1 rational maps in terms of the parameters. In complex analysis, the full duality transformation is called the *Fricke involution* and the partial duality maps are called the *Atkin-Lehner involutions*.

Definition 4. Let $N = \ell^k M$ for prime $\ell \nmid M$. The ℓ-duality map on $X_0(N)$ is denoted by $\mathbf{w}_{N,\ell} = \mathbf{w}_{N,\ell^k}$. It is an involution such that

$$\mathcal{J}_N(t_N) = (j_{\ell^i d})_{0\le i\le k, d|M}, \qquad \mathcal{J}_N(\mathbf{w}_{N,\ell}(t_N)) = (j_{\ell^{k-i} d})_{0\le i\le k, d|M}.$$

For brevity, we extend the notation $\mathbf{w}_{N,d}$ for any composite $d|N$, defined to be a composition of $\mathbf{w}_{N,\ell_i^{e_i}}$ for all prime divisors ℓ_i of d with e_i being maximal such that $\ell_i^{e_i}|N$.

Note that $\mathbf{w}_{N,\ell}$ and $\mathbf{w}_{N,\ell'}$ for primes $\ell \neq \ell'$ commute, and thus, the extended notation is well-defined.

Proposition 7. *The coverings "anticommute" with duality by switching the direction:*

$$\mathbf{L}_{N,\ell} \circ \mathbf{w}_{N,\ell} = \mathbf{w}_{N/\ell,\ell} \circ \mathbf{R}_{N,\ell}$$

for all primes $\ell|N$. This also holds for ℓ not dividing N/ℓ by setting $\mathbf{w}_{N/\ell,\ell}$ to identity.

2.5 Lifting maps

2.5.1 Inverse of the prime-degree cover pair

Lemma 1 claims that the pair of covers

$$\pi_{N,\ell} = (\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell}) : X_0(N) \to (X_0(N/\ell))^2$$

is birational onto its image being another model of $X_0(N)$. For genus-zero $X_0(N/\ell)$, the image is given by $(X_0(N/\ell))^2/\Phi_{N/\ell,\ell}(X,Y)$ (Theorem 1). Therefore, the pair of covers (as rational maps) can be inverted by a rational map $\frac{f(x,y)}{g(x,y)}$ (applicable away from a finite number of points independent of the characteristic, including the singularities of $\Phi_{N/\ell,\ell}(X,Y)$). We denote this rational map by

$$\mathbf{M}_{N/\ell,\ell} : (X_0(N/\ell))^2/\Phi_{N/\ell,\ell} \dashrightarrow X_0(N),$$

We propose to use the following method [GC92, §5] to compute the inverse map algebraically, for the case of genus zero $X_0(N)$. Consider $\mathbb{Q}[t,x,y]$ and choose a monomial order lexicographic in t with arbitrary tie breaking in x, y (e.g., graded lexicographic). Compute any Gröbner basis of the ideal

$$\langle \mathrm{num}(\mathbf{L}_{N,\ell}(t) - x), \mathrm{num}(\mathbf{R}_{N,\ell}(t) - y)\rangle \subseteq \mathbb{Q}[t,x,y].$$

Since $t \cdot g(x,y) - f(x,y)$ belongs to this ideal and has degree 1 in t, a polynomial of this form (with nonzero and coprime f, g) must belong to the computed Gröbner basis (otherwise, it must be divisible by $\Phi_{N/\ell,\ell}(x,y)$ and thus the fraction is non-reduced). One can experiment with different monomial orders to get different expressions for t, since they are defined modulo the modular polynomial $\Phi_{N/\ell,\ell}(x,y)$ and different trade-offs may be possible.

Remark 4. Another related approach [GVR09] would be to compute the first subresultant $S_1(t, x, y)$ of the two polynomials $\mathrm{num}(\mathbf{L}_{N,\ell}(t) - x), \mathrm{num}(\mathbf{R}_{N,\ell}(t) - y)$ with respect to t. It needs to have degree 1 in t exactly, and thus yields a candidate for $f(x, y)$ and $g(x, y)$ as above. However, this does not directly give options to change the shape of the expression.

Remark 5. Similarly to the recursive nature of covering maps, the inverse maps for prime ℓ on different levels N can be composed recursively to compute the inverse of the $\mathcal{J}_N$ mapping.

Remark 6. Inverting the cover pairs pointwise can be equally achieved by a polynomial gcd computation:[2] write $x = \mathbf{L}_{N,\ell}(t), y = \mathbf{R}_{N,\ell}(t)$, then t can be found as a root of

$$f(t) = \gcd(\mathrm{num}(\mathbf{L}_{N,\ell}(t) - x), \mathrm{num}(\mathbf{R}_{N,\ell}(t) - y)) \in \mathbb{F}[t],$$

when x and y are plugged in. Its squarefree version $f_{\mathrm{red}} = \frac{f}{\gcd(f, f')}$ (assuming $\deg f < p$ or characteristic zero) is linear (away from singularities) and thus its root can be easily computed.

Reduction from $\mathbb{Q}$ It is easy to check for which characteristics a given lifting map behaves well.

Lemma 3. *Let $(\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell})$ be a rational parametrization of a genus-zero $X_0(N)$ with good reduction modulo p (Lemma 2), let $\Phi(x, y) = 0$ be the curve describing its image (see Subsection 3.1), and let $\mathbf{M}_{N/\ell,\ell}(x, y) = \frac{f(x,y)}{g(x,y)}$ over $\mathbb{Q}$, with $f, g \in \mathbb{Z}[x, y]$. Then, if p does not divide all coefficients of $\mathrm{Res}_y(g, \Phi)$, the lifting map $\mathbf{M}_{N/\ell,\ell}$ also has good reduction modulo p, meaning that it is a birational inverse of the pair $(\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell})$ over $\mathbb{F}_p$.*

Proof. The identity $\mathbf{M}_{N/\ell,\ell}(\mathbf{L}_{N,\ell}(t), \mathbf{R}_{N,\ell}(t)) = t$ holds over $\mathbb{Q}$ and thus over $\mathbb{F}_p$ if the reduction of $\mathbf{M}_{N/\ell,\ell}$ is a well-defined rational map on the image of the pair of covers. For this $\gcd(g, \Phi) = 1$ is sufficient. Since the image is parametrized by $(\mathbf{L}_{N,\ell}(t), \mathbf{R}_{N,\ell}(t))$, the two curves then have isomorphic function fields and thus are birational. If $\gcd(g, \Phi) \neq 1$ over $\mathbb{F}_p$, then the resultant of the two polynomials is identically zero modulo p. Therefore, p must divide all coefficients of $\mathrm{Res}_y(g, \Phi)$ for this to happen. Otherwise, the polynomials g and Φ reduced modulo p are coprime. □

2.5.2 Inverse of the different prime-degrees covers

Inverse maps to the coverings defined above can be applied recursively to compute the $X_0(\ell^e)$ parameter from $e+1$ ℓ-isogenous j-invariants, when ℓ is prime (away from singularities such as self-loops and double edges). They are also applicable for composite levels, but require the full grid of j-invariants. For example, for $N = 6$ we need the full 2-/3-isogeny rectangle as input, i.e. four j-invariants, in order to compute two $X_0(2)$ parameters related by a 3-isogeny (using $\mathbf{M}_{1,2}$) and then apply $\mathbf{M}_{2,3}$ to get the corresponding $X_0(6)$ parameter. For $N = 12$ we need to have the full grid of six j-invariants (a 4-isogeny combined with a 3-isogeny), etc.

Let $N = \ell \cdot \ell'$ for coprime ℓ, ℓ' (not necessarily primes). It would be more convenient to recover the corresponding parameter $t \in X_0(N)$ from single isogenous pairs/paths of j-invariants, i.e., parameters $t_0 \in X_0(N/\ell)$ and $t_1 \in X_0(N/\ell')$. Since the isogeny degrees ℓ, ℓ' are coprime, we can use the cover in the same direction. Experimentally, we observed much more compact maps when considering two right covers. For the described purpose, we extend the notation of the inverse map $\mathbf{M}_{N/\ell,\ell}$ of $(\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell})$ to the inverse map $\overline{\mathbf{M}}_{\ell,\ell'}$ of $(\mathbf{R}_{N,\ell'}, \mathbf{R}_{N,\ell})$:

$$\overline{\mathbf{M}}_{\ell,\ell'} : (X_0(\ell) \times X_0(\ell'))/{\sim} \to X_0(N).$$

[2] We thank an anonymous reviewer for this suggestion.

To see that $(\mathbf{R}_{N,\ell'}, \mathbf{R}_{N,\ell})$ is a birational equivalence, note that we can still recover j_ℓ and $j_{\ell'}$ from the two components, where $(j_1, \ldots, j_\ell, \ldots, j_{\ell'}, \ldots, j_N)$ is the parametrized level-N structure by $t_N \in X_0(N)$. These are the endpoints parametrized by $\mathbf{w}_{N,\ell}(t_N)$ and so t_N can be recovered from them by the usual argument (Φ_N is a model of $X_0(N)$).

The new inverse map $\overline{\mathbf{M}}_{\ell,\ell'}$ can also be computed using our previous method with a minor modification, by simply choosing two different degrees in the two covers. We compute the reduced Gröbner basis of the ideal

$$\langle \mathrm{num}(\mathbf{R}_{N,\ell'}(t) - x), \mathrm{num}(\mathbf{R}_{N,\ell}(t) - y) \rangle$$

and check for polynomials of the form $t \cdot g(x,y) - f(x,y)$, in order to get the desired expression for t in terms of the parameters $x = \mathbf{R}_{N,\ell'} \in X_0(N/\ell') = X_0(\ell)$ and $y = \mathbf{R}_{N,\ell} \in X_0(N/\ell) = X_0(\ell')$.

These expressions are quite useful since they allow to complete a j-invariant rectangle of ℓ- and ℓ'-isogenies only from the sides, implicitly based on the commutativity of the isogenies of coprime degrees. This also emphasizes that all the properties of modular curves that we describe can be computed from pure j-invariant sequences (although, only away from singularities, which we will discuss later), and do not require any extra information or equation solving. The inverse maps are rational by construction.

2.6 Rotation automorphisms

In the few cases when $X(N)$ has genus 0, we can parametrize all outgoing N-isogenies from a j-invariant by one field element. These cases coincide with the radical covers described above. In fact, it can be shown that, geometrically and with a fixed Weil pairing ζ_N, $X_0(4) \simeq X(2), X_0(9) \simeq X(3), X_0(16) \simeq X(4)$, but $X_0(25) \not\simeq X(5)$ as modular structures (the first two equivalences were shown in [Bea82] and more explicitly in [Mai09]). Thus, in the equivalence cases, given an ℓ^{2e}-isogeny parametrized by $t \in X_0(\ell^{2e})$, we can recover all ℓ^{2e}-isogenies with the same center by rational maps (in the field extension with the chosen ζ_N) from t (the same applies to $X_0(\ell^{2e+1})$ where the center refers to the unordered central edge on the path).

We can organize these maps simply by defining *rotation* automorphisms on these modular curves. Consider a path of length $2e$ (or $2e+1$) in the ℓ-isogeny graph. Split it into two halves (excluding the middle edge in the second case) and call them "tail" and "head". If we fix the tail, the head can be chosen among ℓ^e isogenies. Any operation that cycles through all these choices shall be called a *head rotation*, denoted $\mathbf{H}_{N,\ell^e}$. A *tail rotation* is defined analogously by fixing the head instead, denoted $\mathbf{T}_{N,\ell^e}$ (see Figure 2). Clearly, a head rotation conjugated with the duality involution $\mathbf{w}_{N,\ell^2}$ is a tail rotation: $\mathbf{T}_{N,\ell^e} = \mathbf{w}_{N,\ell^2} \circ \mathbf{H}_{N,\ell^e} \circ \mathbf{w}_{N,\ell^2}$. It is easy to see that all possible length-$2e$ (or $2e+1$) paths with the same center j_{ℓ^e} (or the same central edge) can be obtained by a sequence of rotations and duality maps.

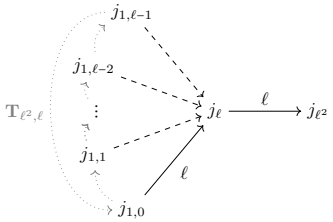

Figure 2: Tail rotation on $X_0(\ell^{2e})$.

An interpretation of the rotation operation is as follows. Let E be an elliptic curve and $E[\ell^e] = \langle P, Q \rangle$ be its full ℓ^e-torsion, ℓ prime. The $\ell^{e-1}(\ell+1)$ its distinct subgroups can be written as $\langle Q + [\ell r]P \rangle$ for $0 \le r < \ell^{e-1}$ and $\langle P + [i]Q \rangle$ for $0 \le i < \ell^e$. If P is fixed, we can cycle through ℓ^e isogenies $\langle P + [i]Q \rangle$ by ranging $i \in \mathbb{Z}/\ell^e\mathbb{Z}$. In particular, the increment of i defines the rotation operation.

Deriving rotation maps In all the cases that we will consider, the rotation will come from the radical expression of the right cover $\mathbf{R}_{N,\ell}(t) = t^\ell$ (up to linear substitutions). It

is easy to see that this cover is in fact the invariant of the tail rotation $\mathbf{T}_{N,\ell}$: $\mathbf{R}_{N,\ell} \circ \mathbf{T}_{N,\ell} = \mathbf{R}_{N,\ell}$, and all the ℓ parameters $\zeta_\ell^i \cdot t \in X_0(N)$ sharing this invariant, $0 \le i < \ell$, correspond to all the tail rotations.

Definition 5. Let $\mathbf{T}_{N,\ell}(t) = \zeta_\ell \cdot t$, $\mathbf{H}_{N,\ell}(t) = \mathbf{w}_{N,\ell} \circ \mathbf{T}_{N,\ell} \circ \mathbf{w}_{N,\ell}$.

Inheritance of automorphisms Note that rotation automorphisms of $X_0(N^2) \simeq X(N)$ for $N = 2, 3$ are inherited into $X_0(12)$ and $X_0(18)$, meaning that we can perform a 2- or 3-isogeny rotations inside these structures. Furthermore, automorphisms on genus zero curves $X_0(N)$ are clearly inherited to isogeny walks on such parameters. We emphasize that this does not require to initially work with modular parameters, as all these extra reachable j-invariants can be computed by rational maps from the corresponding j-invariant paths only, using the inverse maps. As an example, we deduce the following observation (conditional on inverse maps $\mathbf{M}_{1,2}, \mathbf{M}_{2,2}, \mathbf{M}_{4,2}, \mathbf{M}_{8,2}$, which we will provide in the next section):

Proposition 8. *A cyclic 2-isogeny walk of length $n \ge 3$ on $n+1$ j-invariants in fact rationally parametrizes $4n-6$ labelled j-invariants connected by 2-isogenies (see Figure 3), in the field extension containing $\zeta_4 = \sqrt{-1}$ and away from singularities. Similarly, a cyclic 3-isogeny walk of length $n \ge 1$ on j-invariants rationally parametrizes $3n-1$ labelled j-invariants, where each intermediate j-invariant on the main 3-isogeny path has explicit 3-isogenies to two extra j-invariants (requires ζ_3 in the field).*

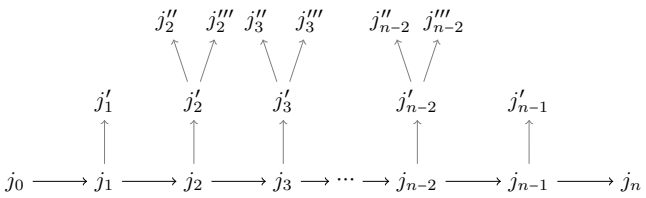

Figure 3: All $4n-6$ j-invariants determined by any cyclic 2-isogeny j-invariant path.

Proof. For $n = 3$ see the standard argument after the proof. Assume $n \ge 4$. For each five consecutive j-invariants on the main path, reconstruct the $X_0(16)$-parameter using the inverse maps recursively, and then use rotation operations and covers to compute the side j-invariants. The proof for 3-isogenies is similar, using three consecutive j-invariants for one $X_0(9) \simeq X(3)$ parameter. □

Remark 7. The aforementioned parametrization requires choice (and existence) of primitive 4th and 3rd roots of unity, which is guaranteed in $\mathbb{F}_{p^2}$.

Note that the statement about the sequence of j-invariants at depth 1 (j_i') for 2-isogenies is rather obvious, since one can divide the classical modular polynomial $\Phi_2(j_i, x)$ by $(x - j_{i-1})(x - j_{i+1})$ and recover the remaining root j_i'. However, for the depth 2 we are not aware of this being noticed in the literature. For 3-isogeny paths, each j_i spans two extra side j-invariants. In this case, even if the new j-invariants are just one 3-isogeny away from the path nodes, it was not clear that they can be computed algebraically, since the division of $\Phi_3(j_i, x)$ by $(x - j_{i-1})(x - j_{i+1})$ leaves a quadratic polynomial, requiring a square root computation.

2.7 Notation summary

Notations from this and the next section are summarized in Table 1. While our main focus will be on the modular curves $X_0(N)$, we will also consider a few other curves C which

Table 1: Notation summary. The subscript N referring to the modular curve $X_0(N)$ is replaced by C when working with a modular curve C instead. ℓ may be composite.

Notation	**Explanation**
$\mathcal{J}_N(t_N),\ t_N \in X_0(N)$	ordered sequence $(j_d)_{d\|N}$ of j-invariants parametrized by $t_N \in X_0(N)$
$\mathbf{L}_{N,\ell}, \mathbf{R}_{N,\ell} : X_0(N) \to X_0(N/\ell)$	coverings satisfying $\mathcal{J}_{N/\ell}(\mathbf{L}_{N,\ell}(t)) = (j_d)_{d\|(N/\ell)}$ and $\mathcal{J}_{N/\ell}(\mathbf{R}_{N,\ell}(t)) = (j_{\ell d})_{d\|(N/\ell)}$, where $\mathcal{J}_N(t) = (j_d)_{d\|N}$
$\mathbf{M}_{N,\ell} : (X_0(N))^2/\Phi_{N,\ell} \dashrightarrow X_0(\ell N)$	inverse of $(\mathbf{L}_{\ell N,\ell}, \mathbf{R}_{\ell N,\ell})$
$\overline{\mathbf{M}}_{\ell,\ell'} : (X_0(\ell) \times X_0(\ell'))/\sim \dashrightarrow X_0(N)$	inverse of $(\mathbf{R}_{N,\ell'}, \mathbf{R}_{N,\ell})$, where $N = \ell \cdot \ell'$
$\mathbf{w}_{N,\ell} : X_0(N) \to X_0(N)$ $N = \ell M$, $\gcd(\ell, M) = 1$	ℓ-duality map (Atkin-Lehner involution): $\mathcal{J}_N(t) = (j_{d\cdot b})_{d\|M, b\|\ell}$, $\mathcal{J}_N(\mathbf{w}_{N,\ell}(t)) = (j_{d\cdot \ell/b})_{d\|M, b\|\ell}$
$\mathbf{T}_{N,\ell}, \mathbf{H}_{N,\ell} : X_0(N) \to X_0(N)$	tail/head rotation - cycling through the ℓ first/last ℓ-isogenies on the parametrized isogeny paths
$\Phi_{C,\ell}, \Phi_{N,\ell}$	the modular polynomial of degree ℓ on the modular curve C or $X_0(N)$

have one or more covers to $X_0(N)$ for some N. Whenever possible, the maps/relations in this section are extended to apply to these curves in a compatible way, acting on the included $X_0(N)$ structures.

3 Isogeny walks over modular curves

In this section, we will study representations of isogeny walks using genus-zero modular curves. Subsection 3.1 describes the key ingredient - non-backtracking modular polynomials - and how to derive them, including radical cases. Subsection 3.2 shows that chaining these yields cyclic isogeny walks, as expected; it also shows that resultants can be used directly to compute modular polynomials of product degrees. Finally, Subsection 3.3 shows how walks over modular curves are getting more smooth with more level structure.

3.1 Non-backtracking modular polynomials

While classical modular polynomials $\Phi_N(j, j')$ relate N-isogenous curves identified by j-invariants, we are also interested in polynomials relating "ℓ-isogenous" elements of $X_0(N)$ (and of some other modular curves). This means that the whole structure of j-invariants parametrized by t_1 is related to that of t_2 by an ℓ-isogeny, and we are looking for the corresponding algebraic relation $\Phi_{N,\ell}(t_1, t_2) = 0$ between t_1 and t_2. This relation is naturally defined as follows.

Definition 6. The *degree-d modular polynomial* for a genus-zero $X_0(N)$ is (up to sign) the primitive integer polynomial $\Phi_{N,d}(X, Y) \in \mathbb{Z}[X, Y]$ defining the affine chart of the image curve of the pair of covers

$$(\mathbf{L}_{Nd,d}, \mathbf{R}_{Nd,d}) : X_0(Nd) \to (X_0(N))^2 \simeq (\mathbb{P}^1)^2.$$

This notion is extended to arbitrary genus-zero modular curves C with a chosen cover π to $X_0(N)$, where a *degree-d modular polynomial* is any nontrivial irreducible and primitive integer polynomial dividing $\mathrm{num}(\Phi_{N,d}(\pi(X), \pi(Y)))$.

This definition requires to work with a model of $X_0(Nd)$ which is allowed to have higher genus, which can be inconvenient. The following theorem shows how to compute such modular polynomials directly from a parametrization of $X_0(N)$ when a prime $d = \ell$ already divides N. We will use the following basic lemma for several proofs.

Lemma 4. *Let $\varphi : A \to D, \psi : B \to D$, be nonconstant separable morphisms of irreducible projective curves over $\mathbb{F}$ (automatically separable if $\mathrm{char}\,\mathbb{F} = 0$ or $\mathrm{char}\,\mathbb{F} \nmid \deg\varphi \cdot \deg\psi$), and consider the fiber-product variety*

$$Z = A \times_D B = \{(a, b) \in A \times B : \varphi(a) = \psi(b)\}.$$

Let $Z_1, \ldots, Z_n \subseteq Z$ be pairwise distinct irreducible curves such that

$$\sum_{i=1}^{n} \deg \pi_i = \deg\varphi \cdot \deg\psi, \quad \pi_i : Z_i \to D : (a, b) \mapsto \varphi(a) = \psi(b).$$

Then the one-dimensional irreducible components of Z are exactly $Z_1, \ldots, Z_n$.

Proof. In the following, work with the algebraic closure of $\mathbb{F}$. Consider a generic point in D. It has $\deg\phi \times \deg\psi$ preimages in Z under $\pi(a, b) = \varphi(a) = \psi(b)$ because the covers are separable and have finite fibers. Therefore, π maps every irreducible curve in Z onto D. Each such curve contributes exactly $\deg\pi_i$ of the preimages (outside of the branch locus). All these points are pairwise distinct (away from the finite intersections of the irreducible curves). If $\sum_i \deg\pi_i = \deg\phi \times \deg\psi$, then there is no space for another irreducible curve in Z. Therefore, Z consists precisely of $Z_1, \ldots, Z_n$, and, possibly, a finite number of isolated points. □

Theorem 1. *For a prime ℓ dividing N, $X_0(N)$ of genus zero we have over $\mathbb{Q}$*

$$\Phi_{N,\ell}(X, Y) = \begin{cases} \mathrm{prim}\left(\mathrm{num}(\mathbf{L}_{N,\ell}(Y) - \mathbf{R}_{N,\ell}(X))\right), & (\ell^2 \mid N), \\ \mathrm{prim}\left(\frac{\mathrm{num}(\mathbf{L}_{N,\ell}(Y) - \mathbf{R}_{N,\ell}(X))}{\mathrm{num}(Y - \mathbf{w}_{N,\ell}(X))}\right), & (\ell^2 \nmid N). \end{cases}$$

Proof. We first describe a general setup for applying Lemma 4. Write $D = X_0(N/\ell)$ and $Z = X_0(N) \times_D X_0(N)$ for the fiber-product induced by the two covers: $\mathbf{R}_{N,\ell}, \mathbf{L}_{N,\ell}$. The double cover $(\mathbf{L}_{N\ell,\ell}, \mathbf{R}_{N\ell,\ell}) : X_0(N\ell) \to (X_0(N))^2$ is birational to its image $Z_1 \subseteq (X_0(N))^2$ (Lemma 1). By Proposition 6, we have $\mathbf{R}_{N,\ell}(\mathbf{L}_{N\ell,\ell}(t)) = \mathbf{L}_{N,\ell}(\mathbf{R}_{N\ell,\ell}(t))$. Therefore, Z_1 belongs to the fiber-product (and is irreducible).

(Case $\ell^2 \mid N$) Then, all the four covers have the same degree ℓ. The degree of $Z_1 \to D$ is the same as the degree of $X_0(N\ell)$ over D which is equal to

$$\deg \mathbf{R}_{N,\ell} \circ \mathbf{L}_{N\ell,\ell} = \deg \mathbf{L}_{N,\ell} \circ \mathbf{R}_{N\ell,\ell} = \ell^2.$$

By Lemma 4, it follows that Z_1 is the only irreducible component of Z. Therefore, $\mathbf{R}_{N,\ell}(X) = \mathbf{L}_{N,\ell}(Y)$ describes the affine chart of the birational image of $X_0(N\ell)$ in $(X_0(N))^2$.

(Case $\ell^2 \nmid N$) The only difference with the previous case is that the degrees of $\mathbf{L}_{N,\ell}$ and $\mathbf{R}_{N,\ell}$ are equal to $\ell + 1$, because they exhaust the full ℓ-level structure. The extra factor corresponds to the degenerate non-cyclic continuation, namely the dual isogeny: $Y = \mathbf{w}_{N,\ell}(X)$. This equation implies (by applying $\mathbf{L}_{N,\ell}$ to both sides)

$$\mathbf{L}_{N,\ell}(Y) = \mathbf{L}_{N,\ell}(\mathbf{w}_{N,\ell}(X)) = \mathbf{R}_{N,\ell}(X),$$

where we used Proposition 6 and the special case of Proposition 7. It follows that the numerator of $Y - \mathbf{w}_{N,\ell}(X)$ defines an irreducible curve $Z_2 \subseteq Z$ and must divide the numerator of $\mathbf{L}_{N,\ell}(Y) - \mathbf{R}_{N,\ell}(X)$ (at least once) with a quotient $Q(X, Y)$. We apply Lemma 4 using

$$\begin{aligned}\deg(Z_1 \to D) + \deg(Z_2 \to D) &= \deg(X_0(N\ell) \to X_0(N/\ell)) + (\ell+1) \\ &= \ell(\ell+1) + (\ell+1) = (\ell+1)^2 = \deg \mathbf{R}_{N,\ell} \cdot \deg \mathbf{L}_{N,\ell}\end{aligned}$$

to show that $Z = Z_1 \cup Z_2$ and the quotient Q defines a curve birational to $Z_1 \simeq X_0(N\ell)$. Indeed, the degree of $\mathbb{Q}$ over D is at most $\ell(\ell+1)$ which is exactly the degree of Z_1 over D, and Q vanishes on Z_1. □

Remark 8. The reduction of $\Phi_{N,\ell}$ modulo $p \nmid N$ follows the same derivation in the characteristic-p field, with prim replaced by an arbitrary constant scaling. The primitivity of $\Phi_{N,\ell}$ thus implies that it can be directly used in such fields.

Radical isogenies When the modular curve has a cover to $X(\ell)$ (genus-zero cases include $X_0(N)$ with $N = 4, 8, 9, 12, 16, 18$ and $X(5)$), we can get $\mathbf{R}_{N,\ell}(t) = t^\ell$ up to a linear change of variables (this follows from concrete maps we will provide in Section 4). We then deduce a (multivalued) radical expression of an isogeny step, where the radicand is simply the ℓth power of the argument composed with the Möbius transformations (duality involutions) on the two sides. We remark that in our expressions we have expressions equivalent to t^ℓ up to a linear substitution, for which we provide the full radicand expressions in Table 4. We also note that all non-backtracking 2-isogeny modular polynomials directly yield radical expressions since every quadratic equation can be solved using a single radical.

Proposition 9. *For the cases mentioned above, when $\mathbf{R}_{N,\ell}(t) = t^\ell$, the modular equation $\mathbf{R}_{N,\ell}(x) - \mathbf{L}_{N,\ell}(y) = 0$ (whose numerator is $\Phi_{N,\ell}(x, y)$) can be written in the radical forms*

$$x = \sqrt[\ell]{\mathbf{w}_{N/\ell,\ell}(\mathbf{w}_{N,\ell}(y)^\ell)}, \qquad y = \mathbf{w}_{N,\ell}\left(\sqrt[\ell]{\mathbf{w}_{N/\ell,\ell}(x^\ell)}\right).$$

Proof. Using Proposition 7, we get

$$\mathbf{R}_{N,\ell}(x) = x^\ell = \mathbf{L}_{N,\ell}(y) = \mathbf{w}_{N/\ell,\ell}(\mathbf{R}_{N,\ell}(\mathbf{w}_{N,\ell}(y))) = \mathbf{w}_{N/\ell,\ell}(\mathbf{w}_{N,\ell}(y)^\ell).$$

The other direction can be done by inverting the duality involutions and radicals/powerings. □

Remark 9. The original radical expressions in [CDV20] were derived based on the cyclic property of the covers $\mathbf{L}, \mathbf{R} : X(N) \to X_1(N)$. In the style of our framework, we can write it as follows. Let $u, v \in X_1(N)$ define a cyclic N^2-isogeny (with additional exact point data). Such a pair in fact defines a full $X(N)$ structure, with covers

$$\begin{aligned}\mathbf{L} &\coloneqq X(N) \to X_1(N) \coloneqq t \mapsto u, \\ \mathbf{R} &\coloneqq X(N) \to X_1(N) \coloneqq t \mapsto v.\end{aligned}$$

An equation (or, in general, an ideal) characterizing this relation between u and v is simply

$$u \in \mathbf{L}(\mathbf{R}^{-1}(v)).$$

In other words, the connection is drawn from the modular curve *above* the one with the parameters u, v (first invert, then project).

In our expression, we use instead the modular curve *below* the one with the parameters (first project, then invert):

$$u \in \overline{\mathbf{R}}^{-1}(\overline{\mathbf{L}}(v)),$$

While this is less generic since it requires radical covers downwards, this leads to simpler derivation when such covers are available. The resulting equations however have to be equivalent since they characterize the same relation between u and v.

3.2 Chaining modular polynomials

The crucial property of any such modular polynomials, in contrast to general expressions of $X_0(N)$ (as e.g., in [Yan06, TY09]), is that they can be directly chained to describe an arbitrarily long, cyclic ℓ-isogeny walk. The following result is a generalization of the modular towers of Elkies [Elk97] to cases when ℓ^2 does not divide N, with a bit more detailed argumentation based on Lemma 4.

Theorem 2. *Let $t_1, \dots, t_{n+1} \in X_0(N)$, genus-zero $X_0(N)$, prime $\ell | N$, and $\Phi_{N,\ell}(t_i, t_{i+1}) = 0$ for $1 \le i \le n$. This variety is birational to $X_0(N\ell^n)$, i.e., it parametrizes cyclic $N\ell^n$-isogenies.*

Proof. By definition, the variety cut out by the modular polynomial $\Phi_{N,\ell}$ is birational to $X_0(N\ell)$ which parametrizes cyclic $N\ell$-isogenies. Therefore, every pair of neighbors $u_i = (t_i, t_{i+1})$ is birational to $X_0(N\ell)$ being an image of the cover pair $(\mathbf{L}_{N\ell,\ell}, \mathbf{R}_{N\ell,\ell})$. Clearly, we have $\mathbf{R}_{N\ell,\ell}(u_i) = t_{i+1} = \mathbf{L}_{N\ell,\ell}(u_{i+1})$ for all i. This is the base case for the induction.

Assume that we are given a variety $(u_1, \dots, u_{m+1}) \in X_0(M)$ for arbitrary M, $\ell^2 \mid M$, such that $\mathbf{R}_{M,\ell}(u_i) = \mathbf{L}_{M,\ell}(u_{i+1})$ for all i. Then, we apply arguments from the first part of the proof of Theorem 1 (note that we may not be in the genus-zero case but the discussion there does not depend on this). Concretely, using Lemma 4, we obtain that each pair of neighbors (u_i, u_{i+1}) when viewed as the fiber product $\mathbf{R}_{M,\ell}(u_i) = \mathbf{L}_{M,\ell}(u_{i+1})$ (degree ℓ each) is birational to $v_i \in X_0(M\ell)$, with $u_i = \mathbf{L}_{M\ell,\ell}(v_i)$ and $u_{i+1} = \mathbf{R}_{M\ell,\ell}(v_i)$. We thus obtain a new sequence $v_i, \dots, v_m \in X_0(M\ell)$ with the same required property but shorter by one element and of level increased by the factor ℓ.

Repeating this procedure n times starting from the initial sequence $t_1, \dots, t_{n+1}$, we obtain that it is birational to $w_1 \in X_0(N\ell^n)$.

□

Note that classical modular polynomials $\Phi_N = \Phi_{1,N}$ are chainable too, but they allow backtracking when chained directly. Using $N = \ell^n$ for some ℓ, n allows to restrict to cyclic isogenies but this leads to very large equations. The non-backtracking property also allows to compute bivariate models for longer walks via resultants. Note that these are still non-backtracking, in contrast to models obtained by similar resultants from classical modular polynomials Φ_ℓ.

Proposition 10. *Let $d_1 \ge 2, d_2 \ge 2$ such that $\mathrm{rad}(d_1 d_2) | N$ for $X_0(N)$ of genus zero, $p \nmid N$. Then, up to a constant scalar α, over $\mathbb{Q}$ or over $\mathbb{F}_p$,*

$$\Phi_{N,d_1 d_2}(X, Y) = \alpha \cdot \mathrm{Res}_Z(\Phi_{N,d_1}(X, Z), \Phi_{N,d_2}(Z, Y)).$$

Proof. Observe that the curve $\Phi_{N,d_1}(X, Z)$ is birational to $X_0(Nd_1)$ and $\Phi_{N,d_2}(Z, Y)$ is birational to $X_0(Nd_2)$, by Lemma 1 and Definition 6. Denote these elements by t_1 and t_2. We have maps $\varphi = \mathbf{R}_{Nd_1,d_1} : X_0(Nd_1) \to X_0(N)$ and $\psi = \mathbf{L}_{Nd_2,d_2} : X_0(Nd_2) \to X_0(N)$, of degrees d_1 and d_2 respectively, due to the radical assumption. Applying Lemma 4, we get that $X_0(Nd_1d_2)$ is the only irreducible component of the fiber product $X_0(Nd_1) \times_{X_0(N)} X_0(Nd_2)$ given by φ and ψ. Therefore, the variety $(X, Y, Z) \in (X_0(N))^3$ cut out by $\Phi_{N,d_1}(X, Z) = \Phi_{N,d_2}(Z, Y) = 0$ is birational to $X_0(Nd_1d_2)$. Furthermore, let $T \in X_0(Nd_1d_2)$ correspond to such a triple (X, Y, Z). We have $X = \mathbf{L}_{Nd_1,d_1}(\mathbf{L}_{Nd_1d_2,d_2}(T))$ and $Y = \mathbf{R}_{Nd_2,d_2}(\mathbf{R}_{Nd_1d_2,d_1}(T))$. The curve defining the image of this pair of covers (which is Φ_{N,d_1d_2} by definition) can be obtained by eliminating Z from the ideal, which is precisely what the resultant $R = \mathrm{Res}_Z(\Phi_{N,d_1}(X, Z), \Phi_{N,d_2}(Z, Y)$ computes. The standard resultant degree bound gives $\max(\deg_X R, \deg_Y R) \le d_1 d_2$ which matches the expected degree of the irreducible Φ_{N,d_1d_2} which must divide the resultant. Therefore, it equals the resultant up to a scalar. The same discussion above applies over $\mathbb{F}_p$ as well. □

Corollary 1. *Let $\ell|N$ be prime, with $X_0(N)$ of genus zero. Then, for any $n \geq 2$,*

$$\Phi_{N,\ell^n}(x,y) = \alpha \cdot \mathrm{Res}_z(\Phi_{N,\ell^{n-1}}(x,z), \Phi_{N,\ell}(z,y))$$

for some nonzero constant α.

We emphasize again that these equations are models of $X_0(Nd_1d_2)$ and $X_0(N\ell^n)$ respectively, which means they are non-backtracking, i.e. they parametrize cyclic isogenies (this requires $\mathrm{rad}(d_1d_2)|N$ resp. $\ell|N$).

3.3 Reduced singularities

The overlapping isogeny parts ($\mathbf{R}_{N,\ell}(u_i) = \mathbf{L}_{N,\ell}(u_{i+1})$) significantly reduce the amount of singularities (compared to using chains of classical modular polynomials, where every double edge in the graph creates a singularity of the whole walk). In fact, when $\ell|N$, singularities may only occur at the cusps or when the parametrized isogeny walks cover the so called *elliptic points*, which can only occur around $j = 0$ or $j = 1728$. Furthermore, for many values of N and ℓ, the parametrization is completely smooth (over non-cusps), meaning in particular that the walks described by $\Phi_{N,\ell}(t_i, t_{i+1}) = 0$ are in bijection with $N\ell^n$-isogenies (up to compositions with pre- and post-isomorphisms).

Definition 7. Let $N \geq 1$. A non-cusp point $t \in X_0(N)$ (i.e., $t \in Y_0(N)$) is called an *elliptic point* if it parametrizes a pair (E, C) (an elliptic curve and its cyclic subgroup of order N) with $\sigma(C) = C$ for some automorphism $\sigma \neq \pm 1$ of E.

Lemma 5. *Let prime $\ell|N$, $p \nmid N$, $X_0(N)$ of genus zero, and consider a field $\mathbb{F}$ of characteristic 0 or $p > 3$ not dividing N. Let $(x,y) \in X_0(N)^2$ be a non-cusp zero of $\Phi_{N,\ell}$. If $\mathbf{R}_{N,\ell}(x) = \mathbf{L}_{N,\ell}(y)$ is not an elliptic point, then neither of the partial derivatives vanish:*

$$\partial_x \Phi_{N,\ell}(x,y) \;\neq\; 0 \;\neq\; \partial_y \Phi_{N,\ell}(x,y).$$

Proof. First, we show that $\partial_t \mathbf{L}_{N,\ell}(t) \neq 0$ when t is not a cusp and $\mathbf{L}_{N,\ell}(t)$ is not an elliptic point. The same applies to $\mathbf{R}_{N,\ell}$ by Proposition 7, noting that the duality operators preserve the properties of being a cusp or an elliptic point. Let (E, D) be the pair (elliptic curve, cyclic subgroup of order N/ℓ) parametrized by $\mathbf{L}_{N,\ell}(t) \in X_0(N/\ell)$. Consider its fibers over $\mathbf{L}_{N,\ell}$, which are pairs (E, C) with C being a degree-N cyclic subgroup on E extending D. There are *exactly* ℓ of them when $\ell \mid N/\ell$, and $\ell + 1$ of them otherwise. Vanishing $\partial_t \mathbf{L}_{N,\ell}(t)$ means reduced number of distinct points in the fiber (defined up to an isomorphism). This implies existence of a repeated fiber - a non-equal (by the counting above) yet isomorphic such pair (E, C_1), (E, C_2). Therefore, there exists an automorphism $\sigma \neq \pm 1$ of E such that $\sigma(C_1) = C_2$. Restricting to the order-N/ℓ subgroup D, we observe that $\sigma(D) = D$, implying that $\mathbf{L}_{N,\ell}(t)$ defines an elliptic point.

Writing Theorem 1 (and using Remark 8) in rational form we get

$$\mathbf{L}_{N,\ell}(y) - \mathbf{R}_{N,\ell}(x) = \frac{\alpha \cdot \Phi_{N,\ell}(x,y) \cdot Q(x,y)}{d_L(y) \cdot d_R(x)}$$

for $Q(x,y) = \mathrm{num}\,(y - \mathbf{w}_{N,\ell}(x))$ if $\ell^2 \nmid N$ and $Q(x,y) = 1$ otherwise, $d_L(y)$ and $d_R(x)$ being the denominators of $\mathbf{L}_{N,\ell}(y)$ and $\mathbf{R}_{N,\ell}(x)$ respectively. Since x, y are non-cusps, the denominators are nonzero - $d_L(y) \neq 0 \neq d_R(x)$ - and we differentiate the equation with respect to x and restrict to $\Phi_{N,\ell}(x,y) = 0$ to get

$$\begin{aligned} -\partial_x \mathbf{R}_{N,\ell}(x) = \alpha \cdot \Phi_{N,\ell}(x,y) \cdot \partial_x \left(\frac{Q(x,y)}{d_L(y) d_R(x)} \right) + \alpha \cdot \partial_x \Phi_{N,\ell}(x,y) \cdot \frac{Q(x,y)}{d_L(y) d_R(x)} \\ = \alpha \cdot \partial_x \Phi_{N,\ell}(x,y) \cdot \frac{Q(x,y)}{d_L(y) d_R(x)}. \end{aligned}$$

Since $\mathbf{R}_{N,\ell}(x)$ is neither an elliptic point nor a cusp, the lefthand side is nonzero and thus all factors on the right too: $\partial_x \Phi_{N,\ell}(x,y) \neq 0$. The case of the partial derivative with respect to y is proven symmetrically. □

In the following, $\mathcal{C}_N \subseteq \mathbb{P}^1$ is the set of cusps of the modular curve $X_0(N)$.

Theorem 3. *Let prime $\ell|N$, $X_0(N)$ of genus zero, and consider a field $\mathbb{F}$ of characteristic 0 or $p > 3$ not dividing N. Let $C = (u_1, \ldots, u_{n+1})$ be the affine curve over $\mathbb{F}$ cut out by the equations $\Phi_{N,\ell}(u_i, u_{i+1}) = 0$ for all $1 \leq i \leq n$ (a model of $X_0(N\ell^n)$ by Theorem 2). Then, a non-cusp point $(t_1, \ldots, t_{n+1}) \in C$ is smooth if for all $1 \leq i \leq n$, $r_i = \mathbf{R}_{N,\ell}(t_i) = \mathbf{L}_{N,\ell}(t_{i+1})$ is not an elliptic point. In particular:*

1. *isogeny walks represented by C away from $j = 0$ and $j = 1728$ are smooth;*
2. *$C \setminus (\mathcal{C}_N)^{n+1}$ is isomorphic to $Y_0(N\ell^n)$ for (N, ℓ) pairs $(8,2)$, $(16,2)$, $(12,2)$, $(18,2)$, $(12,3)$, $(18,3)$.*

Remark 10. If one restricts to the supersingular locus and the characteristic is such that $j = 0$ and/or $j = 1728$ are not supersingular, other pairs may be included. For example, for $p \equiv 1 \pmod{12}$ the curve C is smooth over supersingular isogeny walks for all pairs (N, ℓ) (with $\ell|N$), including the genus-zero ones $(2,2), (3,3), (6,2), (6,3), (9,3), (4,2)$.

Proof. For $T = (t_1, \ldots, t_{n+1}) \in C$, write the Jacobian matrix

$$J = (J_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n+1}, \quad J_{i,j} = \partial_{u_j} \Phi_{N,\ell}(u_i, u_{i+1}) = \begin{bmatrix} a_1 & b_1 & & & \\ & a_2 & b_2 & & \\ & & \ddots & \ddots & \\ & & & a_n & b_n \end{bmatrix}$$

evaluated at $u_i = t_i$ for all i. The curve is nonsingular at T when this matrix has rank n ($n+1$ variables, dimension 1). The Jacobian matrix is bidiagonal: its nonzero entries are only on the diagonals $a_i = J_{i,i}$ and $b_i = J_{i,i+1}$. Removing i-th column gives minor $M_i = \left(\prod_{j=1}^{i-1} a_j\right)\left(\prod_{j=i}^{n} b_j\right)$. The rank is full when at least one such minor is nonzero. One can deduce that degeneracy requires $a_i = b_j = 0$ for some $i \leq j$. By using Lemma 5, we see all $r_i = \mathbf{R}_{N,\ell}(t_i)$ are neither elliptic points nor cusps under the assumption, therefore, none of the b_i is zero and J has full rank n. Thus, the curve C is smooth at $(t_1, \ldots, t_{n+1})$.

The consequence 1 is based on the fact that an elliptic point $v \in X_0(N/\ell)$ has $\mathcal{J}_{N/\ell}(v) = \{0\}$ or $\{1728\}$ as a set. The smoothness in consequence 2 is based on verifying that the corresponding covers (which we will give in Section 4) have derivatives vanishing only over the cusps. More generally, it can be formulated in terms of known counts of elliptic points on $X_0(M)$ with $j(E) = 1728$ and $j(E) = 0$ respectively (see [DS05, Cor.3.7.2]). This implies that $C \setminus (\mathcal{C}_N)^{n+1}$ is smooth.

The covers define recursively a birational morphism $\overline{\pi} : X_0(N\ell^n) \to \overline{C}$, where $\overline{C}$ is the projective closure of C. Since $C \setminus (\mathcal{C}_N)^{n+1}$ is smooth and $X_0(N\ell^n)$ is projective, the restriction of the birational inverse $\overline{\psi} : C \setminus (\mathcal{C}_N)^{n+1} \to X_0(N\ell^n)$ extends to a morphism. Since covers preserve cusps/non-cusps, it restricts to $\psi : C \setminus (\mathcal{C}_N)^{n+1} \to Y_0(N\ell^n)$. Letting $\pi : Y_0(N\ell^n) \to C \setminus (\mathcal{C}_N)^{n+1}$ be the restriction of $\overline{\pi}$, we note that $\pi \circ \psi$ and $\psi \circ \pi$ are the identity maps on $C \setminus (\mathcal{C}_N)^{n+1}$ and $Y_0(N\ell^n)$ respectively. Therefore, these are inverse isomorphisms.

□

4 Instantiation for various genus-zero modular curves

In this section, we instantiate the framework from the previous section concretely, by which we mean choosing a concrete rational model of each considered modular curve. We recall that these models are related by Möbius transformations $t \mapsto \frac{at+b}{ct+d}$. We provide all the basic maps required to work with these models, as well as modular polynomials of small prime levels included in the parametrization. The coverings $\mathbf{L}_{C,\ell}$, $\mathbf{R}_{C,\ell}$ and ℓ-duality maps $\mathbf{w}_{C,\ell}$ were already listed in previous works (most comprehensively in [Mai09] and partially in [Col22]), summarized in Table 2. The inverses $\mathbf{M}_{C,\ell}$ (resp. $\overline{\mathbf{M}}_{\ell,\ell'}$) of the $(\mathbf{L}_{C,\ell}, \mathbf{R}_{C,\ell})$ pairs (resp. $(\mathbf{R}_{C,\ell'}, \mathbf{R}_{C,\ell})$ pairs), the level-ℓ modular polynomials were not explicitly computed systematically in this form before and are presented in Table 3 and Table 6. Some other maps are provided in App. C or in the supplementary material. We report explicit expressions for radicands on modular curves $X_0(N)$ with radical right covers. Let t, u satisfy $\Phi_{N,\ell}(t,u) = 0$. To show a radical isogeny expression in "backwards" direction, we can express t^ℓ as a function of u, namely $\mathbf{w}_{N/\ell,\ell}\left(\mathbf{w}_{N,\ell}(u)^\ell\right)$. To show a radical isogeny expression in the forward direction, we can express $\mathbf{w}_{N,\ell}(u)^\ell$ as a function of t, namely $\mathbf{w}_{N/\ell,\ell}(t^\ell)$. This simplified explanation assumes the normalized coordinates with $\mathbf{R}_{N,\ell}(t) = t^\ell$. The resulting expressions (including the correction from non-normalized coordinates) are given in Table 4, and the additional ones obtained directly from non-backtracking 2-isogeny modular polynomials are given in Table 5.

4.1 Levels $2, 4, 8, 16$

We base our parametrization of $X_0(N)$ for $N \in \{2, 4, 8, 16\}$ (all cases of which have genus 0) on the Montgomery model $E_A : y^2 = x^3 + Ax^2 + x$, mainly due to its widespread use in elliptic and isogeny-based cryptography, but also due to the simplest (sparsest) modular polynomials that it yields. This also helps to explain some arithmetic tricks used in the literature and provides direct access to computing the parameterized 2-/4-isogenies using existing formulas. App. A summarizes the basic structure of the 4-torsion of E_A. The $X_0(N)$ parameters, $N = 1, 2, 4, 8, 16$, are respectively:

- $X_0(1)$: the j-invariant of E_A;
- $X_0(2)$: the Montgomery discriminant $D = 16(A^2 - 4)$;
- $X_0(4)$: the A-coefficient $A = -a - \frac{1}{a}$;
- $X_0(8)$: the x-coefficient a of a nonconstant order-2 point on a Montgomery curve, $a = \frac{1}{2}\left(r + \frac{1}{r}\right)$;
- $X_0(16)$: the x-coefficient r of a nonconstant order-4 point on a Montgomery curve.

Note that $\mathbf{R}_{2,2}(\mathbf{R}_{4,2}(A))$ is the j-invariant of the curve $E_A : y^2 = x^3 + Ax^2 + x$; $\mathbf{R}_{4,2}(A)$ is its discriminant; $\mathbf{L}_{8,2}(a)$ is the A-coefficient of the curve from the x-coordinate a of the order-2 point on it, $\mathbf{R}_{8,2}(a)$ is the A coefficient of the codomain curve of the 2-isogeny defined by that point; $\mathbf{L}_{16,2}(r)$ is the x-coordinate of the doubled order-4 point with x-coordinate r, $\mathbf{R}_{16,2}(r)$ is the x-coordinate of the order-2 point on the codomain of the parametrized 2-isogeny.

One can also define a curve model with a 2-isogeny only: $E_D : y^2 = x^3 + (D+64)x^2 + 16(D+64)x$ with $D \simeq X_0(2)$ compatible with our instantiation (note that this model disallows $D = -64$ leading to the cuspidal curve, although it is a valid $X_0(2)$ parameter around j-invariant 1728).

Table 2: Level-ℓ coverings and ℓ^k-duality maps (k is maximum such that $\ell^k|N$) from modular curves C covering $X_0(N)$ and degree deg covers to the j-line. Note that $Y = X_0(2) \otimes X_{\text{ns}}^+(3)$ and $Z = X_0(3) \otimes X_{\text{ns}}(2)$, where $X_{\text{ns}}^+(3)$ is parametrized by $\sqrt[3]{j}$ and $X_{\text{ns}}(2)$ is parametrized by $\sqrt{j-1728}$, and the coverings listed work with the X_0 component; $c_1 = \frac{11+5\sqrt{5}}{2}$, $c_2 = \frac{1+\sqrt{5}}{2}$, $\sqrt{5} = 2\zeta_5^3 + 2\zeta_5^2 + 1$.

Modular curve C	N	deg	ℓ	$\mathbf{L}_{C,\ell}(t)$	$\mathbf{R}_{C,\ell}(t)$	$\mathbf{w}_{C,\ell}(t)$
Modular curves $X_0(2^k)$						
$X_0(2)$	2	3	2	$\frac{(t+256)^3}{t^2}$	$\frac{(t+16)^3}{t}$	$\frac{4096}{t}$
$X_0(4)$	4	6	2	$\frac{-4(t+2)^2}{t-2}$	$16t^2 - 64$	$\frac{-2t+12}{t+2}$
$X_0(8)$	8	12	2	$-t - \frac{1}{t}$	$-4t^2 + 2$	$\frac{t+1}{t-1}$
$X_0(16)$	16	24	2	$\frac{1}{2}\left(t + \frac{1}{t}\right)$	t^2	$\frac{t+1}{t-1}$
Modular curves $X_0(N)$						
$X_0(3)$	3	4	3	$\frac{(t+27)(t+243)^3}{t^3}$	$\frac{(t+27)(t+3)^3}{t}$	$\frac{729}{t}$
$X_0(5)$	5	6	5	$\frac{(t^2+250t+3125)^3}{t^5}$	$\frac{(t^2+10t+5)^3}{t}$	$\frac{125}{t}$
$X_0(6)$	6	12	2	$\frac{t(t-9)^2}{(t-1)^2}$	$\frac{(t-9)t^2}{t-1}$	$\frac{t-9}{t-1}$
			3	$\frac{(t-1)(t-9)^3}{t^3}$	$\frac{(t-9)(t-1)^3}{t}$	$\frac{9}{t}$
$X_0(9)$	9	12	3	$\frac{(t-3)^3}{t^2+3t+9}$	$t^3 - 27$	$\frac{3t+18}{t-3}$
$X_0(10)$	10	18	2	$\frac{(t+1)(t-4)^2}{t^2}$	$\frac{(t-4)(t+1)^2}{t}$	$-\frac{4}{t}$
			5	$\frac{t(t-4)^5}{(t+1)^5}$	$\frac{(t-4)t^5}{t+1}$	$\frac{-t+4}{t+1}$
$X_0(12)$	12	24	2	$\frac{t^2+3t}{t-1}$	t^2	$\frac{-t+3}{t+1}$
			3	$-\frac{t^4+18t^2-27}{4t^3}$	$-\frac{t^4-6t^2-3}{4t}$	$-\frac{3}{t}$
$X_0(18)$	18	36	2	$\frac{t^3+4}{t^2}$	$\frac{t^3-2}{t}$	$-\frac{2}{t}$
			3	$\frac{(t+1)^3}{t^2-t+1}$	$t^3 + 1$	$\frac{-t+2}{t+1}$
$X_0(25)$	25	30	5	$\frac{(t-1)^5}{t^4+t^3+6t^2+6t+11}$	$t^5 + 5t^3 + 5t - 11$	$\frac{t+4}{t-1}$
Additional modular curves						
Y	2	9	2	$\frac{t^3+256}{t^2}$	$\frac{t^3+16}{t}$	$\frac{16}{t}$
Z	3	8	3	$-\frac{t^4-486t^2-19683}{t^3}$	$-\frac{t^4+18t^2-27}{t}$	$-\frac{27}{t}$
$X_1(5)$	5	12	5	$\frac{-(t^4-228t^3+494t^2+228t+1)^3}{t(t^2+11t-1)^5}$	$\frac{-(t^4+12t^3+14t^2-12t+1)^3}{t^5(t^2+11t-1)}$	$\frac{1-c_1t}{t+c_1}$
$X(5)$	25	60	5	$\frac{t(t^4-3t^3+4t^2-2t+1)}{t^4+2t^3+4t^2+3t+1}$	t^5	$\frac{1-c_2t}{t+c_2}$

Table 3: Lifting maps (inverse maps of level-ℓ covering pairs) and level-ℓ modular polynomials on modular curves C. C' is the image curve of $\mathbf{L}_{C,\ell}$ and $\mathbf{R}_{C,\ell}$, e.g. $C' = X_0(6)$ for $C = X_0(12)$ and $\ell = 2$. Only short expressions reported, the remaining expressions (only with $\ell \geq 3$) are available in the supplementary material or code repository, including $X_1(5), X_0(25), X(5), X_0(7), X_0(13)$ for relevant ℓ.

Modular curve C	ℓ	$\mathbf{M}_{C',\ell}(t,u)$	$\Phi_{C,\ell}(t,u)$
$X_0(2)$	2	$\frac{4096(tu-720t-720u-16250625)}{t^2+195120t+4095u+660960000}$	$t^2u + 48tu - u^2 + 4096t$
$X_0(4)$	2	$\frac{8t-u-128}{4t+64}$	$4(t^2-4)(u-2) + (u+2)^2$
$X_0(8)$	2	$\frac{u-6}{4t}$	$4t^2u - (u+1)^2$
$X_0(16)$	2	$\frac{u+1}{2t}$	$2t^2u - u^2 - 1$
$X_0(6)$	2	$\frac{u(t+u+81)}{tu+9t+9u}$	$t^2u - t^2 - 8tu - u^2 + 9u$
$X_0(9)$	3	$\frac{(t+3)(tu+18u+729)}{tu-243t+9u+729}$	$t^3(u^2+3u+9) - (u+6)^3$
$X_0(10)$	2	$\frac{u^2-5t+20u}{tu+5t+5u}$	$t^2u - 2tu - u^2 - 4t$
$X_0(12)$	2	$\frac{t+u}{t-3}$	$t^2(u-1) - u(u+3)$
	3	$\frac{4tu^3+2t^2+12tu+114u^2-576}{3t^2u-18tu^2-u^3+112t-48u}$	$t^3u^2 - 3t^2u - 6tu^2 - u^3 + 9t$
$X_0(18)$	2	$\frac{u^2-3t}{tu-9}$	$t^2u - u^2 - 2t$
	3	$\frac{(t-1)(tu-6u+9)}{tu+9t-3u+9}$	$t^3(u^2-u+1) - u^3 - 2u^2 - 4u$
Y	2	$\frac{u^2+15t}{tu-225}$	$t^2u - u^2 + 16t$
Z	3	*(omitted)*	$t^3u^2 - 27t^2u + 18tu^2 - u^3 + 729t$
$X(5)$	5	*(omitted)*	$t^5(u^4+2u^3+4u^2+3u+1)$ $-(u^5-3u^4+4u^3-2u^2+u)$

Table 4: Radical expressions of ℓ-isogenies on modular curves $X_0(N)$, $\Phi_{N,\ell}(t,u) = 0$, and $X(5)$, $\Phi_{X(5),5}(t,u) = 0$. $c = 5\zeta_5^3 + 5\zeta_5^2 + 8 = \frac{11+5\sqrt{5}}{2}$.

$X_0(N)$	ℓ	t^ℓ	$\mathbf{w}_{N,\ell}(u)^\ell$
$X_0(4)$	2	$-\frac{(u-6)^2}{4(u-2)}$	$\frac{4t^2}{t^2-4}$
$X_0(8)$	2	$\frac{(u+1)^2}{4u}$	$\frac{t^2}{t^2-1}$
$X_0(12)$	2	$\frac{u(u+3)}{u-1}$	$\frac{t^2-9}{t^2-1}$
$X_0(16)$	2	$\frac{u^2+1}{2u}$	$\frac{t^2+1}{t^2-1}$

$X_0(N)$	ℓ	t^ℓ	$\mathbf{w}_{N,\ell}(u)^\ell$
$X_0(16)$	4	$\frac{(u+1)^4}{8(u(u^2+1))}$	$\frac{t^4}{t^4-1}$
$X_0(9)$	3	$\frac{(u+6)^3}{u^2+3u+9}$	$\frac{27t^3}{t^3-27}$
$X_0(18)$	3	$\frac{u(u^2+2u+4)}{u^2-u+1}$	$\frac{8-t^3}{t^3+1}$
$X(5)$	5	$\frac{u(u^4-3u^3+4u^2-2u+1)}{u^4+2u^3+4u^2+3u+1}$	$\frac{-ct^5+1}{t^5+c}$

Table 5: Radical expressions of 2-isogenies on modular curves covering $X_0(2)$.

Modular curve C	Solution of $\Phi_{C,2}(t,u)=0$
$X_0(2)$	$t = -24 - \frac{2048}{u} \pm \frac{u+256}{u}\sqrt{u+64}$
	$u = \frac{1}{2}t^2 + 24t \pm \frac{t+16}{2}\sqrt{t(t+64)}$
$X_0(6)$	$t = \frac{4u}{u-1} \pm \frac{u+3}{u-1}\sqrt{u}$
	$u = \frac{1}{2}t^2 - 4t + \frac{9}{2} \pm \frac{t-3}{2}\sqrt{(t-9)(t-1)}$
$X_0(10)$	$t = \frac{u+2}{u} \pm \frac{1}{u}\sqrt{(u+1)(u^2+4)}$
	$u = \frac{1}{2}t^2 - t \pm \frac{1}{2}\sqrt{(t-4)t(t^2+4)}$
Y	$t = -\frac{8}{u} \pm \frac{1}{u}\sqrt{u^3+64}$
	$u = \frac{1}{2}t^2 \pm \frac{1}{2}\sqrt{t(t^3+64)}$

Relation to other curve models Many other curve models with constant order-2 or order-4 points fall into our hierarchy. The Legendre curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ parametrized by the famous modular function λ exposes full $X(2)$ structure (the x-coordinates of $E_\lambda[2] \setminus \{\mathcal{O}\}$ are 0, 1, λ). Since $X_0(4) \simeq X(2)$, both λ and Montgomery A parametrize a 4-isogeny (together with the alternative 2-isogeny branch); we have in fact $\lambda = (A+2)/4$. The only difference is that E_λ refers to the curve in the middle, while E_A refers (in our interpretation) to the "front" curve. Colò [Col22, §3.3] also shows how to construct $X_0(16) \simeq X(4)$ from the Legendre model.

Another well-known related model is the Edwards curve [Edw07] $E_d : x^2+y^2 = 1+dx^2y^2$. Its equivalence to the Montgomery form (curve E_A, $j(E_A) = j(E_d)$) is given by $A = 2\frac{1+d}{1-d}$ [BBJ+08].

Similar relation exists with the so-called Jacobi Quartic model [LS01, BJ03, HWCD09]. All of the following can be seen from the j-invariant expression of the curve. The simplified model[3] $E_a : y^2 = x^4 + 2ax^2 + 1$ matches $2a = A$ directly (but E_a is the curve in the middle, i.e. it is isomorphic to the corresponding E_λ). Another variant from [BJ03] is

$$E_k : y^2 = (1-x^2)(1-k^2x^2) = k^2x^4 - (k^2+1)x^2 + 1$$

attributed to Jacobi's studies of elliptic functions. We can see that $j(E_k)$ directly equals $\mathbf{L}_{4,4}(\mathbf{R}_{8,2}(k))$ in our instantiation (i.e., without any Möbius transformation needed). Therefore, E_k is isomorphic to E_A with $A = \mathbf{w}_{4,4}(\mathbf{R}_{8,2}(k)) = -\frac{2(k^2+1)}{k^2-1}$. The closely related Jacobi intersection model

$$E_\kappa : \begin{cases} x^2 + y^2 = 1, \\ \kappa^2 x^2 + z^2 = 1 \end{cases}$$

has $j(E_\kappa) = j(E_\lambda)$ for $1 - \kappa^2 = \lambda$ [FNW10, Thm.1], so it refers to the central curve of the $X_0(4) \simeq X(2)$ structure. The parameter κ itself is again an $X_0(8)$ parameter so that $\mathbf{R}_{8,2}(\kappa) \in X_0(4)$ parametrizes the same 4-isogeny structure as E_λ. Equivalently, for $A = \mathbf{L}_{8,2}(\kappa) \in X_0(4)$ we have $j(E_A) = j(E_\kappa)$.

[3] See https://hyperelliptic.org/EFD/g1p/auto-jquartic.html

Table 6: Lifting maps $\overline{\mathbf{M}}_{\ell,\ell'}$ (inverse maps of the level-ℓ and -ℓ' right covers $(\mathbf{R}_{N,\ell'}, \mathbf{R}_{N,\ell})$), $N = \ell \cdot \ell'$, ℓ and ℓ' coprime. Requires $\mathbf{R}_\ell(t) = \mathbf{R}_{\ell'}(u)$.

Codomain	ℓ	ℓ'	$\overline{\mathbf{M}}_{\ell,\ell'}(t,u)$
$X_0(6)$	2	3	$\frac{tu+u^2+10u-27}{u^2-3t+18u-3}$
$X_0(10)$	2	5	$\frac{tu-4u^2+t-24u-4}{u^3+13u^2-t+35u-1}$
$X_0(12)$	4	3	$\frac{-8t^3u+24t^3-tu^2+18tu-81t}{32t^4-144t^2-2u^2-36u+54}$
$X_0(18)$	2	9	$\frac{-tu^6+28tu^3+64u^3+3t^2-48t-1536}{4tu^4-32u^4-t^2u-104tu+896u}$

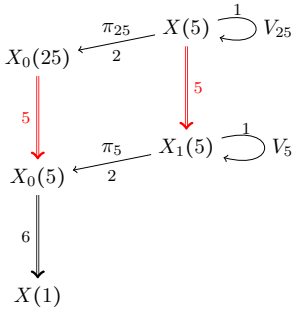

Figure 4: Modular tower for $X(5)$, extended from [Col22].

4.2 Levels $3, 9$

For 3-isogenies, values of $N = 3, 6, 9, 12, 18$ are available and yield compact formulae, in particular, for $N = 9, 18$, where the expression is a radical one, and the head/tail turn maps are available. Similarly to a Montgomery coefficient defining an $X_0(4)$ parameter, we can consider an elliptic curve in the so-called *Deuring Normal Form* $E_\delta : y^2 + \delta xy + y = x^3$, related to the more well-known *Hessian form* [CC86]: $E^H_\delta : x^3 + y^3 + 1 = \delta xy$. Then, our parametrization for $X_0(9)$ is based on δ so that the j-invariant of E_δ is given by $j = \mathbf{R}_{3,3}(\mathbf{R}_{9,3}(\delta)) = \frac{\delta^3(\delta^3-24)^3}{\delta^3-27}$ and $\Delta = \mathbf{R}_{9,3}(\delta) = \delta^3 - 27$ corresponds to the discriminant of E_δ. The Hessian curve's j-invariant is $j(E^H_\delta) = \mathbf{L}_{3,3}(\mathbf{R}_{9,3}(\delta))$ so that it refers to the central curve on the 9-isogeny path, similarly to the λ parameter for 4-isogenies. Due to the available rotation automorphisms, under a choice of ζ_3, δ parametrizes five j-invariants arranged in a 3-isogeny star. One can also use $E_\Delta : y^2 + xy + \frac{1}{\Delta+27}y = x^3$ to restrict the parameter to $X_0(3)$: $j(E_\Delta) = \mathbf{R}_{3,3}(\Delta)$. This model disallows $\Delta = -27$, which is otherwise a valid $X_0(3)$ parameter corresponding to j-invariant 0.

4.3 Levels $5, 25$

The case of 5-isogenies is more complicated. Although $X_0(25)$ and $X(5)$ are both of genus zero, they are not isomorphic, in the modular sense; there is a degree-2 cover from $X(5)$ to $X_0(25)$ which can be propagated to a degree-2 cover from $X_1(5)$ to $X_0(5)$ (see Figure 4). Therefore, computing a preimage of this cover is necessary in order to get to the full 5-torsion structure including the rotation maps. Colò provides the three covers $X(5) \to X_1(5) \to X_0(5) \to X(1)$, from which we completed the construction to include $X_0(25)$ and all the additional maps/relations, such as duality involutions, modular polynomials and the inverse maps to the coverings.

Due to the additional degree-2 covers $\pi_{25} : X(5) \to X_0(25)$, $\pi_5 : X_1(5) \to X_0(5)$, $X(5)$ (resp. $X_1(5)$) is equipped with an order-2 automorphism V_{25} (resp. V_5) such that $\pi_{25} \circ V_{25} = \pi_{25}$ (resp. $\pi_5 \circ V_5 = \pi_5$). In our parametrization, we have (π_5 was taken from [Col22] and composed with $\mathbf{w}_{5,5}$)

$$\pi_5(t) = -\frac{t^2 + 11t - 1}{t}, \quad \pi_{25}(t) = \frac{(1-t^2)}{t}, \quad V_5(t) = -1/t, \quad V_{25}(t) = -1/t.$$

Note that $\mathbf{L}_{X(5),5} \circ V_{25} = V_5 \circ \mathbf{L}_{X(5),5}$ and $\mathbf{R}_{X(5),5} \circ V_{25} = V_5 \circ \mathbf{R}_{X(5),5}$. However, $\mathbf{T}_{X(5),5}$ anticommutes with V_{25}: $\mathbf{T}_{X(5),5} \circ V_{25} = V_{25} \circ \mathbf{T}^{(-1)}_{X(5),5}$. In other words, the choice of the degree-2 cover preimage (of $\pi_5 : X_1(5) \to X_0(5)$ or of $\pi_{25} : X(5) \to X_0(25)$) corresponds to

the choice of the direction of the tail rotation $\mathbf{T}_{X(5),5}$, and the direction can be reversed by applying V_5 and V_{25}. One can derive a very compact lifting map (compared to $\mathbf{M}_{X_1(5),5}$) from a $T \in X_0(25)$ and a $u \in X_1(5)$ satisfying $\mathbf{R}_{25,5}(T) = \pi_5(u)$, to $X(5)$:

$$t = \mathbf{M}_{X_0(25)\otimes X_1(5)}(T, u) = \frac{T^2u + T + u}{T^2 - Tu + 1} \in X(5).$$

This allows to cheaply lift a 5-isogeny path over j-invariants: lift the full path to a sequence of $X_0(25)$, choose a preimage under π_5 (one square root) for a single $X_0(5)$ isogeny and apply the map from above to lift the whole path. This formula is not applicable at the at most four singularities of $\mathbf{R}_{25,5}(T) = \pi_5(u)$ (satisfying $T^4 + 3T^2 + 1 = 0$, $u^2 + 1 = 0$), which correspond to $\mathbf{R}_{25,5}(T)$ being a loop isogeny between $j = 1728$ and itself.

Radical decomposition We observe that the radical 5-isogeny formula on $X(5)$ in the backwards direction (see Table 4) matches (up to sign change $u \mapsto -u$) with the expression from the seminal paper about radical isogenies [CDV20], which is expected due to discussion in Subsection 3.1. However, our construction shows that it can be decomposed as the 5-th powering conjugated with Möbius transformations:

$$t^5 = \frac{u^5 - 3u^4 + 4u^3 - 2u^2 + u}{u^4 + 2u^3 + 4u^2 + 3u + 1} = \left(\frac{1 - c_1 z}{z + c_1}\right) \circ (\cdot)^5 \circ \left(\frac{1 - c_2 z}{z + c_2}\right) \ (u),$$

where $c_1 = \frac{11+5\sqrt{5}}{2}$, $c_2 = \frac{1+\sqrt{5}}{2}$.

4.4 Other composite levels N

For $N \in \{6, 10, 12, 18\}$, we define parameters based on the work of [Mai09], introducing a linear variable change to slightly simplify coverings and modular polynomials. Composite levels lead to a richer automorphism structure due to the partial (Atkin-Lehner) duality involutions and may be useful in applications where commuting isogenies of low degree are needed. In particular, many of the degree-2 modular polynomials are rather compact and similarly enjoy the automatic backtracking prevention (when N is even).

Relation to curve models For $t_{12} \in X_0(12)$, we can let $x_3 = t_{12}/3$ be the x-coordinate of any order-3 point on the Montgomery curve E_A, which matches the cover $A = \mathbf{L}_{12,3}(t_{12})$ with the expression of A from x_3 (given by the 3rd division polynomial of E_A). For $t_{18} \in X_0(18)$, we can choose an order-2 point $Q = (-t_{18}^2/4, t_{18}^3/8)$ on $E_\delta : y^2 + \delta xy + y = x^3$.

4.5 Levels 7,13

The remaining X_0 curves $X_0(7)$, $X_0(13)$ give a basic ℓ-isogeny parametrization which limits their usage, in addition to their relevant expressions being very dense.

4.6 Other modular curves

We consider four more modular curves, related to 2- and 3-isogenies and lying inside the modular towers for $X_0(18)$ and $X_0(12)$. Maier [Mai09] discusses connections between various X_0 parameters and Weber's modular functions $\gamma_2 = \sqrt[3]{j}, \gamma_3 = \sqrt{j - 1728}$. In the following, we describe their role in the modular towers of $X_0(18)$ and $X_0(12)$.

($X^+_{\mathbf{ns}}(3)$ and γ_2) The modular function γ_2 parametrizes the so-called modular curve $X^+_{\mathrm{ns}}(3)$ [Col22, Lemma 3.46]. While this curve does not parametrize any isogeny on itself, it fits in a modular tower depicted in Figure 5 (left). Importantly, the modular curve $Y = X_0(2) \otimes X^+_{\mathrm{ns}}(3)$ includes a level-2 isogeny parametrization which again yields very compact equations (see Table 3). Roughly speaking, it can be seen as the preimage of the cover $X_0(2) \to X_0(1)$ under the cube-root function, which corresponds to the choice of the second 3-isogeny at the higher-level curves $X_0(18)$ and $X_0(9)$. The latter have covers $X_0(18) \to Y$ and $X_0(9) \to X^+_{\mathrm{ns}}(3)$ as shown on the figure, where δ corresponds to an elliptic curve in the Deuring normal form.

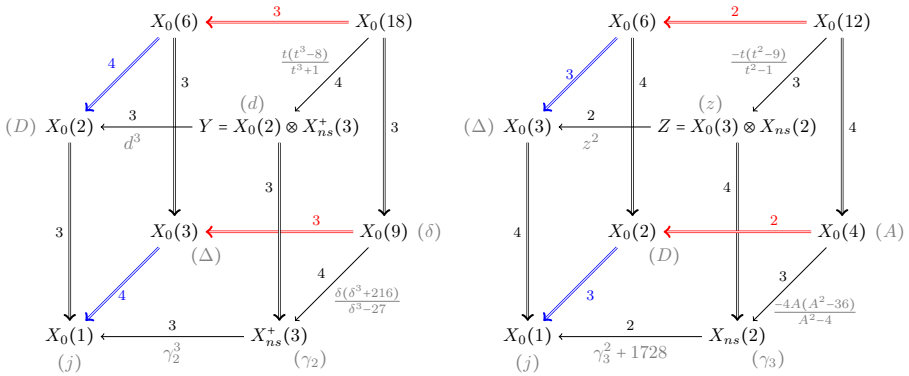

Figure 5: Modular towers for $X_0(18)$ through $Y = X_0(2) \otimes X^+_{\mathrm{ns}}(3)$ and $X_0(12)$ through $Z = X_0(3) \otimes X_{\mathrm{ns}}(2)$. The unspecified maps are given in Table 2. The edge labels correspond to the degree of the covers. The double edges correspond to the two available covers $\mathbf{L}_{C,\ell}$ and $\mathbf{R}_{C,\ell}$; the diagrams commute when red/blue edges are chosen as covers in different directions.

We complete the description of the curve by providing the duality map and the modular polynomial of level 2 (see Table 2 and Table 3). Note that the cover $X_0(18) \to Y \to X_0(2)$ is the same as the cover $\mathbf{L}_{6,3} \circ \mathbf{R}_{18,3}$ (or $\mathbf{R}_{6,3} \circ \mathbf{L}_{18,3}$). In other words, the middle parameter $t \in Y$ parametrizes the 2-isogeny in the middle of the (2×9)-isogeny grid.

($X_{\mathbf{ns}}(2)$ and γ_3) We observe that a similar tower may be formed with a cover from $X_0(12)$ to the j-line through the modular curve[4] $X_{\mathrm{ns}}(2)$ associated with the modular function γ_3. The construction is completely symmetric to the modular tower for $X_0(18)$ above (see Figure 5 right), with 2 and 3 being swapped everywhere. In particular, we also have a modular curve Z which can be viewed as a combination of $X_{\mathrm{ns}}(2)$ and $X_0(3)$ and which is covered by $X_0(12)$, with covers (in addition to the ones given in Table 2):

$$X_0(12) \to Z: \quad t \mapsto -\frac{t(t^2-9)}{t^2-1}, \qquad Z \to X_0(3): \quad z \mapsto z^2,$$
$$X_0(4) \to X_{\mathrm{ns}}(2): \quad A \mapsto \frac{-4A(A^2-36)}{A^2-4}, \qquad X_{\mathrm{ns}}(2) \to X(1): \quad \gamma_3 \mapsto \gamma_3^2 + 1728.$$

where A corresponds to an elliptic curve in the Montgomery model and the cover $X_0(12) \to Z \to X_0(3)$ returns the middle 3-isogeny (i.e., the one between the middle j-invariants parameterized by the included 4-isogenies).

[4] See e.g. https://beta.lmfdb.org/ModularCurve/Q/2.2.0.a.1/

4.7 Statements and discussion

We provide formal statements about the framework instantiation. Naturally, it satisfies the theory from Subsection 3.1 (e.g., that the coverings compute the $\mathcal{J}$ sequence of rational maps defined in Proposition 4, that coverings "commute" with each other and "anticommute" with the duality operators, which act on $\mathcal{J}$ as claimed in Definition 4, etc.), which can in addition be verified symbolically over $\mathbb{Q}(x)$. The following check is also computational/symbolic.

Proposition 11. *For $p \nmid N$, the covers from Table 2 satisfy Lemma 2 and the inverse maps from Table 3 satisfy Lemma 3.*

The following proposition clarifies that the hierarchy of covers is the same as one in [Mai09]. The changes were done to simplify the expressions, to match the Montgomery/Deuring curve models, as well as to exhibit the radical nature of some covers.

Proposition 12. *For $N \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$, the hierarchy of coverings $\mathbf{R}_{N,\ell}, \mathbf{L}_{N,\ell}$ coincides with Maier's covers up to linear change of variables [Mai09, Table 6], with left and right sides of the table corresponding to R, L respectively.*

Proof. Maier's canonical Hauptmoduln M_N for $X_0(N)$, as a function of our $t \in X_0(N)$ are given by $M_N(t) = t$ for prime N, and

$$M_4 = -4t - 8,\ M_8 = 4t - 4, \quad M_{10}(t) = t - 4,\ M_{16} = 2t - 2, \quad M_{25}(t) = t - 1,$$
$$M_6(t) = t - 9,\ M_9(t) = t - 3,\ M_{12}(t) = t - 3,\ M_{18}(t) = t - 2.$$

The equivalence of coverings can be verified directly by substitution. □

On the supersingular locus Currently, supersingular elliptic curves pose the main interest for isogeny-based cryptography. The following proposition shows that $X_0(N)$ parameters do not require to extend the field of definition for such curves.

Proposition 13 ([CK26, Thm.11,Cor.12])**.** *Over a field of positive characteristic p, the supersingular locus of $X_0(N)$ is defined over $\mathbb{F}_{p^2}$. If $p \equiv \pm 1 \pmod N$, then the supersingular locus of $X_1(N)$ and $X(N)$ is also defined over $\mathbb{F}_{p^2}$.*

Corollary 2. *The supersingular parameters $X_0(N)$ (and $X_1(N)$, $X(N)$, when $p \equiv \pm 1 \pmod N$) from this section are defined over $\mathbb{F}_{p^2}$, assuming $p \nmid N$.*

Proof. Let F_N be the curve defined by $\Phi_N(X, Y) = 0$ over $\mathbb{F}_p$. Since $X_0(N)$ has good reduction mod p and F_N is its model, we have $\mathbb{F}_p(F_N) \simeq \mathbb{F}_p(X_0(N))$. Since the covers $\mathbf{L}_{N,N}, \mathbf{R}_{N,N}$ are defined over $\mathbb{Q}$ and have good reduction modulo p, we also get $\mathbb{F}_p(t) \simeq \mathbb{F}_p(F_N)$, where t is the rational parameter of $X_0(N)$. This implies $\mathbb{F}_p(t) \simeq \mathbb{F}_p(X_0(N))$ and isomorphism over $\mathbb{F}_p$ of the two curves $\mathbb{P}^1$ and $X_0(N)$, since both are smooth projective curves. Therefore, t and the corresponding elements of $X_0(N)$ are defined over the same extension of $\mathbb{F}_p$. The cases of $X_1(N), X(N)$ follow analogously, where for the latter we need to note that $\mathbb{F}_p[\zeta_N] \subseteq \mathbb{F}_{p^2}$ when $p \equiv \pm 1 \pmod N$. □

Delay issue Working with modular parameters instead of j-invariants requires some care and understanding of the carried information, which is provided by our framework. Consider a 2-isogeny path of length n over j-invariants: $j_1, \ldots, j_{n+1}$ with relations $\Phi_2(j_i, j_{i+1}) = 0$. Working with $X_0(16)$, the path can be encoded as a sequence of field elements $t_1, \ldots, t_{n-3}$ each representing an $X_0(16)$ element, with relations $\Phi_{16,2}(t_i, t_{i+1}) = 0$. In protocols, a party usually reveals endpoints of an isogeny path: j_1 and j_{n+1}. However, revealing full endpoints t_1 and t_{n-3} leaks four 2-isogeny steps from each side. We call this a *delay*

issue. Variations of this problem occurred in many protocols, especially the ones based on Montgomery curves ($X_0(4)$ leaking 2 steps), see e.g. SIKE [JAC+20, CLN+20], and a discussion in [dHMSS26, Sec.6].

There are two basic approaches to countering this problem. The first one is either to accept a small security loss, or to extend the path length to counter the leakage: extending the isogeny by four steps from each side arbitrarily almost removes the leakage: only one of the "wrong" directions is leaked from each side. The second method is to only reveal j_1, j_{n+1} but to enforce the relations $j_1 = \mathbf{L}_{16,16}(t_1)$, $j_{n+1} = \mathbf{R}_{16,16}(t_{n-3})$ (similar idea was proposed recently in [CSS26]). For example, in the zero-knowledge proof applications (Section 5), one encodes these constraints in the proof system, resulting in a small additive constant overhead. In the algebraic cryptanalysis, one may manipulate the roots of the polynomials to apply the covers. This option is the cleanest modeling solution but it adds a level of complexity.

Algebraic parametrization of isogeny walks One of the most natural applications of new framework is the algebraic approach to solving the isogeny problem. Classically, the 2^n-isogeny search problem can be formulated using classical modular polynomials $\Phi_2(x_i, x_{i+1}) = 0$ [TKF+21].

Problem 1 (Supersingular ℓ^n-Isogeny)**.** *Given two j-invariants $j_0, j_n \in \mathbb{F}_{p^2}$ corresponding to two supersingular elliptic curves, and two integers $n \geq 1$, $\ell \geq 2$, ℓ coprime to p, find a cyclic ℓ^n-isogeny between two elliptic curves with the given j-invariants.*

Theorem 4. *The supersingular 2^n-isogeny problem (Problem 1) over $\mathbb{F}_{p^2}$, $p > 3$, can be reduced to solving at most 4 instances of the equation system $\{x_{i+1}^2 = 2x_i^2 x_{i+1} - 1\}_{0 \leq i < n+4}$ where $x_0, x_{n+4} \in \mathbb{F}_{p^2}$ are known and $x_1, \ldots, x_{n+3} \in \mathbb{F}_{p^2}$ are unknowns.*

Proof. For each of j_0, j_n, we will guess a 2-isogeny edge not included in the secret path (or, more precisely, an edge that can be extended to the secret path; this includes special cases such as $j = 0, 1728$). This can be done by considering two arbitrary edges (potentially collapsing to one by an automorphism at the curve) on each endpoint. Then, we extend them arbitrarily to 16-isogenies, getting $x_0, x_{n+4} \in X_0(16)$ such that $\mathbf{R}_{16,16}(x_0) = j_0$, $\mathbf{L}_{16,16}(x_{n+4}) = j_n$, two candidates for each. Clearly, for any existing 2^n-isogeny, at least one of the guesses for x_0 can be extended by n steps to follow the path until $\mathbf{R}_{16,16}(x_n) = j_n$, and extended by four further steps to match one of the guesses for x_{n+4}. By Theorem 2 and Theorem 3, the equation system smoothly parametrizes 2^n-isogenies, up to pre-/post-isomorphisms which are not relevant. □

An analogous statement can be done for $\ell = 3, 5, 7, 13$ using various corresponding modular polynomials (with delay reduced to 1-2 steps). It is also easy to show that a decision oracle for the above equation system is sufficient, by reconstructing the path step-by-step, see e.g. [CD23].

Note that between two arbitrary supersingular elliptic curves exist 2-isogeny paths of length $\mathcal{O}(\log p)$ [Koh96, Thm.79]. Therefore, one may also guess the path length and use the reduction to solve the general supersingular isogeny problem by solving the corresponding equation systems.

We conclude that the fundamental supersingular 2-isogeny path problem / general supersingular isogeny problem for elliptic curves is reducible to solving an extremely structured and compact algebraic equation system over a finite field, parametrized only by two field elements (the endpoints). Clearly, this formulation deserves careful analysis. In particular, one can notice that the equation system with x_{n+4} being kept as a variable forms a Gröbner basis with respect to lexicographic monomial order with $x_1 < x_2 < \ldots < x_{n+4}$, and the corresponding ideal degree is 2^{n+4} (this follows from the fact that the leading monomials are pairwise coprime, and the degree is determined by their product, see e.g. [CLO13, Chap.2,§9,Prop.4&Thm.3]).

5 Proving isogeny walks in R1CS

The authors of [CLL23] proposed to prove knowledge of an isogeny using generic zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) systems. The idea is to represent the statement (a 2-isogeny path) in terms of rank-1 constraint system (R1CS), which consists of statements of the form $a(x) \cdot b(x) = c(x)$, where $x \in \mathbb{F}^n$ is the vector of public and secret (witness) variables, and a, b, c are linear functions. Roughly speaking, one constraint corresponds to one multiplication in the field. We will denote one auxiliary variable by $1\mathbf{V}$, one $\mathbb{F}_{p^2}$ multiplication/squaring constraint by $1\mathbf{M}$ and $1\mathbf{S}$ respectively. The public and witness variables are counted equally (excluding the constant 1 variable), and specializing to hardcoded public variables can lead to small improvements, when the use-case permits. The authors of [dHKM+25] also observed that the number of nonzero coefficients in the R1CS constraints matters for performance, and thus we will evaluate this metric for comparison as well, denoted by nnz.

5.1 Previous work

The authors of [CLL23] applied the idea to the classical modular polynomial $\Phi_2(j_i, j_{i+1}) = 0$, which requires to introduce variables for $j_i, j_i^2, j_i^3, j_i j_{i+1}$ and the corresponding constraints, as well as one constraint for the modular polynomial itself. In total, their scheme requires $4n + 3$ variables and $4n + 2$ constraints ($1\mathbf{S} + 3\mathbf{M}$ per step) over the finite field $\mathbb{F}_{p^2}$. When expressing the conditions over $\mathbb{F}_p$ (using $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[\alpha]$ for $\alpha^2 = d$ a non-residue of $\mathbb{F}_p$), one $\mathbb{F}_{p^2}$-multiplication (resp. squaring) costs three (resp. two) $\mathbb{F}_p$-multiplications; the number of variables doubles and each $\mathbb{F}_{p^2}$-multiplication (except squaring) requires one auxiliary $\mathbb{F}_p$-variable. The $\mathbb{F}_p$ R1CS system of [CLL23] has then $11n + 7$ variables (expansion of the four $\mathbb{F}_{p^2}$ variables and three auxiliary for multiplications, per step) and $11n + 5$ constraints. Furthermore, adding the non-backtracking (cyclic isogeny) constraint induces a 25% overhead.

The recent work [dHKM+25] uses "canonical modular polynomials", which essentially describe the input-output relation of our coverings $\mathbf{L}_{\ell,\ell}, \mathbf{R}_{\ell,\ell}$ for prime ℓ (up to degree-1 change of variables). The authors model both sequence j_i of j-invariants and the sequence of modular parameters $t_i \in X_0(\ell)$ covering them. Then, they prove that $\mathbf{R}_{\ell,\ell}(t_i) = j_i$ and $\mathbf{L}_{\ell,\ell}(t_{i+1}) = \mathbf{R}_{\ell,\ell}(\mathbf{w}_{\ell,\ell}(t_{i+1})) = j_i$. For canonical modular parameters, the dualization is just inversion and scaling by a constant. The authors exploit the general shape of the coverings $\mathbf{R}_{\ell,\ell}(t) = f(t)/t$.

This more recent work [dHMSS26] also considers modular polynomials with respect to the Atkin and Weber modular functions. The proposed modular polynomials do not contain the necessary level structure for backtracking prevention. Furthermore, [LP25] suggested to use radical 2-isogeny formulas [CDV20], which prevent backtracking by design. However, this model is based on a two-variable state per curve. Another recent work [dHLM+26] also used these formulas but outside of R1CS.

5.2 Our approach

($\ell = 2$) Our modular equation $\Phi_{16,2}(x, y) = y^2 - 2x^2y + 1$ naturally improves the constraint system. Over $\mathbb{F}_{p^2}$, we use variables for x, x^2 (we don't need x^2 for the last one). Then, the equation is implemented by one constraint:

$$(2x^2 - y) \times (y) = 1.$$

In order to represent a 2^n-isogeny $(t_0, \ldots, t_n)$ over $X_0(16)$, we need $2n + 1$ variables (t_i, t_i^2 excluding t_n^2) and $2n$ constraints ($1\mathbf{S} + 1\mathbf{M}$ per step, 7 nnz). Over $\mathbb{F}_p$, we get $5n + 2$ variables (expansion of the two $\mathbb{F}_{p^2}$ variables and one auxiliary variable for multiplication, per step) and $5n$ constraints.

We note that using many other degree-2 modular polynomials from our framework leads to similar results. In particular, using $\Phi_{18,2}(x,y) = y^2 - x^2y + 2x$ we obtain the same cost (plus one extra nnz per step over $\mathbb{F}_p$) but we carry a whole 9-isogeny along the way, proving a 9×2^n-isogeny rectangle.

Resolving the delay issue Note that our variables correspond to $X_0(16)$ and thus themselves parameterize 2^4-isogenies. This has to be taken into account in the R1CS proofs. We describe the clean method of resolving it, which only adds a small modeling cost. For a 2^n-isogeny path $j_0, \ldots, j_n \in X_0(1)$, $n \geq 4$, we define 2^n-isogeny path $x_0, \ldots, x_{n-4} \in X_0(16)$, satisfying $\mathbf{L}_{16,16}(x_0) = j_0$ and $\mathbf{R}_{16,16}(x_{n-4}) = j_n$. These two statements have to be proven, in addition to the modular 2-isogeny path $x_0, \ldots, x_{n-4}$. We detail the model in Table 7. They incur small additive costs $9\mathbf{V} + 3\mathbf{M} + 8\mathbf{S}$ in total for the two endpoints. Note that these are partially offset by the reduction of the isogeny path length by four steps, which saves $8\mathbf{V} + 4\mathbf{S} + 4\mathbf{M}$. This count did not include the two public variables for the j-invariant endpoints. Thus, the total fixed cost of resolving the delay problem is just $3\mathbf{V} + 4\mathbf{S} - 1\mathbf{M}$. We conclude with the final cost of the j-invariant 2^n-isogeny path being $2n + 4$ variables and $2n + 3$ constraints, over $\mathbb{F}_{p^2}$. For $\mathbb{F}_p$, this translates to $5n + 7$ variables and $5n + 5$ constraints.

Table 7: R1CS models for the relations $j = \mathbf{R}_{16,16}(t_{16})$ and $j = \mathbf{L}_{16,16}(\hat{t}_{16}) = \mathbf{R}_{16,16}(\mathbf{w}_{16,2}(\hat{t}_{16}))$, i.e., $\hat{t}_{16}$ is the starting parameter, t_{16} is the ending parameter. The first equation (*) is only used in the second model. The total cost is $4\mathbf{V} + 1\mathbf{M} + 4\mathbf{S}$ (21 nnz) and $5\mathbf{V} + 2\mathbf{M} + 4\mathbf{S}$ (26 nnz) constraints respectively for the two relations (variables j and t_{16} (or $\hat{t}_{16}$ in (*)) are not counted).

	Equation	Constraint	Cost ($\mathbb{F}_{p^2}$)	nnz ($\mathbb{F}_{p^2}$)
*	$t_{16} = \mathbf{w}_{16,2}(\hat{t}_{16}) = \frac{\hat{t}_{16}+1}{\hat{t}_{16}-1}$	$(t_{16}-1)(\hat{t}_{16}-1) = 2$	$1\mathbf{V} + 1\mathbf{M}$	5
	$t_8 = \mathbf{R}_{16,2}(t_{16}) = t_{16}^2$	$t_{16}^2 = t_8$	$1\mathbf{V} + 1\mathbf{S}$	3
	$t_4 = \mathbf{R}_{8,2}(t_8) = -4t_8^2 + 2$	$(2t_8)^2 = 2 - t_4$	$1\mathbf{V} + 1\mathbf{S}$	4
	$t_2 = \mathbf{R}_{4,2}(t_4) = 16t_4^2 - 64$	$(4t_4)^2 = t_2 + 64$	$1\mathbf{V} + 1\mathbf{S}$	4
	$j = \mathbf{R}_{2,2}(t_2) = \frac{(t_2+16)^3}{t_2}$	$(t_2+16)^2 = r$, $(t_2+16)(r-j) = -16j$	$1\mathbf{V} + 1\mathbf{S} + 1\mathbf{M}$	10

($\ell = 3$) We are going to use $X_0(18)$ and its radical $\Phi_{18,3}$:

$$x^3(y^2 - y + 1) = y^3 + 2y^2 + 4y$$

Here we naturally use the basic approach and introduce variables x_i, x_i^2, x_i^3. This allows to represent the two terms in y linearly, and we are in any case required to compute x^3. Then, the constraint above becomes one multiplication. We obtain the cost of $3n + 3$ variables, $(n+1)\mathbf{S} + (2n+1)\mathbf{M}$ over $\mathbb{F}_{p^2}$, 13 nnz per step. The delay resolution requires computing $\mathbf{L}_{18,9}$ and $\mathbf{R}_{18,9}$ (descending to $X_0(2)$ is sufficient to solve the delay issue, descending further to $X(1)$ may be needed if the public values are given as j-invariants), which we can do in the same way as for $\ell = 2$ at a small cost, reducing the main isogeny path length n by 2. Using $X_0(12)$ instead of $X_0(18)$, we obtain similar performance but carry a 4-isogeny along the 3-isogeny path essentially for free.

($\ell = 5$) Similarly, we are going to use $X_0(25)$, which unfortunately is not radical (however, we can use its radical version $X(5)$ over $\mathbb{F}_{p^2}$ when $p \equiv \pm 1 \pmod 5$, with comparable performance). Reconstructing the modular equation as $\mathbf{R}_{25,5}(x) = \mathbf{L}_{25,5}(y)$, we get expression for $\Phi_{25,5}$ as

$$(x^5 + 5x^3 + 5x - 11) \times (y^4 + y^3 + 6y^2 + 6y + 11) = (y-1)^5 = y^5 - 5y^4 + 10y^3 - 10y^2 + 5y - 1.$$

This approach is somewhat similar to that of [dHKM+25]. However, we benefit from sparser and lower-degree equations of $X_0(25)$, compared to those of $X_0(5)$, and from native backtracking protection. We store, as before, x, x^2, x^3, x^4, x^5 (requires three squarings and one multiplication using $x^3 = \frac{1}{2}((x+x^2)^2 - x^2 - x^4)$ for the $\mathbb{F}_p$ target). Then, the equation above immediately becomes a single R1CS multiplication. Note that substituting variables $x'_i = x_i - 1$, etc. saves 4 nnz coefficients for the main constraint by changing the righthand side to y'^5. For $p \equiv \pm 1 \pmod 5$, over $X(5)$ we get the equation

$$(x^5 - y)(y^4 + 2y^3 + 4y^2 + 3y + 1) = -5y^4 - 5y^2$$

saving 2 nnz over $\mathbb{F}_{p^2}$ and even more over $\mathbb{F}_p$.

5.3 Discussion

Summary of our results with comparison to state-of-the-art is given in Table 8. It also illustrates the backtracking prevention overhead from [dHKM+25]. Their method checks for $j_i \neq j_{i+2}$ by showing that the product of terms $(j_i - j_{i+2})$ folded to $\mathbb{F}_p$ is invertible. This introduces a negligible completeness loss, and is different from the isogeny cyclicity check (a multiple edge may introduce a cyclic isogeny continuation backtracking in the graph sense). We used the software script provided by [dHMSS26][5] to optimize the $\mathbb{F}_p$ nnz count.

Table 8: Comparison of variable/constraint counts of R1CS models for ℓ^n-isogenies. Small additive constants omitted for presentation. For non-backtracking walks, [CLL23, dHKM+25, dHMSS26] need extra n constraints/variables and $6n/4n$ nnz (for $\mathbb{F}_p/\mathbb{F}_{p^2}$ resp., using the method from [dHKM+25]), shown in square brackets. Our models enforce cyclicity directly.

		$\mathbb{F}_{p^2}$			$\mathbb{F}_p$		
ℓ	Ref.	Vars.	Constr.	nnz	Vars.	Constr.	nnz
2	[CLL23]	$4n$+[n]	$4n$+[n]	$21n$+[$4n$]	$11n$+[n]	$11n$+[n]	$79n$+[$6n$]
	[dHKM+25]	$3n$+[n]	$3n$+[n]	$13n$+[$4n$]	$7n$+[n]	$7n$+[n]	$41n$+[$6n$]
	[dHMSS26]	$2n$+[n]	$2n$+[n]	$12n$+[$4n$]	$5n$+[n]	$5n$+[n]	$46n$+[$6n$]
	[LP25]	$2n$	$2n$	$10n$	$5n$	$5n$	$36n$
	Ours	$2n$	$2n$	$7n$	$5n$	$5n$	$25n$
3	[dHKM+25]	$4n$+[n]	$4n$+[n]	$18n$+[$4n$]	$11n$+[n]	$11n$+[n]	$65n$+[$6n$]
	[dHMSS26]	$3n$+[n]	$3n$+[n]	$16n$+[$4n$]	$8n$+[n]	$8n$+[n]	$60n$+[$6n$]
	Ours	$3n$	$3n$	$13n$	$8n$	$8n$	$46n$
5	[dHKM+25]	$6n$+[n]	$6n$+[n]	$28n$+[$4n$]	$15n$+[n]	$15n$+[n]	$97n$+[$6n$]
	[dHMSS26]	$5n$+[n]	$5n$+[n]	$17n$+[$4n$]	$12n$+[n]	$12n$+[n]	$72n$+[$6n$]
	Ours	$5n$	$5n$	$23n$	$12n$	$12n$	$89n$
	Ours ($p \equiv \pm 1 \pmod 5$)	$5n$	$5n$	$21n$	$12n$	$12n$	$77n$

For $\ell = 2, 3, 5$, our proofs provide the smallest amount of R1CS variables and constraints, tying only with the concurrent [LP25] for $\ell = 2$, but significantly improving nnz in this case. Although our path is represented by one variable per curve, compared to two in [LP25], this advantage is diminished by the R1CS limitations, which force us to introduce more variables. Generally, our nnz numbers are slightly lower than previous works, except $\ell = 5$ where the more sparse Weber polynomials from [dHMSS26] are available. In contrast to the latter, our expressions naturally capture the non-backtracking property.

For $\ell = 7, 13$ we could not obtain better proofs than [dHKM+25] since their approach of proving the covering maps becomes more efficient for large-degree maps. While we can also view their approach as a part of our framework, we cannot benefit in this case from

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

backtracking prevention since it requires proving $(\mathbf{R}_{\ell,\ell}(x) - \mathbf{L}_{\ell,\ell}(y))/(y - \mathbf{w}_{\ell,\ell}(x))$ instead of proving $\mathbf{R}_{\ell,\ell}(x) = j$, $\mathbf{L}_{\ell,\ell}(y) = j'$ separately.

As mentioned in Subsection 5.2, at roughly the same costs, we can transport a 9-isogeny ($\ell = 2$) or a 4-isogeny ($\ell = 3$) along the main path using $X_0(18)$ and $X_0(12)$ walks respectively. Combining 2- and 5- isogenies is also feasible using $X_0(10)$. Such proofs can be beneficial for extending many protocols (such thin isogeny stripes occur e.g. in LIT-SiGamal [MS25]).

AI usage disclosure AI tools were used for literature search and review, sketching proofs, and proofreading. The paper is fully written by the author. AI was also used for a minimal easy-to-verify implementation of new modular polynomials in the $\mathbb{F}_p$-nnz optimization tool of [dHMSS26]. A Python library with a collection of all the formulas and verifications is written by the author.

References

[AAA+25] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign. Technical report, National Institute of Standards and Technology, 2025. URL: https://sqisign.org.

[ABCP23a] Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen. Practical robust DKG protocols for CSIDH. In Mehdi Tibouchi and Xiaofeng Wang, editors, *ACNS 2023, Part II*, volume 13906 of *LNCS*, pages 219–247. Springer, Cham, June 2023. doi:10.1007/978-3-031-33491-7_9.

[ABCP23b] Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen. VSS from distributed ZK proofs and applications. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part I*, volume 14438 of *LNCS*, pages 405–440. Springer, Singapore, December 2023. doi:10.1007/978-981-99-8721-4_13.

[BBJ+08] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In Serge Vaudenay, editor, *AFRICACRYPT 08*, volume 5023 of *LNCS*, pages 389–405. Springer, Berlin, Heidelberg, June 2008. doi:10.1007/978-3-540-68164-9_26.

[Bea82] Arnaud Beauville. Les familles stables de courbes elliptiques sur P1 admettant quatre fibres singulieres. *CR Acad. Sci. Paris Sér. I Math*, 294(19):657–660, 1982.

[BJ03] Olivier Billet and Marc Joye. The Jacobi model of an elliptic curve and side-channel analysis. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 34–42, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[BLS12] Reinier Bröker, Kristin Lauter, and Andrew Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012. doi:10.1090/S0025-5718-2011-02508-1.

[BRS25] Razvan Barbulescu, Damien Robert, and Nicolas Sarkis. Models of Kummer lines and Galois representations. Cryptology ePrint Archive, Report 2025/543, 2025. URL: https://eprint.iacr.org/2025/543.

[CC86] D.V Chudnovsky and G.V Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986. URL: https://www.sciencedirect.com/science/article/pii/0196885886900230, doi:10.1016/0196-8858(86)90023-0.

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 423–447. Springer, Cham, April 2023. doi:10.1007/978-3-031-30589-4_15.

[CDV20] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 493–519. Springer, Cham, December 2020. doi:10.1007/978-3-030-64834-3_17.

[CK26] Leonardo Colò and David Kohel. Weber modular curves and modular isogenies, 2026. URL: https://arxiv.org/abs/2603.29802, arXiv:2603.29802.

[CLL23] Kelong Cong, Yi-Fu Lai, and Shai Levin. Efficient isogeny proofs using generic techniques. In Mehdi Tibouchi and Xiaofeng Wang, editors, *ACNS 2023, Part II*, volume 13906 of *LNCS*, pages 248–275. Springer, Cham, June 2023. doi:10.1007/978-3-031-33491-7_10.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Cham, December 2018. doi:10.1007/978-3-030-03332-3_15.

[CLN+20] Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of SIKE in practice. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020, Part II*, volume 12111 of *LNCS*, pages 505–534. Springer, Cham, May 2020. doi:10.1007/978-3-030-45388-6_18.

[CLO13] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Science & Business Media, 2013.

[Col22] Leonardo Colò. *Oriented supersingular elliptic curves and class group actions*. PhD thesis, 2022. Thèse de doctorat dirigée par Kohel, David R. Mathématiques et informatique Aix-Marseille 2022. URL: http://www.theses.fr/2022AIXM0580.

[CSS26] Alessio Caminata, Andrea Sanguineti, and Silvia Sconza. Algebraic modelings of the supersingular isogeny problem. Cryptology ePrint Archive, Paper 2026/1369, 2026. URL: https://eprint.iacr.org/2026/1369.

[Dec24] Thomas Decru. Radical $\sqrt[N]{\text{élu}}$ isogeny formulae. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part V*, volume 14924 of *LNCS*, pages 107–128. Springer, Cham, August 2024. doi:10.1007/978-3-031-68388-6_5.

[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. doi:10.1007/978-3-032-01855-7_5.

[dHLM+26] Thomas den Hollander, Shai Levin, Marzio Mula, Robi Pedersen, Daniel Slamanig, and Sebastian A. Spindler. SPRINT: New isogeny proofs of knowledge and isogeny-based signatures. Cryptology ePrint Archive, Paper 2026/364, 2026. To appear at ASIACRYPT 2026. URL: https://eprint.iacr.org/2026/364.

[dHMSS26] Thomas den Hollander, Marzio Mula, Daniel Slamanig, and Sebastian A. Spindler. On the use of Atkin and Weber modular polynomials in isogeny proofs of knowledge. In Magali Bardet and Ruben Niederhagen, editors, *Post-Quantum Cryptography*, pages 39–73, Cham, 2026. Springer Nature Switzerland. doi:10.1007/978-3-032-22698-3_2.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem, Providence, RI*, pages 39–133, 1995.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular Functions of One Variable II: Proceedings International Summer School University of Antwerp, RUCA July 17–August 3, 1972*, pages 143–316. Springer, 1973.

[DS05] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[Edw07] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 04 2007. doi:10.1090/S0273-0979-07-01153-6.

[Elk97] Noam Elkies. Explicit modular towers. In *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing*, 1997.

[ES10] Andreas Enge and Andrew V. Sutherland. Class invariants by the CRT method. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory*, pages 142–156, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[FJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[FK90] R. Fricke and F. Klein. *Vorlesungen über die Theorie der elliptischen Modulfunctionen*. B.G. Teubner, 1890. URL: https://books.google.lu/books?id=kIYmzQEACAAJ.

[FNW10] Rongquan Feng, Menglong Nie, and Hongfeng Wu. Twisted Jacobi intersections curves. In Jan Kratochvíl, Angsheng Li, Jiří Fiala, and Petr Kolman, editors, *Theory and Applications of Models of Computation*, pages 199–210, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[Gal12] Steven D Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012.

[GC92] Xiao-Shan Gao and Shang-Ching Chou. Implicitization of rational parametric equations. *Journal of Symbolic Computation*, 14(5):459–470, 1992. URL: https://www.sciencedirect.com/science/article/pii/074771719290017X, doi:10.1016/0747-7171(92)90017-X.

[Gie79] J Gierster. Notiz über modulargleichungen bei zusammengesetztem transformationsgrad. *Mathematische Annalen*, 14(4):537–544, 1879.

[GSR03] Arnaldo Garcia, Henning Stichtenoth, and Hans-Georg Rück. On tame towers over finite fields. *Journal für die reine und angewandte Mathematik*, 2003(557):53–80, 2003. doi:10.1515/crll.2003.034.

[GVR09] Laureano Gonzalez-Vega and I.F. Rúa. Solving the implicitization, inversion and reparametrization problems for rational curves through subresultants. *Computer Aided Geometric Design*, 26(9):941–961, 2009. URL: https://www.sciencedirect.com/science/article/pii/S0167839609000764, doi:10.1016/j.cagd.2009.07.003.

[HWCD09] Hüseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Jacobi quartic curves revisited. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 09*, volume 5594 of *LNCS*, pages 452–468. Springer, Berlin, Heidelberg, July 2009. doi:10.1007/978-3-642-02620-1_31.

[Igu59a] Jun-Ichi Igusa. Fibre systems of Jacobian varieties: (iii. fibre systems of elliptic curves). *American Journal of Mathematics*, 81(2):453–476, 1959. URL: http://www.jstor.org/stable/2372751.

[Igu59b] Jun-ichi Igusa. Kroneckerian model of fields of elliptic modular functions. *American Journal of Mathematics*, 81(3):561–577, 1959.

[JAC+20] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular Isogeny Key Encapsulation. https://sike.org/files/SIDH-spec.pdf, October 2020. NIST Post-Quantum Cryptography Round 3 - Alternate Candidate.

[Kle78] Felix Klein. Ueber die transformation der elliptischen functionen und die auflösung der gleichungen fünften grades. *Mathematische Annalen*, 14(1):111–172, 1878.

[KM85] Nicholas M Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Number 108. Princeton University Press, 1985.

[Koh96] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley, 1996. PhD Thesis.

[LM25] Juan Jesús León and Vicente Muñoz. On some non-linear recurrences over finite fields linked to isogeny graphs. Cryptology ePrint Archive, Report 2025/608, 2025. URL: https://eprint.iacr.org/2025/608.

[LP25] Shai Levin and Robi Pedersen. Faster proofs and VRFs from isogenies. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part IV*, volume 16248 of *LNCS*, pages 307–340. Springer, Singapore, December 2025. doi:10.1007/978-981-95-5113-2_10.

[LS01] Pierre-Yvan Liardet and Nigel P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In Çetin Kaya Koç, David Naccache, and Christof Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 391–401. Springer, Berlin, Heidelberg, May 2001. doi:10.1007/3-540-44709-1_32.

[Mai09] Robert S. Maier. On rationally parametrized modular equations. *J. Ramanujan Math. Soc.*, 24:1–73, 2009.

[Mil17] James S. Milne. Modular functions and modular forms (v1.31), 2017. URL: https://www.jmilne.org/math/.

[MN23] Jonas Meers and Julian Nowakowski. Solving the Hidden Number Problem for CSIDH and CSURF via automated Coppersmith. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part IV*, volume 14441 of *LNCS*, pages 39–71. Springer, Singapore, December 2023. doi:10.1007/978-981-99-8730-6_2.

[MS25] Tomoki Moriya and Miha Stopar. LIT-SiGamal: An efficient isogeny-based PKE based on a LIT diagram. In Goichiro Hanaoka and Bo-Yin Yang, editors, *ASIACRYPT 2025, Part IV*, volume 16248 of *LNCS*, pages 275–306. Springer, Singapore, December 2025. doi:10.1007/978-981-95-5113-2_9.

[OM22] Hiroshi Onuki and Tomoki Moriya. Radical isogenies on Montgomery curves. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part I*, volume 13177 of *LNCS*, pages 473–497. Springer, Cham, March 2022. doi:10.1007/978-3-030-97121-2_17.

[OT20] Hiroshi Onuki and Tsuyoshi Takagi. On collisions related to an ideal class of order 3 in CSIDH. In Kazumaro Aoki and Akira Kanaoka, editors, *IWSEC 20*, volume 12231 of *LNCS*, pages 131–148. Springer, Cham, September 2020. doi:10.1007/978-3-030-58208-1_8.

[Pri24] Valentina Pribanić. Radical isogenies and modular curves. *Advances in Mathematics of Communications*, 18(6):1748–1767, 2024. doi:10.3934/amc.2023019.

[Ren18] Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In Tanja Lange and Rainer Steinwandt, editors, *PQCrypto 2018*, pages 229–247. Springer, Cham, 2018. doi:10.1007/978-3-319-79063-3_11.

[Sag26] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026. `https://www.sagemath.org`.

[TKF+21] Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, and Kazuhiro Yokoyama. Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology*, 15(1):31–44, 2021. doi:10.1515/jmc-2020-0072.

[Tsu13] Kiminori Tsukazaki. *Explicit isogenies of elliptic curves*. PhD thesis, University of Warwick, 2013.

[TY09] Fang-Ting Tu and Yifan Yang. Defining equations of $X_0(2^{2n})$. *Osaka J. Math.*, 46(1):105–113, 2009.

[Yan06] Yifan Yang. Defining equations of modular curves. *Advances in Mathematics*, 204(2):481–508, 2006. doi:10.1016/j.aim.2005.05.019.

A 4-torsion on Montgomery curves

First, we recall the 2nd and 4th x-only torsion polynomials on Montgomery curves.

Proposition 14. *Let E_A be a Montgomery curve. Then, its 2nd and 4th x-only torsion polynomials ψ_2 and ψ_4 are given by (up to a constant factor)*

$$\psi_2 = x^3 + Ax^2 + x,$$
$$\psi_4 = \psi_2 \cdot (x-1) \cdot (x+1) \cdot (x^4 + 2Ax^3 + 6x^2 + 2Ax + 1).$$

It then follows that solely from the x-coordinate of a nonconstant order-4 point we can compute the x-coordinate of its double, and the A coefficient by simple rational maps.

Corollary 3. *Let $E_A[n]$ denote the n-torsion subgroup of E_A. For $(a, _) \in E_A[2], a \neq 0$, we have*

$$A = -\frac{a^2+1}{a} = -a - \frac{1}{a};$$

for $(r, _) \in E_A[4] \setminus E_A[2], r \notin \{-1, 1\}$, we have

$$A = -\frac{r^4 + 6r^2 + 1}{2r(r^2+1)} = -\frac{r + \frac{1}{r}}{2} - \frac{2}{r + \frac{1}{r}}.$$

The three order-2 and six order-4 points (the x-coordinates) on a curve E_A can be arranged as shown on Figure 6.

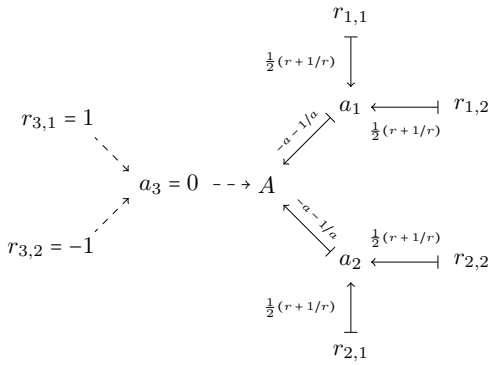

Figure 6: The structure of the 4-torsion $E_A[4]$ of a Montgomery curve E_A (x-coordinates only). The order-2 points are $a_1, a_2, a_3 = 0$, and the order-4 points are $r_{1,1}, r_{1,2}, r_{2,1}, r_{2,2}, r_{3,1} = 1, r_{3,2} = -1$. The six outer arrows correspond to the doubling operation on E_A.

The correspondence between our modular parameters and entities related to Montgomery curves are summarized in Table 9.

Table 9: Correspondence of $X_0(N)$ parameters and objects related to the Montgomery curve model.

Modular curve	Symbol	Parameter	Relation
$X_0(1)$	j	j-invariant of E_A	
$X_0(2)$	D	Montgomery discriminant D	$j = \mathbf{R}_{2,2}(D) = \frac{(D+16)^3}{D}$
$X_0(4)$	A	A-coefficient	$D = \mathbf{R}_{4,2}(A) = 16(A^2-4)$
$X_0(8)$	a	x-coefficient of a nonconstant order-2 point on a Montgomery curve	$A = \mathbf{L}_{8,2}(a) = -a - \frac{1}{a}$
$X_0(12)$	z	$z = 3x$ for the x-coordinate of an order-3 point on a Montgomery curve	$A = \mathbf{L}_{12,3}(z) = -\frac{z^4+18z^2-27}{4z^3}$
$X_0(16)$	r	x-coefficient of a nonconstant order-4 point on a Montgomery curve	$a = \mathbf{L}_{16,2}(r) = \frac{1}{2}\left(r + \frac{1}{r}\right)$

B Rotation maps

In Table 10, we report explicit rotation maps.

Table 10: Tail/head rotation maps with respect to level ℓ on modular curves C, and their order. Here, $i = \zeta_4 = \sqrt{-1}$, ζ_n is a primitive n^{th} root of unity.

Modular curve C	ℓ	$\mathbf{T}_{C,\ell}(t)$	$\mathbf{H}_{C,\ell}(t)$
$X_0(4)$	2	$-t$	$\frac{2t+12}{t-2}$
$X_0(8)$	2	$-t$	$\frac{1}{t}$
$X_0(12)$	2	$-t$	$\frac{t+3}{t-1}$
$X_0(16)$	2	$-t$	$\frac{1}{t}$
$X_0(16)$	4	it	$\frac{-it+1}{t-i}$
$X_0(9)$	3	$\zeta_3 t$	$\frac{(-3\zeta_3-3)t+18}{t-3\zeta_3}$
$X_0(18)$	3	$\zeta_3 t$	$\frac{(\zeta_3+1)t+2}{t+\zeta_3}$
$X(5)$	5	$\zeta_5 t$	$\frac{(-\zeta_5^2-\zeta_5-1)t+1}{t-\zeta_5^2-\zeta_5}$

C Additional maps

This section provides additional maps that did not fit in the main tables. Yet, in a few cases the expressions are too huge to be included even here, and are available in the supplementary code repository.

Additional modular polynomials for Table 3 are given by:

$$\begin{aligned}
\Phi_{3,3}(t,u) &= t^3u^2 + 36t^2u^2 + 729t^2u + 270tu^2 - u^3 + 26244tu + 531441t,\\
\Phi_{6,3}(t,u) &= -t^3u^2 + 12t^2u^2 - 9t^2u - 30tu^2 + u^3 + 108tu - 81t,\\
\Phi_{5,5}(t,u) &= t^5u^4 + 30t^4u^4 + 125t^4u^3 + 315t^3u^4 + 3750t^3u^3 + 1300t^2u^4\\
&\quad + 15625t^3u^2 + 39375t^2u^3 + 1575tu^4 - u^5 + 468750t^2u^2 + 162500tu^3\\
&\quad + 1953125t^2u + 4921875tu^2 + 58593750tu + 244140625t.\\
\Phi_{10,5}(t,u) &= -t^5u^4 - 4t^5u^3 + 5t^4u^4 - 6t^5u^2 + 15t^4u^3 - 5t^3u^4 - 4t^5u + 15t^4u^2 + 10t^3u^3\\
&\quad + 5t^2u^4 - t^5 + 5t^4u + 35t^3u^2 - 35t^2u^3 - 5tu^4 + u^5 + 20t^3u + 40t^2u^2\\
&\quad + 60tu^3 - 16u^4 + 80t^2u - 240tu^2 + 96u^3 + 320tu - 256u^2 + 256u,
\end{aligned}$$

$$\begin{aligned}\Phi_{25,5}(t,u) &= t^5u^4+t^5u^3+6t^5u^2+5t^3u^4+6t^5u+5t^3u^3+11t^5+30t^3u^2+5tu^4-u^5\\ &\quad+30t^3u+5tu^3-6u^4+55t^3+30tu^2-21u^3+30tu-56u^2+55t-71u-120,\\ \Phi_{X_1(5),5}(t,u) &= t^5u^4+22t^5u^3+25t^4u^4+119t^5u^2+475t^4u^3+200t^3u^4-22t^5u\\ &\quad+2175t^4u^2+1675t^3u^3+525t^2u^4+t^5-200t^4u+9650t^3u^2\\ &\quad-9650t^2u^3+200tu^4-u^5+525t^3u+1675t^2u^2+2175tu^3\\ &\quad-22u^4-200t^2u-475tu^2-119u^3+25tu+22u^2-u.\end{aligned}$$

We do not provide here modular polynomials for composite ℓ, they can be easily computed with the same methods. Below, we provide additional covering pairs inverse maps to complete the framework:

$$\begin{aligned}\mathbf{M}_{1,3}(t,u) &= (tu^3+19129644tu^2-756u^3+531440t^2+76509442080tu\\ &\quad+23150726640u^2-48430448640000t-14204206448640000u\\ &\quad+97844723712000000000)/(729t^2u+196830tu^2+u^3-524880t^2\\ &\quad+18821147040tu-103456080u^2+14229831680000t\\ &\quad+276373831680000u-3623878656000000000),\\ \mathbf{M}_{2,3}(t,u) &= (tu^3-900tu^2+28u^3+80t^2-17568tu+27216u^2+32768t\\ &\quad+2654208u)/(9t^2u+270tu^2+u^3+144t^2-25632tu+2448u^2\\ &\quad+32768t+294912u),\\ \mathbf{M}_{X_{\mathrm{ns}}(2),3}(t,u) &= \frac{tu^3+728t^2-339696tu+264600u^2-3755372544}{27t^2u+486tu^2-u^3+7388416t+10273536u}.\\ \mathbf{M}_{5,5}(t,u) &= (-50t^3u^2+t^2u^3-750t^2u^2+11tu^3-3125t^2u-2625tu^2+20u^3\\ &\quad-59375tu+2625u^2-390625t+62500u+390625)/(tu^3+375tu^2\\ &\quad+5u^3+34375tu+1375u^2+390625t+46875u+390625),\\ \mathbf{M}_{X_1(5),5}(t,u) &= (20t^4u^3+655t^4u^2+390t^3u^3+4765t^4u+10510t^3u^2+2165t^2u^3-2tu^4\\ &\quad-435t^4+52405t^3u+23760t^2u^2+2816tu^3-10u^4+3155t^3+75980t^2u\\ &\quad-58248tu^2+435u^3-1195t^2-111tu+6005u^2+93t-545u)/(15625t^3u\\ &\quad-75t^2u^2+145tu^3-2u^4-9375t^3+115425t^2u-36745tu^2+391u^3\\ &\quad+8200t^2+7490tu+4452u^2-1660t-1436u+93)\ \ (\text{to } X(5)).\end{aligned}$$