ISOGENOUS ELLIPTIC SUBCOVERS OF GENUS TWO CURVES

L. BESHAJ, A. ELEZI, AND T. SHASKA

Abstract. We prove that for $N = 2, 3, 5, 7$ there are only finitely many genus two curves $\mathcal{X}$ (up to isomorphism) defined over $\mathbb{Q}$ with $(2,2)$-split Jacobian and $\mathrm{Aut}\,(\mathcal{X}) \cong V_4$, such that their elliptic subcovers are N-isogenous. Also, there are only finitely many genus two curves $\mathcal{X}$ (up to isomorphism) defined over $\mathbb{Q}$ with $(3,3)$-split Jacobian such that their elliptic subcovers are 5-isogenous.

1. Introduction

Genus 2 curves with (n,n)-decomposable Jacobians are the most studied type of genus 2 curves due to work of Jacobi, Hermite, et al. They provide examples of genus two curves with large Mordell-Weil rank of the Jacobian [13], many rational points [3], nice examples of descent [7], etc. Such curves have received new attention lately due to interest on their use on cryptographic applications and their suggested use on post-quantum crypto-systems and random self-reducibility of discrete logarithm problem; see [14] for details.

Let $\mathcal{X}$ be a genus 2 curve defined over an field k, K its function field, and $\psi : \mathcal{X} \to E$ a degree n maximal covering to an elliptic curve E defined over k. We call E a *degree n elliptic subcover* of $\mathcal{X}$. Degree n elliptic subcovers occur in pairs, say (E_1, E_2). It is well known that there is an isogeny of degree n^2 between the Jacobian $\mathrm{Jac}\,\mathcal{X}$ and the product $E_1 \times E_2$. Such curve $\mathcal{X}$ is said to have (n,n)-decomposable (or (n,n)-split) Jacobian. The focus of this paper is on the isogenies among the elliptic cures E_1 and E_2.

Let $n = 2$ or n an odd integer. The locus of genus 2 curves $\mathcal{X}$ with (n,n)-decomposable Jacobian, denoted by $\mathcal{L}_n$, is a 2-dimensional algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves; see [12] for details. Hence, we can get an explicit equation of $\mathcal{L}_n$ in terms of the Igusa invariants J_2, J_4, J_6, J_{10}; see [11] for $\mathcal{L}_2$, [9] for $\mathcal{L}_3$, and [6] for $\mathcal{L}_5$. There is a more recent paper on the subject [4] where results of [6, 9] are confirmed and equations for $n > 5$ are studied. One of the main questions that has been considered historically is: what is the number of elliptic subcovers for a genus 2 curve or equivalently a genus 2 field $e_n(K)$? For $n = 2$, $e_2(K)$ is the number of non-hyperelliptic involutions of the automorphism group $\mathrm{Aut}\,(K/k)$. In [9] it was shown that $e_3(K) = 0, 2$, or 4.

Consider the following question: how often are E_1 and E_2 isogenous to each other for $\mathcal{X}$ defined over $\mathbb{Q}$? In other words, for a fixed $n \geq 2$, such that n odd and for a fixed integer $N \geq 2$, how many genus 2 curves $\mathcal{X}$, defined over $\mathbb{Q}$, are there such that E_1 is N-isogenous to E_2? The focus of this paper is to answer this question for $n = 2$ and 3 and small N.

The case when $n = 2$ is very different from the case when n is odd. Since degree 2 coverings correspond to Galois extensions of function fields, the elliptic subcover is fixed by an involution in $\mathrm{Aut}\,(K/k)$. There is a group theoretic aspect of the

$n = 2$ case which was discussed in detail in [11]. The number of elliptic subcovers in this case correspond to the number of non-hyperelliptic involutions in $\mathrm{Aut}\,(K/k)$, which are called *elliptic involutions*. The equation of $\mathcal{X}$ is given by

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1$$

and in [2] it was shown that when defined over $\mathbb{Q}$ this equation is minimal. Hence, for $(s_1, s_2) \in k^2$, such that the corresponding discriminant is nonzero, we have a genus 2 curve $\mathcal{X}_{(s_1,s_2)}$ and two corresponding elliptic subcovers. Two such curves $(\mathcal{X}_{(s_1,s_2)}, \xi_{s_1,s_2})$ and $(\mathcal{X}_{(s_1',s_2')}, \xi_{s_1',s_2'})$ are isomorphic if and only if their dihedral invariants u and v are the same (cf. Section 2). Thus, the points $(s_1, s_2) \in k^2$ correspond to elliptic involutions of Aut $\mathcal{X}$ while the points $(u, v) \in k^2$ correspond to elliptic involutions of $\overline{\mathrm{Aut}}\ \mathcal{X}$ (see below for the notations used in this paper).

In Section 3 we prove that for $n = 2$ there are finitely many genus 2 curves $\mathcal{X}$ defined over $\mathbb{Q}$ with $\mathrm{Aut}\,(\mathcal{X}) \cong V_4$ whose elliptic components are N-isogenous for $N = 2, 3, 5, 7$. That $\mathcal{X}$ is defined over $\mathbb{Q}$ follows from the important fact that the invariants u and v are in the field of moduli of the curve $\mathcal{X}$ and that for every curve in $\mathcal{L}_2$, the field of moduli is a field of definition; see [5]. This is not necessarily true for curves in $\mathcal{L}_n$, when $n > 2$. However, a proof of the above result it is still possible using the computational approach by using invariants χ, ψ in [9]. The rest of the proof (see Theorem **??**) is computational; it is based on the fact that E_1 and E_2 are N-isogenous if and only if their j-invariants satisfy the modular polynomial $\phi_N(x, y)$. Expressing the $j_1 = j(E_1)$ and $j_2 = j(E_2)$ in terms of u and v and substituting them in the equation of the modular curve $X_0(N)$, reduces the problem in finding rational points on $X_0(N)$. For our purposes it is enough to show that such curve has genus $g \geq 2$.

In Section 4 we deal with the $n = 3$ case. The equation of $\mathcal{L}_3$ was computed in [9]. A birational parametrization of $\mathcal{L}_3$ was also found there in terms of the invariants r_1, r_2 of two cubics. These invariants are denoted by χ and ψ here. We are able to compute the j-invariants of E_1 and E_2 in terms of χ and ψ and find the conditions that χ and ψ must satisfy. Since ordered pairs (χ, ψ) are on a one to one correspondence with genus two curves with $(3, 3,)$-split Jacobians, then we try to determine pairs (χ, ψ) satisfying the equation of the modular curve $X_0(N)$. This case is different from $n = 2$ in that a rational ordered pair (χ, ψ) does not necessarily correspond to a genus two defined over $\mathbb{Q}$. However, a genus two curve defined over $\mathbb{Q}$ gives rise to rational invariants $\chi, \psi \in \mathbb{Q}$. Hence, it is enough to count the rational ordered pairs (χ, ψ) that satisfy the equation of the modular curve $X_0(N)$.

We are able to prove that for $N = 5$ there are only finitely many genus two curves $\mathcal{X}$ such that they have $(3, 3)$-split Jacobian and E_1 and E_2 are 5-isogenous. We could not prove such result for $N = 2, 3$, and 7 since the corresponding curve $X_0(\chi, \psi)$ has genus zero components in such cases. It remains open to further investigation if there is any theoretical interpretation of such surprising phenomena.

Notation: Throughout this paper $\mathcal{X}$ denotes a genus 2 curve defined over a field k and K its function field. By $G = \mathrm{Aut}\,(\mathcal{X})$ we denote the automorphism group of $\mathcal{X}$ or equivalently $\mathrm{Aut}\,(K/k)$. The elliptic involution of $\mathcal{X}$ is denoted by σ_0. The reduced automorphism group is denoted by $\bar{G} = \overline{\mathrm{Aut}}\,(\mathcal{X})$ and images of $\sigma \in G$ are $\bar{\sigma} \in \bar{G}$. Notice that an involution $\bar{\sigma} \in \bar{G}$ which comes from an elliptic involution $\sigma \in G$ is again called an elliptic involution in $\bar{G}$. The Jacobian of $\mathcal{X}$ is denoted by

$\mathrm{Jac}\,\mathcal{X}$ and by $X_0(N)$ we denote the modular curve of level N. By D_n we denote the dihedral group of order $2n$ and by V_4 the Klein 4-group.

2. Preliminaries

Throughout this section $\mathcal{X}$ is a genus 2 curve defined over an algebraically closed field k, $\mathrm{char}\, k = 0$, and K the function field of $\mathcal{X}$. Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a degree n covering from a curve $\mathcal{X}$ of genus 2 to an elliptic curve E_1; see [12] for the basic definitions. The covering $\psi_1 : \mathcal{X} \longrightarrow E_1$ is called a **maximal covering** if it does not factor through a nontrivial isogeny. A map of algebraic curves $f : X \to Y$ induces maps between their Jacobians $f^* : \mathrm{Jac}\, Y \to \mathrm{Jac}\, X$ and $f_* : \mathrm{Jac}\, X \to \mathrm{Jac}\, Y$. When f is maximal then f^* is injective and $\ker(f_*)$ is connected.

Let $\psi_1 : \mathcal{X} \longrightarrow E_1$ be a covering as above which is maximal. Then ${\psi^*}_1 : E_1 \to \mathrm{Jac}\,\mathcal{X}$ is injective and the kernel of $\psi_{1,*} : \mathrm{Jac}\,\mathcal{X} \to E_1$ is an elliptic curve which we denote by E_2. For a fixed Weierstrass point $P \in \mathcal{X}$, we can embed $\mathcal{X}$ to its Jacobian via

$$
\begin{aligned}
i_P : \mathcal{X} &\longrightarrow \mathrm{Jac}(\mathcal{X}) \\
x &\to [(x) - (P)]
\end{aligned}
\tag{1}
$$

Let $g : E_2 \to \mathrm{Jac}\,\mathcal{X}$ be the natural embedding of E_2 in $\mathrm{Jac}\,\mathcal{X}$, then there exists $g_* : \mathrm{Jac}\,\mathcal{X} \to E_2$. Define $\psi_2 = g_* \circ i_P : \mathcal{X} \to E_2$. So we have the following exact sequence

$$0 \to E_2 \xrightarrow{g} \mathrm{Jac}\,\mathcal{X} \xrightarrow{\psi_{1,*}} E_1 \to 0.$$

The dual sequence is also exact

$$0 \to E_1 \xrightarrow{\psi_1^*} \mathrm{Jac}\,\mathcal{X} \xrightarrow{g_*} E_2 \to 0.$$

If $\deg(\psi_1) = 2$ or it is an odd number then the maximal covering $\psi_2 : \mathcal{X} \to E_2$ is unique (up to isomorphism of elliptic curves). The Hurwitz space $\mathcal{H}_\sigma$ of such covers is embedded as a subvariety of the moduli space of genus two curves $\mathcal{M}_2$; see [9] for details. It is a 2-dimensional subvariety of $\mathcal{M}_2$ which we denote it by $\mathcal{L}_n$. An explicit equation for $\mathcal{L}_n$, in terms of the arithmetic invariants of genus 2 curves, can be found in [11] or [5] for $n = 2$, in [9] for $n = 3$, and in [6] for $n = 5$. From now on, we will say that a genus 2 curve $\mathcal{X}$ has an (n, n)-decomposable Jacobian if $\mathcal{X}$ is as above and the elliptic curves E_i, $i = 1, 2$ are called the components of $\mathrm{Jac}(\mathcal{X})$.

Consider the following question: how often are E_1 and E_2 isogenous to each other for $\mathcal{X}$ defined over $\mathbb{Q}$? In other words, for a fixed $n \geq 2$, such that n odd and for a fixed integer $N \geq 2$, how many genus 2 curves $\mathcal{X}$, defined over $\mathbb{Q}$, are there such that E_1 is N-isogenous to E_2? The focus of this paper is to answer this question for $n = 2, 3$ and small degree isogenies.

2.1. Genus 2 curves with degree 2 elliptic subcovers.

Notice that degree 2 coverings $\psi : \mathcal{X} \to E$ are Galois coverings. So it is enough to consider involutions in the automorphism group of $\mathcal{X}$ which fix genus one quotient spaces. However, the hyperelliptic involution fixes a genus zero quotient space and is unique. From Riemann-Hurwitz formula all other involutions must fix genus one quotient spaces. This leads to the following definitions.

Let $\mathcal{X}$ be a genus 2 curve, $\mathrm{Aut}\,(\mathcal{X})$ its automorphism group, σ_0 the hyperelliptic involution, and $\overline{\mathrm{Aut}}\,(\mathcal{X}) := \mathrm{Aut}\,(\mathcal{X})/\langle\sigma_0\rangle$ the reduced automorphism group. If $\mathrm{Aut}\,(\mathcal{X})$ has another involution σ_1, then the quotient space $\mathcal{X}/\langle\sigma_1\rangle$ has genus one.

We call such involution an *elliptic involution*. There is another elliptic involution $\sigma_2 := \sigma_0 \, \sigma_1$. So the elliptic involutions come naturally in pairs. The corresponding coverings $\psi_i : \mathcal{X} \to \mathcal{X}/\langle \sigma_i \rangle$, $i = 1, 2$, are the maximal covers as above and $E_i := \mathcal{X}/\langle \sigma_i \rangle$ the elliptic subcovers of $\mathcal{X}$ of degree 2. Also the corresponding Hurwitz space of such coverings is an irreducible algebraic variety which is embedded into $\mathcal{M}_2$. We denote its image in $\mathcal{M}_2$ by $\mathcal{L}_2$.

An involution in $\overline{\mathrm{Aut}}\,(\mathcal{X})$ is called an **elliptic involution** in $\overline{\mathrm{Aut}}\,(\mathcal{X})$ if it is an image of an elliptic involution from $\mathrm{Aut}\,(\mathcal{X})$. We will consider pairs (K, β) with K a genus 2 field and β an elliptic involution in $\bar{G}$. Two such pairs (K, β) and (K', β') are called isomorphic if there is a k-isomorphism $\alpha : K \to K'$ with $\beta' = \alpha \beta \alpha^{-1}$. The following was proved in [11].

Lemma 1. *Let $\mathcal{X}$ be a genus 2 curve and σ_0 its hyperelliptic involution. If σ_1 is an elliptic involution of $\mathcal{X}$, then so is $\sigma_2 = \sigma_1 \sigma_0$. Moreover, $\mathcal{X}$ is isomorphic to a curve with affine equation*

$$Y^2 = X^6 - s_1 X^4 + s_2 X^2 - 1 \tag{2}$$

for some $s_1, s_2 \in k$ and $\Delta_{\sigma_1, \sigma_2} := 27 - 18 s_1 s_2 - s_1^2 s_2^2 + 4 s_1^3 + 4 s_2^3 \neq 0$. The equations for the elliptic subcovers $E_i = \mathcal{X}/\langle \sigma_i \rangle$, for $i = 1, 2$, are given by

$$E_1 : \; y^2 = x^3 - s_1 x^2 + s_2 x - 1, \quad \textit{and} \quad E_2 : \; y^2 = x\,(x^3 - s_1 x^2 + s_2 x - 1)$$

Our main goal of the next section is to determine when E_1 and E_2 are isogenous.

In [11] it was shown that $\mathcal{X}$ is determined up to a coordinate change by the subgroup $H \cong D_3$ of $SL_2(k)$ generated by $\tau_1 : X \to \xi_6 X$, $\tau_2 : X \to \frac{1}{X}$, where ξ_6 is a primitive 6-th root of unity. Let $\xi_3 := \xi_6^2$. The coordinate change by τ_1 replaces s_1 by $\xi_3 s_2$ and s_2 by $\xi_3^2 s_2$. The coordinate change by τ_2 switches s_1 and s_2. Invariants of this H-action are:

$$u := s_1 s_2, \quad v := s_1^3 + s_2^3 \tag{3}$$

Let $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ be the absolute Igusa invariants as in [7] or in [5]. Then we have the following:

Proposition 1. *The mapping*

$$A : (u, v) \longrightarrow (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3),$$

gives a birational parametrization of $\mathcal{L}_2$. The fibers of A of cardinality > 1 correspond to those curves $\mathcal{X}$ with $|\,\mathrm{Aut}\,(\mathcal{X})| > 4$.

Proof. See [11] for the details. □

The map

$$(s_1, s_2) \mapsto (u, v),$$

is a branched Galois covering with group S_3 of the set $\{(u, v) \in k^2 : \Delta(u, v) \neq 0\}$ by the corresponding open subset of s_1, s_2-space if $\mathrm{char}(k) \neq 3$. In any case, it is true that if s_1, s_2 and s_1', s_2' have the same u, v-invariants then they are conjugate under $\langle \tau_1, \tau_2 \rangle$.

Lemma 2. *For $(s_1, s_2) \in k^2$ with $\Delta \neq 0$, equation (2) defines a genus 2 field $K_{s_1, s_2} = k(X, Y)$. Its reduced automorphism group contains the elliptic involution $\xi_{s_1, s_2} : X \mapsto -X$. Two such pairs $(K_{s_1, s_2}, \xi_{s_1, s_2})$ and $(K_{s_1', s_2'}, \xi_{s_1', s_2'})$ are isomorphic if and only if $u = u'$ and $v = v'$ (where u, v and u', v' are associated with s_1, s_2 and s_1', s_2', respectively, by (3)).*

However, the ordered pairs (u, v) classify the isomorphism classes of such elliptic subfields as it can be seen from the following theorem proved in [11].

Theorem 1. *i) The $(u, v) \in k^2$ with $\Delta \neq 0$ bijectively parameterize the isomorphism classes of pairs (K, ξ) where K is a genus 2 field and ξ an elliptic involution of $\overline{\mathrm{Aut}}\,(K)$. This parametrization is defined in Lemma 2.*

ii) The (u, v) satisfying additionally

$$(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0 \tag{4}$$

bijectively parameterize the isomorphism classes of genus 2 fields with $\mathrm{Aut}\,(K) \cong V_4$*; equivalently, genus 2 fields having exactly 2 elliptic subfields of degree 2.*

Our goal in the next section is to investigate when the pairs of elliptic subfields K_{s_1,s_2} (respectively isomorphism classes (K, ξ)) are isogenous. We want to find if that happens when $\mathcal{X}$ is defined over $\mathbb{Q}$. Hence, the following result is crucial.

Lemma 3. *Let $\mathcal{X}$ be a genus 2 curve with $(2, 2)$-decomposable Jacobian and E_i, $i = 1, 2$ its elliptic components. Then $\mathcal{X}$ is defined over $\mathbb{Q}$ if and only if $u, v \in \mathbb{Q}$.*

See [10] for details, where an explicit equation of $\mathcal{X}$ is provided with coefficients in $\mathbb{Q}(u, v)$ or [5] for a more general setup.

3. Isogenies between elliptic subcovers

Next we study pairs of degree 2 elliptic subfields of $\mathcal{X}$ which are isogenous. We denote by $\phi_N(x, y)$ the N-th modular polynomial. Two elliptic curves with j-invariants j_1 and j_2 are n-isogenous if and only if $\phi_N(j_1, j_2) = 0$. The equation $\phi_N(x, y) = 0$ is the canonical equation of the modular curve $X_0(N)$. We display $\phi_N(x, y)$ for $N = 2, 3$.

$$\begin{aligned}
\phi_2 &= x^3 - x^2y^2 + y^3 + 1488xy(x + y) + 40773375xy - 162000(x^2 + y^2)\\
&\quad + 8748000000(x + y) - 157464000000000\\
\phi_3 &= -x^3y^3 + 2232x^3y^2 + 2232y^3x^2 + x^4 - 1069956x^3y + 2587918086x^2y^2\\
&\quad - 1069956y^3x + y^4 + 36864000x^3 + 8900222976000x^2y + 8900222976000y^2x\\
&\quad + 36864000y^3 + 452984832000000x^2 - 770845966336000000xy + 452984832000000y^2\\
&\quad + 1855425871872000000000x + 1855425871872000000000y
\end{aligned}$$

Notice that all polynomials $\phi_n(x, y)$ are symmetric in x and y, as expected. We denote $s = x + y$ and $t = xy$ and express $\phi_n(x, y)$ in terms of $\phi_n(s, t)$. Such expressions are much simpler and more convenient for our computations.

$$\begin{aligned}
\phi_2(s, t) &= s^3 - 162000s^2 + 1485\,ts - t^2 + 8748000000\,s + 41097375\,t - 157464000000000\\
\phi_3(s, t) &= s^4 + 36864000s^3 - 1069960s^2t + 2232\,st^2 - t^3 + 452984832000000s^2\\
&\quad + 8900112384000\,ts + 2590058000\,t^2 + 1855425871872000000000\,s\\
&\quad - 771751936000000000\,t
\end{aligned}$$

Let j_1 and j_2 denote the j-invariants of the elliptic curves E_1 and E_2 from Lemma 1. Then j-invariants of elliptic subcovers are given by

$$j_1 = -256\,\frac{\left({s_1}^2 - 3\,s_2\right)^3}{-{s_1}^2{s_2}^2 + 4\,{s_1}^3 + 4\,{s_2}^3 - 18\,s_1\,s_2 + 27}$$
$$j_2 = 256\,\frac{\left(-{s_2}^2 + 3\,s_1\right)^3}{-{s_1}^2{s_2}^2 + 4\,{s_1}^3 + 4\,{s_2}^3 - 18\,s_1\,s_2 + 27}$$

We have the following.

Proposition 2. *Let $\mathcal{X}$ be a genus 2 curve with $(2,2)$-decomposable Jacobian and E_i, $i = 1,2$ its elliptic components. There is a one to one correspondence between genus 2 curves $\mathcal{X}$ defined over $\mathbb{Q}$ such that there is a degree N isogeny $E_1 \to E_2$ and rational points on the modular curve $X_0(N)$ given in terms of u and v.*

Proof. If $\mathcal{X}$ is defined over $\mathbb{Q}$ then the corresponding $(u,v) \in \mathbb{Q}^2$ since they are in the field of moduli of $\mathcal{X}$. Conversely, if u and v satisfy the equation of $X_0(N)$ then we can determine the equation of $\mathcal{X}$ in terms of u and v as in [10].

□

Let us now explicitly check whether elliptic subfields of K are isogenous to each other. First we focus on the d-dimensional loci, for $d \geq 1$.

Theorem 2. *For $N = 2,3,5,7$ there are only finitely many curves $\mathcal{X}$ defined over $\mathbb{Q}$ with $(2,2)$-decomposable Jacobian and $\mathrm{Aut}\,(\mathcal{X}) \cong V_4$ such that E_1 is N-isogenous to E_2.*

Proof. Let us know check if elliptic subfields are isogenous for $N = 2,3,5,7$. By replacing j_1, j_2 in the modular curve we get a curve

$$F(s_1, s_2) = 0$$

This curve is symmetric in s_1 and s_2 and fixed by the H-action of Lem. 1. Therefore, such curve can be written in terms of the u and v,

$$G_N(u,v) = 0.$$

We display all the computations below.

Let $N = 2$. $G_2(u,v)$ is

$$G_2(u,v) = f_1(u,v) \cdot f_2(u,v)$$

where f_1 and f_2 are

$$\begin{split} f_1 = -16v^3 - 81216v^2 - 892296v - 2460375 + 3312uv^2 + 707616vu + 3805380u + \\ 18360vu^2 - 1296162u^2 - 1744u^3v - 140076u^3 + 801u^4 + 256u^5 \end{split} \tag{5}$$

$$\begin{split} f_2 = {} & 4096u^7 + 256016u^6 - 45824u^5v + 4736016u^5 - 2126736vu^4 + 23158143u^4 \\ & - 25451712u^3v - 119745540u^3 + 5291136v^2u^2 - 48166488vu^2 - 2390500350u^2 \\ & - 179712uv^3 + 35831808uv^2 + 1113270480vu + 9300217500u - 4036608v^3 \\ & - 1791153000v - 8303765625 - 1024v^4 + 163840u^3v^2 - 122250384v^2 + 256u^2v^3 \end{split} \tag{6}$$

Notice that each one of these components has genus $g \geq 2$ and therefore only finitely many rational points.

Let $N = 3$. Then, from equation (10) and $\phi_3(j_1, j_2) = 0$ we have:

$$(4v - u^2 + 110u - 1125) \cdot g_1(u,v) \cdot g_2(u,v) = 0 \tag{7}$$

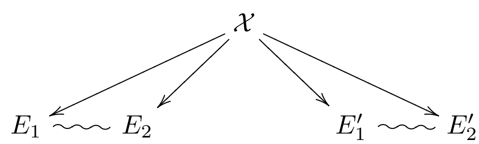

FIGURE 1. Elliptic subcovers for $\mathcal{X}$, when $\mathrm{Aut}\,(\mathcal{X}) \cong D_4$

where g_1 and g_2 are

$$
\begin{aligned}
g_1 = & -27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^3v^2 - 6692v^3u - 1755067500u \\
& + 2419308v^3 - 34553439u^4 + 127753092vu^2 + 16274844vu^3 - 1720730u^2v^2 \\
& - 1941120u^5 + 381631500v + 1018668150u^2 - 116158860u^3 + 52621974v^2 \\
& + 387712u^4v - 483963660vu - 33416676v^2u + 922640625
\end{aligned} \tag{8}
$$

$$
\begin{aligned}
g_2 = & \ 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^4v^2 + 17032u^5v^2 \\
& + 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478v^4u \\
& - 77908736u^5v + 9516699v^4 + 307234984u^3v^2 - 419583744v^3u - 826436736v^3 \\
& + 27502903296u^4 + 28808773632vu^2 - 23429955456vu^3 + 5455334016u^2v^2 \\
& - 41278242816v + 82556485632u^2 - 108737593344u^3 - 12123095040v^2 \\
& + 41278242816vu + 3503554560v^2u + 5341019904u^5 - 2454612480u^4v
\end{aligned} \tag{9}
$$

Thus, there is a isogeny of degree 3 between E_1 and E_2 if and only if u and v satisfy equation (7). The vanishing of the first factor is equivalent to $G \cong D_6$. So, if $Aut(\mathbb{C}) \cong D_6$ then E_1 and E_2 are isogenous of degree 3. The other factors are curves of genus $g \geq 2$ and therefore they have only finitely many rational points.

For cases $N = 5, 7$ we only get one irreducible component, which in both cases is a curve of genus $g \geq 2$. We don't display those equations here. This completes the proof.

□

Next we consider the case when $|\,\mathrm{Aut}\,(\mathcal{X})| > 4$. First notice that the invariants j_1 and j_2 are roots of the quadratic

$$
x^2 - sx + t = 0, \tag{10}
$$

where

$$
\begin{aligned}
s &:= j_1 + j_2 = -2^8 \cdot \frac{(2u^3 - 54u^2 + 9uv - v^2 + 27v)}{(u^2 + 18u - 4v - 27)} \\
t &:= j_1 j_2 = 2^{16} \cdot \frac{(3v - u^2 - 9u)^3}{(u^2 + 18u - 4v - 27)^2}
\end{aligned} \tag{11}
$$

If $G \cong D_4$, then σ_1 and σ_2 are in the same conjugacy class. There are again two conjugacy classes of elliptic involutions in G. Thus, there are two degree 2 elliptic subfields (up to isomorphism) of K. One of them is determined by double root j of the Eq. (10), for $v^2 - 4u^3 = 0$. Next, we determine the j-invariant j' of the other degree 2 elliptic subfield and see how it is related to j.

If $v^2 - 4u^3 = 0$ then $\bar{G} \cong V_4$ and the set of Weierstrass points

$$
\mathcal{W} = \{\pm 1, \pm\sqrt{a}, \pm\sqrt{b}\}.
$$

Then, $s_1 = a + \frac{1}{a} + 1 = s_2$. Involutions of $\mathcal{X}$ are $\tau_1 : X \to -X$, $\tau_2 : X \to \frac{1}{X}$, $\tau_3 : X \to -\frac{1}{X}$. Since τ_1 and τ_3 fix no points of $\mathcal{W}$ the they lift to involutions in G. They each determine a pair of isomorphic elliptic subfields. The j-invariant of elliptic subfield fixed by τ_1 is the double root of Eq. (10), namely

$$j = 256 \frac{v^3}{v+1}. \tag{12}$$

To find the j-invariant of the elliptic subfields fixed by τ_3 we look at the degree 2 covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, such that $\phi(\pm 1) = 0$, $\phi(a) = \phi(-\frac{1}{a}) = 1$, $\phi(-a) = \phi(\frac{1}{a}) = -1$, and $\phi(0) = \phi(\infty) = \infty$. This covering is, $\phi(X) = \frac{\sqrt{a}}{a-1} \frac{X^2-1}{X}$. The branch points of ϕ are $q_i = \pm \frac{2i\sqrt{a}}{\sqrt{a-1}}$. From lemma 1 the elliptic subfields E_1' and E_2' have 2-torsion points $\{0, 1, -1, q_i\}$. The j-invariants of E_1' and E_2' are

$$j' = -16 \frac{(v-15)^3}{(v+1)^2}. \tag{13}$$

Then, we have the following result.

Proposition 3. *Let $\mathcal{X}$ be a genus 2 curve with* $\operatorname{Aut}(\mathcal{X}) \cong D_4$ *and E_i, E_i', $i = 1, 2$, as above. Then E_i is 2-isogenous with E_i' and there are only finitely many genus 2 curves $\mathcal{X}$ defined over $\mathbb{Q}$ such that E_i is N-isogenous to E_i' for $N = 3, 5, 7$.*

Proof. By substituting j and j' into the $\phi_N(x, y) = 0$ we get that

$$\begin{aligned}
\phi_2(j, j') &= 0 \\
\phi_3(j, j') &= (v^2 + 138v + 153)(v + 5)^2(v^2 - 70v - 55)^2 \,(256v^4 + 240v^3 + 191745v^2 \\
&\quad + 371250v + 245025)(4096v^6 - 17920v^5 + 55909200v^4 - 188595375v^3 \\
&\quad - 4518125v^2 + 769621875v + 546390625)
\end{aligned}$$

We don't display the $\phi_5(j, j')$ and $\phi_7(j, j')$, but they are high genus curves. This completes the proof.

□

4. Genus 2 curves with degree 3 elliptic subcovers

In this section we focus on genus 2 curves with $(3,3)$-split Jacobians. This case was studied in detail in[9]. The main theorem was:

Theorem 3. *Let K be a genus 2 field and $e_3(K)$ the number of* $\operatorname{Aut}(K/k)$*-classes of elliptic subfields of K of degree 3. Then;*

i) $e_3(K) = 0, 1, 2,$ or 4

ii) $e_3(K) \geq 1$ if and only if the classical invariants of K satisfy the irreducible equation $F(J_2, J_4, J_6, J_{10}) = 0$ displayed in [9, Appendix A].

There are exactly two genus 2 curves (up to isomorphism) with $e_3(K) = 4$. The case $e_3(K) = 1$ (resp., 2) occurs for a 1-dimensional (resp., 2-dimensional) family of genus 2 curves, see [9]. We focus on the 2-dimensional family, since the cases $e_3(K) = 1$ is the singular locus of the case $e_3(K) = 2$ studied in detail in [1]. Most of the basic definitions are taken from [7] or [8].

Definition 1. *A* **non-degenerate pair** *(resp.,* **degenerate pair***) is a pair $(\mathcal{C}, \mathcal{E})$ such that $\mathcal{C}$ is a genus 2 curve with a degree 3 elliptic subcover $\mathcal{E}$ where $\psi : \mathcal{C} \to \mathcal{E}$ is ramified in two (resp., one) places. Two such pairs $(\mathcal{C}, \mathcal{E})$ and $(\mathcal{C}', \mathcal{E}')$ are called isomorphic if there is a k-isomorphism $\mathcal{C} \to \mathcal{C}'$ mapping $\mathcal{E} \to \mathcal{E}'$.*

If $(\mathcal{C}, \mathcal{E})$ is a non-degenerate pair, then $\mathcal{C}$ can be parameterized as follows

$$Y^2 = (\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1)\,(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1), \tag{14}$$

where $\mathfrak{u}, \mathfrak{v} \in k$ and the discriminant

$$\Delta = -16\,\mathfrak{v}^{17}\,(\mathfrak{v} - 27)\,(27\mathfrak{v} + 4\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{u}\mathfrak{v})^3$$

of the sextic is nonzero. We let $R := (27\mathfrak{v} + 4\mathfrak{v}^2 - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{u}\mathfrak{v}) \neq 0$. For $4\mathfrak{u} - \mathfrak{v} - 9 \neq 0$ the degree 3 coverings are given by $\phi_1(X, Y) \to (U_1, V_1)$ and $\phi_2(X, Y) \to (U_2, V_2)$ where

$$\begin{aligned}
& U_1 = \frac{\mathfrak{v} X^2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \quad U_2 = \frac{(\mathfrak{v} X + 3)^2\,(\mathfrak{v}(4\mathfrak{u} - \mathfrak{v} - 9)X + 3\mathfrak{u} - \mathfrak{v})}{\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)}, \\
& V_1 = Y\,\frac{\mathfrak{v}^2 X^3 - \mathfrak{v} X - 2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1}, \\
& V_2 = (27 - \mathfrak{v})^{\frac{3}{2}}\,Y\,\frac{\mathfrak{v}^2(\mathfrak{v} - 4\mathfrak{u} + 8)X^3 + \mathfrak{v}(\mathfrak{v} - 4\mathfrak{u})X^2 - \mathfrak{v} X + 1}{(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)^2}
\end{aligned} \tag{15}$$

and the elliptic curves have equations:

$$\begin{aligned}
\mathcal{E}: &\quad V_1^2 = R\,U_1^3 - (12\mathfrak{u}^2 - 2\mathfrak{u}\mathfrak{v} - 18\mathfrak{v})U_1^2 + (12\mathfrak{u} - \mathfrak{v})U_1 - 4 \\
\mathcal{E}': &\quad V_2^2 = c_3 U_2^3 + c_2 U_2^2 + c_1 U_2 + c_0
\end{aligned} \tag{16}$$

where

$$\begin{aligned}
c_0 &= -(9\mathfrak{u} - 2\mathfrak{v} - 27)^3 \\
c_1 &= (4\mathfrak{u} - \mathfrak{v} - 9)\,(729\mathfrak{u}^2 + 54\mathfrak{u}^2\mathfrak{v} - 972\mathfrak{u}\mathfrak{v} - 18\mathfrak{u}\mathfrak{v}^2 + 189\mathfrak{v}^2 + 729\mathfrak{v} + \mathfrak{v}^3) \\
c_2 &= -\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)^2\,(54\mathfrak{u} + \mathfrak{u}\mathfrak{v} - 27\mathfrak{v}) \\
c_3 &= \mathfrak{v}^2\,(4\mathfrak{u} - \mathfrak{v} - 9)^3
\end{aligned} \tag{17}$$

The mapping $k^2 \setminus \{\Delta = 0\} \to \mathcal{L}_3$ such that

$$(\mathfrak{u}, \mathfrak{v}) \to (i_1, i_2, i_3)$$

has degree 2. The invariants of two cubics, called r_1 and r_2 in [9], defined as

$$\begin{aligned}
\chi &= 27\frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^3}{4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3} \\
\psi &= -1296\frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^4}{(\mathfrak{v} - 27)(4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3)},
\end{aligned}$$

uniquely determine the isomorphism class of curves in $\mathcal{L}_3$.

4.1. **Elliptic subcovers.**

We express the j-invariants j_i of the elliptic subfields E_i of K, from Eq. (16), in terms of u and v as follows:

$$\begin{aligned}
j_1 &= 16\mathfrak{v}\frac{(\mathfrak{v}\mathfrak{u}^2 + 216\mathfrak{u}^2 - 126\mathfrak{v}\mathfrak{u} - 972\mathfrak{u} + 12\mathfrak{v}^2 + 405\mathfrak{v})^3}{(\mathfrak{v} - 27)^3(4\mathfrak{v}^2 + 27\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{v}\mathfrak{u} - \mathfrak{v}\mathfrak{u}^2)^2} \\
j_2 &= -256\frac{(\mathfrak{u}^2 - 3\mathfrak{v})^3}{\mathfrak{v}(4\mathfrak{v}^2 + 27\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{v}\mathfrak{u} - \mathfrak{v}\mathfrak{u}^2)}
\end{aligned} \tag{18}$$

where $\mathfrak{v} \neq 0, 27$. Moreover, we can express $s = j_1 + j_2$ and $t = j_1 j_2$ in terms of the χ and ψ invariants as follows:

Lemma 4. *The j-invariants of the elliptic subfields satisfy the following quadratic equations over $k(\chi, \psi)$;*

$$j^2 - s\,j + t = 0 \tag{19}$$

where

$$\begin{aligned}
s =& \frac{1}{16777216\psi^3\chi^8}\big(1712282664960\psi^3\chi^6 + 1528823808\psi^4\chi^6 + 49941577728\psi^4\chi^5 \\
&- 38928384\psi^5\chi^5 - 258048\psi^6\chi^4 + 12386304\psi^6\chi^3 + 901736973729792\psi\chi^{10} \\
&+ 966131712\psi^5\chi^4 + 16231265527136256\chi^{10} + 480\psi^8\chi + 101376\psi^7\chi^2 \\
&+ 479047767293952\psi\chi^8 + 7827577896960\psi^2\chi^9 + 2705210921189376\chi^9 \\
&+ 21641687369515008\chi^{12} + 32462531054272512\chi^{11} + \psi^9 \\
&+ 619683250176\psi^3\chi^7 + 1408964021452800\psi\chi^9 + 45595641249792\psi^2\chi^8 \\
&+ 7247757312\psi^3\chi^8 + 37572373905408\psi^2\chi^7\big) \\
t =& -\frac{1}{68719476736\chi^{1}2\psi^3}\big(84934656\chi^5 + 1179648\chi^4\psi - 5308416\chi^4 \\
&-442368\chi^3\psi - 13824\chi^2\psi^2 - 192\chi\psi^3 - \psi^4\big)^3
\end{aligned} \tag{20}$$

Proof. Substitute j_1 and j_2 as in Eq. (18) in equation Eq. (19). ☐

The computation of the above equation is rather involved; see [9] or [8] for details. Notice that if $\mathcal{C}$ is defined over $\mathbb{Q}$ then $\chi, \psi \in \mathbb{Q}$. The converse is not necessarily true.

In an analogous way with the case $n = 2$ we will study the locus $\phi_N(x, y) = 0$ which represents the modular curve $X_0(N)$. For N prime, two elliptic curves E_1, E_2 are N-isogenous if and only if $\phi_N(j(E_1), j(E_2)) = 0$. We will consider the case when $N = 2, 3, 5$, and 7. We will omit part of the formulas since they are big to display.

Proposition 4. *Let $\mathcal{C}$ be a genus 2 curve with $(3,3)$-split Jacobian and E_1, E_2 its elliptic subcovers. There are only finitely many genus 2 curves $\mathcal{X}$ defined over $\mathbb{Q}$ such that E_1 is 5-isogenous to E_2.*

Proof. Let $\phi_5(x, y)$ be the modular polynomial of level 5. As in the previous section, we let $s = x + y$ and $t = xy$. Then, $\phi_5(x, y)$ can be written in terms of s, t. We replace s and t by expressions in Eq. (20). We get a curve in χ, ψ of genus 169. From Faltings theorem there are only finitely many rational points (χ, ψ). Since, $\mathbb{Q}(\chi, \psi)$ is the field of moduli of $\mathcal{C}$, then $\mathcal{C}$ can not be defined over $\mathbb{Q}$ if χ, ψ are not in $\mathbb{Q}$. This completes the proof.

☐

Let us now consider the other cases. If $N = 2$, then the curve $\phi_2(s, t)$ can be expressed in terms of the invariants χ, ψ and computations show that the locus $\phi_2(\chi, \psi)$ becomes

$$g_1(\chi, \psi) \cdot g_2(\chi, \psi) = 0,$$

where $g_1(\chi, \psi) = 0$ is a genus zero component given by

(21)

$$\begin{aligned}
&\psi^9 + 10820843684757504\,\chi^{12} + 16231265527136256\,\chi^{11} + 4057816381784064\,\chi^{10}\psi \\
&+2348273369088\,\chi^8\psi^3 + 8115632763568128\,\chi^{10} + 253613523861504\,\chi^9\psi \\
&-1834588569600\,\chi^7\psi^3 - 45864714240\,\chi^6\psi^4 - 525533184\,\chi^5\psi^5 - 2322432\,\chi^4\psi^6 \\
&+1352605460594688\,\chi^9 + 253613523861504\,\chi^8\psi + 21134460321792\,\chi^7\psi^2 \\
&+32105299968\,\chi^5\psi^4 + 668860416\,\chi^4\psi^5 + 9289728\,\chi^3\psi^6 + 82944\,\chi^2\psi^7 + 432\,\chi\psi^8 \\
&+190210142896128\,\chi^9\psi^2 - 26418075402240\,\chi^8\psi^2 + 1027369598976\,\chi^6\psi^3 = 0,
\end{aligned}$$

while the other component has genus $g = 29$. To conclude about the number of 2-isogenies between E_1 and E_2 we have to check for rational points in the conic $g_1(\chi, \psi) = 0$.

The computations for the case $N = 3$ shows similar results. The locus $\phi_3(\chi, \psi)$ becomes

$$g_1(\chi, \psi) \cdot g_2(\chi, \psi) = 0,$$

where $g_1(\chi, \psi) = 0$ is a genus zero component and $g_2(\chi, \psi) = 0$ is a curve with singularities.

Also the case $N = 7$ show that the curve $\phi_7(\chi, \psi)$ becomes

$$g_1(\chi, \psi) \cdot g_2(\chi, \psi) = 0,$$

where $g_1(\chi, \psi) = 0$ is a genus zero component and $g_2(\chi, \psi) = 0$ is a genus one curve. Summarizing we have the following remark.

Remark 1. *Let $\mathcal{C}$ be a genus 2 curve with $(3,3)$-split Jacobian and E_1, E_2 its elliptic subcovers. There are possibly infinite families of genus 2 curves $\mathcal{X}$ defined over $\mathbb{Q}$ such that E_1 is 5-isogenous to E_2, when $N = 2, 3, 7$.*

As a final remark we would like to mention that we can perform similar computations for $n = 5$ by using the equation of $\mathcal{L}_5$ as computed in [6]. One can possibly even investigate cases for $n > 5$ by using results of [4]. However, the computations will be much more complicated.

References

[1] Lubjana Beshaj, *Singular locus on the space of genus 2 curves with decomposable Jacobians*, Albanian J. Math. **4** (2010), no. 4, 147–160. MR2755393

[2] L. Beshaj, *Minimal weierstrass equations for genus 2 curves* (2016), available at 1612.08318.

[3] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364. MR1748483

[4] Abhinav Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, Res. Math. Sci. **2** (2015), Art. 24, 46. MR3427148

[5] A. Malmendier and T. Shaska, *A universal genus-two curve from Siegel modular forms* (201607), available at 1607.08294.

[6] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800

[7] Tony Shaska, *Genus 2 curves with (3,3)-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218. MR2041085

[8] ———, *Genus two curves with many elliptic subcovers*, Comm. Algebra **44** (2016), no. 10, 4450–4466, DOI 10.1080/00927872.2015.1027365. MR3508311

[9] T. Shaska, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100

[10] ———, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, 2005, pp. 206–231. MR2182041

[11] T. Shaska and H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 2004, pp. 703–723. MR2037120

[12] T. Shaska, *Curves of genus 2 with* (n, n)*–decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706

[13] Tetsuji Shioda, *Genus two curves over* $\mathbf{Q}(t)$ *with high rank*, Comment. Math. Univ. St. Paul. **46** (1997), no. 1, 15–21. MR1448471

[14] Katsuyuki Takashima, *Efficient algorithms for isogeny sequences and their cryptographic applications*, Mathematical modelling for next-generation cryptography, 2018, pp. 97–114.

Department of Mathematical Sciences, United States Military Academy at West Point, West Point, NY, 10996.

E-mail address: `Lubjana.Beshaj@usma.edu`

Department of Mathematics and Statistics, American University, 4400 Mass. Ave., NW, Washington DC, 20016.

E-mail address: `aelezi@american.edu`

Department of Mathematics, Oakland University, Rochester, MI, 48309-4485.

E-mail address: `shaska@oakland.edu`