WEBER MODULAR CURVES AND MODULAR ISOGENIES

LEONARDO COLÒ AND DAVID KOHEL

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 describe a degree-72 covers 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 ℓ, 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. Gee [8] developed the theoretical foundations of class invariants for arbitrary modular functions, using Shimura 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 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 this curve and its quotients in the Galois cover from $X(48)$ to $X(1)$. In particular, a quotient to the 8-th 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 $\mathscr{X}_G/\mathbb{F}_p$ be a modular curve associated to level N open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, and ℓ prime to N. The modular ℓ-isogeny supersingular graph is determined by a set of supersingular moduli points on $\mathscr{X}_G$, with edge relations given by points in the correspondence,

$$\mathscr{X}_G(B_0(\ell)) \rightrightarrows \mathscr{X}_G.$$

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

$$\mathscr{X}_G(B_0(\ell^t)) \rightrightarrows \mathscr{X}_G,$$

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

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

$$\begin{aligned} x^3 - x^2y^2 + y^3 + 1488x^2y + 1488xy^2 - 162000x^2 - 162000y^2 + 40773375xy \\ + 8748000000x + 8748000000y - 157464000000000. \end{aligned}$$

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 $\Gamma(3)$ of index 12 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

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

of the family of modular polynomials with respect to the particular normalized modular function on $\mathscr{X}_G = \mathscr{X}(3)$. In particular, only the monomials $x^i y^j$ satisfying $i + \ell j \equiv \ell + 1 \bmod 3$ can occur. In the next section we derive similar results for the modular polynomials defined in terms of Weber functions.

Weber modular polynomials. The best known reduction in coefficient size as well as in sparsity of coefficients is obtained for the Weber function $\mathfrak{f}$ of level 48,

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

which generates a degree-72 cover of the j-line, given by

$$j = \frac{(\mathfrak{f}^{24} - 16)^3}{\mathfrak{f}^{24}}.$$

The modular polynomials with respect to $\mathfrak{f}$ are the integral polynomials $\Phi_\ell(x,y)$ such that

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

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 1. *The modular polynomial $\Phi_\ell(x,y)$ of prime level ℓ with respect to the Weber function satisfies the transformation:*

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

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

Asymptotically, modular polynomials have $(\ell+1)^2$ monomials, but due to the sparseness of the Weber polynomials the number of nonzero coefficients 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.

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

Going further, the modular polynomial $\Phi_{71}(x,y)$ has exactly $3 \cdot 71 = 213$ nonzero coefficients, ignoring the symmetry $\Phi_\ell(x,y) = \Phi_\ell(y,x)$, 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 $\Phi_2(x,y)$ and $\Phi_3(x,y)$ a particular form. We descend the 2-level structure by setting $t = -\mathfrak{f}^8$, so that

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

With respect to this function, we obtain the modular polynomial:

$$\Psi_2(x,y) = (x^2 - y)y + 16x$$

and the Weber modular polynomial $\Phi_2(x,y) = -\Psi_2(-x^8, -y^8)$ remains irreducible.[1] A similar descent of the 3-level to the function $r = \mathfrak{f}^3$, gives the modular polynomial

$$\Psi_3(x,y) = x^4 - x^3y^3 + 8xy + y^4,$$

such that $\Psi_3(r(\tau), r(3\tau)) = 0$, for which $\Phi_3(x,y) = \Psi_3(x^3, y^3)$ 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 1, the lift to the orbit can be chosen to be compatible with isogeny relations of other prime degrees.

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

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

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

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

[1] More correctly, the modular polynomial $\Psi_2(x,y)$ satisfies $\Psi_2(\mathfrak{f}_1^8(\tau), \mathfrak{f}_1^8(2\tau)) = 0$, where $\mathfrak{f}_1$ is the conjugate Weber function

$$\mathfrak{f}_1^8(\tau) = -\mathfrak{f}(\tau+3)^8 = \left(\frac{\eta(\frac{\tau}{2})}{\eta(\tau)}\right)^8$$

and hence $\Psi_2(\mathfrak{f}^8(\tau), \mathfrak{f}^8(2\tau-3)) = 0$. 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.

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

Setting $(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2) = (\mathfrak{f},\zeta_{16}\mathfrak{f}_1(\tau),\zeta_{16}^{-1}\mathfrak{f}_2(\tau))$ the triple $(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)$ satisfies the common relations

$$j = \frac{(\mathfrak{u}_0^{24}-16)^3}{\mathfrak{u}_0^{24}} = \frac{(\mathfrak{u}_1^{24}-16)^3}{\mathfrak{u}_1^{24}} = \frac{(\mathfrak{u}_2^{24}-16)^3}{\mathfrak{u}_2^{24}},$$

and one verifies that the three orbits $\{\zeta_{24}^j\mathfrak{u}_i \ : \ j \in \mathbb{Z}/24\mathbb{Z}\}$, 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 $\mathbb{Q}(\zeta_{48})[\![q^{1/48}]\!]$. The proposition which follows summarizes the action of the modular group on the normalized Weber functions.

Proposition 3. *The action of* $\mathrm{PSL}_2(\mathbb{Z}) = \langle S,T\rangle$ *on Weber triples* $(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)$ *maps through the quotient* $\mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})/\{\pm 1\}$*, and is defined on generators by:*

$$(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ S = (\mathfrak{u}_0,\zeta_8\mathfrak{u}_2,\zeta_8^{-1}\mathfrak{u}_1) \text{ and } (\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ T = (\zeta_{12}^{-1}\mathfrak{u}_1,\zeta_{24}\mathfrak{u}_0,\zeta_{24}\mathfrak{u}_2).$$

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

$$(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ U = (\mathfrak{u}_2,\mathfrak{u}_1,\mathfrak{u}_0), \quad (\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ V = (\mathfrak{u}_0,\mathfrak{u}_2,\mathfrak{u}_1), \quad (\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ W = (\mathfrak{u}_2,\mathfrak{u}_0,\mathfrak{u}_1).$$

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 $(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2) = (\mathfrak{f},\zeta_{48}^3\mathfrak{f}_1(\tau),\zeta_{48}^{-3}\mathfrak{f}_2(\tau))$ and the transformations (1), we obtain:

$$(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ S = (\mathfrak{f},\zeta_{48}^3\mathfrak{f}_2,\zeta_{48}^{-3}\mathfrak{f}_1) = (\mathfrak{u}_0,\zeta_{48}^6\mathfrak{u}_2,\zeta_{48}^{-6}\mathfrak{u}_1),$$

and

$$(\mathfrak{u}_0,\mathfrak{u}_1,\mathfrak{u}_2)\circ T = (\zeta_{48}^{-1}\mathfrak{f}_1,\zeta_{48}^2\mathfrak{f},\zeta_{48}^{-1}\mathfrak{f}_2) = (\zeta_{24}^{-2}\mathfrak{u}_1,\zeta_{24}\mathfrak{u}_0,\zeta_{24}\mathfrak{u}_2).$$

The permutation actions of U, V, and W follow from the actions of S and T. □

N.B. The right action on Weber triples gives a homomorphism $\iota : \mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$, 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 $\mathscr{W}_{24} \to X(1)$ 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 $S_3 \ltimes \boldsymbol{\mu}_{24}^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$, and there exists an exact sequence

$$1 \longrightarrow D \longrightarrow G \longrightarrow S_3 \longrightarrow 1.$$

where $D = G \cap \boldsymbol{\mu}_{24}^3$ 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 4. *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* $D \subset \boldsymbol{\mu}_{24}^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$ *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* $\{\mathfrak{u}_0^{24},\mathfrak{u}_1^{24},\mathfrak{u}_2^{24}\}$*, 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 $D[m] = D \cap \boldsymbol{\mu}_m^3 \subset \mathrm{GL}_3(\mathbb{Q}(\zeta_{24}))$.

3. WEBER CURVES

We are now able to use the conjugate Weber functions to define a curve with projective embedding given by the functions $\mathfrak{u}_0$, $\mathfrak{u}_1$, and $\mathfrak{u}_2$. Let m and n be integers such that $mn = 8$. The map determined by the normalized Weber functions $(\mathfrak{u}_0^m : \mathfrak{u}_1^m : \mathfrak{u}_2^m : 1)$ determines a *Weber modular curve* $\mathscr{W}_{3n}$ in $\mathbb{P}^3$

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

with quotient Weber curve $\mathscr{W}_n$ defined as the image of $(\mathfrak{u}_0^{3m} : \mathfrak{u}_1^{3m} : \mathfrak{u}_2^{3m} : 1)$ in $\mathbb{P}^3$:

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

These defining relations follow directly from the relations $\mathfrak{f}^8 = \mathfrak{f}_1^8 + \mathfrak{f}_2^8$ and $\mathfrak{f}\mathfrak{f}_1\mathfrak{f}_2 = \sqrt{2}$, and the curves are equipped with maps $\mathscr{W}_{mn} \to \mathscr{W}_n$ for each product mn dividing 24.

The curves $\mathscr{W}_n$ 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 $\pi_i : \mathscr{W}_n \to \mathscr{X}_n \cong \mathbb{P}^1$ 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 $\mathscr{X}_n \to X(1)$ given by

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

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

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

of j-invariant $j(u)$, discriminant $(u^n - 64)^3 u^n$, and 2-torsion point $(0,0)$. The quotient curve is

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

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

By eliminating the function u_2, it is clear that the cover $\mathscr{W}_n \to \mathscr{X}_n$ is of degree $2n$, and the expression for j shows that $\mathscr{X}_n \to X(1)$ is of degree $3n$. This gives a degree $6n^2$ cover $\mathscr{W}_n \to X(1)$. 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 $\mathscr{W}_n$ and the Fermat curve $\mathscr{F}_n : X^n + Y^n + Z^n = 0$. In particular the cover $\mathscr{W}_{3n} \to \mathscr{W}_n$ factors through the quotient

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

Indeed this is the quotient by the group of automorphisms

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

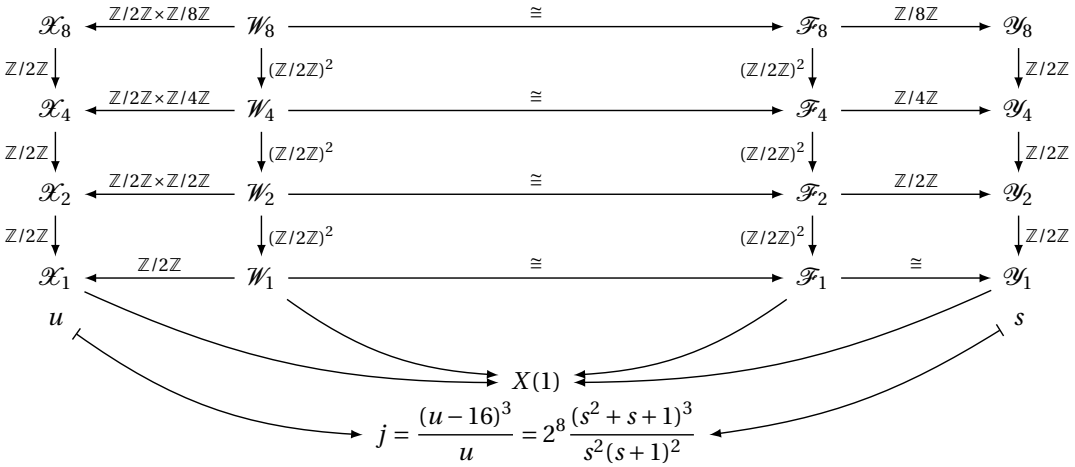
which stabilizes the fibers of the quotient $\mathscr{W}_{3n} \to \mathscr{W}_n$, which must factor through $\mathscr{F}_n$. In view of the defining equations for $\mathscr{W}_{3n}$, we infer that the induced map $\mathscr{F}_n \to \mathscr{W}_n$ is given by:

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

In what follows, we prove that $\mathscr{W}_{3n} \to \mathscr{W}_n$ has degree 3, hence $\mathscr{F}_n \to \mathscr{W}_n$ is an isomorphism. As with the Weber curves, the Fermat curves come equipped with a triple of projections $\pi_i : \mathscr{F}_n \to \mathscr{Y}_n \cong \mathbb{P}^1$:

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

parametrized by the modular functions $(\mathfrak{u}_1/\mathfrak{u}_2)^m$, $(\mathfrak{u}_0/\mathfrak{u}_2)^m$ and $(\mathfrak{u}_0/\mathfrak{u}_1)^m$, respectively. This gives the diagram of morphisms between Weber and Fermat curves and their quotients:



The isomorphisms $\mathscr{W}_n \to \mathscr{F}_n$ appear in the appendix, for all divisors n of 8. In particular, for $n = 1$, the isomorphism is given by the following map:

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

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

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

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

$$\mathscr{C}_0/\mathscr{Y}_1 : y^2 = x(x-1)(x+t) = x(x-1)(x-(s+1)) \text{ and } \mathscr{C}_1/\mathscr{Y}_1 : y^2 = x((x+s)^2 + 4x). \tag{7}$$

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.

Modular group. To each factorization $mn = 24$, the Weber curve $\mathscr{W}_n$ in $\mathbb{P}^3$, defined by the triple of Weber functions $(\mathfrak{u}_0^m, \mathfrak{u}_1^m, \mathfrak{u}_2^m)$, 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.

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

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 $\mathscr{W}_n \to X(1)$.

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

Let $\boldsymbol{\mu}_m = \langle \zeta_m \rangle$ be the group of m-th roots of unity. We identify $\boldsymbol{\mu}_m^3$ with the subgroup (scheme) of $\mathbb{G}_m^3$, acting on affine space $\mathbb{A}^3$. We define the antidiagonal group,

$$\nabla(\boldsymbol{\mu}_m^2) = \left\{ \left(\zeta_m^i, \zeta_m^j, \zeta_m^{-i-j}\right) \in \boldsymbol{\mu}_m^3 \mid i, j \in \mathbb{Z}/m\mathbb{Z} \right\},$$

and the diagonal group $\Delta(\boldsymbol{\mu}_m) = \{(\zeta_m^i, \zeta_m^i, \zeta_m^i) \in \boldsymbol{\mu}_m^3 \mid i \in \mathbb{Z}/m\mathbb{Z}\}$. If $m \equiv 0 \bmod 3$, then $\Delta(\boldsymbol{\mu}_3) \subset \nabla(\boldsymbol{\mu}_m^2)$, otherwise the groups $\Delta(\boldsymbol{\mu}_m)$ and $\nabla(\boldsymbol{\mu}_m)$ are independent.

Proposition 5. *For each divisor mn of 24, the morphism $\mathscr{W}_{mn} \to \mathscr{W}_n$ is the quotient by a subgroup of automorphisms in $\boldsymbol{\mu}_m^3$, isomorphic to Γ_n/Γ_{mn}.*

- *If $m = 3$, then the automorphism group of the cover is $\Delta(\boldsymbol{\mu}_3)$.*
- *If m divides 8, then the automorphism group of the cover is $\nabla(\boldsymbol{\mu}_m^2)$.*

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

Proof. The quotients $\mathscr{W}_{mn} \to \mathscr{W}_n$ are induced by the restriction, to the affine Weber curves, of the quotients $\mathbb{A}^3 \to \mathbb{A}^3$ by $\boldsymbol{\mu}_m^3$, 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 $\mathscr{W}_{mn} \to \mathscr{W}_n$ is $(\mathrm{PSL}_2(\mathbb{Z})/\Gamma_n)\,/\,(\mathrm{PSL}_2(\mathbb{Z})/\Gamma_{mn}) \cong \Gamma_n/\Gamma_{mn}$.

We first consider $m = 3$: the affine Weber curve $\mathscr{W}_{3n}$ ($X_3 \neq 0$) 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 $\boldsymbol{\mu}_3^3$ stabilizing the curve is the intersection of the group $\Delta(\boldsymbol{\mu}_3)$, stabilizing $x^n + y^n + z^n$, and $\nabla(\boldsymbol{\mu}_3)$, fixing xyz. Since $\Delta(\boldsymbol{\mu}_3) \subset \nabla(\boldsymbol{\mu}_3)$, the automorphism group of the cover is $\Delta(\boldsymbol{\mu}_3)$, and $\mathscr{W}_{3n} \to \mathscr{W}_n$ is of degree 3.

Now we consider 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 $\boldsymbol{\mu}_m^3$, hence the automorphism group of the cover is the subgroup $\nabla(\boldsymbol{\mu}_m)$ fixing the form xyz. The degrees of the morphisms $\mathscr{W}_{mn} \to \mathscr{W}_n$ follows since $|\Delta(\boldsymbol{\mu}_3)| = 3$ and $|\nabla(\boldsymbol{\mu}_m)| = m^2$. □

Proposition 6. *The Weber kernel group Γ_1 equals $\Gamma(2)$ and $\mathscr{W}_1 \cong X(2)$.*

Proof. The Weber curve $\mathscr{W}_2$ is parametrized by the three normalized η-quotients:

$$\mathfrak{u}_0^{24} = -\left(\frac{\eta((\tau+1)/2)}{\eta(\tau)}\right)^{24}, \quad \mathfrak{u}_1^{24} = -\left(\frac{\eta(\tau/2)}{\eta(\tau)}\right)^{24}, \quad \mathfrak{u}_2^{24} = -2^{12}\left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{24},$$

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

Proposition 7. *The Weber kernel group Γ_3 equals $\Gamma(2) \cap \Gamma_{ns}^+(3)$, and for each n dividing 8*

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

Proof. By Proposition 6 we have $\Gamma_1 = \Gamma(2)$ and by Proposition 5, we have $\Gamma_3/\Gamma_1 \cong \Delta(\boldsymbol{\mu}_3)$ 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 $\Gamma_{ns}^+(3)$ of $\mathrm{PSL}_2(\mathbb{Z})$. □

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

Proposition 8. *The Weber kernel group Γ_2 equals $\Gamma(4)$ and $\mathscr{W}_2 = X(4)$.*

Proof. By Proposition 5, the Weber kernel group of $\mathscr{W}_2 \to \mathscr{W}_1$ satisfies $\Gamma_2/\Gamma_1 \cong \Delta(\boldsymbol{\mu}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$, where $\Gamma_1 = \Gamma(2)$ by Proposition 6. From the transformation of the η-quotients defining the Weber functions, it is clear that the triple $(\mathfrak{u}_0^{12}, \mathfrak{u}_1^{12}, \mathfrak{u}_2^{12})$ are invariant under $\Gamma(4)$. Since $\Gamma(4)/\Gamma(2) \cong (\mathbb{Z}/2\mathbb{Z})^2$, it follows that $\Gamma_2 = \Gamma(4)$. □

Proposition 9. *The Weber kernel group Γ_4 equals $\Gamma_s(8)$ and $\mathscr{W}_4 = X_s(8)$.*

Proof. The triple $(\mathfrak{u}_0^6, \mathfrak{u}_1^6, \mathfrak{u}_2^6)$ 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, isomorphic to $(\mathbb{Z}/8\mathbb{Z})^*$, hence equals $\Gamma_s(8)$. □

It remains to characterize the group Γ_8 under which the triple of functions $(\mathfrak{u}_0^3, \mathfrak{u}_1^3, \mathfrak{u}_2^3)$ is invariant. This group is not the split Cartan subgroup $\Gamma_s(16)$, but we can show that

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

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

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

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

Proposition 10. *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 in the center of $\mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})$:

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

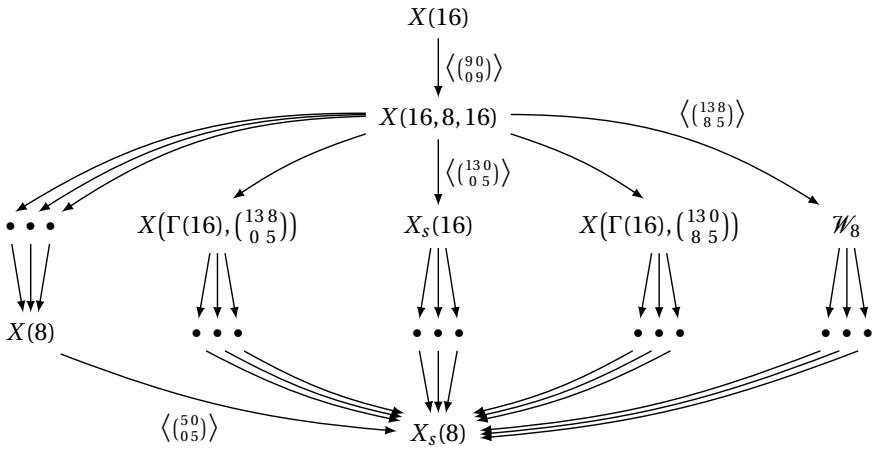
hence contains the subgroup

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

Given that $\Gamma_s(8)/\Gamma(16)$ is an abelian group:

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

so that $\Gamma_s(8)/\Gamma(16,8,16) \cong C_2 \times V_4 = C_2^3$; we have the following diagram of 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 will show that the supersingular points split completely over $\mathbb{F}_{p^2}$ on the quotients of $X(16,8,16)$ not covering $X(8)$, for every odd prime p.

Supersingular fields of definition.

Theorem 11. *For any positive integer* N*, the supersingular invariants on the modular curve* $X_0(N)$ *are defined over* $\mathbb{F}_{p^2}$*, and if* $p \equiv \pm 1 \bmod N$*, then the supersingular invariants also split over* $\mathbb{F}_{p^2}$ *on* $X_1(N)$.

Proof. 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 $\mathcal{O}/N\mathcal{O} \cong \mathbb{M}_2(\mathbb{Z}/N\mathbb{Z})$ on the $E[N]$ is defined over $\mathbb{F}_{p^2}$, it follows that the Galois action on $E[N]$, which commutes with $\mathcal{O}/N\mathcal{O}$, 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 $E[N]$. Consequently, the lines are Galois stable and every cyclic N-isogeny is defined over $\mathbb{F}_{p^2}$. In view of the action of Frobenius, if $p \equiv \pm 1 \bmod N$, the Galois action on the N-torsion of E or its twist is trivial, so the supersingular moduli are defined in $\mathbb{F}_{p^2}$. □

Remark. Equivalently, for $X_0(N)$ we can state that every supersingular j-invariant j_0 splits completely under the map $X_0(N) \to X(1)$, 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 $X_s(N)$, defined by the congruence subgroup

$$\Gamma_s(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv c \equiv 0 \bmod N \right\},$$

parametrizing elliptic curves with a disjoint pair of cyclic N-isogenies, also splits the supersingular moduli.

Corollary 12. *For any positive integer N, then the supersingular invariants on the split Cartan modular curve $X_s(N)$ are defined over $\mathbb{F}_{p^2}$. In particular if $p \equiv \pm 1 \bmod N$, 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 $p \equiv \pm 1 \bmod N$, the points of each kernel are fixed, hence a basis is defined over $\mathbb{F}_{p^2}$ (up to twist). □

Remark. 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 $\mathscr{W}_{24}$. To show the splitting of supersingular points on $\mathscr{W}_{24}$ it suffices to prove it for $\mathscr{W}_3$ and $\mathscr{W}_8$. However, $X(6)$ covers $\mathscr{W}_3$, so the supersingular moduli on $\mathscr{W}_3$ split over $\mathbb{F}_{p^2}$ by the previous theorem. To prove that they split on $\mathscr{W}_8$ it is necessary to consider the factorization

$$\begin{array}{ccc} X(16,8,16) & \longrightarrow & X(8) \\ \left\langle \left(\begin{smallmatrix} 13 & 8 \\ 8 & 5 \end{smallmatrix}\right) \right\rangle \downarrow & & \downarrow \left\langle \left(\begin{smallmatrix} 5 & 0 \\ 0 & 5 \end{smallmatrix}\right) \right\rangle \\ \mathscr{W}_8 & \longrightarrow & X_s(8), \end{array}$$

where $X(16,8,16)$ is the quotient of $X(16)$ by the diagonal matrix group $\langle \pm 9 I_2 \rangle \subset \mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})/\{\pm 1\}$.

The supersingular points split in $X_s(8)$ by the previous theorem. On the other hand, for the classes $p \bmod 8$ in the coset $\{\pm 5\} \subset (\mathbb{Z}/8\mathbb{Z})^*/\{\pm 1\}$ form an obstruction to lifting supersingular points to $X(8)$ over $\mathbb{F}_{p^2}$. Clearly, since $\langle 9 I_2 \rangle \subset \Gamma(16,8,16)/\Gamma(16)$, for the primes p such that $p \bmod 16$ lie in the kernel

$$\langle -1, 9 \rangle = \{\pm 1, \pm 9\} \subset (\mathbb{Z}/16)^*/\{\pm 1\} \longrightarrow (\mathbb{Z}/8)^*/\{\pm 1\},$$

the supersingular invariants in $X(16,8,16)$ split over $\mathbb{F}_{p^2}$. It remains to show that the obstruction vanishes also on the coset $\{\pm 3, \pm 5\}$. However, this follows since the subgroup of $\Gamma_8/\Gamma(16)$ surjects on the diagonal subgroup of $\Gamma_s(8)/\Gamma(8)$:

$$\left\langle \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix} \right\rangle \longrightarrow \left\langle \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \right\rangle$$

under $\mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})$, corresponding to the fact that $\mathscr{W}_8$ does not factor through $X(8)$. This establishes the following theorem.

Theorem 13. *The supersingular Weber invariants on $\mathscr{W}_{24}$ are defined over $\mathbb{F}_{p^2}$.*

Remark. A point (u_0, u_1, u_2) on $\mathscr{W}_{24}$ 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 $\{\zeta_{24}^i u_j \ : \ 0 \le i < 24, 0 \le j < 3\}$. The property that j_0 splits completely under $\mathscr{W}_{24} \to X(1)$ over $\mathbb{F}_{p^2}$ is equivalent to this polynomial splitting completely over $\mathbb{F}_{p^2}$.

Elliptic curves over Weber and Fermat curves

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

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

which implies a morphism $X(2) \cong \mathscr{Y}_1 \longrightarrow \mathscr{X}_1 \cong X_0(2)$.

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

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

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

$$\mathscr{C}_0/\mathscr{Y}_n : y^2 = x(x-1)(x+t^n) = x(x-1)(x-s^n-1),$$

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

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

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 $K(\mathscr{F}_8) \cong K(\mathscr{W}_8)$ requires a square root of 2 in K, and moreover the chain of isogenies which follow require an 8-th root of unity ζ_8, for which we set $i = \zeta_8^2$, so we assume K contains a homomorphic image of $\mathbb{Z}[\zeta_8]$.

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 $\mathscr{C}_0$. We describe a 2-isogeny chain over $K(\mathscr{Y}_8)$, starting from $\mathscr{C}_0$, of the form

$$\mathscr{C}_0 \xrightarrow{\phi_0} \mathscr{C}_1 \xrightarrow{\phi_1} \mathscr{C}_2 \xrightarrow{\phi_2} \mathscr{C}_3.$$

The base extension to $K(\mathscr{F}_8)$ gives rise to an explicit action on the chains by the automorphism group of $K(\mathscr{F}_8)/K(X(1))$, which, by Proposition 5, is isomorphic to $S_3 \ltimes \nabla(\boldsymbol{\mu}_8^2)$.

We normalize the curves $\mathscr{C}_i$ and isogenies ϕ_i of the chain such that the isogenies are defined successive quotients by a 2-torsion point $(0,0)$. On the curve $\mathscr{C}_k$ we give, for each k in $\{0,1\}$, a point $T_k \in \mathscr{C}_k[4]$ such that $2T_k = (0,0)$ and $\phi_k(T_k) = (0,0)$ on the codomain $\mathscr{C}_{k+1}$. The quotient by $(0,0)$ in $\mathscr{C}_0[2]$ gives the 2-isogeny:

$$\begin{aligned} \phi_0 : \mathscr{C}_0 : y^2 = x(x-1)(x+t_0) &\longrightarrow \mathscr{C}_1 : y^2 = x(x+4c_0)(x+e_0^2) \\ (x,y) &\longmapsto \left(\frac{(x-c_0)^2}{x}, \frac{x^2-c_0^2}{x^2}y\right) \end{aligned}$$

where $c_0 = it_1$ and $e_0 = t_1 + i$. The point $T_0 = (c_0, c_0e_0) \in \mathscr{C}_0[4]$ satisfies $2T_0 = (0,0) \in \mathscr{C}_0[2]$ and $\phi_0(T_0) = (0,0) \in \mathscr{C}_1[2]$. The quotient by $(0,0)$ in $\mathscr{C}_1[2]$ gives the next step in the 2-isogeny chain:

$$\begin{aligned} \phi_1 : \mathscr{C}_1 : y^2 = x(x+4c_0)(x+e_0^2) &\longrightarrow \mathscr{C}_2 : y^2 = x(x+4c_1))(x+e_1^2) \\ (x,y) &\longmapsto \left(\frac{(x-c_1)^2}{x}, \frac{x^2-c_1^2}{x^2}y\right) \end{aligned}$$

where $c_1 = 2\zeta_8 t_2(t_1+i)$ and $e_1 = (t_2+\zeta_8)^2$. The point $T_1 = (c_1, c_1e_1)$ satisfies $2T_1 = (0,0) \in \mathscr{C}_1[2]$ and $\phi_1(T_1) = (0,0) \in \mathscr{C}_2[2]$. Finally, the quotient by $(0,0)$ in $\mathscr{C}_2[2]$ gives the 2-isogeny:

$$\begin{aligned} \phi_2 : \mathscr{C}_2 : y^2 = x(x+4c_1)(x+e_1^2) &\longrightarrow \mathscr{C}_3 : y^2 = (x^2+4c_2)(x+c_3) \\ (x,y) &\longmapsto \left(\frac{x^2-c_2}{x}, \frac{x^2+c_2}{x^2}y\right) \end{aligned}$$

where $c_2 = -4c_1e_1^2$ 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 $\mathscr{C}_0$.

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 $\mathscr{W}_{3n}$, the nonsplit Cartan structure $\Gamma^+_{ns}(3)$ 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 $(u_0, u_1, \ldots, u_r)$ 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 $\mathscr{X}_{24}$ (or when $\ell = 3$, of one of the quotients, $\mathscr{X}_8$ or $\mathscr{Y}_8$ of $\mathscr{W}_8 \cong \mathscr{F}_8$).

4. 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 $N = mp$. 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 level structure is developed in [3]. For prime level, Bennett, Gherga, and Rechnitzer [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 the following table, we give the numbers of isogeny classes of pseudo elliptic factors coming from the Weber curves $\mathscr{X}_n$, where n divides 12, or Fermat curves $\mathscr{Y}_n$, 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 1. Counts of Weber and Fermat pseudo elliptic factors

$B-1000 < p < B$		1000	2000	3000	4000	5000	6000	7000	8000	$N = mp$
# Weber :	$\mathscr{X}_{12}$	160	104	80	132	92	60	84	68	$288 \cdot p$
# orbits :		40	26	20	22	23	15	21	17	
# Weber :	$\mathscr{X}_6$	212	132	98	78	106	92	80	76	$72 \cdot p$
# orbits :		106	66	49	39	53	46	40	38	
# Weber :	$\mathscr{X}_3$	450	288	222	212	262	208	206	194	$18 \cdot p$
# orbits :		225	144	111	106	131	104	103	97	
# Weber :	$\mathscr{X}_4$	142	110	80	66	48	60	56	56	$32 \cdot p$
# orbits :		71	55	40	33	24	30	28	28	
# Weber :	$\mathscr{X}_2$	174	99	91	79	94	84	90	63	$8 \cdot p$
# Weber :	$\mathscr{X}_1$	274	256	184	194	175	186	155	126	$2 \cdot p$
# Fermat :	$\mathscr{Y}_8$	100	60	32	32	72	24	24	24	$256 \cdot p$
# orbits :		25	15	8	8	18	6	6	6	
# Fermat :	$\mathscr{Y}_4$	974	538	538	544	502	498	396	336	$64 \cdot p$
# orbits :		487	269	269	272	251	249	298	168	
# Fermat :	$\mathscr{Y}_2$	545	364	309	287	281	279	248	193	$16 \cdot p$
# Fermat :	$\mathscr{Y}_1$	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 1 collects the counts of pseudo elliptic factors associated to the supersingular Hecke modules on the Weber curves $\mathscr{X}_n$, for n dividing 12 and the Fermat curves $\mathscr{F}_n$, 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 $\mathscr{W}_{24}$ admits a level 48, 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 $\mathscr{X}_{24}$ and $\mathscr{X}_8$, 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 $\mathscr{X}_{12}$, of level $288p$, aligns roughly with the numbers of isogeny classes of elliptic curves of conductor p, while the numbers of orbits for $\mathscr{Y}_8$, of level $256p$, appears 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 gives levels $288p$ or $256p$ exceeding 2×10^6, which is beyond what has been systematically treated for composite levels.

5. Conclusion

The Weber modular curves $\mathscr{W}_{24}$, and their Fermat modular quotients $\mathscr{F}_8$, present highly symmetric models for modular curves of level 48 and 16, whose quotients $\mathscr{X}_{24}$ and $\mathscr{Y}_8$ 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 $\mathscr{W}_{24}$ 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 with admitting multiplicative reduction at a large prime and whose conductor is simultaneously divisible by a large power of 2 and 3.

References

[1] M. A. Bennett, A. Gherga, and A. Rechnitzer. Computing elliptic curves over $\mathbb{Q}$. *Mathematics of Computation*, **88** (317), pp. 1341–1390, 2019.

[2] A. Bostan, F. Morain, B. Salvy and É. Schost. Fast algorithms for computing isogenies between elliptic curves. In *Mathematics of Computation*, vol. **77**, no. 263, pp. 1755–1778, 2008.

[3] L. Colò and D. Kohel. Supersingular isogeny graphs and Hecke modular with level structure. preprint, 2026.

[4] A. Cowan, Computing newforms using supersingular isogeny graphs. *Research in Number Theory* **8**, 96, 2022.

[5] L. De Feo and D. Jao. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography (PQCrypto 2011), Lecture Notes in Computer Science*, vol. **7071**, pp. 19–34, 2011.

[6] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratic fields. In *Algorithmic Number Theory (ANTS 2002), Lecture Notes in Computer Science*, vol. **2369**, Springer, 2002.

[7] A. Enge and F. Morain. Generalised Weber functions. In *Acta Arithmetica*, vol. **164**, pp. 309–341, 2009.

[8] A. Gee. Class invariants by Shimura's reciprocity law. In *Journal de Théorie des Nombres de Bordeaux*, vol. **11**, no. 1, pp. 45–72, 1999.

[9] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Ph.D. Thesis, U. C. Berkeley, 1996.

[10] R. Lercier and F. Morain. Algorithms for computing isogenies between elliptic curves. In *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin, AMS/IP Studies in Advanced Mathematics*, vol. **7**, pp. 77–96, 1998.

[11] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2026.

[12] J.-F. Mestre. Sur la méthode des graphes, exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, Nagoya University, pp. 217–242, 1986.

[13] R. Schoof. Elliptic curves over finite fields and computing square roots mod p. In *Mathematics of Computation*, vol. **44**, no. 170, pp. 483–494, 1985.

[14] R. Schoof. Counting points on elliptic curves over finite fields. In *Journal de Théorie des Nombres de Bordeaux*, vol. **7**, no. 1, pp. 219–254, 1995.

[15] H. Weber. *Lehrbuch der Algebra*. Band III, Braunschweig, 1908.

[16] J. Vélu. Isogénies entre courbes elliptiques. In *Comptes-rendus de l'Académie des Sciences*, vol. **273**, pp. 238–241, 1971. `https://gallica.bnf.fr`

[17] N. Yui and D. Zagier. On the singular values of Weber modular functions. In *Mathematics of Computation*, vol. **66**, no. 220, pp. 1645–1662, 1997.

APPENDIX

ISOMORPHISMS BETWEEN WEBER AND FERMAT CURVES

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

$$\mathscr{W}_8 : \begin{cases} X_0^8 + X_1^8 + X_2^8 = 48X_3^8, \\ X_0X_1X_2 = \sqrt{8}X_3^3 \end{cases} \longrightarrow \mathscr{F}_8 : X^8 + Y^8 + Z^8 = 0$$

$$(u_0 : u_1 : u_2 : u_3) \longmapsto (\sqrt{2}u_2^5u_3 - u_0^3u_1^3 : u_1^6 - 2u_0^2u_2^2u_3^2 : \sqrt{2}u_0^5u_3 - u_1^3u_2^3)$$

$$(\sqrt{2}s_0^3 : \sqrt{2}s_1^3 : \sqrt{2}s_2^3 : s_0s_1s_2) \longmapsto (s_0 : s_1 : s_2)$$

$$\mathscr{W}_4 : \begin{cases} X_0^4 + X_1^4 + X_2^4 = 48X_3^4, \\ X_0X_1X_2 = 8X_3^3 \end{cases} \longrightarrow \mathscr{F}_4 : X^4 + Y^4 + Z^4 = 0$$

$$(u_0 : u_1 : u_2 : u_3) \longmapsto (u_0^3 - 2u_1u_2u_3 : u_1^3 - 2u_0u_2u_3 : u_2^3 - 2u_0u_1u_3)$$

$$(2s_0^3 : 2s_1^3 : 2s_2^3 : s_0s_1s_2) \longmapsto (s_0 : s_1 : s_2)$$

$$\mathscr{W}_2 : \begin{cases} X_0^2 + X_1^2 + X_2^2 = 48X_3^2, \\ X_0X_1X_2 = 64X_3^3 \end{cases} \longrightarrow \mathscr{F}_2 : X^2 + Y^2 + Z^2 = 0$$

$$(u_0 : u_1 : u_2 : u_3) \longmapsto \begin{cases} (-u_0^2 + 16u_3^2 : u_0u_1 - 4u_2u_3 : u_0u_2 - 4u_2u_3) \\ (u_0u_1 - 4u_2u_3 : -u_1^2 - 16u_3^2 : u_1u_2 - 4u_0u_3) \\ (u_0u_2 - 4u_1u_3 : u_1u_2 - 4u_0u_3 : -u_2^2 + 16u_3^2) \end{cases}$$

$$(4s_0^3 : 4s_1^3 : 4s_2^3 : s_0s_1s_2) \longmapsto (s_0 : s_1 : s_2)$$

$$\mathscr{W}_1 : \begin{cases} X_0 + X_1 + X_2 = 48X_3^2, \\ X_0X_1X_2 = 4096X_3^3 \end{cases} \longrightarrow \mathscr{F}_1 : X + Y + Z = 0$$

$$(u_0 : u_1 : u_2 : u_3) \longmapsto (u_0 - 16u_3 : u_1 - 16u_3 : u_2 - 16u_3)$$

$$(16s_0^3 : 16s_1^3 : 16s_2^3 : s_0s_1s_2) \longmapsto (s_0 : s_1 : s_2)$$

ELLIPTIC CURVES OVER TWISTED FERMAT CURVES

Let $\mathscr{F}_n^t : s^n + t^n = 1$ be the twist by ζ_{2n} of the Fermat curve $\mathscr{F}_n : s^n + t^n + 1 = 0$. The symmetry of the Fermat modular curve simplifies the study of automophisms, 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 3 in terms of this twisted Fermat curve, in relation to the following -1-twist of the family of elliptic curves:

$$\mathscr{C}_0^t/\mathscr{F}_n^t : y^2 = x(x+1)(x+t^n).$$

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

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

is a sequence of quadratic extensions (relative to the previous functions t_i, these generators are scaled by $\zeta_{2n}^{2^i}$). Over $K(\mathscr{Y}_8)$ we can define a chain of 2-isogenies starting from $\mathscr{C}_0$,

$$\mathscr{C}_0^t \xrightarrow{\phi_0} \mathscr{C}_1^t \xrightarrow{\phi_1} \mathscr{C}_2^t \xrightarrow{\phi_2} \mathscr{C}_3^t$$

normalized such that the isogenies are defined successive quotients by a 2-torsion point $(0,0)$ gives cyclic extension over the base curve $\mathscr{Y}_8$. On $\mathscr{C}_k$ 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 $\mathscr{C}_{k+1}$.

$$\begin{aligned} \phi_0 : \mathscr{C}_0^t : y^2 = x(x+1)(x+t_0) &\longrightarrow \mathscr{C}_1^t : y^2 = x(x+4c_0)(x+e_0^2) \\ (x,y) &\longmapsto \left(\frac{(x-c_0)^2}{x}, \frac{x^2-c_0^2}{x^2}y\right) \end{aligned}$$

where $c_0 = t_1$ and $e_0 = t_1 + 1$. The point $T_0 = (c_0, c_0 e_0)$ satisfies $2T_0 = (0,0) \in \mathscr{C}_0^t[2]$ and $\phi_0(T_0) = (0,0) \in \mathscr{C}_1^t[2]$. Moreover, the image of $\mathscr{C}_0^t[2]$ is generated by $\phi_0\big((1,0)\big) = \phi_0\big((t_1^2,0)\big) = \big((t_1-1)^2,0\big)$.

$$\begin{aligned} \phi_1 : \mathscr{C}_1^t : y^2 = x(x+4c_0)(x+e_0^2) &\longrightarrow \mathscr{C}_2^t : y^2 = x(x+4c_1)(x+e_1^2) \\ (x,y) &\longmapsto \left(\frac{(x-c_1)^2}{x}, \frac{x^2-c_1^2}{x^2}y\right) \end{aligned}$$

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 $2T_1 = (0,0) \in \mathscr{C}_1^t[2]$ and $\phi_1(T_1) = (0,0) \in \mathscr{C}_2^t[2]$. Finally, the quotient by $(0,0)$ in $\mathscr{C}_2^t$ gives the 2-isogeny:

$$\begin{aligned} \phi_2 : \mathscr{C}_2^t : y^2 = x(x+4c_1)(x+e_1^2) &\longrightarrow \mathscr{C}_3^t : y^2 = x(x+4c_2)(x+e_2^2) \\ (x,y) &\longmapsto \left(\frac{x^2+c_2^2}{x}, \frac{x^2-c_2^2}{x^2}y\right) \end{aligned}$$

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:

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

satisfying the modular equation

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