Genus 3 curves whose Jacobians have endomorphisms by $\mathbb{Q}(\zeta_7 + \bar{\zeta}_7)$

J. William Hoffman

Department of Mathematics
Louisiana State University
Baton Rouge, Louisiana 70803, USA

Zhibin Liang

School of Mathematical Sciences
Capital Normal University
Beijing, China, 100048
and Beijing International Center for Mathematical Research,
Peking University

Yukiko Sakai

Department of Mathematics, College of Liberal Arts and Sciences, Kitasato University, Kanagawa 252-0373, Japan

Haohao Wang

Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701, USA

Abstract

In this work we consider constructions of genus three curves $X$ such that $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q}$ contains the totally real cubic number field $\mathbb{Q}(\zeta_7 + \bar{\zeta}_7)$. We construct explicit two-dimensional families defined over $\mathbb{Q}(s,t)$ whose generic member is a nonhyperelliptic genus 3 curve with this property. The case when $X$ is hyperelliptic was studied in (7). We calculate the zeta function of one of these curves. Conjecturally this zeta function is described by a modular form.

1. Introduction

Let $\mathcal{M}_g$ be the (coarse) moduli space of projective smooth curves of genus $g$. Recently there has been a lot of progress in understanding the loci in $\mathcal{M}_g$ defined by those curves $X$ such that the Jacobian variety $\text{Jac}(X)$ has special endomorphisms, when $g = 2$ (see, e.g., (3), (6), (14), (16)). The situation for $g \geq 3$ is much less studied. Recall that for any polarized abelian variety $A$, $\text{End}(A) \otimes \mathbb{Q}$ is a semisimple algebra of finite dimension with involution, and the
explicit types possible can be listed (see (20, §X) and (12)). For a generic curve \( X \), we have \( \text{End}(\text{Jac}(X)) \otimes \mathbb{Q} = \mathbb{Q} \) so special endomorphisms means: \( \text{End}(\text{Jac}(X)) \otimes \mathbb{Q} \) contains, but is larger than \( \mathbb{Q} \). Throughout this paper we work with varieties over fields of characteristic 0.

Let \( \mathcal{A}_3 \) be the moduli space of principally polarized abelian varieties of dimension 3. The map \( X \mapsto \text{Jac}(X) : \mathcal{M}_3 \to \mathcal{A}_3 \) is a birational equivalence of 6-dimensional varieties. However not every genus 3 curve is hyperelliptic. The general genus 3 curve is isomorphic via the canonical embedding to a smooth projective plane quartic. The locus of hyperelliptic curves \( \mathcal{M}_3^{\text{hyper}} \subset \mathcal{M}_3 \) is a 5-dimensional irreducible subvariety. A hyperelliptic genus 3 curve can be given by an equation \( y^2 = f(x) \) where the polynomial \( f(x) \) is of degree 7 or 8 and has distinct roots. In (7) we showed via the method of Humbert and Mestre, that given a Poncelet 7-gon, there is a genus 3 hyperelliptic curve \( X \) canonically constructed from it, which had the property that \( \text{End}(\text{Jac}(X)) \otimes \mathbb{Q} \supset \mathbb{Q}(\zeta_7 + \bar{\zeta}_7) := \mathbb{Q}(\zeta_7^+) \), where \( \zeta_7 \) is a primitive 7th root of unity.

In this paper we give a construction of nonhyperelliptic curves of genus 3 with this property via a generalization of the method of Humbert and Mestre. As Mestre pointed out to us on visit to Beijing (summer 2012) our method can be viewed as a special case of results of Ellenberg (4). Actually Ellenberg defines coverings of Riemann surfaces which define algebraic curves with special endomorphism algebras of their Jacobians, but his method cannot provide explicit equations for those curves because of the nonalgebraic nature of Riemann’s Existence Theorem.

We construct explicit 2-dimensional families of nonhyperelliptic curves, defined over the field \( \mathbb{Q}(s,t) \). As an application, we calculate the zeta function of one of these curves. We find that the numerators of this zeta factor into 3 quadratic polynomials over the field \( \mathbb{Q}(\zeta_7 + \bar{\zeta}_7) \) (at primes of good reduction), as is expected from the existence of the extra endomorphisms in the Jacobian. Conjecturally these quadratic factors define the \( L \)-function of a modular form.

Let \( K/\mathbb{Q} \) be a totally real number field of degree 3. The moduli space principally polarized abelian varieties \( A \) such that \( \text{End}(A) \) contains a fixed order \( R \subset K \) is a Hilbert modular variety \( H_R \) of dimension 3 (for the general theory, see (5), (17), (18)). As mentioned above, we can (generically) identify \( A = \text{Jac}(X) \) for a genus 3 curve \( X \). We obtain in this way a morphism \( H_R \to \mathcal{M}_3 \). The construction in this paper gives explicit families of nonhyperelliptic curves of genus 3 whose Jacobians have endomorphisms by \( \mathbb{Q}(\zeta_7^+) \). These families have 2 independent moduli and therefore do not get the generic member of \( H_R \). Nonetheless ours is an explicit algorithm to construct families of curves which may be useful in other contexts. A sequel to this paper (8) will discuss another approach which does give families with 3 independent moduli.

**Connections to previous work.** This paper derives from the works of Mestre and Ellenberg mentioned above. However, Mestre’s works only gave hyperelliptic examples, and Ellenberg’s work only gave Riemann surface - no polynomial equations. The referees have brought to our attention the papers of I. Boyer (2) and B. Smith (19) which were unknown to us as we worked on this paper and its sequel (8). Here is our understanding:

1. Smith’s work constructs explicit families of nonhyperelliptic curves with nontrivial isogenies in their Jacobians. Moreover his curves are variable-separated in the sense that they have equations \( f(y) = g(x) \). Our curves are also variable-separated, and moreover our result can be viewed as a construction of a family of explicit isogenies in a Jacobian. From this point of view the problem is to give families of genus 2 curves with an explicit 7-isogeny in its Jacobian. See remark 4.2. However, a glance at the table in Theorem 1.1 of (19) does not give any \( \mathbb{Z}/7 \)-example.

2. In the case at hand, Boyer (2) proves a general result for \( \mathbb{Q}(\zeta_7^+) \) in Proposition 2.3. In this paper we treat only \( l = 7 \), but our method is quite different. Both of us give 2-dimensional rational families with explicit formulas. That paper contains several families of one and two parameter curves with real multiplication by \( \mathbb{Q}(\zeta_7^+) \), given by explicit quartic equations. In the sequel to this paper (8) we build a 3-parameter family with explicit polynomial equations; (2) also outlines a construction of 3-dimensional families of curves with real multiplication by \( \mathbb{Q}(\zeta_7^+) \) but even in the case \( l = 7 \) no really explicit formulas are given.

While there is considerable overlap with these two papers, our results were obtained independently. The main contribution is to show that the constructions of Mestre can be generalized to give families of curves with nontrivial
endomorphism algebras in their Jacobians. While we limit to the case \( l = 7 \), the techniques developed in this paper can be generalized to other cases.

The outline of this paper is as follows: we first review Mestre’s method, and give a generalization of it in section 2; then we provide a step by step construction for genus 3, non-hyperelliptic curves in section 3. We relate this in section 4 to Ellenberg’s approach, and in particular show that the Jacobians of these curves have a endomorphisms by \( \mathbb{Q}(\zeta_7^7) \). An illustrative example is calculated in section 5, and the key computer programming code is included in section 6. We compute the Euler factors of the zeta function for some values of the rational prime \( p \) of good reduction, and experimentally at least, verify their expected behavior, namely the factorization of their numerators into quadratic pieces mentioned above. Many of the calculations in this paper were carried out with Mathematica (21), Magma (1), pari/gp (13) and Sage (15).

Acknowledgements. We would like to thank Dr. J. F. Mestre for his helpful comments during his visit to Beijing in summer 2012. This work was conducted during an invited academic visit to Beijing International Center for Mathematical Research and the Chinese Academy of Science, and we would like to thank the hosting institutions, in particular Zhibin Liang and Lihong Zhi, for the invitations, and the hospitality during the visit. We also would like to thank the referees for valuable suggestions. The first author was supported in part by NSA grant 115-60-5012 and NSF grant OISE-1318015; the second author is supported by NSFC11571241; the last author would like to thank the GRFC grant from Southeast Missouri State University.

2. Generalization of Mestre’s construction

We will first briefly review the construction of Mestre; for details see his papers (10) and (11).

Let \( E \) be an elliptic curve and \( G \subset E \) a finite subgroup. Let \( x : E \to \mathbb{P}^1 \) be a rational function such that \( x(-P) = x(P) \), for instance the \( x \)-coordinate in a Weierstrass model of \( E \). We also assume that \( x(O) = \infty \). If \( p : E \to E / G \), then there is a rational function \( u : \mathbb{P}^1 \to \mathbb{P}^1 \) making the diagram commute:

\[
\begin{array}{ccc}
E & \xrightarrow{p} & E / G = E' \\
\downarrow{x} & & \downarrow{z} \\
\mathbb{P}^1 & \xrightarrow{u} & \mathbb{P}^1
\end{array}
\]

For later purposes, we will label the left-hand projective line as \( \mathbb{P}^1_x \), the right-hand projective line as \( \mathbb{P}^1_z \) and the projection \( z : E' \to \mathbb{P}^1_z \). We define a family of hyperelliptic curves by

\[ X_s : y^2 = u(x) - s, \text{ where } s \text{ is a parameter.} \]

The special case of interest for us is when \( G = \langle S \rangle \) is the subgroup generated by a point of order 7. We have the universal family \((E,S)\) of elliptic curves with a point of order 7 parametrized by the modular curve \( X_1(7) \cong \mathbb{P}^1 \), given by the equation:

\[ E_t : y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2, \quad S = (0, 0). \]

The subgroup scheme \( G = \langle S \rangle \) is defined by the equation \( x(x - t^3 + t^2)(x - t^2 + t) = 0 \). The quotient \( E / G \) is

\[ y^2 + (-t^2 + t + 1)xy + (-t^3 + t^2)y = x^3 + (-t^3 + t^2)x^2 + a(t)x + b(t) \]

where

\[
\begin{align*}
a(t) &= -5(-1 + t)t(1 - t + t^2)(1 - 5t + 2t^2 + t^3), \\
b(t) &= -(1 + t)t(1 - 18t + 76t^2 - 182t^3 + 211t^4 - 132t^5 + 70t^6 - 37t^7 + 9t^8 + t^9). 
\end{align*}
\]

\[ 3 \]
The map $E \to E/G$ is given by $(x, y) \to (u(x), v(x, y))$ where

$$u(x) = u_t(x) = \frac{w(x)}{(-t + t^2 - x)(-t^2 + t^3 - x)^2 x^2},$$

and

$$w(x) = w_t(x) = x^7 - 2(-1 + t)t(1 + t)x^6 + (-1 + t)t(1 - 7t + 5t^2 - 3t^3 + 2t^4 + t^5)x^5$$

$$- (-1 + t)^2 t^3(-1 - 13t + 12t^2 - 9t^3 + 6t^4)x^4 + (-1 + t)^3 t^4(-1 - 7t - 8t^2 + 4t^3 + t^4 + t^5)x^3$$

$$- (-1 + t)^4 t^6(1 + t)(-3 - 5t + 3t^2)x^2 + (-1 + t)^5 t^8(-3 - 3t + t^2)x + (-1 + t)^6 t^{10}.$$

Note that the denominator above is $[(x - x(S))(x - x(2S))(x - x(3S))]^2$. We obtain in this way a 2-parameter family of genus 3 hyperelliptic curves, which are studied in detail in (7).

These curves $X_s$ have correspondences induced by the elements of $G$. Any $x \in \mathbb{P}^1_2$ is of the form $x = x(P)$ for a $P \in E$ unique up to $\pm P$. Because of $z \circ p = u \circ x$ we have $u(x(P + M)) = u(x(P))$ for any $M \in G$. Therefore the map $X_s \to \text{Sym}^2(X_s)$ such that

$$(x, y) = (x(P), y) \mapsto (x(P + M), y) + (x(P - M), y)$$

is well-defined, and one can show that it is a morphism of varieties.

These constructions of Mestre were applied to the hyperelliptic case. In fact, the method is more general. If $X : f(u, y) = 0$ is any algebraic curve ($f$ is a rational function), then the curve $f(u(x), y) = 0$ will have correspondences induced from elements of the subgroup $G \subset E$. The essential point is the property $u(x(P + S)) = u(x(P))$ for any point $P \in E$ and $S \in G$, which follows immediately from the definition of $u(x)$. Hence if $(x(P), y)$ is on $X$ so is $(x(P + S), y)$. The correspondence is

$$(x, y) = (x(P), y) \mapsto (x(P + S), y) + (x(P - S), y).$$

This is well-defined: any $(x, y)$ on $X$ is of the form $(x(P), y)$ for some $P \in E$, unique up to $\pm P$. Replacing $P$ by $-P$ in the above expression gives the same result.

If $f(y) = y^2 - t$ for a parameter $t$, Mestre’s family is $f(y) - u(x) = 0$. That the genus of a curve $X_t$ in this family is 3 can be seen from the ramification properties of the maps

$$y \mapsto z = f(y) = y^2 - t : \mathbb{P}^1_y \to \mathbb{P}^1_z, \quad x \mapsto z = u(x) : \mathbb{P}^1_x \to \mathbb{P}^1_z.$$

For nonhyperelliptic case, we would like to find an equation $f(y) = u(x)$, where the function $f(y)$ is chosen such that the curve $f(y) = u(x)$ is of genus 3. The key is in the ramification properties of the map $u$. The morphism $u$ has degree 7. Since both source and target have genus 0, the genus formula tells us that the total ramification of the map

$$z = u(x) : \mathbb{P}^1_x \to \mathbb{P}^1_z$$

is 12. We can identify the ramification points easily. Let $Q_i = O, Q_i, i = 2, 3, 4$ be the points of order 2 on $E$, and define $q_i = x(Q_i)$, so $q_i = \infty$. Since $x(Q + jS) = x(Q - jS)$ for any multiple of $S$, a generating point of order 7, and any point $Q$ of order 2, we let $\{r_i, r'_i, r''_i\}$ be the values $\{x(Q + jS)\}$ for $j \neq 0 \mod 7$. Because 7 is prime to 2, $Q'_i = f(Q_i)$ are the points of order 2 on $E' = E/\langle P \rangle$. Finally remember that the ramification of the maps $x : E \to \mathbb{P}^1_x$ and $z : E' \to \mathbb{P}^1_z$ occur only at the points of order 2, and that the map $f$ is unramified.
Lemma 2.1. The map \( z = u(x) : \mathbb{P}^1_x \to \mathbb{P}^1_z \) is ramified of type 2,2,2,1 above each of the four points \( q'_i = x(Q'_i) \). In fact, \( u \) is étale at \( q_i = x(Q_i) \) and branched of order 2 at each of \( r_i, r'_i, r''_i \), as in the picture below.

\[
\begin{array}{c}
q_i \\
\downarrow \quad u \\
q'_i \\
\end{array}
\]

\[
\begin{array}{c}
\cdots \\
r''_i \\
r'_i \\
r_i \\
\end{array}
\]

Proof. Look at the ramification of the composite map \( u \circ x = z \circ f \). Since \( f \) is everywhere unramified, the branching of this function can only occur at

\[
f^{-1}(\text{branch points of } z) = f^{-1}(Q'_i) = \{Q_i + jS\},
\]

and these are branch points of order 2. On the other hand, \( Q_i \) is a branch point of order 2 for \( x : E \to \mathbb{P}^1_x \), so there cannot be any further branching at this point under \( u \circ x \), which means that \( u \) must be unramified at \( q_i = x(Q_i) \). But \( x : E \to \mathbb{P}^1_z \) is unramified at \( Q_i + jS \) if \( j \) is not 0 mod 7 (these are not points of order 2), and since \( u \circ x \) does ramify of order 2 at this point and \( x \) does not, we must have that \( u \) ramifies of order 2 at each of \( r_i, r'_i, r''_i \) as claimed. □

One can understand Mestre’s method as follows: he base-extends a double cover \( a : \mathbb{P}^1_y \to \mathbb{P}^1_z \) in the shape \( z = f(y) = y^2 + c \) for an constant \( c \), via the map \( z = u(x) : \mathbb{P}^1_x \to \mathbb{P}^1_z \), and normalizes to obtain a smooth curve \( X \). The point \( S \) of order 7 on the elliptic curve \( E \) gives rise to a correspondence which defines an endomorphism of the Jacobian of \( X \), as outlined above. The fact that the genus of \( X \) is 3 can be immediately seen from the explicit equations, but in fact, it can also be seen from the ramification properties of the map \( g : X \to \mathbb{P}^1_x \) which is the base-extension of \( f : \mathbb{P}^1_y \to \mathbb{P}^1_z \) via \( u \). The essential point is that \( a \) has ramification index 2 above \( q'_i = \infty \) and that \( u \) has ramification type 2,2,2,1 over that point. Upon base-extension, \( g \) ramifies over \( q_1, r_1, r'_1, r''_1 \) respectively of type 2,1,1,1. The point is that, \( u \) is unbranched at \( q_1 \), but branched of order 2 at \( r_1, r'_1, r''_1 \). Pulling back along an étale map does not change the ramification, but pulling back a double branching along a double branching “unscrews” it,
The general case is this:

Lemma 2.2. Let $D_w$ be the open unit disk in the complex $w$-line. Consider the map $f : D_t \to D_s$ given by $s = f(t) = t^n$ for a positive integer $n$. Let $g : D_z \to D_s$ be given by $s = g(z) = z^d$ for a positive integer $d$. Let $e$ be the greatest common divisor of $n$ and $d$. Then the normalization of the base-change is a disjoint union of $e$ analytic disks $D_w$:

$$D_z \times_{D_s} D_t = \bigsqcup_{i=1}^{e} D_w.$$  

Proof. The base-change is $\{(z, t) \mid z^d = t^n\}$. Write $d = ed_0$, $n = en_0$, with $d_0$, $n_0$ relatively prime. Choose any primitive $e$th root of unity $\eta$. This set breaks up into $e$ sets

$$M_i = \{(z, t) \mid z^{d_0} = \eta^i t^{n_0}\}, \quad i = 0, \ldots, e-1.$$  

These are irreducible and mutually disjoint except for the one common solution $(0, 0)$. The normalization will be the disjoint union of the normalization of each, and each of these is a disk. A one-to-one parametrization $D_w \to M_i$ is given by $w \mapsto (\xi w^{n_0}, w^{d_0})$, where $\xi^{d_0} = \eta^i$. One checks that it is a bijection. If $(\xi w^{n_0}, w^{d_0}) = (\xi w_1^{n_0}, w_1^{d_0})$, then $(w/w_1)^{d_0} = (w/w_1)^{n_0}$, which shows that $w/w_1 = 1$ since $d_0$ and $n_0$ are relatively prime, which shows injectivity. To see surjectivity, for a given $(z, t)$, let $w^{d_0} = t$. Since

$$(\xi w^{n_0})^{d_0} = \eta^i t^{n_0} = z^{d_0},$$

we have $\xi w^{n_0} = \zeta z$, with $\zeta^{d_0} = 1$. Let $a$ be an integer such that $an_0 \equiv -1 \pmod{d_0}$, which exists since $d_0$ and $n_0$ are relatively prime. Let $w_1 = \zeta^a w$. Then $w_1^{d_0} = t$, and $z = \zeta^{-1} \xi w^{n_0} = \zeta^{-1} \xi \zeta^{-an_0} w_1^{n_0} = \xi w_1^{n_0}$. □

In summary: the projection $g : X \to \mathbb{P}_1^1$ ramifies only once above the points $u^{-1}(\infty)$, as in the above picture. The other branch points occur at $u^{-1}(\text{the other branch point of } f)$, but $u$ is unbranched over these, so we get 7 branch points of order 2. The total is $e = 1 + 7 = 8$, so that the genus of $X$ is indeed 3.
We change the notation a bit by setting \( q_1 = \infty, q_2' = m, q_2'' = n, q_3 = p \). The ramification of the function \( u(x) \) is of type \( 2, 2, 1 \) over the four points \( m, n, p, \infty \), which are the images of the points \( x(Q_i) \) for the 4 points \( Q_1, Q_2, Q_3, Q_4 \in E \) of order 2 in the group law of \( E \).

We generalize Mestre’s construction by pulling back a triple covering \( f : \mathbb{P}^1_y \to \mathbb{P}^1_x \) along the map \( u \). For essentially the same reason as in the hyperelliptic case, we obtain a correspondence on this curve \( X \). We arrange so that the map \( f \) has branching of type \( 2, 1 \) over each of the points \( m, n, p \). There is one further branch point of \( f \) which is left arbitrary. Because of the branching behavior of the map \( u \) above the points \( m, n, p \) (see the picture in lemma 2.1) we get by the reasoning of the previous section that the ramification of the map \( g : X \to \mathbb{P}^1_x \) is of the following type: Above the points \( u^{-1}(m), u^{-1}(n), u^{-1}(p) \) only one ramification point in each set. Above each of the seven points in \( u^{-1}(\text{the other branch point of } f) \), a single double branch point. The total ramification is thus 10 and since \( g \) is a triple cover, this gives a genus of 3 for \( X \). We will show in section 4 that the correspondence gives an endomorphism of the Jacobian of \( X \) which is \( \zeta_7 + \zeta_7^{-1} \) by connecting our construction with more general results of Ellenberg.

**Remark 2.3.** One can consider more generally curves of the shape \( f(y) = u(x) \) where \( u(x) \) comes from a quotient \( E \to E/G \) for any finite subgroup \( G \subset E \) of an elliptic curve, and \( f(y) \) is any rational function. However, the genus of the resulting curve will generally be quite high. The interest of this method is to give curves of relatively low genus with nontrivial endomorphisms in their Jacobians. In order to get low genus, the ramifications of the functions \( f(y) \) and \( u(x) \) must mesh in a special way, and this explains the close analysis of ramification above. Nonetheless, it should be possible to give nontrivial families of curves of low genus by these methods.

### 3. Construction of the Curves

We will construct a family of curves in the affine \((x, y)\) plane which will depend rationally on parameters \((s, t)\). These curves will have equations \( f_s(y) = u_t(x) \), where \( u_t(x) \) is the function that appears in displayed formulas (2) and (3) in section 2. We first build a family of degree 3 rational functions \( f_s(a, m, n, p, y) \) depending on the parameter \( a \) which has the following properties: Let \( m, n, p \) be the \( x \)-coordinates of the points of order 2 other than \( O \) on the elliptic curve \( E/G \) whose equations are given in formula (1) in section 2. Then:

\[
    f_s(a(m) = m, \quad f_s(a(n) = n, \quad f_s(a(p) = p; \quad f_s'(a(m) = 0, \quad f_s'(a(n) = 0, \quad f_s'(a(p) = 0. \tag{4}
\]

This is a composite of three functions \( f_s(y) = S(T_a(z(y))) \). Next we will symmetrize \( f(a, m, n, p, y) \) in \( m, n, p \). This is necessary because \( m, n, p \) will be given to us as the roots of a cubic polynomial whose coefficients will be polynomials in \( t \). This is accomplished by defining a linear fractional expression in \( s, a(s, m, n, p) \), with certain properties. Then \( f(a(s, m, n, p), m, n, p, y) \) depends only on the symmetric functions \( \sigma_1, \sigma_2, \sigma_3 \) of \( m, n, p \). The final formula for \( f_s(y) \) is gotten by equating \( -\sigma_1, -\sigma_2, -\sigma_3 \) with the coefficients of the polynomial \((x - m)(x - n)(x - p)\). This latter polynomial is calculated as the discriminant with respect to \( y \) of the Weierstrass equation for the curve \( E/G \).

**Step 1.** Construct a degree 3 rational function \( T_a(z) \) such that

\[
    T_a(0) = 0, \quad T_a'(0) = 0; \quad T_a \text{ has a double pole at } z = \infty; \quad T_a(1) = 1, \quad T_a'(1) = 0.
\]

Let \( T(z) = \frac{a z^3 + b z^2}{z^2 + c} \). This has degree 3 as long as \( a \neq 0 \), and it satisfies the first two sets of conditions above.

To satisfy the last two equalities, we set \( T(1) = 1, T'(1) = 0, \) and this gives equations \( a + b = c + 1 \) and \( c = \frac{2a - b}{3a + 2b} = a + b - 1 \). The solution \( b = -a, \ c = -1 \) is rejected because it reduces the degree of \( T \) to 2. The other solution is \( b = (1 - 3a)/2 \), and we remove the denominator in \( b \) by replacing \( a \rightarrow 1 + 2a \). It leads to the expression

\[
    T_a(z) = \frac{(1 + 2a) z^3 + (-1 - 3a) z^2}{z - 1 - \alpha}, \quad \text{with } \alpha \neq -1/2.
\]

In what follows we rename the variable \( \alpha \) as \( a \). We thus obtain a one-dimensional family of coverings depending on the parameter \( a \).
Step 2. Construct a function satisfying the properties required in (4). To do so, we move the branching from 0, 1, \( \infty \) to an arbitrary set \( m,n,p \), and define

\[
z(y) = z(m,n,p,y) = \frac{(y-m)(p-n)}{(m-n)(y-p)}, \quad \text{where } z(m) = 0, z(n) = 1, z(p) = \infty,
\]

\[
S(t) = S(m,n,p,t) = \frac{pt(m-n) + m(n-p)}{t(m-n) + n-p}, \quad \text{where } S(0) = m, S(1) = n, S(\infty) = p,
\]

\[
f_a(y) = f(a,m,n,p,y) = S(T_a(z(y))).
\]

The function \( f_a(y) \) clearly has the properties required in (4), and

\[
f(a,m,n,p,y) = \frac{\alpha(y)}{\beta(y)}, \quad \text{where}
\]

\[
\alpha(y) = (2am^2n^2p - am^2np - amn^2p + m^2n^2p - mn^2p^2)
\]

\[
+ (-3am^2np - 3amn^2p + 6amnp^2 - 3m^2np + 3mn^2p^2)y
\]

\[
+ (3am^2p - 3amn^2p - 3ap^2 + m^2p - mn^2 - 2mp^2 + n^2p - np^2)y^2
\]

\[
+ (-am^2 + 2amn - amp - an^2 - anp + 2ap^2 - m^2 + mn - np + p^2)y^3,
\]

\[
\beta(y) = (2am^2n^2 - am^2np - amn^2p + 2amnp^2 - an^2p^2 + m^2n^2p - mn^2np + mn^2 - n^2p^2)
\]

\[
+ (-3am^2n + 3amn^2p - 3am^2p - 3an^2p - m^2n + m^2p - 2mn^2 - mp^2 + 2n^2p + np^2)y
\]

\[
+ (6amn - 3amp + 3mn - 3np)y^2
\]

\[
+ (-am - an + 2ap - m + p)y^3.
\]

Step 3. Find the parameter \( a \) so that \( f \) is symmetric with respect to \( m,n,p \). Our approach is to make \( a \) a function of \( m,n,p \). To do so, we observe that

\[
f(a,m,n,p,y) = f(b,n,m,p,y) \quad \Rightarrow \quad b = -1 - a,
\]

\[
f(a,m,n,p,y) = f(b,p,n,m,y) \quad \Rightarrow \quad b = \frac{-a}{1 + 3a},
\]

\[
f(a,m,n,p,y) = f(b,m,p,n,y) \quad \Rightarrow \quad b = \frac{1 + 2a}{2 + 3a},
\]

\[
f(a,m,n,p,y) = f(b,p,m,n,y) \quad \Rightarrow \quad b = \frac{-1 - a}{2 + 3a},
\]

\[
f(a,m,n,p,y) = f(b,n,p,m,y) \quad \Rightarrow \quad b = \frac{-1 + 2a}{1 + 3a}.
\]

In other words, \( a \) undergoes a group of linear fractional transformations as above isomorphic to \( S_3 \) as we permute \( m,n,p \). We can realize this group of linear fractional transformations by a rational function of degree 1. The reader can check that

\[
a(m,n,p,s) = \frac{(mn - 2mp + np) + (m - 2n + p)s}{3(m-n)(p-s)}
\]

undergoes the same transformations as above when the \( m,n,p \) are permuted, e.g.,

\[
a(n,m,p) = -1 - a(m,n,p,s), \quad a(n,p,m) = -1 + 2a(m,n,p,s)
\]

\[
a(n,p,m) = \frac{1 + 2a(m,n,p,s)}{1 + 3a(m,n,p,s)}.
\]
and this is sufficient since these permutations generate $S_3$. This function $a$ is the cross-ratio of $-1/3, -2/3, \infty, s$. Note that $\{-1/3, -2/3, \infty\}$ is exactly the set of poles of the expressions for $b$ above. In other words, $a$ is the solution to the equation

$$-3a - 1 = \frac{(s - m)(n - p)}{(n - m)(s - p)} = \lambda(m, n, p, s),$$

where the left-hand side takes the values $0, 1, \infty$ at $-1/3, -2/3, \infty$ respectively. It is well-known that $\lambda(m, n, p, s)$ undergoes a group of linear fractional transformations isomorphic to $S_3$ as the $m, n, p$ are permuted. The above expression for $a$ carries the group of $\lambda$-transformations into the group of $a$-transformations given by the formulas for $b$.

Define

$$f_s(y) = f_s(m, n, p, y) = f(a(m, n, p, s), m, n, p, y).$$

By its very construction, $f_s(m, n, p, y)$ is invariant under all permutations of $m, n, p$. We get a one-parameter family of coverings $\mathbb{P}^1 \to \mathbb{P}^1$, depending on $s$, which is branched above $m, n, p$ of type 2, 1 with the double points occurring at $y = m, n, p$ respectively. We have:

$$f_s(y) = \frac{\alpha_s(y)}{\beta_s(y)}$$

where

$$\alpha_s(y) = (2m^3n^3p - 2m^3n^2p^2 - 2m^2n^3p^2 + 2m^3np^3 - 2m^2n^2p^3 + 2mn^3p^3)$$

$$+ (-m^3n^2p - m^2n^3p^2 + 6m^2n^2p^2 - mn^3p^2 - m^2np^3 - mn^2p^3)s$$

$$+ (-3m^3n^3p - 3m^2n^3p - 3m^3np^3 + 18m^2n^2p^2 - 3mn^3p^2 - 3m^2np^3 - 3mn^2p^3)y$$

$$+ (6m^3np - 6m^2n^2p + 6mn^3p - 6mn^2p^2 + 6mnp^3)$$

$$+ (6m^3np - 6m^2n^2p + 6mn^3p - 6mn^2p^2 + 6mnp^3)y^2$$

$$+ (-3m^3n + 6m^2n^2p - 3mn^2p - 3m^3p - 3n^3p + 6m^2p^2 - 6n^2p^2)$$

$$+ (-m^3n + 2m^2n^2 - mn^2 - m^3p - n^3p + 2m^2p^2 + 2n^2p^2 - mp^3 - np^3)y^3$$

$$+ (2m^3 - 2m^2n - 2mn^2 + 2n^3 - 2m^2p + 6mnp - 2n^2p - 2np^2 - 2p^3)$$

$$+ (2m^3 - 2m^2n - 2mn^2 + 2n^3 - 2m^2p + 6mnp - 2n^2p - 2np^2 - 2p^3)$$

$$\beta_s(y) = (2m^3n^3 - 2m^2n^3p - 2m^3np^2 + 6m^2n^2p^2 - 2m^3p^3 + 2m^2np^3 - 2mn^2p^3 + 2n^3p^3)$$

$$+ (-m^3n^2 - m^2n^3 + 2m^3np + 2mn^3p - m^3p^2 - n^3p^2 - m^2np^3 + 2mn^2 - n^3p^3)s$$

$$+ (-3m^3n^2 - 3m^2n^3 + 6m^3np + 6mn^3p - 3m^3p^2 - 3n^3p^2 - 3m^2p^3 + 6mnp^3 - 3n^3p^3)y$$

$$+ (6m^2np - 6m^2np - 6mn^2p + 6mnp - 6mnp^3 + 6mnp^3)$$

$$+ (-3m^2n^2 - 3m^2n - 2mn^3p + 18mnp - 3n^2p^2 - 3np^3)$$

$$+ (-m^2n - mn^2 - m^3p + 6mnp - n^2p - mp^3 - np^3)y^3$$

$$+ (2m^2 - 2mn + 2n^2p - 2np - 2p^3)$$

$$\frac{\alpha_s(y)^2}{\beta_s(y)^2}.$$

**Remark 3.1.** There is a second solution to equations that intertwine the $S_3$-action given by the expressions for $b$ with the $S_3$-action given by the action on $\lambda(m, n, p, s)$. It is

$$a(m, n, p, s) = \frac{(m - p)(n - s)}{-2mn + mp + ms + np + ns - 2ps}.$$

This will give a different family of curves over $\mathbb{Q}(s, \sigma_1, \sigma_2, \sigma_3)$ induces the same family over $\mathbb{Q}(a, m, n, p)$ as the original $a(m, n, p, s)$. We have not analyzed all the possible descents of the curve over $\mathbb{Q}(a, m, n, p)$ to a curve over...
subfields $\mathbb{Q}(s, \sigma_1, \sigma_2, \sigma_3)$ for various $a(m, n, p, s)$. In what follows, we use the expression for $a(m, n, p, s)$ given in (5).

Step 4. Express function $f_s(y)$ in terms of the elementary symmetric functions of $m, n,$:

$$f_s(y) = \frac{\alpha_s(y)}{\beta_s(y)}$$

where

$$\alpha_s(y) = y^3 \left( s \left( 2\sigma_1^3 - 8\sigma_2\sigma_1 + 18\sigma_3 \right) - \sigma_2\sigma_1^2 - 3\sigma_3\sigma_1 + 4\sigma_2^3 \right)$$

$$+ y^2 \left( s \left( -3\sigma_2\sigma_1 - 9\sigma_3\sigma_1 + 12\sigma_2^2 \right) + 6\sigma_3\sigma_1^2 - 18\sigma_2\sigma_3 \right)$$

$$+ y \left( s \left( 6\sigma_3\sigma_3 - 18\sigma_2\sigma_3 \right) + 27\sigma_2^2 - 3\sigma_1\sigma_2\sigma_3 \right)$$

$$+ s \left( 9\sigma_3^2 - \sigma_1\sigma_2\sigma_3 \right) - 6\sigma_1\sigma_3^2 + 2\sigma_2^2\sigma_3,$$

$$\beta_s(y) = y^3 \left( s \left( 2\sigma_1^3 - 6\sigma_2 \right) - \sigma_1\sigma_2 + 9\sigma_3 \right)$$

$$+ y^2 \left( s \left( 27\sigma_3 - 3\sigma_1\sigma_2 \right) + 6\sigma_2^2 - 18\sigma_1\sigma_3 \right)$$

$$+ y \left( s \left( 6\sigma_2^2 - 18\sigma_1\sigma_3 \right) + 12\sigma_3\sigma_1^2 - 3\sigma_2^2\sigma_1 - 9\sigma_2\sigma_3 \right)$$

$$+ s \left( 4\sigma_3\sigma_1^2 - \sigma_2^2\sigma_1 - 3\sigma_2\sigma_3 \right) + 2\sigma_2^2 + 18\sigma_3^2 - 8\sigma_1\sigma_2\sigma_3.$$

Step 5. Construct a 2 dimensional family of curves $X_{s,t}$ defined by $f_s(y) = u_t(x)$. To construct our family, we must take for $m, n, p$ to be the $x$-coordinates of the points of order 2 other than $O$ on the quotient curve $E/G$. These are the roots of the discriminant with respect to $y$ of the Weierstrass equation $g(x, y) = 0$ for $E/G$ which is

$$g(x, y) = y^2 + (-t^2 + t + 1)xy + (-t^3 + t^2)y - (x^3 + (-t^3 + t^2)x^2 + a(t)x + b(t)),$$

where

$$a(t) = -5(-1 + t)(1 - t + t^2)(1 - 5t + 2t^2 + t^3),$$

$$b(t) = -(-1 + t)(1 - 18t + 76t^2 - 182t^3 + 211t^4 - 132t^5 + 70t^6 - 37t^7 + 9t^8 + t^9).$$

The symmetric functions $4\sigma_1, 4\sigma_2, 4\sigma_3$ are up to signs the coefficients of this discriminant. The reason for the factor 4 is that the discriminant starts with the term $4x^3$. The discriminant is

$$( -4t^{11} - 32t^{10} + 184t^9 - 428t^8 + 808t^7 - 1371t^6 + 1570t^5 - 1031t^4 + 376t^3 - 76t^2 + 4t)$$

$$( -20t^7 + 142t^6 - 284t^5 + 280t^3 - 138t^2 + 20t)x + (t^4 - 6t^3 + 3t^2 + 2t + 1)x^2 + 4x^3,$$

and

$$4\sigma_1 = -1 - 2t - 3t^2 + 6t^3 - t^4,$$

$$4\sigma_2 = -20t^7 + 142t^6 - 284t^5 + 280t^3 - 138t^2 + 20t,$$

$$4\sigma_3 = 4t^1 + 32t^{10} - 184t^9 + 428t^8 - 808t^7 + 1371t^6 - 1570t^5 + 1031t^4 - 376t^3 - 76t^2 - 4t.$$

Hence, we have a 2 dimensional family of curves $X_{s,t}$ defined by $f_s(y) = u_t(x)$, that is

$$\alpha_s(y)(-t + t^2 - x)^2(-t^2 + t^3 - x)^2x^2 = w_t(x)\beta_s(y),$$

where the definitions of $u_t, w_t$ are in the displayed formulas (2) and (3). We will see in the next section that their Jacobians have endomorphisms by the cubic field $\mathbb{Q}(\zeta_7 + \overline{\zeta_7}).$

4. Relation to Ellenberg’s construction

Let $D_7 = \langle \sigma, \tau \mid \sigma^7 = \tau^2 = e, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ be the dihedral group of order 14, symmetries of a regular 7-gon. It has 7 involutions $\tau_i = \sigma^i\tau\sigma^{-i}, i = 0, ..., 6$. Corresponding to the lattice of subgroups of $D_7$ we have the tower of
curves and morphisms as in the following diagram.

Here $E$ is an elliptic curve and $S \in E$ is a point of order 7 as in Mestre’s construction. $p$ is the canonical projection, which is an étale cyclic covering of degree 7. The curves $E/\langle \tau \rangle$ are all abstractly $\mathbb{P}^1$, and we choose one coordinate $x$ for all of them. We do this as follows: We let $x = x_1 : E \to \mathbb{P}^1$ be projection modulo the involution $\tau_1 = \tau : P \mapsto -P$, then $x_i$ is the projection modulo the involution $\tau_i : P \mapsto -P + iS$. The diagram on the right results by base-change along the map $z \mapsto u = z^2 + c : \mathbb{P}^1 \to \mathbb{P}^1$ for a constant $c$. Strictly speaking, this is base-change followed by normalization. However, the map $q$ really is the base-change of $p$ via the map $C \to E'$, since $p$ is étale, and no normalization is required. It follows that $q$ is an étale cyclic covering of degree 7. We can see that the curves $X_i = Y/\langle \tau_i \rangle$, all isomorphic, are of genus 3, the curve $C$ is of genus 2 and the curve $Y$ is of genus 8.

In the following diagram:

the front, bottom and back faces are defined as pull-back squares. More precisely, they are pull-backs followed by normalization. Actually, the back face is just a pull-back as mentioned, because the map $p$ is an étale map of smooth curves, so its base-change gives an étale map of smooth curves $q$. The dotted arrow $h$ exists commuting the diagram. In view of universal properties of normalization and fiber-products, it suffices to verify that $f \circ (y \circ q) = u \circ (x \circ l)$, which is immediate. Note also that this diagram clearly shows an action of $D_7$ on the curve $Y$. The maps $P \mapsto P + S$ on $E$ and the identity on $C$ lift to give an automorphism $\sigma$ of order 7 on $Y$ by base-change. The map $P \mapsto -P$ on $E'$, and the identity on $\mathbb{P}^1_y$ lifts to the hyperelliptic involution on $C$. In turn, the hyperelliptic involution on $C$, and the identity map on $E$ lifts to an automorphism $\tau$ of order 2. These generate a dihedral group of symmetries. The
ramifications in this picture conform to Ellenberg’s branching for this example: The overall projection $Y \to \mathbb{P}_y^1$ is a Galois $D_7$ covering branched above 6 points of branching type $2,2,2,2,2,2$. The six branch points $\Sigma \subset \mathbb{P}_y^1$ are the branch points of the projection of the genus 2 curve $C \to \mathbb{P}_y^1$. Thus the branched covering $a : Y(\mathbb{C}) \to \mathbb{P}_y^1(\mathbb{C})$ is topologically described by the monodromy homomorphism

$$\rho : \pi_1(\mathbb{P}_y^1(\mathbb{C}) \setminus \Sigma, \ast) \to \text{Aut}(a^{-1}(\ast)) \sim S_7$$

acting transitively. The image of $\rho$ is isomorphic to $D_7$. That the action is a transitive Galois action means that, as $D_7$-set, $a^{-1}(\ast)$ is isomorphic to $D_7$ with its natural $D_7$-action by (right) translation. Finally, this image is generated by the 6 involutions $\tau_i \in D_7$ gotten by walking from $\ast$ around each of the 6 points in $\Sigma$. These satisfy $\tau_1 \tau_2 \tau_3 \tau_4 \tau_5 \tau_6 = 1$.

In terms of the generators $\sigma, \tau$ of $D_7$, this means that $\tau_i = \sigma^{b_i} \tau$, $i = 1, \ldots, 6$. It is not difficult to see that the action is transitive if and only if at least two of the $b_i$ are distinct modulo 7.

Recall the general set-up in Ellenberg’s paper. We let $Y$ be a smooth projective curve an $G$ be a finite group acting on $Y$. There is a homomorphism of algebras

$$\mathbb{Z}[G] \to \text{End}(\text{Jac}(Y)),$$

and similar maps to endomorphism algebras of $H^i(Y)$ for various cohomology theories $H^i$. After $\otimes \mathbb{Q}$, both sides above are semisimple algebras of finite dimension. If $H \subset G$ is a subgroup, we have the idempotent

$$\frac{1}{\#H} \sum_{h \in H} h := \pi_H \in \mathbb{Q}[G].$$

One defines a “Hecke algebra” $\mathbb{Q}[H \backslash G/H]$ as the subalgebra of $\mathbb{Q}[G]$ generated by $\pi_H g \pi_H$ for all $g \in G$. If $X = Y/H$, then we have a homomorphism

$$\mathbb{Q}[H \backslash G/H] \to \text{End}(\text{Jac}(X))$$

since $\text{Jac}(X) = \pi_H \text{Jac}(Y)$. Similar results apply to endomorphisms of $H^i(X)$.

Our case is the genus 8 curve $Y$ with the action of $G = D_7$ described above. The curve $X = Y/H$ has genus 3, where $H = \langle \tau \rangle$ is generated by any involution. One can show directly that $\mathbb{Q}[H \backslash G/H]$ is isomorphic to $\mathbb{Q}(\zeta_7 + \overline{\zeta_7})$, but in any case, this is one of a family of examples studied in Ellenberg’s paper.

In view of the classical isomorphism $\text{End}(\text{Jac}(X)) = \text{Corr}(X)$ of the ring of endomorphisms of the Jacobian with the ring of correspondence classes of $X$, for any curve $X$, we can describe geometrically the action of the generator $\pi_H \sigma \pi_H$ as follows: if $h : Y \to X = Y/H$ is the canonical projection, we get a second projection $h \circ \sigma : Y \to X$. These two projections define the correspondence, which therefore has degrees $(2,2)$.

Thus we have shown our main result:

**Theorem 4.1.** Let $X_{s,t}$ be the smooth and projective model of the curve defined by $f_s(y) = u_t(x)$. For general values of $(s,t)$ this is a genus 3 nonhyperelliptic curve and there is an endomorphism $\phi$ of the Jacobian of $X_{s,t}$ which satisfies the equation $\phi^3 + \phi^2 - 2\phi - 1 = 0$. The endomorphism is defined over the field $\mathbb{Q}(s,t)$.

**Remark 4.2.** The key point is the existence of the genus 8 curve $Y$ with the $D_7$-action in the cube diagram above. The quotient by the 7-cycle $\sigma$ gives an unramified projection to a genus 2 curve: $Y \to C$. However, the genus 2 curve $C$ is special. Since it has a map to an elliptic curve $E/G$, the Jacobian $\text{Jac}(C)$ will split off an elliptic curve factor.

One can consider cyclic degree 7 coverings of a general genus 2 curve $C$ and this will lead to 3-parameter families of genus 3 curves with multiplications by $\mathbb{Q}(\zeta_7 + \overline{\zeta_7})$. A cyclic unramified covering of $C$ is essentially equivalent to a 7-isogeny of $\text{Jac}(C)$. These are discussed in the sequel to this paper (8).
5. An example

We take the values \( s = 0, t = -2 \) in the equation \( f_s(y) = u_t(x) \). This is a plane curve of geometric genus 3, but it is highly singular. For the calculations that follow, we need a smooth projective model. The canonical model of a nonhyperelliptic genus 3 curve is a smooth projective plane quartic. Magma (Magma code is included in the Appendix) calculated the canonical model of this curve as

\[
\begin{align*}
    x^4 + & \frac{345x^3y}{4} - \frac{16038x^3z}{7} + \frac{14499x^2y^2}{14} - \frac{553623x^2yz}{2} + \frac{4273137x^2z^2}{28} + \frac{2153679xyz}{7} - \frac{28405935y^4}{28405935} + \frac{20973087y^3z}{20973087} - 10692058320y^2z^2 - 205496736912yz^3 + 1321162646760z^4 = 0.
\end{align*}
\]

We compute the zeta function of the scheme \( X/\mathbb{Z} \). This means that we compute

\[
Z(X/\mathbb{F}_p, x) = \exp \left( \sum_{\nu \geq 1} \frac{N_\nu x^\nu}{\nu} \right) = \frac{1 + a_p x + b_p x^2 + c_p x^3 + pb_p x^4 + p^2 a_p x^5 + p^3 x^6}{(1 - x)(1 - px)}
\]

for the primes \( p \neq 2, 3, 7, 73, 109, 829, 967 \) (divisors of the discriminant of the ternary quartic above), where \( N_\nu = \# X(\mathbb{F}_{p^\nu}) \). Since the curve has genus 3 we need only compute \( N_\nu \) for \( \nu = 1, 2, 3 \). The numerator in the above expression equals

\[
h_p(x) := \det (1 - x \rho(\text{Frob}_p) \mid H^1_{et}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l)), \ l \neq p,
\]

where \( \rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GSp}(H^1_{et}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l)) \) is the canonical Galois representation in étale cohomology, and \( \text{Frob}_p \) is a Frobenius element at \( p \). Since the Jacobian of \( X \) has endomorphisms in the field \( K = \mathbb{Q}(\zeta_7 + \overline{\zeta_7}) \), and these endomorphisms are defined over \( \mathbb{Q} \), \( V_l = H^1_{et}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l) \) becomes a free \( K_l = K \otimes \mathbb{Q}_l \)-module of rank 2, and the operators in \( K \) commute with those in \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \), so that the representation \( \rho \) factors as

\[
\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(V_l) \subset \text{GSp}_6(\mathbb{Q}_l).
\]

This implies that the characteristic polynomials \( h_p(x) \) factor as \( g_p(x)g_p^\sigma(x)g_p^{\sigma^2}(x) \) for a quadratic polynomial \( g_p(x) \in O_K[x] \), where \( O_K = \mathbb{Z}[t]/(t^3 + t^2 - 2t - 1) \) is the ring of integers of \( K \) and \( \sigma \) generates the Galois group of \( K \) over \( \mathbb{Q} \). These polynomials, as well as the trace of \( \text{Frob}_p \), are displayed in Table 1.

Using the solution to Serre’s conjecture, (9) it follows that these quadratic factors coincide with the Hecke polynomials of modular form, modulo \( l \). In fact, one can show that these quadratic factors coincide with the Hecke polynomials of a weight 2 newform.
Table 1. Factorization of $h_p(x) = g_p(x)g_p^g(x)g_p^{g^2}(x)$, trace of Frob$_p$ at good primes.

| $p$ | $g_p(x)$ | Trace |
|-----|-----------|-------|
| 5   | $1 - tx + 5x^2$ | $-1$ |
| 11  | $1 - tx + 11x^2$ | $-1$ |
| 13  | $1 + (3 - t)x + 13x^2$ | $-10$ |
| 17  | $1 + (-1 - 4t)x + 17x^2$ | $-1$ |
| 19  | $1 + (6 - 3t - 2t^2)x + 19x^2$ | $-11$ |
| 23  | $1 + (8 - t - 3t^2)x + 23x^2$ | $-10$ |
| 29  | $1 + (8 - 5t - 6t^2)x + 29x^2$ | $1$ |
| 31  | $1 + (7 - t - 2t^2)x + 31x^2$ | $-12$ |
| 37  | $1 + (6 - 4t - 5t^2)x + 37x^2$ | $3$ |
| 41  | $1 + 8x + 41x^2$ | $-24$ |
| 43  | $1 + (4 - 2t)x + 43x^2$ | $-3$ |
| 47  | $1 + (10 - t - 4t^2)x + 47x^2$ | $-11$ |
| 53  | $1 + (6 + 2t - 5t^2)x + 53x^2$ | $9$ |
| 59  | $1 + (10 - 6t - 9t^2)x + 59x^2$ | $9$ |
| 61  | $1 + (-2 + 3t)x + 61x^2$ | $9$ |
| 67  | $1 + (4 - 2t - 4t^2)x + 67x^2$ | $-3$ |
| 71  | $1 + (10 - 4t - 5t^2)x + 71x^2$ | $-9$ |
| 79  | $1 + (7 - 8t - 9t^2)x + 79x^2$ | $16$ |
| 83  | $1 + (1 - 3t - 6t^2)x + 83x^2$ | $24$ |
| 89  | $1 + (19 - t - 11t^2)x + 89x^2$ | $-3$ |

6. Appendix

Calculation for this paper were done in Mathematica and in Sage worksheets. These can be made available to the reader by sending a request to one of the authors.

Mathematica code.

\[
\begin{align*}
T[a,z] &:= \frac{(2a + 1)z^3 + (-3a - 1)z^2}{-a + z - 1}, \\
S[m,n,p,s] &:= \frac{(y - m)(p - n)}{(m - n)(y - p)}, \\
\text{lambda}[m,n,p,s] &:= \frac{(s - m)(n - p)}{(m - p)(s - n)}, \\
\text{a}[m,n,p,s] &:= \frac{mn - 2mp + ms + np - 2ns + ps}{3(m - s)(n - p)}.
\end{align*}
\]

To solve for $a(m, n, p, s)$:
Now,
\[ u_7[x_-, t_+] := \frac{U}{V}, \]

where
\[
U = t^{16} - 6t^{15} + 15t^{14} - 20t^{13} + 15t^{12} - 6t^{11} + t^{10} + (2t - 2t^3) x^6 \\
+ (t^7 + t^6 - 5t^5 + 8t^4 - 12t^3 + 8t^2 - t) x^5 \\
+ (-6t^9 + 21t^8 - 36t^7 + 46t^6 - 37t^5 + 11t^4 + t^3) x^4 \\
+ (t^{15} - 8t^{14} + 22t^{13} - 25t^{12} + 5t^{11} + 14t^{10} - 12t^9 + 3t^8) x \\
+ (-3t^{13} + 14t^{12} - 18t^{11} - 5t^{10} + 25t^9 - 12t^8 + 4t^7 + 3t^6) x^2 \\
+ (t^{12} - 2t^{11} + 4t^{10} - 18t^9 + 28t^8 - 8t^7 - 10t^6 + 4t^5 + t^4) x^3 + x^7.
\]

For Step 4 we use:
\[
h[m_- n_- p_- x_-, z_+] := \text{Together}[f[a[m, n, p, s], m, n, p, z]]; \\
exprnum = \text{Numerator}[h[m, n, p, x, z]] \\
exprdenom = \text{Denominator}[h[m, n, p, x, z]] \\
\text{SymmetricReduction}[\text{Coefficient}[\text{Coefficient}[\text{exprnum}, y, 2], s, 0], m, n, p, s1, s2, s3]
\]

The symmetrized covering:
\[
symcov[s1_-, s2_-, s3_-, x_-, z_+ := \frac{H}{K},
\]

where
\[
H = 2s1^3x^3 + s1^2s2 (-3x^2 - z^3) + s1^2s3 (6xz + 6z^2) + s1s2s3 (-x - 3z) - 8s1s2xz^3 \\
-6s1s3^2 + s1s3 (5 (3x^2 + z^3) + 2 (-6xz^2 - 2 (3x^2 + z^3) - 2z^3)) \\
+2s2s3 + s2^2 (6xz^2 + 2 (3x^2 + z^3) + 2z^3) + s2s3 (2 (-6xz - 6z^2) - 6xz - 6z^2) \\
+s2^2 (3(x + 3z) + 6z + 18z) + 18s3x^3, \\
K = s1^2s3(2(x + 3z) + 2x + 6z) + 2s1^2x^2z + s1s2^2 (-x - 3z) - 8s1s2s3 + s2s3 (3 x^2 - z^3) \\
+2s3 (2 (-6xz - 6z^2) - 6xz - 6z^2) + 2s2^2 (6xz + 6z^2) + s2s3(5(x + 3z) \\
+2(-2(x + 3z) - 2x - 6z)) - 6s2x^3 + 18s3^2 + s3 (18xz^2 + 3 (3x^2 + z^3) + 6z^3). 
\]

And,
\[ 15 \]
The final formula

\[ a = \frac{1}{4} (-t^4 + 6t^3 - 3t^2 - 2t - 1), \]

\[ b = \frac{1}{4} (-20t^7 + 142t^5 - 284t^4 + 280t^3 - 138t^2 + 20t), \]

\[ c = \frac{1}{4} (4t^{11} + 32t^{10} - 184t^9 + 428t^8 - 808t^7 + 1371t^6 - 1570t^5 + 1031t^4 - 376t^3 + 76t^2 - 4t). \]

The final formula \( F(s, t, x, y) \) for the family of curves is defined by:

\[ expr1 = Together[Symcov[a, b, c, s, y]]; expr2 = u7[x, t]; expr3 = Together[expr2 - expr1]; expr4 = Numerator[expr3]; F(s, t, x, y) := Collect[expr4, {x, y}]. \]

**Magma code.** For finding the canonical quartic curve associated to \( f_s(y) = u_t(x) \) with \( s = 0, t = -2 \).

\[
A < x, z >=: \text{AffineSpace}((\mathbb{R});)
\]

\[
C := \text{Curve}(A, 570227392512 - 332632645632 * x + 16865210880 * x^2 + 31838365440 * x^3 + 14470813728 * x^4 + 135287712 * x^5 - 2093784 * x^6 + 763872 * x^7 + 9493936128 * z - 5538129408 * x * z - 6361213824 * x^2 * z + 1637090784 * x^3 * z + 379305360 * x^4 * z - 13122564 * x^5 * z - 1316112 * x^6 * z + 12718 * x^7 * z + 206032896 * z^2 - 120185856 * x * z^2 - 78563520 * x^2 * z^2 + 25613280 * x^3 * z^2 + 6992244 * x^4 * z^2 - 147084 * x^5 * z^2 - 17087 * x^6 * z^2 + 276 * x^7 * z^2 + 295984 * x^3 * z^3 - 1741824 * x * z^3 - 181440 * x^2 * z^3 + 211680 * x^3 * z^3 + 81396 * x^4 * z^3 + 84 * x^5 * z^3 - 63 * x^6 * z^3 + 4 * x^7 * z^3); \]

IsIrreducible(C);

IsHyperelliptic(C);

phi := CanonicalMap(C);

P3 < a, b, c >=: Codomain(phi);

CC := phi(C).

The zeta function calculations are given by

\[
R < t >=: \text{PolynomialRing}((\mathbb{R});)
\]

\[
K < z >=: \text{NumberField}(t^3 + t^2 - 2 * t - 1);
\]

\[
S < t >=: \text{PolynomialRing}(K);
\]

zet := function(n);

\[
P < a, b, c >=: \text{ProjectiveSpace}(GF(n), 2);
\]

\[
C := \text{Curve}(P, a^4 + 345/4 * a^3 + b + 14499/14 * a^2 + b^2 + 2153679/28 * a + b^3 - 28405935/7 * b^4 - 16038/7 * a^3 + c - 553623/4 * a^2 + b * c + 28315359/7 * a + b^2 + c - 20973087 * b^3 + c + 4273137/2 * a^2 + c^2 + 659015811/7 * a + b * c^2 - 10692058320/7 * b^2 + c^2 - 6866481456/7 * a + c^3 - 205496736912/7 * b + c^3 + 1321162646760/7 * c^4);
\]

return[n, StNumerator(ZetaFunction(C, 1))];

end function;

[n*Factorization(Slzet(n)[2])[1][1] : n in [11..72] | IsPrime(n) ].
References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235–265.
[2] I. Boyer, Real multiplication curves by subfields of cyclotomic fields, arxiv:1310.2582v1, (2013).
[3] N. Elkies and A. Kumar, K3 surfaces and equations for Hilbert modular surfaces, arXiv:1209.3527v1, (2012).
[4] J. Ellenberg, Endomorphism algebras of Jacobians, Advances in Mathematics, Vol. 162, No. 2 (2001), 243–271.
[5] E. Z. Goren, Lectures on Hilbert modular varieties and modular forms, With the assistance of Marc-Hubert Nicole, CIRM Monograph Series, 14, Amer. Math. Soc. 2002.
[6] David Gruenewald, Explicit algorithms for Humbert surfaces. thesis, U. Sydney (2009), http://echidna.maths.usyd.edu.au/~davidg/ .
[7] J. W. Hoffman and H. Wang, 7-gons and genus 3 hyperelliptic curves, Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matemàticas, 107 (2013), 35-52.
[8] J. W. Hoffman, Dun Liang, Zhibin Liang, Ryotaro Okazaki, Y. Sakai, H. Wang, Genus 3 curves whose Jacobians have endomorphisms by $\mathbb{Q}(\zeta_7 + \bar{\zeta}_7)$, II. arXiv:1411.2152
[9] C. Khare and J.-P. Wintenberger, On Serre’s conjecture for 2-dimensional mod p representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math., Vol. 169, No. 2 (2009), no. 1, 229–253.
[10] J. F. Mestre, Courbes hyperelliptiques à multiplications réelles, C. R. Acad. Sci. Paris, Ser. I Math., 307 (1988), 721–724.
[11] J. F. Mestre, Courbes hyperelliptiques à multiplications réelles, Progr. Math., 89 (1991), 193-208.
[12] D. Mumford, Abelian Varieties, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970.
[13] The PARI Group, PARI/GP, version 2.5.0, 2011, Bordeaux, available from http://pari.math.u-bordeaux.fr/ .
[14] B. Runge, Endomorphism rings of abelian surfaces and projective models of their moduli spaces, Tohoku Math. J., Vol. 51, No. 3(1999), 283–303.
[15] SAGE Mathematics Software, Version 4.6, http://www.sagemath.org/ .
[16] Y. Sakai, Construction of genus two curves with real multiplication by Poncelet’s theorem, (2010) dissertation, Waseda University.
[17] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, Ann. of Math., Vol. 78, NO. 2 (1963), 149–192.
[18] G. Shimura, Abelian varieties with complex multiplication and modular functions, Princeton Mathematical Series, 46. Princeton University Press, Princeton, NJ, 1998.
[19] B. Smith, Families of explicit isogenous Jacobians of variable-separated curves, London Mathematical Society: LMS Journal of Computation and Mathematics, 2011, 14, pp.179-199.
[20] A. Weil, Variétés abéliennes et courbes algébriques, Hermann & Cie., Paris, 1948.
[21] Wolfram Research, Inc., Mathematica, Version 7.0, Champaign, IL (2008).