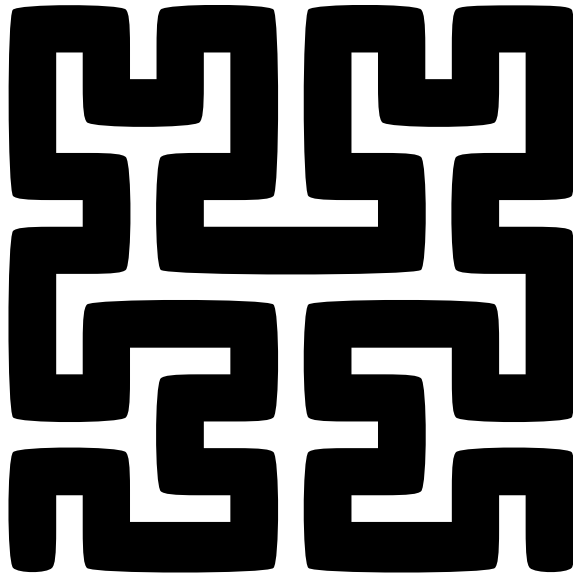




Polynesian Journal of Mathematics

Volume 4, Issue 13

Special volume AĴAX in honor of René Schoof

Weber modular curves and modular isogenies

Leonardo Colò David Kohel

Received 3 Mar 2026

Revised 25 Jun 2026

Accepted 6 Jul 2026

Published 28 Sep 2026

Communicated by Valerio Talamanca

DOI: 10.69763/polyjmath.4.13

Weber modular curves and modular isogenies

Leonardo Colò¹ David Kohel²

¹University of Waterloo, Ontario, Canada

²Institut de Mathématiques de Marseille, Aix-Marseille Université, France

Abstract

We study the modular curves defined by Weber functions, and associated modular polynomials, action of $\mathrm{SL}_2(\mathbb{Z})$, and parametrizations of elliptic curves with a view to the study of the isogeny graphs that they determine, particularly for supersingular elliptic curves. In addition to applications to efficient isogeny computation in cryptographic applications, we present an application to explicit Galois representations.

1 Introduction

We describe explicit models of modular curves defined by Weber functions, with their parametrizations of families of elliptic curves. These functions, appearing in Weber [15], are modular functions of level 48, each of which describes a degree-72 cover of the j -line by a genus-0 modular curve. This degree is the largest known of any modular function covering the j -line, and the properties of the resulting class polynomials and modular polynomials make them attractive for explicit algorithms for class groups and isogeny computations. Collectively the functions generate the function field of a high-genus quotient of $X(48)$ which admits many symmetries.

Various cryptographic algorithms rely on the explicit computation of modular isogenies: given an elliptic curve $E/\mathbb{F}_q$ or its j -invariant $j(E)$ and a prime $\ell \nmid p$, one needs to determine one or all $\ell + 1$ of the moduli of ℓ -isogenous elliptic curves. The data of an ℓ -isogeny can be specified by the x -coordinates of points in an ℓ -torsion subgroup [16], corresponding to a point on $X_1(\ell)$, or a kernel polynomial vanishing on these points (see [9, Chapter 2] and [10]) associated to a point on $X_0(\ell)$. Conversely, one can recover the isogeny data on E from the associated point on $X_0(\ell)$ [14].

Yui and Zagier [17] investigated Weber functions for constructing small class invariants. These class polynomials exhibited remarkably small coefficient size, asymptotically 72 times smaller in height than their counterparts of level 1. Gee [8] developed the theoretical foundations of class invariants for arbitrary modular functions, using Shimura

Leonardo Colò was supported by an NSERC Alliance Consortia Quantum Grant, ALLRP 578463-22.

reciprocity, and Enge and Morain [6, 7] investigated the height reduction in terms of Dedekind eta and generalized Weber functions. To date, no modular function is known which achieves the same height reduction, and the factor 72 is conjecturally maximal.

In this work, we describe the modular polynomials, curves, and elliptic curve parametrizations defined by the Weber functions. The modular polynomials have the same advantage of height reduction, as for class polynomials, in addition to a sparseness condition, which makes them much smaller and efficient to use for isogeny computations. The curves are defined by the triple of classical Weber functions (with a suitable twist), which are skew conjugate under the action of $\mathrm{SL}_2(\mathbb{Z})$. We describe the position of these curves and their quotients in the Galois cover from $X(48)$ to $X(1)$. In particular, a quotient to the 8th Fermat curve gives an alternative curve of level 16 admitting a degree-48 cover of $X(1)$. We provide explicit models for these curves, their morphisms and the action of $\mathrm{SL}_2(\mathbb{Z})$, as well as the elliptic curve parametrizations and isogenies that they describe.

The level structure determined by Weber functions is particularly suited to traversal of supersingular isogeny graphs. The SIDH protocol [5] works with j -invariants of level 1, but the CSIDH protocol already incorporates the level-4 structure of a function a on $X_1(4)$ such that $j = 256(a^2 - 3)^3 / (a^2 - 4)$. In addition to admitting small modular polynomials, the supersingular points on the Weber curves split completely over $\mathbb{F}_{p^2}$, exactly as for the j -invariants. No further base extension is required to split the supersingular isogenies or to define their isogenies.

In addition to cryptographic applications, the structure of supersingular isogeny graphs permits one to compute representations associated to spaces of modular forms, in which the level structure of the invariants used, and the characteristic of the base field $\mathbb{F}_{p^2}$, controls the level of the representations. Mestre's method of graphs [12] gives a construction for Galois representations of prime level p or level mp where m is one of the levels m in $\{2, 3, 4, 5, 7, 13\}$ for which the modular curve $X_0(m)$ is of genus 0. We conclude with examples of this application of Weber curves to the study of Galois representations, particularly associated to modular elliptic curves with prescribed ramification at 2 and 3.

2 Weber functions and modular polynomials

Let $X_G/\mathbb{F}_p$ be a modular curve associated to an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N , and ℓ prime to Np . Given arbitrary open subgroups H and G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, we denote by $X_G(H)$ the modular curve associated to $G \cap H$, equipped with the cover $X_G(H) \rightarrow X_G$.

The modular ℓ -isogeny supersingular graph is determined by a set of supersingular moduli points on X_G , with edge relations given by points in the correspondence

$$X_G(B_0(\ell)) \rightrightarrows X_G.$$

When ℓ is not coprime to N , we replace the above correspondence with

$$X_G(B_0(\ell^t)) \rightrightarrows X_G,$$

where t is the minimal integer such that $G \not\subseteq B_0(\ell^t)$.

2.1 Modular polynomials

One advantage of working with a modular curve $\mathcal{X}_G$ of higher level, still of genus 0, is that the logarithmic coefficient size of the modular polynomials $\Phi_\ell^{(f)}(x, y)$ with respect to a degree one function f on $\mathcal{X}_G$ is reduced by a factor of the degree of the cover $\mathcal{X}_G \rightarrow X(1)$. If we consider the smallest correspondence, for $\ell = 2$, for the j -invariant we have the modular polynomial

$$x^3 - x^2y^2 + y^3 + 1488x^2y + 1488xy^2 - 162000x^2 - 162000y^2 + 40773375xy \\ + 8748000000x + 8748000000y - 15746400000000.$$

In comparison, for the group $\Gamma_0(3)$ of index 4, this becomes

$$x^3 - x^2y^2 - 24x^2y - 24xy^2 - 729xy + y^3$$

and, for the full congruence subgroup $\Gamma(3)$ with index 12 and associated modular curve $\mathcal{X}(3)$, we have

$$x^3 - x^2y^2 + 9xy + y^3 - 54.$$

It is worth noting that the sparsity of monomials of the latter polynomial can be explained by the transformation

$$\Phi_\ell^{(f)}(\zeta_3x, \zeta_3^\ell y) = \zeta_3^{\ell+1} \Phi_\ell^{(f)}(x, y),$$

where ζ_3 denotes a primitive third root of unity, for the family of modular polynomials with respect to the particular normalized modular function on $\mathcal{X}_G = \mathcal{X}(3)$. In particular, only the monomials $x^i y^j$ satisfying $i + \ell j \equiv \ell + 1 \pmod{3}$ can occur.

After introducing the normalized Weber functions which form the central objects of this article, we derive similar results for the modular polynomials defined in terms of these Weber functions.

2.2 Weber modular functions

The definition of a modular polynomial requires a genus 0 modular curve or fixed function on a modular curve. In order to understand the transformation properties of this function, one needs to study its images under the images of transformations by the generators of $\mathrm{SL}_2(\mathbb{Z})$.

The classically-defined triple of Weber functions,

$$\mathfrak{f}(\tau) = \zeta_{48}^{-1} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)}, \quad \mathfrak{f}_1(\tau) = \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)}, \quad \mathfrak{f}_2(\tau) = \sqrt{2} \cdot \frac{\eta(2\tau)}{\eta(\tau)},$$

are modular functions, the first two with rational integral q -expansions in $q^{1/48} = e^{2\pi i \tau/48}$, and the third with q -expansion in $q^{1/24}$ with coefficients in $\sqrt{2}\mathbb{Z}$. Each satisfies the relations

$$j = \frac{(\mathfrak{f}^{24} - 16)^3}{\mathfrak{f}^{24}} = \frac{(\mathfrak{f}_1^{24} + 16)^3}{\mathfrak{f}_1^{24}} = \frac{(\mathfrak{f}_2^{24} + 16)^3}{\mathfrak{f}_2^{24}},$$

on which the standard generators

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

of $\mathrm{SL}_2(\mathbb{Z})$ induce (see Yui and Zagier [17], Gee [8])

$$(\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ S = (\mathfrak{f}, \mathfrak{f}_2, \mathfrak{f}_1) \quad \text{and} \quad (\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2) \circ T = (\zeta_{48}^{-1} \mathfrak{f}_1, \zeta_{48}^{-1} \mathfrak{f}, \zeta_{48}^2 \mathfrak{f}_2). \quad (1)$$

It is well-known that the Weber functions satisfy $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$ and based on the identity

$$\zeta_{48}^{-1} \eta\left(\frac{\tau+1}{2}\right) \eta\left(\frac{\tau}{2}\right) \eta(2\tau) = \eta(\tau)^3$$

it follows from the definition of the Weber functions that $\mathfrak{f} \mathfrak{f}_1 \mathfrak{f}_2 = \sqrt{2}$.

Setting $(u_0, u_1, u_2) = (\mathfrak{f}, \zeta_{16} \mathfrak{f}_1, \zeta_{16}^{-1} \mathfrak{f}_2)$, the triple (u_0, u_1, u_2) satisfies the common relations

$$j = \frac{(u_0^{24} - 16)^3}{u_0^{24}} = \frac{(u_1^{24} - 16)^3}{u_1^{24}} = \frac{(u_2^{24} - 16)^3}{u_2^{24}},$$

and one verifies that the three orbits $\{\zeta_{24}^j u_i : j \in \mathbb{Z}/24\mathbb{Z}\}$, for $i \in \mathbb{Z}/3\mathbb{Z}$, run over the 72 roots of the modular polynomial

$$(x^{24} - 16)^3 - j(q)x^{24}$$

in $\mathbb{Q}(\zeta_{48})[[q^{1/48}]]$.

2.3 Weber modular polynomials

The best known reduction in coefficient size as well as in sparsity of coefficients is obtained for the Weber function $\mathfrak{f} = \mathfrak{f}(\tau)$ of level 48 defined above. The modular polynomials with respect to $\mathfrak{f}$ are the integral polynomials $\Phi_\ell^{(\mathfrak{f})}(x, y)$ such that

$$\Phi_\ell^{(\mathfrak{f})}(\mathfrak{f}(\tau), \mathfrak{f}(\ell\tau)) = 0.$$

Although the Weber function does not generate the full modular curve $X(48)$, which has genus 2689, it still satisfies a transformation giving the following symmetry of its induced modular polynomials.

Proposition 2.1. *The modular polynomial $\Phi_\ell^{(\mathfrak{f})}(x, y)$ of prime level ℓ with respect to the Weber function $\mathfrak{f}$ satisfies the transformation*

$$\Phi_\ell^{(\mathfrak{f})}(\zeta_{24} x, \zeta_{24}^\ell y) = \zeta_{24}^{\ell+1} \Phi_\ell^{(\mathfrak{f})}(x, y)$$

with respect to a primitive 24^{th} root of unity ζ_{24} .

This gives the following sparsity result for the coefficients of the Weber modular polynomials.

Corollary 2.2. *The coefficient of the monomial $x^i y^j$ in the Weber modular polynomial $\Phi_\ell^{(f)}(x, y)$ is nonzero only if $i + \ell j \equiv \ell + 1 \pmod{24}$.*

Asymptotically, modular polynomials have $(\ell + 1)^2$ monomials, but due to the sparseness coming from Corollary 2.2, the number of nonzero coefficients of Weber modular polynomials is of the order of $(\ell + 1)^2/24$. Combined with the height reduction of the coefficients this makes the Weber modular polynomials attractive for constructing isogeny invariants. The first few examples are as follows.

$$\begin{aligned}\Phi_5^{(f)}(x, y) &= x^6 - x^5 y^5 + 4xy + y^6 \\ \Phi_7^{(f)}(x, y) &= x^8 - x^7 y^7 + 7x^4 y^4 - 8xy + y^8 \\ \Phi_{11}^{(f)}(x, y) &= x^{12} - x^{11} y^{11} + 11x^9 y^9 - 44x^7 y^7 + 88x^5 y^5 - 88x^3 y^3 + 32xy + y^{12} \\ \Phi_{13}^{(f)}(x, y) &= x^{14} - x^{13} y^{13} + 13x^{12} y^2 + 52x^{10} y^4 + 78x^8 y^6 + 78x^6 y^8 + 52x^4 y^{10} \\ &\quad + 13x^2 y^{12} + 64xy + y^{14}\end{aligned}$$

Going further, the modular polynomial $\Phi_{71}^{(f)}(x, y)$ has exactly $3 \cdot 71 = 213$ nonzero coefficients, ignoring the symmetry $\Phi_\ell^{(f)}(x, y) = \Phi_\ell^{(f)}(y, x)$, which implies an even smaller number of distinct coefficients.

In the interest of constructing ℓ -isogeny chains, especially for $\ell = 2$ or $\ell = 3$, we note that the 48-level structure gives the modular polynomials $\Phi_2^{(f)}(x, y)$ and $\Phi_3^{(f)}(x, y)$ a particular form. We descend the 2-level structure by setting $t = -f^8$, so that

$$j = \left(\frac{t^3 + 16}{t} \right)^3.$$

With respect to this function, we obtain the modular polynomial

$$\Phi_2^{(t)}(x, y) = (x^2 - y)y + 16x$$

and the Weber modular polynomial $\Phi_2^{(f)}(x, y) = -\Phi_2^{(t)}(-x^8, -y^8)$ remains irreducible.¹ A similar descent of the 3-level to the function $r = f^3$, gives the modular polynomial

$$\Phi_3^{(r)}(x, y) = x^4 - x^3 y^3 + 8xy + y^4,$$

such that $\Phi_3^{(r)}(r(\tau), r(3\tau)) = 0$, for which $\Phi_3^{(f)}(x, y) = \Phi_3^{(r)}(x^3, y^3)$ is irreducible. For a given supersingular Weber invariant, these relations determine orbits under multiplication by ζ_8 or ζ_3 , but in view of the global relation of Proposition 2.1, the lift to the orbit can be chosen to be compatible with isogeny relations of other prime degrees.

¹More correctly, the modular polynomial $\Phi_2^{(t)}(x, y)$ satisfies $\Phi_2^{(t)}(f_1^8(\tau), f_1^8(2\tau)) = 0$, where f_1 is the conjugate Weber function

$$f_1^8(\tau) = -f(\tau + 3)^8 = \left(\frac{\eta(\frac{\tau}{2})}{\eta(\tau)} \right)^8$$

and hence $\Phi_2^{(t)}(f^8(\tau), f^8(2\tau - 3)) = 0$. Nevertheless, this modular relation describes a 2-isogeny relation of the underlying curves, extending the parametrized 2-isogeny to a 4-isogeny, and will be used for defining our 2-isogeny chains.

2.4 Modular group action

The proposition which follows summarizes the action of the modular group on the triples of normalized Weber functions.

Proposition 2.3. *The action of $\mathrm{PSL}_2(\mathbb{Z}) = \langle S, T \rangle$ on Weber triples (u_0, u_1, u_2) maps through the quotient $\mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})/\{\pm 1\}$, and is defined on generators by*

$$(u_0, u_1, u_2) \circ S = (u_0, \zeta_8 u_2, \zeta_8^{-1} u_1) \quad \text{and} \quad (u_0, u_1, u_2) \circ T = (\zeta_{12}^{-1} u_1, \zeta_{24} u_0, \zeta_{24} u_2).$$

In particular the elements $U = T^{-1}ST$, $V = T^{-2}ST^2$, and $W = ST^3$ act by permutations:

$$(u_0, u_1, u_2) \circ U = (u_2, u_1, u_0), \quad (u_0, u_1, u_2) \circ V = (u_0, u_2, u_1), \quad (u_0, u_1, u_2) \circ W = (u_2, u_0, u_1).$$

Proof. The quotient via $\mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})$ follows from the definition of the Weber functions, as η quotients of level 48. From the definition $(u_0, u_1, u_2) = (f, \zeta_{48}^3 f_1(\tau), \zeta_{48}^{-3} f_2(\tau))$ and the transformations (1), we obtain

$$\begin{aligned} (u_0, u_1, u_2) \circ S &= (f, \zeta_{48}^3 f_2, \zeta_{48}^{-3} f_1) = (u_0, \zeta_{48}^6 u_2, \zeta_{48}^{-6} u_1), \\ (u_0, u_1, u_2) \circ T &= (\zeta_{48}^{-1} f_1, \zeta_{48}^2 f, \zeta_{48}^{-1} f_2) = (\zeta_{24}^{-2} u_1, \zeta_{24} u_0, \zeta_{24} u_2). \end{aligned}$$

The permutation actions of U , V , and W follow from the actions of S and T . $\square$

Remark 2.4. The right action on Weber triples gives a homomorphism $\iota: \mathrm{PSL}_2(\mathbb{Z}) \rightarrow \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$, defined on generators by

$$\iota(S) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \zeta_8^{-1} \\ 0 & \zeta_8 & 0 \end{pmatrix}, \quad \iota(T) = \begin{pmatrix} 0 & \zeta_{24} & 0 \\ \zeta_{24}^{-2} & 0 & 0 \\ 0 & 0 & \zeta_{24} \end{pmatrix}.$$

In the next section we describe the image as the automorphism group of a Galois cover $\mathcal{W}_{24} \rightarrow X(1)$ of the j -line, of order 1152 whose kernel Γ_{24} contains $\mathrm{PSL}_2(\mathbb{Z}/48\mathbb{Z})$ of index 32. Since $\mathrm{PSL}_2(\mathbb{Z})$ acts by skew permutations, its image $G = \iota(\mathrm{PSL}_2(\mathbb{Z}))$ lies in the subgroup $S_3 \ltimes \mu_{24}^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$, where S_3 denotes the symmetric group on three letters, acting by permutation matrices on the coordinates, and μ_{24}^3 denotes the subgroup of diagonal matrices whose entries are 24th roots of unity. There exists an exact sequence

$$1 \longrightarrow D \longrightarrow G \longrightarrow S_3 \longrightarrow 1,$$

where $D = G \cap \mu_{24}^3$ is the subgroup of diagonal matrices. By the existence of the permutation subgroup $S_3 = \langle U, V, W \rangle \subset G$, the sequence splits, from which the corollary follows.

Corollary 2.5. *The subgroup D of diagonal matrices in $G = \iota(\mathrm{PSL}_2(\mathbb{Z}))$ is a normal subgroup, generated by the order-24 matrices*

$$\iota(T)^2 = \begin{pmatrix} \zeta_{24}^{-1} & 0 & 0 \\ 0 & \zeta_{24}^{-1} & 0 \\ 0 & 0 & \zeta_{24}^2 \end{pmatrix} \quad \text{and} \quad \iota(STS)^2 = \begin{pmatrix} \zeta_{24}^{-1} & 0 & 0 \\ 0 & \zeta_{24}^2 & 0 \\ 0 & 0 & \zeta_{24}^{-1} \end{pmatrix},$$

subject to the relation $\iota(T)^{16} = \iota(STS)^{16} = \zeta_3^{-1}I$. In particular $D \subset \mu_{24}^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$ is abelian of order $3 \cdot 8^2 = 192$. The quotient G/D is isomorphic to the symmetric group S_3 , acting by permutation on the Weber functions $\{u_0^{24}, u_1^{24}, u_2^{24}\}$, and $G \cong S_3 \ltimes D$.

In the following section we consider the embeddings given by the normalized Weber functions, and their quotients by subgroups $D[m] = D \cap \mu_m^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$.

3 Weber curves

We are now able to use the conjugate Weber functions to define a curve with projective embedding given by the functions u_0, u_1 , and u_2 . Let m and n be integers such that $mn = 8$. The map determined by the normalized Weber functions $(u_0^m : u_1^m : u_2^m : 1)$ determines a *Weber modular curve* $\mathcal{W}_{3n}$ in $\mathbb{P}^3$

$$\mathcal{W}_{3n} : \begin{cases} X_0^n + X_1^n + X_2^n = 0, \\ X_0 X_1 X_2 = \sqrt{2}^m X_3^3, \end{cases} \quad (2)$$

with quotient Weber curve $\mathcal{W}_n$ defined as the image of $(u_0^{3m} : u_1^{3m} : u_2^{3m} : 1)$ in $\mathbb{P}^3$

$$\mathcal{W}_n : \begin{cases} X_0^n + X_1^n + X_2^n = 48X_3^n, \\ X_0 X_1 X_2 = \sqrt{8}^m X_3^3. \end{cases} \quad (3)$$

These defining relations follow directly from the relations $f^8 = f_1^8 + f_2^8$ and $f f_1 f_2 = \sqrt{2}$, and the curves are equipped with maps $\mathcal{W}_{nr} \rightarrow \mathcal{W}_n$ for each product nr dividing 24. When n is not divisible by 8, clearly the curve $\mathcal{W}_n$ is defined over $\mathbb{Q}$, and at the loss of symmetry, one can descend $\mathcal{W}_8$ and $\mathcal{W}_{24}$ to $\mathbb{Q}$.

Explicitly the projection $(x, y) = (u_0^m, u_1^m)$ determines a birational map to an affine plane curve

$$\mathcal{W}_{3n}^0 : x^{2n}y^n + x^n y^{2n} + 2^4 = 0,$$

with inverse $(x, y) \mapsto (x : y : \sqrt{2}^m / xy : 1)$, and the projection to $(x, y) = (u_0^{3m}, u_1^{3m})$ is birational to the affine plane curve

$$\mathcal{W}_n^0 : x^{2n}y^n + x^n y^{2n} - 48x^n y^n + 2^{12} = 0.$$

with inverse $(x, y) \mapsto (x : y : \sqrt{2}^{3m} / xy : 1)$. The affine curves $\mathcal{W}_{3n}^0$ and $\mathcal{W}_n^0$ are defined over $\mathbb{Q}$ but the splittings to $\mathcal{W}_{3n}$ and $\mathcal{W}_n$ require $\mathbb{Q}(\sqrt{2}^m)$ in the base field in order to preserve the symmetry of the coordinate functions as roots of $j = (u^{3n} - 16)^3 / u^{3n}$ or $j = (u^n - 16)^3 / u^n$, respectively.

In the application to supersingular curves and moduli in characteristic $p > 3$, the existence of a square root of 2 or of 24th roots of unity, does not present any additional constraint since the field of definition $\mathbb{F}_{p^2}$ contains all 24th roots of unity.

The curves $\mathcal{W}_n$ form Galois covers of the j -line $X(1)$. In order to define modular polynomials, as correspondences in $\mathbb{P}^1 \times \mathbb{P}^1$, we will work with the quotients $\pi_i : \mathcal{W}_n \rightarrow$

$\mathcal{X}_n \cong \mathbb{P}^1$ determined by the projection $(u_0 : u_1 : u_2 : 1) \mapsto (u : 1) = (u_i : 1)$, and equipped with the map to the j -line $\mathcal{X}_n \rightarrow X(1)$ given by

$$j(u) = \frac{(u^n - 16)^3}{u^n}.$$

In particular, the curve $\mathcal{X}_n$ parametrizes the family of elliptic curves

$$\mathcal{E}_0/\mathcal{X}_n: y^2 = x \left(x^2 - \frac{(u^n - 64)}{4}x - (u^n - 64) \right) \quad (4)$$

of j -invariant $j(u)$, discriminant $(u^n - 64)^3 u^n$, and 2-torsion point $(0, 0)$. Quotienting $\mathcal{E}_0$ by the subgroup generated by $(0, 0)$ gives the 2-isogenous family

$$\mathcal{E}_1/\mathcal{X}_n: y^2 = x \left(x^2 + \frac{(u^n - 64)}{2}x + \frac{(u^n - 64)}{16}u^n \right) \quad (5)$$

with j -invariant $-(u^n - 256)^3/u^{2n}$, discriminant $-(u^n - 64)^3 u^{2n}$, and 2-torsion point $(0, 0)$.

Using the defining equations of $\mathcal{W}_n$ and projecting via $\pi_0: (u_0 : u_1 : u_2 : 1) \mapsto (u_0 : 1)$, one recovers u_2 from the two relations up to $2n$ choices. It follows that the cover $\mathcal{W}_n \rightarrow \mathcal{X}_n$ has degree $2n$, while the expression for $j(u)$ shows that $\mathcal{X}_n \rightarrow X(1)$ has degree $3n$. This gives a degree $6n^2$ cover $\mathcal{W}_n \rightarrow X(1)$. In the next section we determine the structure of the Galois group of this cover.

We conclude this section with an observation of an isomorphism, for n dividing 8, between the Weber curve $\mathcal{W}_n$ and the Fermat curve $\mathcal{F}_n: X^n + Y^n + Z^n = 0$. In particular the cover $\mathcal{W}_{3n} \rightarrow \mathcal{W}_n$ factors through the quotient

$$\begin{array}{ccc} \mathcal{W}_{3n} & \longrightarrow & \mathcal{F}_n \\ (X_0 : X_1 : X_2 : X_3) & \longmapsto & (X_0 : X_1 : X_2). \end{array}$$

Indeed this is the quotient by the group of automorphisms

$$\{(X_0 : X_1 : X_2 : X_3) \mapsto (\zeta_3^i X_0 : \zeta_3^i X_1 : \zeta_3^i X_2 : X_3) : i \in \mathbb{Z}/3\mathbb{Z}\},$$

which stabilizes the fibers of the quotient $\mathcal{W}_{3n} \rightarrow \mathcal{W}_n$, which must factor through $\mathcal{F}_n$. In view of the defining equations for $\mathcal{W}_{3n}$, we infer that the induced map $\mathcal{F}_n \rightarrow \mathcal{W}_n$ is given by

$$(X : Y : Z) \mapsto \left(X^3 : Y^3 : Z^3 : \frac{XYZ}{\sqrt{2}^m} \right).$$

When $n \neq 8$, this morphism is defined over $\mathbb{Q}$, and otherwise $\mathcal{F}_8$ gives a model for a descent of $\mathcal{W}_8$ to $\mathbb{Q}$. In Proposition 3.1, we prove that $\mathcal{W}_{3n} \rightarrow \mathcal{W}_n$ has degree 3, which implies that $\mathcal{F}_n \rightarrow \mathcal{W}_n$ is an isomorphism. Either by a generic computation or application of genus formulas for modular curves, using the characterizations which follow, Table 1 gives the genera of the curves.

n	1	2	4	8
$g(\mathcal{W}_{3n})$	1	4	19	85
$g(\mathcal{F}_n) = g(\mathcal{W}_n)$	0	0	3	21

Table 1: Genera of Weber modular curves and quotient Weber curves.

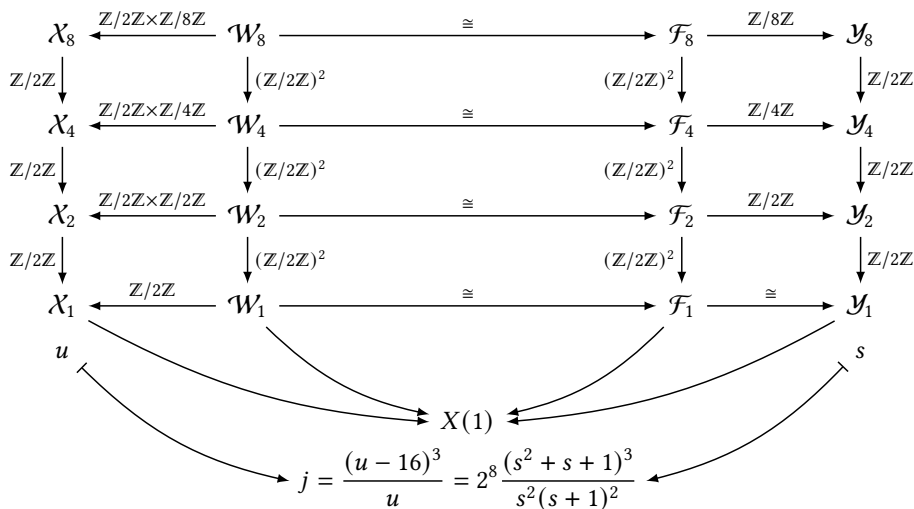


Figure 1: Morphisms between Weber and Fermat curves and their quotients.

As with the Weber curves, the Fermat curves come equipped with projections $\pi_i: \mathcal{F}_n \rightarrow \mathcal{Y}_n \cong \mathbb{P}^1$ given by

$$\pi_i((X : Y : Z)) = \begin{cases} (Y : Z) & \text{if } i = 0, \\ (X : Z) & \text{if } i = 1, \\ (X : Y) & \text{if } i = 2, \end{cases}$$

and parametrized by the modular functions $(u_1/u_2)^m$, $(u_0/u_2)^m$ and $(u_0/u_1)^m$, respectively. This gives the diagram of morphisms between Weber and Fermat curves and their quotients displayed in Figure 1. The isomorphisms $\mathcal{W}_n \rightarrow \mathcal{F}_n$ appear in Appendix A,

for all divisors n of 8. In particular, for $n = 1$, the isomorphism is given by

$$\begin{aligned} \mathcal{W}_1: \begin{cases} X_0 + X_1 + X_2 = 48X_3, \\ X_0X_1X_2 = 4096X_3^3 \end{cases} &\longrightarrow \mathcal{F}_1: X + Y + Z = 0 \\ (u_0 : u_1 : u_2 : u_3) &\longmapsto (u_0 - 16u_3 : u_1 - 16u_3 : u_2 - 16u_3) \\ (16s_0^3 : 16s_1^3 : 16s_2^3 : s_0s_1s_2) &\longleftarrow (s_0 : s_1 : s_2). \end{aligned} \quad (6)$$

The affine parametrization $(s : t : 1)$ of $\mathcal{F}_1$ by $s = -(t + 1)$ gives the parametrization of $\mathcal{W}_1$

$$\begin{aligned} (u_0 : u_1 : u_2 : 1) &= \left(-\frac{16s^2}{(s+1)} : \frac{16(s+1)^2}{s} : -\frac{16}{s(s+1)} : 1 \right) \\ &= \left(\frac{16(t+1)^2}{t} : -\frac{16t^2}{(t+1)} : -\frac{16}{t(t+1)} : 1 \right). \end{aligned}$$

After the substitution $u = -16s^2/(s+1)$ and quadratic twist of the models $\mathcal{E}_0/\mathcal{X}_1$ and $\mathcal{E}_1/\mathcal{X}_1$, we obtain the isogenous families

$$\begin{aligned} C_0/\mathcal{Y}_1: y^2 &= x(x-1)(x+t) = x(x-1)(x-(s+1)) \text{ and} \\ C_1/\mathcal{Y}_1: y^2 &= x((x+s)^2 + 4x). \end{aligned} \quad (7)$$

of j -invariants $256(s^2+s+1)^3/s^2(s+1)^2$ and $16(s^2+16s+16)^3/s^4(s+1)$, and discriminants $16s^2(s+1)^2$ and $256s^4(s+1)$, respectively.

3.1 Modular group

To each factorization $mn = 24$, the Weber curve $\mathcal{W}_n$ in $\mathbb{P}^3$, defined by the triple of Weber functions (u_0^m, u_1^m, u_2^m) , comes equipped with an action of $\mathrm{PSL}_2(\mathbb{Z})$. We denote the kernel of the action by Γ_n , identifying the Weber curves with the modular curve $X(\Gamma_n)$. The action of $\mathrm{PSL}_2(\mathbb{Z})$ on Weber functions induces a representation in $\mathrm{GL}_3(\mathbb{Q}(\zeta_n))$ determined by the images of the generators S and T :

$$\begin{aligned} \mathrm{PSL}_2(\mathbb{Z}) &\longrightarrow \mathrm{GL}_3(\mathbb{Q}(\zeta_n)) \\ S, T &\longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \bar{\zeta}_8^m \\ 0 & \zeta_8^m & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta_{24}^m & 0 \\ \bar{\zeta}_{24}^{2m} & 0 & 0 \\ 0 & 0 & \zeta_{24}^m \end{pmatrix}. \end{aligned}$$

The image group is finite, whose kernel Γ_n is a normal congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, such that $\mathrm{PSL}_2(\mathbb{Z})/\Gamma_n$ is the Galois group of the cover $\mathcal{W}_n \rightarrow X(1)$.

We reduce the computation of Γ_n by first proving that $\Gamma_1 = \Gamma(2)$, then noting that $\Gamma_3 \cap \Gamma_8 = \Gamma_{24}$, which reduces to determining Γ_3 and the chain $\Gamma_8 \subset \Gamma_4 \subset \Gamma_2 \subset \Gamma_1 = \Gamma(2)$.

Let $\mu_m = \langle \zeta_m \rangle$ be the group of m^{th} roots of unity. We identify μ_m^3 with the subgroup (scheme) of G_m^3 , acting on affine space $\mathbb{A}^3$. We define the two complementary subgroups of diagonal matrices

$$\begin{aligned}\nabla(\mu_m^2) &= \left\{ (\zeta_m^i, \zeta_m^j, \zeta_m^{-i-j}) \in \mu_m^3 : i, j \in \mathbb{Z}/m\mathbb{Z} \right\} \text{ and} \\ \Delta(\mu_m) &= \left\{ (\zeta_m^i, \zeta_m^i, \zeta_m^i) \in \mu_m^3 : i \in \mathbb{Z}/m\mathbb{Z} \right\}.\end{aligned}$$

If $m \equiv 0 \pmod{3}$, then $\Delta(\mu_3) \subset \Delta(\mu_m) \cap \nabla(\mu_m^2)$, otherwise the groups $\Delta(\mu_m)$ and $\nabla(\mu_m^2)$ are independent.

Proposition 3.1. *For each divisor mn of 24, the morphism $\mathcal{W}_{mn} \rightarrow \mathcal{W}_n$ is the quotient by a subgroup of automorphisms in μ_m^3 isomorphic to Γ_n/Γ_{mn} .*

- If $m = 3$, then the automorphism group of the cover is $\Delta(\mu_3)$.
- If m divides 8, then the automorphism group of the cover is $\nabla(\mu_m^2)$.

In particular, the degree of $\mathcal{W}_{3n} \rightarrow \mathcal{W}_n$ is 3 and, if m divides 8, the degree of $\mathcal{W}_{mn} \rightarrow \mathcal{W}_n$ is m^2 .

Proof. The quotients $\mathcal{W}_{mn} \rightarrow \mathcal{W}_n$ are induced by the restriction, to the affine Weber curves, of the quotients $\mathbb{A}^3 \rightarrow \mathbb{A}^3$ by μ_m^3 , sending (x_0, x_1, x_2) to (x_0^m, x_1^m, x_2^m) . Each Weber curve is a normal cover of $X(1)$, and the relative Galois group of the cover $\mathcal{W}_{mn} \rightarrow \mathcal{W}_n$ is $(\text{PSL}_2(\mathbb{Z})/\Gamma_{mn}) / (\text{PSL}_2(\mathbb{Z})/\Gamma_n) \cong \Gamma_n/\Gamma_{mn}$.

We first consider $m = 3$: the affine Weber curve $\mathcal{W}_{3n}$ ($X_3 \neq 0$) is given by equations $x^n + y^n + z^n = 0$ and $xyz = c_{3n} \neq 0$, with n coprime to 3. Consequently the subgroup of μ_3^3 stabilizing the curve is the intersection of the group $\Delta(\mu_3)$, stabilizing $x^n + y^n + z^n$, and $\nabla(\mu_3^2)$, fixing xyz . Since $\Delta(\mu_3) \subset \nabla(\mu_3^2)$, the automorphism group of the cover is $\Delta(\mu_3)$, and $\mathcal{W}_{3n} \rightarrow \mathcal{W}_n$ is of degree 3.

Now assume that m divides 8. The affine Weber curve is defined by equations $x^{mn} + y^{mn} + z^{nm} = 48$, if n is coprime to 3, or otherwise $x^{mn/3} + y^{mn/3} + z^{nm/3} = 0$, and $xyz = c_{mn} \neq 0$. The former is fixed by μ_m^3 , hence the automorphism group of the cover is the subgroup $\nabla(\mu_m^2)$ fixing the form xyz . The degrees of the morphisms $\mathcal{W}_{mn} \rightarrow \mathcal{W}_n$ follow since $|\Delta(\mu_3)| = 3$ and $|\nabla(\mu_m^2)| = m^2$. $\square$

Proposition 3.2. *The Weber kernel group Γ_1 equals $\Gamma(2)$ and $\mathcal{W}_1 \cong X(2)$.*

Proof. The Weber curve $\mathcal{W}_1$ is parametrized by the three normalized η -quotients

$$u_0^{24} = -\left(\frac{\eta((\tau+1)/2)}{\eta(\tau)}\right)^{24} \quad u_1^{24} = -\left(\frac{\eta(\tau/2)}{\eta(\tau)}\right)^{24} \quad u_2^{24} = -2^{12} \left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{24}$$

invariant under $\Gamma(2)$, which generate the $S_3 = \text{PSL}_2(\mathbb{F}_2)$ -extension $\mathbb{Q}(X(2))/\mathbb{Q}(X(1))$. $\square$

We recall that the nonsplit Cartan normalizer subgroup $\Gamma_{\text{ns}}^+(3)$ is the index 3 normal subgroup of $\text{SL}_2(\mathbb{Z})$, containing $\Gamma(3)$, whose function field is generated by a cube root of the j -invariant.

Proposition 3.3. *The Weber kernel group Γ_3 equals $\Gamma(2) \cap \Gamma_{\text{ns}}^+(3)$ and, for each n dividing 8,*

$$\Gamma_{3n} = \Gamma_n \cap \Gamma_{\text{ns}}^+(3).$$

Proof. By Proposition 3.2 we have $\Gamma_1 = \Gamma(2)$ and by Proposition 3.1, we have $\Gamma_1/\Gamma_3 \cong \Delta(\mu_3)$ of order 3. Thus Γ_3 is a congruence subgroup satisfying $\Gamma(6) \subset \Gamma_3 \subset \Gamma(2)$, of index 3 in $\Gamma(2)$. This uniquely characterizes Γ_3 as the intersection of $\Gamma(2)$ with the normal subgroup $\Gamma_{\text{ns}}^+(3)$ of $\text{PSL}_2(\mathbb{Z})$. $\square$

It thus suffices to characterize the groups Γ_n for n dividing 8.

Proposition 3.4. *The Weber kernel group Γ_2 equals $\Gamma(4)$ and $\mathcal{W}_2 \cong X(4)$.*

Proof. By Proposition 3.1, the Weber kernel group of $\mathcal{W}_2 \rightarrow \mathcal{W}_1$ satisfies $\Gamma_1/\Gamma_2 \cong \Delta(\mu_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$, where $\Gamma_1 = \Gamma(2)$ by Proposition 3.2. From the transformation of the η -quotients defining the Weber functions, it is clear that the triple $(u_0^{12}, u_1^{12}, u_2^{12})$ is invariant under $\Gamma(4)$. Since $\Gamma(2)/\Gamma(4) \cong (\mathbb{Z}/2\mathbb{Z})^2$, it follows that $\Gamma_2 = \Gamma(4)$. $\square$

We recall that the split Cartan modular curve $X_s(N)$ is defined by the congruence subgroup

$$\Gamma_s(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \pmod{N} \right\},$$

parametrizing elliptic curves with a disjoint pair of cyclic N -isogenies.

Proposition 3.5. *The Weber kernel group Γ_4 equals $\Gamma_s(8)$ and $\mathcal{W}_4 \cong X_s(8)$.*

Proof. The triple (u_0^6, u_1^6, u_2^6) is invariant under $\Gamma(8)$, but the quotient $\Gamma(4)/\Gamma(8)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, so that Γ_4 is an index 2 subgroup. An explicit calculation with the above images of the generators, shows that Γ_4 contains the diagonal subgroup modulo $\Gamma(8)$, isomorphic to $(\mathbb{Z}/8\mathbb{Z})^*$, hence equals $\Gamma_s(8)$. $\square$

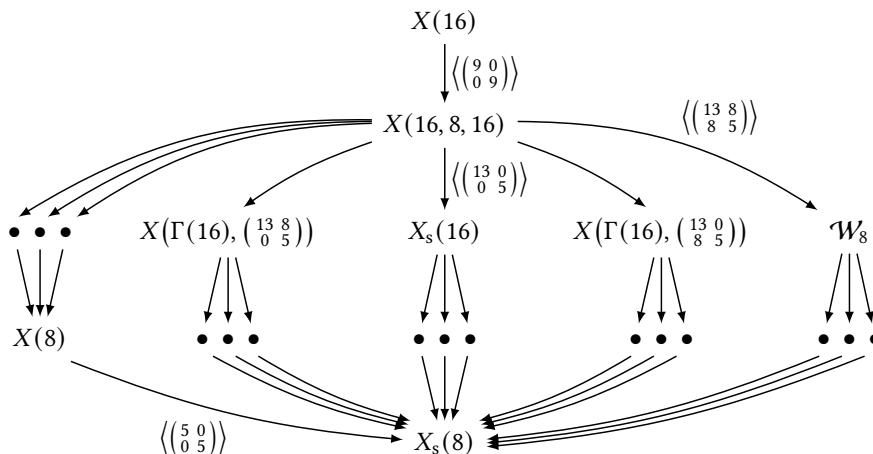
It remains to characterize the group Γ_8 under which the triple of functions (u_0^3, u_1^3, u_2^3) is invariant. This group is not the split Cartan subgroup $\Gamma_s(16)$, but we can show that

$$\Gamma(16) \subset \Gamma_8 \subset \Gamma_s(8) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv c \equiv 0 \pmod{8} \right\}$$

and that the group $\Gamma_8/\Gamma(16)$ is cyclic of order 4 generated by

$$T^2 U^2 T^{-2} U^{-2} \equiv \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} \pmod{16},$$

where $U = STS^{-1}$. The equality is easily verified in $\text{SL}_2(\mathbb{Z}/16\mathbb{Z})$ and the word expression on the left maps to the identity under the above homomorphism to $\text{GL}_3(\mathbb{Q}(\zeta_8))$, showing that the element is in the kernel of the action on $\mathcal{W}_8$. Moreover, the matrix on the right lifts to $\text{SL}_2(\mathbb{Z})$. Given that the degree of $\mathcal{W}_8 \rightarrow \mathcal{W}_4 \cong X_s(8)$ is 4, and $X(16) \rightarrow X(8)$ is of degree 8, this proves the following description of the kernel group Γ_8 .

Figure 2: Diagram of modular curves between $X(16)$ and $X_s(8)$.

Proposition 3.6. *The Weber kernel group Γ_8 is the group generated by $\Gamma(16)$ and $\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}$.*

In particular, we note that Γ_8 contains the diagonal matrix

$$\begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}^2 \equiv \begin{pmatrix} 9 & 0 \\ 0 & 9 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})$$

in the center of $\mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})$, hence it contains the subgroup

$$\Gamma(16, 8, 16) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{8}, b \equiv c \equiv 0 \pmod{16} \right\}.$$

Given that $\Gamma_s(8)/\Gamma(16)$ is an abelian group, we obtain

$$\Gamma_s(8)/\Gamma(16) = \left\langle \begin{pmatrix} 13 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix} \right\rangle \cong C_4 \times V_4,$$

so that $\Gamma_s(8)/\Gamma(16, 8, 16) \cong C_2 \times V_4 = C_2^3$; Figure 2 shows modular curves between $X(16)$ and $X_s(8)$. where the curves represented by dots are intermediate quotients by the subgroups of $V_4 = \langle T^8, U^8 \rangle$.

In what follows, we describe the Galois group of the full cover $\mathcal{W}_{24} \rightarrow X(1)$, characterize the splitting of supersingular points, and apply this to the splitting of supersingular points on $\mathcal{W}_{24}$ over $\mathbb{F}_{p^2}$.

3.2 Galois groups of Weber covers

In general, the geometric Galois group of the cover $X(N) \rightarrow X(1)$ of modular curves is $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, with the constant field $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ extension determined by the cyclotomic character $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow (\mathbb{Z}/N\mathbb{Z})^*$. Restricting the case $N = 48$ to the Weber modular curve, we obtain the following result.

Theorem 3.7. *The geometric Galois group of $\mathcal{W}_{24} \rightarrow X(1)$ is $S_3 \ltimes D$ where $D = \Delta(\mu_3)\nabla(\mu_8^2)$, defined over $\mathbb{Q}(\zeta_{24})$, and the constant field extension is $\mathbb{Q}(\zeta_{24})/\mathbb{Q}$.*

Proof. The structure of the geometric Galois group follows from Proposition 3.1 and Proposition 3.2. In particular the factorization $\mathcal{W}_{24} \rightarrow \mathcal{W}_1 \rightarrow X(1)$ gives the splitting of the exact sequence

$$1 \rightarrow D \rightarrow S_3 \ltimes D \rightarrow S_3 \rightarrow 1,$$

where $D = \Delta(\mu_3)\nabla(\mu_8^2)$ is the automorphism group of the cover $\mathcal{W}_{24} \rightarrow \mathcal{W}_1$ and where S_3 is the automorphism group of $\mathcal{W}_1 \cong X(2)$ over $X(1)$. The Galois action on Weber triples is given by coordinate permutations and scaling by μ_{24} , which determines the field of definition $\mathbb{Q}(\zeta_{24})$. The constant field necessarily contains this field of definition and is contained in the constant field $\mathbb{Q}(\zeta_{48})$ of the cover $X(48) \rightarrow X(1)$. However, the splitting field for the points over the CM j -invariant $j = -2^{15}$ of discriminant -11 does not contain the 16^{th} roots of unity, so the exact constant field is $\mathbb{Q}(\zeta_{24})$. A similar proof follows from the splitting of the supersingular points over $\mathbb{F}_{5^2}$, which does not contain the 16^{th} roots of unity. $\square$

Remark 3.8. The choice of normalization of the Weber functions (u_0, u_1, u_2) by 48^{th} roots of unity, such that $j = (u_i^{24} - 16)^3/u_i^{24}$, allows the descent of the constant field to $\mathbb{Q}(\zeta_{24})$.

3.3 Supersingular fields of definition

For any elliptic curve E in the isogeny class of a curve over $\mathbb{F}_p$, the full endomorphism ring $\mathcal{O}$ is defined over $\mathbb{F}_{p^2}$. Since the action of $\mathcal{O}/NO \cong \mathrm{M}_2(\mathbb{Z}/N\mathbb{Z})$ on the $E[N]$ is defined over $\mathbb{F}_{p^2}$, it follows that the Galois action on $E[N]$, which commutes with $\mathcal{O}/NO$, acts through the center $(\mathbb{Z}/N\mathbb{Z})^*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and more precisely, Frobenius acts as $-p$ on $E[N]$.

Theorem 3.9. *For any positive integer N , the supersingular invariants on the modular curve $X_0(N)$ are defined over $\mathbb{F}_{p^2}$, and if $p \equiv \pm 1 \pmod{N}$, then the supersingular invariants also split over $\mathbb{F}_{p^2}$ on $X_1(N)$.*

Proof. For any supersingular elliptic curve $E/\mathbb{F}_{p^2}$, in the isogeny class of a curve over $\mathbb{F}_p$, the lines in $E[N]$ are Galois stable. Hence every cyclic N -isogeny is defined over $\mathbb{F}_{p^2}$, and the supersingular points of $X_0(N)$ split over $\mathbb{F}_{p^2}$. Moreover, since Frobenius acts by $-p$, if $p \equiv \pm 1 \pmod{N}$, the N -torsion is pointwise fixed up to automorphisms, giving the splitting of the supersingular points on $X_1(N)$. $\square$

Remark 3.10. Equivalently, for $X_0(N)$ we can state that every supersingular j -invariant j_0 splits completely under the map $X_0(N) \rightarrow X(1)$, or that the polynomial $\Phi_N(x, j_0)$

splits completely, where $\Phi_N(x, y)$ is the classical modular polynomial. For $X_1(N)$, the splitting of the supersingular points is recognized by the factorization of the N -division polynomial ψ_N .

As a consequence, the split Cartan modular curve $X_s(N)$, also splits the supersingular moduli.

Corollary 3.11. *For any positive integer N , the supersingular invariants on the split Cartan modular curve $X_s(N)$ are defined over $\mathbb{F}_{p^2}$. In particular if $p \equiv \pm 1 \pmod{N}$, then the supersingular invariants on the modular curve $X(N)$ are defined over $\mathbb{F}_{p^2}$.*

Proof. The first statement follows from the splitting of N -isogenies over $\mathbb{F}_{p^2}$. In addition if $p \equiv \pm 1 \pmod{N}$, the points of each kernel are fixed, hence a basis is defined over $\mathbb{F}_{p^2}$ (up to twist). $\square$

Remark 3.12. For the levels N in $\{1, 2, 3, 4, 6\}$, the unit group $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$ is trivial so the supersingular points split for all p . This corresponds to the geometric equalities $X_1(N) = X_0(N)$ and $X(N) = X_s(N)$.

The Weber moduli are functions on $X(48)$ which map through $\mathcal{W}_{24}$. The Frobenius action on the 48-torsion, relative to $\mathbb{F}_{p^2}$, acts by scalar multiplication by $-p$ on the torsion module $E[48]$. The image of the determinant map on $\mathrm{GL}_2(\mathbb{Z}/48\mathbb{Z})$ gives p^2 in the cyclotomic group $(\mathbb{Z}/48\mathbb{Z})^*$, which is trivial unless $p \equiv \pm 5 \pmod{8}$. However since the constant field is $\mathbb{Q}(\zeta_{24})$ by Theorem 3.7, the image lies in $(\mathbb{Z}/24\mathbb{Z})^*$, which is an elementary 2-group, hence p^2 is trivial. This proves that $\mathbb{F}_{p^2}$ is the field of definition.

Theorem 3.13. *The supersingular Weber invariants on $\mathcal{W}_{24}$ are defined over $\mathbb{F}_{p^2}$.*

Remark 3.14. A point (u_0, u_1, u_2) on $\mathcal{W}_{24}$ over the j -invariant j_0 consists of a triple of common roots of the polynomial $(x^{24} - 16)^3 - j_0 x^{24}$, and the set of roots is precisely $\{\zeta_{24}^i u_j : 0 \leq i < 24, 0 \leq j < 3\}$. The property that j_0 splits completely under $\mathcal{W}_{24} \rightarrow X(1)$ over $\mathbb{F}_{p^2}$ is equivalent to this polynomial splitting completely over $\mathbb{F}_{p^2}$.

4 Elliptic curves over Weber and Fermat curves

We now turn to the problem of explicit families of elliptic curves over Weber curves $\mathcal{W}_n$ and Fermat curves $\mathcal{F}_n$ and the isogeny structures that they parametrize. We construct models over the quotients $\mathcal{W}_n \rightarrow X_n$ and $\mathcal{F}_n \rightarrow \mathcal{Y}_n$. For each n dividing 8, we have an isomorphism $\mathcal{W}_n \cong \mathcal{F}_n$ (given explicitly in Appendix A), but this does not imply a morphism between X_n and $\mathcal{Y}_n$, except for $n = 1$, we have seen in (6) the isomorphisms

$$\mathcal{W}_1 \xrightarrow{\cong} \mathcal{F}_1 \xrightarrow{\cong} \mathcal{Y}_1,$$

which imply a morphism $X(2) \cong \mathcal{Y}_1 \rightarrow X_1 \cong X_0(2)$.

We have also seen that the family (4) of elliptic curves

$$\mathcal{E}_0/X_n: y^2 = x \left(x^2 - \frac{(u^n - 64)}{4}x - (u^n - 64) \right)$$

is parametrized by the Weber modular curve $\mathcal{X}_n$, hence by base extension by $\mathcal{W}_n$. We also recall from (7) that the affine Fermat curve $\mathcal{F}_n : s^n + t^n + 1 = 0$ parametrizes the following model through its quotient to $\mathcal{Y}_n$:

$$C_0/\mathcal{Y}_n : y^2 = x(x-1)(x+t^n) = x(x-1)(x-s^n-1).$$

In order to set up the notation for the extension of base field, from $K(\mathcal{Y}_1)$ to $K(\mathcal{Y}_8)$, we set $t_3 = t$ a generator for $K(\mathcal{Y}_8)$ and $t_{k-1} = t_k^2$ for $1 \leq k \leq 3$, such that, for a field K ,

$$\begin{array}{ccccccc} K(\mathcal{F}_1) \cong K(\mathcal{W}_1) & \hookrightarrow & K(\mathcal{F}_2) \cong K(\mathcal{W}_2) & \hookrightarrow & K(\mathcal{F}_4) \cong K(\mathcal{W}_4) & \hookrightarrow & K(\mathcal{F}_8) \cong K(\mathcal{W}_8) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K(\mathcal{Y}_1) = K(t_0) & \hookrightarrow & K(\mathcal{Y}_2) = K(t_1) & \hookrightarrow & K(\mathcal{Y}_4) = K(t_2) & \hookrightarrow & K(\mathcal{Y}_8) = K(t_3) \end{array}$$

is a sequence of quadratic extensions $K(t_k)/K(t_{k-1})$, which will permit us to build a chain of 2-isogenies. We note that the final isomorphism $K(\mathcal{F}_8) \cong K(\mathcal{W}_8)$ requires a square root of 2 in K , and moreover the chain of isogenies which follow require an 8th root of unity ζ_8 , for which we set $i = \zeta_8^2$, so we assume K contains a homomorphic image of $\mathbb{Z}[\zeta_8]$.

4.1 Explicit 2-isogeny chains

We prioritize the Fermat model as the base curve parametrizing chains of 2-isogenies, with a view to constructing explicit equations for the isogeny chains from C_0 . We describe a 2-isogeny chain over $K(\mathcal{Y}_8)$, starting from C_0 , of the form

$$C_0 \xrightarrow{\phi_0} C_1 \xrightarrow{\phi_1} C_2 \xrightarrow{\phi_2} C_3.$$

The base extension to $K(\mathcal{F}_8)$ gives rise to an explicit action on the chains by the automorphism group of $K(\mathcal{F}_8)/K(X(1))$. By Proposition 3.2, we have $\mathcal{F}_1 \cong \mathcal{W}_1 \cong X(2)$, and since $S_3 = \text{Aut}(K(X(2))/K(X(1))) = \text{SL}_2(\mathbb{Z})/\Gamma(2)$, it follows from Proposition 3.1 that the automorphism group $\text{Aut}(K(\mathcal{F}_8)/K(X(1)))$ is isomorphic to $S_3 \rtimes \nabla(\mu_8^2)$, a subgroup of the automorphism group of Corollary 2.5.

We normalize the curves C_i and isogenies ϕ_i of the chain such that the isogenies are defined by successive quotients by a 2-torsion point $(0, 0)$. On the curve C_k we give, for each k in $\{0, 1\}$, a point $T_k \in C_k[4]$ such that $2T_k = (0, 0)$ and $\phi_k(T_k) = (0, 0)$ on the codomain C_{k+1} . The quotient by $(0, 0)$ in $C_0[2]$ gives the 2-isogeny

$$\begin{aligned} \phi_0 : C_0 : y^2 = x(x-1)(x+t_0) &\longrightarrow C_1 : y^2 = x(x+4c_0)(x+e_0^2) \\ (x, y) &\longmapsto \left(\frac{(x-c_0)^2}{x}, \frac{x^2-c_0^2}{x^2}y \right) \end{aligned}$$

where $c_0 = it_1$ and $e_0 = t_1 + i$. The point $T_0 = (c_0, c_0 e_0) \in C_0[4]$ satisfies $2T_0 = (0, 0) \in C_0[2]$ and $\phi_0(T_0) = (0, 0) \in C_1[2]$. The quotient by $(0, 0)$ in $C_1[2]$ gives the next step in

the 2-isogeny chain

$$\begin{aligned} \phi_1: C_1: y^2 = x(x + 4c_0)(x + e_0^2) &\longrightarrow C_2: y^2 = x(x + 4c_1)(x + e_1^2) \\ (x, y) &\longmapsto \left(\frac{(x - c_1)^2}{x}, \frac{x^2 - c_1^2}{x^2} y \right) \end{aligned}$$

where $c_1 = 2\zeta_8 t_2(t_1 + i)$ and $e_1 = (t_2 + \zeta_8)^2$. The point $T_1 = (c_1, c_1 e_1)$ satisfies $2T_1 = (0, 0) \in C_1[2]$ and $\phi_1(T_1) = (0, 0) \in C_2[2]$. Finally, the quotient by $(0, 0)$ in $C_2[2]$ gives the 2-isogeny

$$\begin{aligned} \phi_2: C_2: y^2 = x(x + 4c_1)(x + e_1^2) &\longrightarrow C_3: y^2 = (x^2 + 4c_2)(x + c_3) \\ (x, y) &\longmapsto \left(\frac{x^2 - c_2}{x}, \frac{x^2 + c_2}{x^2} y \right) \end{aligned}$$

where $c_2 = -4c_1 e_1^2$ and $c_3 = e_1^2 + 4c_1$. In terms of the coordinates $(s_3, t_3) = (s_3 : t_3 : 1)$, the coordinate permutations and scalar multiplications $(s_3, t_3) \mapsto (\zeta_8^{i_1} s_3, \zeta_8^{i_2} t_3)$ permute all possible 2-isogeny chains from C_0 .

4.2 Explicit ℓ -isogeny chains

Unlike for $\ell = 2$, the Weber functions do not parametrize a $\Gamma_0(\ell)$ -structure for any odd prime ℓ . Even on $\mathcal{W}_{3n}$, the nonsplit Cartan structure $\Gamma_{\text{ns}}^+(3)$ determined by the Weber curve is independent of a $\Gamma_0(3)$ structure parametrizing 3-isogenies. An ℓ -isogeny chain is parametrized by a sequence of moduli $(u_0, u_1, \dots, u_r)$ which are successive roots $\Phi_\ell(u_{i-1}, u_i) = 0$ of the level- ℓ modular polynomial $\Phi_\ell(x, y)$ with respect to $\mathcal{X}_{24}$ (or when $\ell = 3$, of one of the quotients, $\mathcal{X}_8$ or $\mathcal{Y}_8$ of $\mathcal{W}_8 \cong \mathcal{F}_8$).

5 Weber supersingular modules

Mestre's method of graphs [12] permits one to construct a *supersingular Hecke module*: a free abelian group on supersingular points equipped with Hecke operators, given by correspondences on the underlying modular curves. In terms of the supersingular isogeny graphs, the Hecke operator T_ℓ arises as the adjacency matrices of the ℓ -isogeny graph. Mestre's construction was defined for modular curves of level 1, or one of the models $X_0(m)$ of genus 0 given by quotients of the Dedekind η function, for $m \in \{2, 3, 4, 5, 7, 13\}$. This gives rise to Galois representations of type GL_2 and level $N = mp$, where p is the characteristic of the base field of the supersingular points. As an application, Cowan [4] exploits Mestre's method with sieving to enumerate newforms associated to low dimensional isogeny factors of the Jacobian $J_0(N)$ of $X_0(N)$. In particular, this permits one to gather statistics for the distribution of elliptic curves and low dimensional modular abelian varieties of prime level, or nearly prime level.

The Weber and Fermat modular curves permit one to study modular isogeny factors of levels with higher powers of 2 and 3. A general framework for isogeny graphs with

$B - 1000 < p < B$		1000	2000	3000	4000	5000	6000	7000	8000	$N = mp$
# Weber	$\mathcal{X}_{12}$	160	104	80	132	92	60	84	68	$288 \cdot p$
# orbits		40	26	20	22	23	15	21	17	
# Weber	$\mathcal{X}_6$	212	132	98	78	106	92	80	76	$72 \cdot p$
# orbits		106	66	49	39	53	46	40	38	
# Weber	$\mathcal{X}_3$	450	288	222	212	262	208	206	194	$18 \cdot p$
# orbits		225	144	111	106	131	104	103	97	
# Weber	$\mathcal{X}_4$	142	110	80	66	48	60	56	56	$32 \cdot p$
# orbits		71	55	40	33	24	30	28	28	
# Weber	$\mathcal{X}_2$	174	99	91	79	94	84	90	63	$8 \cdot p$
# Weber	$\mathcal{X}_1$	274	256	184	194	175	186	155	126	$2 \cdot p$
# Fermat	$\mathcal{Y}_8$	100	60	32	32	72	24	24	24	$256 \cdot p$
# orbits		25	15	8	8	18	6	6	6	
# Fermat	$\mathcal{Y}_4$	974	538	538	544	502	498	396	336	$64 \cdot p$
# orbits		487	269	269	272	251	249	298	168	
# Fermat	$\mathcal{Y}_2$	545	364	309	287	281	279	248	193	$16 \cdot p$
# Fermat	$\mathcal{Y}_1$	96	60	48	39	37	39	34	26	$4 \cdot p$
# Level 1	$X(1)$	69	41	34	35	25	26	21	22	p
# primes	$\mathbb{Z}$	168	135	127	120	119	114	117	107	1

Table 2: Counts of Weber and Fermat pseudo elliptic factors.

level structure is developed in [3]. For prime level, Bennett, Gherga, and Reznitz [1] have enumerated all elliptic curves of prime conductor up to $2 \cdot 10^9$, but datasets for elliptic curves of composite level are less complete. In particular, the higher powers of 2 and 3 imply that the supersingular modules associated to moderately large primes rapidly exceed conductor bounds in typical datasets such as the LMFDB [11]. In Table 2, we give the numbers of isogeny classes of pseudo elliptic factors coming from the Weber curves $\mathcal{X}_n$, where n divides 12, or Fermat curves $\mathcal{Y}_n$, where n divides 8. By pseudo elliptic factors, we refer to an eigenspace on which the Hecke operators away from $6p$ act by scalar multiplication in $\mathbb{Z}$.

Table 2 collects the counts of pseudo elliptic factors associated to the supersingular Hecke modules on the Weber curves $\mathcal{X}_n$, for n dividing 12 and the Fermat curves $\mathcal{F}_n$, for n dividing 8. When the factors appear in orbits of twists with respect to $\mathbb{Q}(\zeta_n)$, we report in a second line the number of such orbits (dividing the counts by 2 or 4).

The full Weber curve $\mathcal{W}_{24}$ carries level-48 structure, equipped with an action of Galois group of $\mathbb{Q}(\zeta_{48})$, which is not of exponent 2, and we observe that every modular isogeny factor associated to the Weber curves $\mathcal{X}_{24}$ and $\mathcal{X}_8$ has even degree Hecke algebra, and in particular, gives rise to no pseudo elliptic factors. More specifically, the Hecke algebra systematically contains the quadratic field $\mathbb{Q}(\sqrt{2})$.

Although this represents a limited dataset, the numbers of such orbits for $\mathcal{X}_{12}$, of level $288p$, align roughly with the numbers of isogeny classes of elliptic curves of conductor p , while the numbers of orbits for $\mathcal{Y}_8$, of level $256p$, appear to be smaller by a factor of four in this range. Each of the curves of lower levels give rise to a much larger number of pseudo elliptic factors of levels mp compared to the numbers of elliptic curves of prime level p , for p in the same range. The vast majority of the pseudo elliptic factors are in fact isogeny classes of modular elliptic curves. The high powers of 2 and 3 in the cofactor m imply that we are able to enumerate data for isogeny classes of elliptic curves of conductor exceeding typical bounds on the level in datasets such as the LMFDB [11]. In particular the levels attained for primes p up to 8000 give levels $288p$ or $256p$ exceeding 2×10^6 , which is beyond what has been systematically treated for composite levels.

6 Conclusion

The Weber modular curve $\mathcal{W}_{24}$, and its Fermat modular quotient $\mathcal{F}_8$, present highly symmetric models for modular curves of level 48 and 16, whose quotients $\mathcal{X}_{24}$ and $\mathcal{Y}_8$ give high-degree covers of the j -line. This high degree and the symmetry properties make them practical for computation of isogenies. In particular the small coefficient size and sparseness provide both elegant and efficient isogeny relations. While not all curves admit a Weber structure, we show that the supersingular points on $\mathcal{W}_{24}$ are all defined over $\mathbb{F}_{p^2}$. This makes the Weber curves interesting for the local study and navigation of supersingular isogeny graphs, with application to modern isogeny-based cryptographic protocols. On the other hand, the ℓ -isogeny graphs also play an important role in the theory of modular forms and Galois representations, coming from supersingular Hecke modules. In particular, sieving for the pseudo elliptic factors of such modules shows that one can compute data of elliptic modular curves of conductor beyond what can be systematically computed for arbitrary level, and can be used to understand the distribution of such curves admitting multiplicative reduction at a large prime and whose conductor is simultaneously divisible by a large power of 2 and 3.

References

- [1] Michael A. Bennett, Adela Gherga, and Andrew Rechnitzer. Computing elliptic curves over $\mathbb{Q}$. *Mathematics of Computation*, 88(317):1341–1390, 2019. doi: 10.1090/mcom/3370.
- [2] Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263):1755–1778, 2008. doi: 10.1090/S0025-5718-08-02066-8.
- [3] Leonardo Colò and David Kohel. Supersingular isogeny graphs and Hecke modules with level structure. Preprint, 2026. doi: 10.48550/arXiv.2604.00184.
- [4] Alex Cowan. Computing newforms using supersingular isogeny graphs. *Research in Number Theory*, 8:96, 2022. doi: 10.1007/s40993-022-00392-z.

- [5] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography*, volume 7071 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2011. doi: 10.1007/978-3-642-25405-5_2.
- [6] Andreas Enge and François Morain. Comparing invariants for class fields of imaginary quadratic fields. In *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 252–266. Springer, 2002. doi: 10.1007/3-540-45455-1_21.
- [7] Andreas Enge and François Morain. Generalised Weber functions. *Acta Arithmetica*, 164(4):309–341, 2014. doi: 10.4064/aa164-4-1.
- [8] Alice Gee. Class invariants by Shimura’s reciprocity law. *Journal de Théorie des Nombres de Bordeaux*, 11(1):45–72, 1999. doi: 10.5802/jtnb.238.
- [9] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkeley, 1996.
- [10] Reynald Lercier and François Morain. Algorithms for computing isogenies between elliptic curves. In *Computational Perspectives on Number Theory*, volume 7 of *Studies in Advanced Mathematics*, pages 77–96. American Mathematical Society, 1998. <https://bookstore.ams.org/AMSIP/7>.
- [11] The LMFDB Collaboration. The L-functions and modular forms database. <https://www.lmfdb.org/>.
- [12] Jean-François Mestre. La méthode des graphes, exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, pages 217–242. Nagoya University, 1986.
- [13] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Mathematics of Computation*, 44(170):483–494, 1985. doi: 10.1090/S0025-5718-1985-0777280-6.
- [14] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995. doi: 10.5802/jtnb.142.
- [15] Heinrich Weber. *Lehrbuch der Algebra: dritter Band*. Braunschweig, 1908.
- [16] Jacques Vélou. Isogénies entre courbes elliptiques. *Comptes rendus de l’académie des sciences de Paris*, 273:238–241, 1971.
- [17] Noriko Yui and Don Zagier. On the singular values of Weber modular functions. *Mathematics of Computation*, 66(220):1645–1662, 1997. doi: 10.1090/S0025-5718-97-00854-5.

A Isomorphisms between Weber and Fermat curves

The isomorphisms $\mathcal{W}_n \rightarrow \mathcal{F}_n$ and their inverses $\mathcal{F}_n \rightarrow \mathcal{W}_n$ are given as follows:

$$\begin{aligned} \mathcal{W}_8: \begin{cases} X_0^8 + X_1^8 + X_2^8 = 48X_3^8 \\ X_0X_1X_2 = \sqrt{8}X_3^3 \end{cases} &\longrightarrow \mathcal{F}_8: X^8 + Y^8 + Z^8 = 0 \\ (u_0 : u_1 : u_2 : u_3) &\longmapsto (\sqrt{2}u_2^5u_3 - u_0^3u_1^3 : u_1^6 - 2u_0^2u_2^2u_3^2 : \sqrt{2}u_0^5u_3 - u_1^3u_2^3) \\ (\sqrt{2}s_0^3 : \sqrt{2}s_1^3 : \sqrt{2}s_2^3 : s_0s_1s_2) &\longleftarrow (s_0 : s_1 : s_2) \end{aligned}$$

$$\begin{aligned} \mathcal{W}_4: \begin{cases} X_0^4 + X_1^4 + X_2^4 = 48X_3^4 \\ X_0X_1X_2 = 8X_3^3 \end{cases} &\longrightarrow \mathcal{F}_4: X^4 + Y^4 + Z^4 = 0 \\ (u_0 : u_1 : u_2 : u_3) &\longmapsto (u_0^3 - 2u_1u_2u_3 : u_1^3 - 2u_0u_2u_3 : u_2^3 - 2u_0u_1u_3) \\ (2s_0^3 : 2s_1^3 : 2s_2^3 : s_0s_1s_2) &\longleftarrow (s_0 : s_1 : s_2) \end{aligned}$$

$$\begin{aligned} \mathcal{W}_2: \begin{cases} X_0^2 + X_1^2 + X_2^2 = 48X_3^2 \\ X_0X_1X_2 = 64X_3^3 \end{cases} &\longrightarrow \mathcal{F}_2: X^2 + Y^2 + Z^2 = 0 \\ (u_0 : u_1 : u_2 : u_3) &\longmapsto \begin{cases} (-u_0^2 + 16u_3^2 : u_0u_1 - 4u_2u_3 : u_0u_2 - 4u_1u_3) \\ (u_0u_1 - 4u_2u_3 : -u_1^2 - 16u_3^2 : u_1u_2 - 4u_0u_3) \\ (u_0u_2 - 4u_1u_3 : u_1u_2 - 4u_0u_3 : -u_2^2 + 16u_3^2) \end{cases} \\ (4s_0^3 : 4s_1^3 : 4s_2^3 : s_0s_1s_2) &\longleftarrow (s_0 : s_1 : s_2) \end{aligned}$$

$$\begin{aligned} \mathcal{W}_1: \begin{cases} X_0 + X_1 + X_2 = 48X_3 \\ X_0X_1X_2 = 4096X_3^3 \end{cases} &\longrightarrow \mathcal{F}_1: X + Y + Z = 0 \\ (u_0 : u_1 : u_2 : u_3) &\longmapsto (u_0 - 16u_3 : u_1 - 16u_3 : u_2 - 16u_3) \\ (16s_0^3 : 16s_1^3 : 16s_2^3 : s_0s_1s_2) &\longleftarrow (s_0 : s_1 : s_2) \end{aligned}$$

B Elliptic curves over twisted Fermat curves

Let $\mathcal{F}_n^t: s^n + t^n = 1$ be the twist by ζ_{2n} of the Fermat curve $\mathcal{F}_n: s^n + t^n + 1 = 0$. The symmetry of the Fermat modular curve simplifies the study of automorphisms, but the 2-isogenies extend more naturally along a prescribed chain by breaking the S_3 -symmetry by this twist. We revisit the 2-isogeny chains of Section 4 in terms of this twisted Fermat curve, in relation to the following (-1) -twist of the family of elliptic curves

$$C_0^t / \mathcal{F}_n^t: y^2 = x(x+1)(x+t^n).$$

As above, we set $t = t_0$ and $t_{i-1} = t_i^2$ for $0 \leq i \leq 3$, such that, for a field K ,

$$K(\mathcal{Y}_1) = K(t_0) \subset K(\mathcal{Y}_2) = K(t_1) \subset K(\mathcal{Y}_4) = K(t_2) \subset K(\mathcal{Y}_8) = K(t_3)$$

is a sequence of quadratic extensions (relative to the previous functions t_i , these generators are scaled by $\zeta_{2n}^{2^i}$). Over $K(\mathcal{Y}_8)$, starting from C_0 , we can define a chain of 2-isogenies

$$C_0^t \xrightarrow{\phi_0} C_1^t \xrightarrow{\phi_1} C_2^t \xrightarrow{\phi_2} C_3^t$$

normalized such that the isogenies are defined by successive quotients by a 2-torsion point $(0, 0)$ gives cyclic extension over the base curve $\mathcal{Y}_8$. On C_k we give T_k , for k in $\{0, 1\}$, such that $2T_k = (0, 0)$ and $\phi_k(T_k) = (0, 0)$ on the codomain C_{k+1} .

First, we have the 2-isogeny

$$\begin{aligned} \phi_0: C_0^t: y^2 = x(x+1)(x+t_0) &\longrightarrow C_1^t: y^2 = x(x+4c_0)(x+e_0^2) \\ (x, y) &\longmapsto \left(\frac{(x-c_0)^2}{x}, \frac{x^2-c_0^2}{x^2}y \right) \end{aligned}$$

where $c_0 = t_1$ and $e_0 = t_1 + 1$. The point $T_0 = (c_0, c_0 e_0)$ satisfies $2T_0 = (0, 0) \in C_0^t[2]$ and $\phi_0(T_0) = (0, 0) \in C_1^t[2]$. Moreover, the image of $C_0^t[2]$ is generated by $\phi_0((1, 0)) = \phi_0((t_1^2, 0)) = ((t_1 - 1)^2, 0)$.

Second, consider

$$\begin{aligned} \phi_1: C_1^t: y^2 = x(x+4c_0)(x+e_0^2) &\longrightarrow C_2^t: y^2 = x(x+4c_1)(x+e_1^2) \\ (x, y) &\longmapsto \left(\frac{(x-c_1)^2}{x}, \frac{x^2-c_1^2}{x^2}y \right) \end{aligned}$$

where $c_1 = 2t_2 e_0$ and $e_1 = (t_2 + 1)^2$. The point $T_1 = (c_1, c_1 e_1^2)$ satisfies $2T_1 = (0, 0) \in C_1^t[2]$ and $\phi_1(T_1) = (0, 0) \in C_2^t[2]$.

Finally, the quotient by $(0, 0)$ in C_2^t gives the 2-isogeny

$$\begin{aligned} \phi_2: C_2^t: y^2 = x(x+4c_1)(x+e_1^2) &\longrightarrow C_3^t: y^2 = x(x+4c_2)(x+e_2^2) \\ (x, y) &\longmapsto \left(\frac{x^2+c_2^2}{x}, \frac{x^2-c_2^2}{x^2}y \right) \end{aligned}$$

where $c_2 = u_3 e_1^2$ and $e_2 = t_3 u_3 + e_1$ where $u_3^2 = 8e_0$.

After renormalization, these curves define the sequence of Legendre invariants

$$(\lambda_0, \lambda_1, \lambda_2, \lambda_3) = \left(t_0, \frac{e_0^2}{4c_0}, \frac{e_1^2}{4c_1}, \frac{e_2^2}{4c_2} \right)$$

satisfying the modular equation

$$\lambda_{i+1}(\lambda_{i+1} - 1) = \frac{(\lambda_i - 1)^2}{16\lambda_i}.$$