# ISOGENOUS COMPONENTS OF JACOBIAN SURFACES

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

Abstract. Let $\mathcal{C}$ be a genus 2 curve defined over a field $K$, $\operatorname{char} K = p \geq 0$, and $\operatorname{Jac}(\mathcal{C}, \iota)$ its Jacobian, where $\iota$ is the principal polarization of $\operatorname{Jac}(\mathcal{C})$ attached to $\mathcal{C}$. Assume that $\operatorname{Jac}(\mathcal{C})$ is $(n, n)$- geometrically reducible with $E_1$ and $E_2$ its elliptic components. We prove that there are only finitely many curves $\mathcal{C}$ (up to isomorphism) defined over $K$ such that $E_1$ and $E_2$ are $N$-isogenous for $n = 2$ and $N = 2, 3, 5, 7$ with $\operatorname{Aut}(\operatorname{Jac} \mathcal{C}) \cong V_4$ or $n = 2$, $N = 3, 5, 7$ with $\operatorname{Aut}(\operatorname{Jac} \mathcal{C}) \cong D_4$. The same holds if $n = 3$ and $N = 5$. Furthermore, we determine the Kummer and the Shioda-Inose surfaces for the above $\operatorname{Jac} \mathcal{C}$ and show how such results in positive characteristic $p > 2$ suggest nice applications in cryptography.

## 1. Introduction

An Abelian variety $\mathcal{A}$, defined over a field $k$, is simple if it has no proper non-zero Abelian subvariety over $k$. $\mathcal{A}$ is called reducible (or decomposable) if it is isogenous to a direct product of Abelian varieties. We call $\mathcal{A}$ geometrically simple (or absolutely simple) if it is simple over the algebraic closure of $k$, analogously $\mathcal{A}$ is geometrically reducible when it is reduced over the algebraic closure of $k$. A 2-dimensional Jacobian variety is geometrically reducible if and only if it is $(n, n)$-decomposable for some $n > 1$. Reducible Jacobian varieties have been studied extensively since the XIX-century, most notably by Friecke, Clebch, and Bolza. In the late XX-century they became the focus of many mathematicians through the work of Frey [7, 8], Shaska and Völklein [17, 24, 27], Kumar [13] and many others. If $\mathcal{A}/k$ is a 2-dimensional reducible Jacobian variety defined over a field $k$, then there is a degree $n^2$ isogeny to a product $\mathcal{A} \cong E_1 \times E_2$, where $E_i$, $i = 1, 2$ are 1-dimensional. The main focus of this paper is to investigate when $E_1$ and $E_2$ are isogenous to each other and how often does this occurs for a fixed $n$?

The question has received attention lately for different reasons. In [14] the authors were able to determine the rank of the Mordell-Weil rank of elliptic fibrations $F^{(i)}$, for $i = 1, \ldots, 6$; when $E_1$ and $E_2$ were isogenous and show that in this case both $F^5$ and $F^6$ have rank 18. In recent developments in supersingular isogeny based cryptography (SIDH) Costello [4] focuses on the $(2, 2)$ reducible Jacobians, where the addition is done via the Kummer surface. More importantly, it seems as the most interesting case is exactly the case when $E_1$ is isogenous to $E_2$. In this case, since the decomposition of the Abelian varieties is determined up to isogeny, the 2-dimensional Jacobian is isogenous to $E^2$. There are several interesting questions that arise when we consider such Jacobians over the finite field $\mathbb{F}_p$.

The focus of this paper is to investigate when the two elliptic components of the $(n, n)$ reducible 2-dimensional Jacobians are isogenous to each other. The space of genus 2 curves with $(n, n)$ reducible Jacobians, for $n = 2$ or $n$ is odd is a 2-dimensional irreducible locus $\mathcal{L}_n$ in the moduli space of curves $\mathcal{M}_2$. For $n = 2$

this is the well known locus of curves with extra involutions [19, 20, 27], for $n$ odd such spaces were computed for the first time in [22], [24], [17]. If $E_1$ and $E_2$ are $N$-isogenous then their $j$-invariants $j_1$ and $j_2$ satisfy the equation of the modular curve $X_0(N)$, say $\mathcal{S}_N := \phi_N(j_1, j_2) = 0$. Such curve can be embedded in $\mathcal{M}_2$. So we want to study the intersection between $\mathcal{L}_n$ and $\mathcal{S}_N$ for given $n$ and $N$. More precisely, for any number field $K$ we want to determine the number of $K$-rational points of this intersection.

Our approach is computational. We will focus on the cases when $n = 2, 3$ and $N = 2, 3, 5, 7$. We prove that for $n = 2$ and $N = 2, 3, 5, 7$ there are only finitely many curves $\mathcal{C}$ defined over $K$ such that $E_1$ and $E_2$ are $N$-isogenous, unless $\mathrm{Aut}\,(\mathcal{C})$ is isomorphic to the dihedral group $D_4$ (resp. $D_6$) in which case there is a 1-dimensional family such that $E_1$ and $E_2$ are 2-isogenous (resp. 3-isogenous), and for $n = 3$ and $N = 3, 5, 7$ there are only finitely many curves $\mathcal{C}$ defined over $K$ such that $E_1, E_2$ are $N$-isogenous. Our proof makes repeated use of the Falting's theorem [6].

Our paper is organized as follows. In Section 2 we give a brief account of the basic definitions of Abelian varieties and their isogenies. In Section 3 we first prove that for $n = 2$ there are finitely many genus 2 curves $\mathcal{C}$ defined over a number field $K$ with $\mathrm{Aut}\,(\mathcal{C}) \cong V_4$ whose elliptic components are $N$-isogenous for $N = 2, 3, 5, 7$. Also, for $n = 2$ and $N = 3, 5, 7$, there are only finitely many such $\mathcal{C}$ (up to isomorphism) with $\mathrm{Aut}\,(\mathcal{C}) = D_4$. That $\mathcal{C}$ is defined over $K$ follows from the important fact that the invariants $u$ and $v$ are in the field of moduli of the curve $\mathcal{C}$ and that for every curve in $\mathcal{L}_2$, the field of moduli is a field of definition; see [19]. 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 $r_1$, $r_2$ of two cubics in [24]. These invariants are denoted by $\chi$ and $\psi$ here.

Then we study with the $n = 3$ case. The equation of $\mathcal{L}_3$ was computed by the third author in his thesis [22] and summarized in [24]. A birational parametrization of $\mathcal{L}_3$ exists in terms of the invariants $\chi$ and $\psi$. We are able to compute the $j$-invariants of $E_1$ and $E_2$ in terms of $\chi$ and $\psi$ and find the conditions that $\chi$ and $\psi$ must satisfy. Since ordered pairs $(\chi, \psi)$ are on a one to one correspondence with genus two curves with $(3, 3)$-split Jacobians, then we determine pairs $(\chi, \psi)$ such that the corresponding $j$-invariants $j_1$ and $j_2$ satisfy the equation of the modular curve $X_0(N)$. This case is different from $n = 2$ in that a rational ordered pair $(\chi, \psi)$ does not necessarily correspond to a genus two defined over $K$. However, a genus two curve defined over $K$ gives rise to rational invariants $\chi, \psi \in K$. Hence, it is enough to count the rational ordered pairs $(\chi, \psi)$ that satisfy the equation $\phi_N(j_1, j_2) = 0$ of the modular curve $X_0(N)$. We are able to prove that for $N = 5$ there are only finitely many genus two curves $\mathcal{C}$ 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 $\phi_N(j_1, j_2) = 0$ has genus zero components in such cases. It remains open to further investigation if there is any theoretical interpretation of such surprising phenomena.

In the last section we consider the Kummer and Shioda-Inose surfaces of $(n, n)$-reducible Jacobians. We classify such surfaces when $n = 2, 3$ (cf. Prop. 10 and Cor. 2).

## 2. Preliminaries

An Abelian variety defined over $k$ is an absolutely irreducible projective variety defined over $k$ which is a group scheme. We will denote an Abelian variety defined over a field $k$ by $\mathcal{A}_k$ or simply $\mathcal{A}$ when there is no confusion. A morphism from the Abelian variety $\mathcal{A}_1$ to the Abelian variety $\mathcal{A}_2$ is a homomorphism if and only if it maps the identity element of $\mathcal{A}_1$ to the identity element of $\mathcal{A}_2$.

An abelian variety over a field $k$ is called *simple* if it has no proper non-zero Abelian subvariety over $k$, it is called *absolutely simple* (or *geometrically simple*) if it is simple over the algebraic closure of $k$. An Abelian variety of dimension 1 is called an *elliptic curve*.

A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is called an *isogeny* if $\operatorname{Img} f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \to \mathcal{B}$ exists we say that $\mathcal{A}$ and $\mathcal{B}$ are isogenous. This relation is symmetric. The degree of an isogeny $f : \mathcal{A} \to \mathcal{B}$ is the degree of the function field extension $\deg f := [k(\mathcal{A}) : f^\star k(\mathcal{B})]$. It is equal to the order of the group scheme $\ker(f)$, which is, by definition, the scheme theoretical inverse image $f^{-1}(\{0_\mathcal{A}\})$.

The group of $\bar{k}$-rational points has order $\#(\ker f)(\bar{k}) = [k(A) : f^\star k(B)]^{sep}$, where $[k(A) : f^\star k(B)]^{sep}$ is the degree of the maximally separable extension in $k(\mathcal{A})/f^\star k(\mathcal{B})$. We say that $f$ is a *separable isogeny* if and only if $\# \ker f(\bar{k}) = \deg f$.

For any Abelian variety $\mathcal{A}/k$ there is a one to one correspondence between the finite subgroup schemes $H \leq \mathcal{A}$ and isogenies $f : \mathcal{A} \to \mathcal{B}$, where $\mathcal{B}$ is determined up to isomorphism. Moreover, $H = \ker f$ and $\mathcal{B} = \mathcal{A}/H$. $f$ is separable if and only if $K$ is étale, and then $\deg f = \#H(\bar{k})$. The following is often called the fundamental theorem of Abelian varieties. Let $\mathcal{A}$ be an Abelian variety. Then $\mathcal{A}$ is isogenous to

$$\mathcal{A}_1^{n_1} \times \mathcal{A}_2^{n_2} \times \cdots \times \mathcal{A}_r^{n_r},$$

where (up to permutation of the factors) $\mathcal{A}_i$ , for $i = 1, \dots, r$ are simple, non-isogenous, Abelian varieties. Moreover, up to permutations, the factors $\mathcal{A}_i^{n_i}$ are uniquely determined up to isogenies.

When $k = \bar{k}$, then let $f$ be a nonzero isogeny of $\mathcal{A}$. Its kernel $\ker f$ is a subgroup scheme of $\mathcal{A}$. It contains $0_\mathcal{A}$ and so its connected component, which is, by definition, an Abelian variety.

Let $\mathcal{C}$ be a curve of genus 2 defined over a perfect field $k$ such that $\operatorname{char} k \neq 2$ and $\mathrm{J} = \operatorname{Jac}(\mathcal{C})$ its Jacobian. Fix a prime $\ell \geq 3$ and let $S$ be a maximal $\ell$-Weil isotropic subgroup of $\mathrm{J}[n]$, then we have $S \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Let $\mathrm{J}' := \mathrm{J}/S$ be the quotient variety and $\mathcal{Y}$ a genus 2 curve such that $\operatorname{Jac}(\mathcal{Y}) = \mathrm{J}'$. Hence, the classical isogeny problem becomes to compute $\mathcal{Y}$ when given $\mathcal{C}$ and $S$.

If $\ell = 2$ this problem is done with the Richelot construction. Over finite fields this is done by Lubicz and Robert in [16] using theta-functions. In general, if $\phi : \mathrm{J}(\mathcal{C}) \to \mathrm{J}(\mathcal{Y})$ is the isogeny and $\Theta_\mathcal{C}$, $\Theta_Y$ the corresponding theta divisors, then $\phi(\Theta_\mathcal{C})$ is in $|\ell\Theta_\mathcal{Y}|$. Thus, the image of $\phi(\Theta_\mathcal{C})$ in the Kummer surface $\mathcal{K}_\mathcal{Y} = \mathrm{J}(\mathcal{Y})/\langle \pm 1 \rangle$ is a degree $2\ell$ genus zero curve in $\mathbb{P}^3$ of arithmetic genus $\frac{1}{2}(\ell^2 - 1)$. This curve can be computed without knowing $\phi$; see [5] or [9] for details.

For $\mathcal{C}$ given by $y^2 = f(x)$, we have the divisor at infinity

$$D_\infty := (1 : \sqrt{f(x)} : 0) + (1 : -\sqrt{f(x)} : 0)$$

The Weierstrass points of $\mathcal{C}$ are the projective roots of $f(x)$, namely $w_i := (x_i, z_i)$, for $i = 1, \dots, 6$ and the Weierstrass divisor $W_\mathcal{C}$ is $W_\mathcal{C} := \sum_{i=1}^6 (x_i, 0, z_i)$. A canonical divisor on $\mathcal{C}$ is $\mathcal{K}_\mathcal{C} = W_\mathcal{C} - 2D_\infty$. Let $D \in \operatorname{Jac} \mathcal{C}$, be a divisor expressed as $D = P + Q - D_\infty$. The effective divisor $P + Q$ is determined by an ideal of the form $(a(x), b(x)$ such that $a(x) = y - b(x))$, where $b(x)$ is a cubic and $a(x)$ a monic polynomial of degree $d \leq 2$.

We can define the $\ell$-tuple embedding $\rho_{2\ell} : \mathbb{P}^2 \to \mathbb{P}^{2\ell}$ by

$$(x, y, z) \to (z^{2\ell}, \dots, x^i z^{2\ell-i}, x^{2\ell})$$

and denote the image of this map by $\mathcal{R}_{2\ell}$. It is a rational normal curve of degree $2\ell$ in $\mathbb{P}^{2\ell}$. Hence, any $2\ell+1$ distinct points on $\mathcal{R}_{2\ell}$ are linearly independent. Therefore, the images under $\rho_{2\ell}$ of the Weierstrass points of $\mathcal{C}$ are linearly independent for $\ell \geq 3$. Thus, the subspace $W := \langle \rho_{2\ell}(W_\mathcal{C}) \rangle \subset \mathbb{P}^{2\ell}$ is 5-dimensional. For any pair of points $P, Q$ in $\mathcal{C}$, the secant line $\mathcal{L}_{P,Q}$ is defined to be the line in $\mathbb{P}^{2\ell}$ intersecting $\mathcal{R}_{2\ell}$ in $\rho_{2\ell}(P) + \rho_{2\ell}(Q)$. In other words,

$$\mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2\ell}(P), \rho_{2\ell}(Q) \rangle & \text{if } P \notin \{Q, \tau(Q)\} \\ T_{\rho_{2\ell}(P)}(\mathcal{R}_{2\ell}) & \text{otherwise .} \end{cases}$$

The most classical example of an isogeny is the scalar multiplication by $n$ map $[n] : \mathcal{A} \to \mathcal{A}$. The kernel of $[n]$ is a group scheme of order $n^{2 \dim \mathcal{A}}$. Denote by $\mathcal{A}[n]$ the group $\ker[n](\bar{k})$. The elements in $\mathcal{A}[n]$ are called *n-torsion points* of $\mathcal{A}$. Let $f : \mathcal{A} \to \mathcal{B}$ be a degree $n$ isogeny. Then there exists an isogeny $\hat{f} : \mathcal{B} \to \mathcal{A}$ such that

$$f \circ \hat{f} = \hat{f} \circ f = [n].$$

Next we consider the case when $\operatorname{char} k = p$. Let $\mathcal{A}/k$ be an Abelian variety, $p = \operatorname{char} k$, and $\dim \mathcal{A} = g$.

i) If $p \nmid n$, then $[n]$ is separable, $\#\mathcal{A}[n] = n^{2g}$ and $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.
ii) If $p \mid n$, then $[n]$ is inseparable. Moreover, there is an integer $0 \leq i \leq g$ such that
$$\mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i, \text{ for all } m \geq 1.$$

If $i = g$ then $\mathcal{A}$ is called *ordinary.* If $\mathcal{A}[p^s](\bar{k}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ then the abelian variety has *p-rank t*. If $\dim \mathcal{A} = 1$ (elliptic curve) then it is called *supersingular* if it has $p$-rank 0. An abelian variety $\mathcal{A}$ is called *supersingular* if it is isogenous to a product of supersingular elliptic curves. If $\dim \mathcal{A} \leq 2$ and $\mathcal{A}$ has $p$-rank 0 then $\mathcal{A}$ is supersingular. This is not true for $\dim \mathcal{A} \geq 3$.

2.1. **Jacobian varieties.** Let $\mathcal{C}$ be a curve of positive genus and assume that there exists a $k$-rational point $P_0 \in \mathcal{C}(k)$ with attached prime divisor $\mathfrak{p}_0$. There exists an abelian variety $\operatorname{Jac}_k(\mathcal{C})$ defined over $k$ and a uniquely determined embedding

$$\phi_{P_0} : \mathcal{C} \to \operatorname{Jac}_k(\mathcal{C}) \text{ with } \phi_{P_0}(P_0) = 0_{\operatorname{Jac}_k(\mathcal{C})}$$

such that

(1) for all extension fields $L$ of $k$ we get $\operatorname{Jac}_L \mathcal{C} = \operatorname{Pic}^0_{\mathcal{C}_L}(L)$ where this equality is given in a functorial way and
(2) if $\mathcal{A}$ is an Abelian variety and $\eta : \mathcal{C} \to \mathcal{A}$ is a morphism sending $P_0$ to $0_\mathcal{A}$ then there exists a uniquely determined homomorphism $\psi : \operatorname{Jac}(\mathcal{C}) \to \mathcal{A}$ with $\psi \circ \phi_{P_0} = \eta$.

$\operatorname{Jac}(\mathcal{C})$ is uniquely determined by these conditions and is called the *Jacobian variety* of $\mathcal{C}$. The map $\phi_{P_0}$ is given by sending a prime divisor $\mathfrak{p}$ of degree 1 of $\mathcal{C}_\mathcal{L}$ to the class of $\mathfrak{p} - \mathfrak{p}_0$ in $\operatorname{Pic}^0_{\mathcal{C}_L}(L)$.

Let $L/k$ be a finite algebraic extension. Then the Jacobian variety $\mathrm{Jac}_L\,\mathcal{C}$ of $\mathcal{C}_L$ is the scalar extension of $\mathrm{Jac}\,\mathcal{C}$ with $L$, hence a fiber product with projection $p$ to $\mathrm{Jac}\,\mathcal{C}$. The norm map is $p_*$, and the conorm map is $p^*$. By universality we get that if $f : \mathcal{C} \to \mathcal{D}$ is a surjective morphism of curves sending $P_0$ to $Q_0$, then there is a uniquely determined surjective homomorphism $f_* : \mathrm{Jac}\,\mathcal{C} \to \mathrm{Jac}\,\mathcal{D}$, such that $f_* \circ \phi_{P_0} = \phi_{Q_0}$. A useful observation is that if $\mathrm{Jac}\,\mathcal{C}$ is a simple abelian variety, and that $\eta : \mathcal{C} \to \mathcal{D}$ is a separable cover of degree $> 1$, then $\mathcal{D}$ is the projective line. For more details on the general setup see [9] among many other authors.

2.2. **Jacobian surfaces.** Abelian varieties of dimension 2 are often called Abelian (algebraic) surfaces. We focus on Abelian surfaces which are Jacobian varieties. Let $\mathcal{C}$ be a genus 2 curve defined over a field $k$. Then its gonality is $\gamma_\mathcal{C} = 2$. Hence, genus 2 curves are hyperelliptic and we denote the hyperelliptic projection by $\pi : \mathcal{C} \to \mathbb{P}^1$. By the Hurwitz's formula this covering has $r = 6$ branch points which are images of the Weierstrass points of $\mathcal{C}$. The moduli space has dimension $r - 3 = 3$.

The arithmetic of the moduli space of genus two curves was studied by Igusa in his seminal paper [11] expanding on the work of Clebsch, Bolza, and others. Arithmetic invariants by $J_2, J_4, J_6, J_8, J_{10}$ determine uniquely the isomorphism class of a genus two curve. Two genus two curves $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic over $\bar{k}$ if and only if there exists $l \in \bar{k}^\star$ such that $J_{2i}(\mathcal{C}) = l^{2i} J_{2i}(\mathcal{C}')$, for $i = 1, \dots, 5$. If $\mathrm{char}\, k \neq 2$ then the invariant $J_8$ is not needed.

From now on we assume $\mathrm{char}\, k \neq 2$. Then $\mathcal{C}$ has an affine Weierstrass equation

$$y^2 = f(x) = a_6 x^6 + \cdots + a_1 x + a_0, \tag{1}$$

over $\bar{k}$, with discriminant $\Delta_f = J_{10} \neq 0$. The moduli space $\mathcal{M}_2$ of genus 2 curves, via the Torelli morphism, can be identified with the moduli space of the principally polarized abelian surfaces $\mathbb{A}_2$ which are not products of elliptic curves. Its compactification $\mathbb{A}_2^\star$ is the weighted projective space $\mathbb{WP}^3_{(2,4,6,10)}(k)$ via the Igusa invariants $J_2, J_4, J_6, J_{10}$. Hence,

$$A_2 \cong \mathbb{WP}^3_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}.$$

Given a moduli point $\mathfrak{p} \in \mathcal{M}_2$, we can recover the equation of the corresponding curve over a minimal field of definition following [19].

It is well known that 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, see [21] for more details.

Let $\mathcal{C}$ be a genus 2 curve and $\psi_1 : \mathcal{C} \longrightarrow E_1$ be a degree $n$ maximal covering from $\mathcal{C}$ to an elliptic curve $E_1$. Then ${\psi^*}_1 : E_1 \to \mathrm{Jac}(\mathcal{C})$ is injective and the kernel of $\psi_{1,*} : \mathrm{Jac}(\mathcal{C}) \to E_1$ is an elliptic curve which we denote by $E_2$. For a fixed Weierstrass point $P \in \mathcal{C}$, we can embed $\mathcal{C}$ to its Jacobian via

$$\begin{aligned} i_P : \mathcal{C} &\longrightarrow \mathrm{Jac}(\mathcal{C}) \\ x &\to [(x) - (P)] \end{aligned} \tag{2}$$

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

$$0 \to E_2 \xrightarrow{g} \mathrm{Jac}(\mathcal{C}) \xrightarrow{\psi_{1,*}} E_1 \to 0. \tag{3}$$

The dual sequence is also exact

$$0 \to E_1 \xrightarrow{\psi_1^*} \mathrm{Jac}(\mathcal{C}) \xrightarrow{g^*} E_2 \to 0.$$

If $\deg(\psi_1) = 2$ or it is an odd number then the maximal covering $\psi_2 : \mathcal{C} \to E_2$ 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 [24] 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 [27] or [19] for $n = 2$, in [24] for $n = 3$, and in [17] for $n = 5$. From now on, we will say that a genus 2 curve $\mathcal{C}$ has an $(n, n)$-decomposable Jacobian if $\mathcal{C}$ is as above and the elliptic curves $E_i$, $i = 1, 2$ are called the components of $\mathrm{Jac}(\mathcal{C})$.

For every $D := J_{10} > 0$ there is a Humbert hypersurface $H_D$ in $\mathcal{M}_2$ which parametrizes curves $\mathcal{C}$ whose Jacobians admit an optimal action on $\mathcal{O}_D$; see [10]. Points on $H_{n^2}$ parametrize curves whose Jacobian admits an $(n, n)$-isogeny to a product of two elliptic curves. Such curves are the main focus of our study. We have the following result; see [15, Prop. 2.14].

**Proposition 1.** $\mathrm{Jac}(\mathcal{C})$ *is a geometrically simple Abelian variety if and only if it is not* $(n, n)$*-decomposable for some* $n > 1$.

A point lying on the intersection of two Humbert surfaces $\mathcal{H}_{m^2} \cap \mathcal{H}_{n^2}$ with $n \neq m$ corresponds either to a simple abelian surface with quaternionic multiplication by an (automatically indefinite) quaternion algebra over $\mathbb{Q}$, or to the square of an elliptic curve. This is in particular true for points lying on Shimura curves.

We study pairs $(E_1, E_2)$ elliptic components and try to determine their number (up to isomorphism over $\bar{k}$) when they are isogenous of degree $N$, for an integer $N \geq 2$. 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 $X_0(N)$. The equations of $X_0(N)$ are well known.

2.3. **Kummer surface and Shioda-Inose surface.** To the Jacobian variety $\mathrm{Jac}(\mathcal{C})$ one can naturally attach two K3 surfaces, the Kummer surface and a double cover of it called the Shioda-Inose surface. Let $\mathfrak{i}$ be the involution automorphism on the Jacobian given by $\mathfrak{i} : \mathfrak{p} \to -\mathfrak{p}$. The quotient $\mathrm{Jac}(\mathcal{C})/\{\mathbb{I}, \mathfrak{i}\}$, is a singular surface with sixteen ordinary double points. Its minimal resolution is called the *Kummer surface* and denoted by $\mathrm{Kum}(\mathrm{Jac}(\mathcal{C}))$. We refer to [18, 19] for further details.

The Inose surface, denoted by $\mathcal{Y} := SI(\mathrm{Jac}(\mathcal{C}))$, was originally constructed as a double cover of the Kummer surface. Shioda and Inose then showed that the following diagram of rational maps, called a Shioda-Inose structure, induces an isomorphism of integral Hodge structures on the transcendental latices of $\mathrm{Jac}(\mathcal{C})$ and $\mathcal{Y}$, see [28] for more details.

$$\begin{tikzcd}
\mathrm{Jac}(\mathcal{C}) \arrow[dr, dashed, "\pi_0"] & & \mathcal{Y} \arrow[dl, dashed, "\pi_1"] \\
& \mathrm{Kum}(\mathrm{Jac}(\mathcal{C})) &
\end{tikzcd}$$

A K3 surface $\mathcal{Y}$ has *Shioda-Inose* structure if it admits an involution fixing the holomorphic two-form, such that the quotient is the Kummer surface $\mathrm{Kum}(\mathcal{A})$ of a principally polarized abelian surface and the rational quotient map $p : \mathcal{Y} \to$

$\mathrm{Kum}(\mathcal{A})$ of degree two induces a hodge isometry between the transcendental latices $T(\mathcal{Y})(2)^3$ and $T(\mathrm{Kum}(\mathcal{A}))$, see [19] for more details.

An elliptic surface $\mathcal{E}(\overline{k}(t))$ fibered over $\mathbb{P}^1$ with section can be described by a Weierstrass equation of the form

$$y^2 + a_1(t)xy + a_3(t)y = x^2 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

and $a_i(t)$ rational functions. If we assume that the elliptic fibration has at least one singular fiber then the following question is fundamental in arithmetic geometry. Find generators for the Mordell-Weil group of this elliptic surface fibered over $\mathbb{P}^1$.

A theorem of Shioda and Tate connects the Mordel-Weil group $\mathcal{E}(\overline{k}(t)$ with the Picard group of the Néron-Severi group of $\mathcal{E}$. Therefore, determining the Mordell-Weil group it is equivalent to finding the Picard group of the Néron-Severi lattice of K3 surface.

A surface is called an *elliptic fibration* if it is a minimal elliptic surface over $\mathbb{P}^1$ with a distinguished section $S_0$. The complete list of possible singular fibers has been given by Kodaira [12]. To each elliptic fibration $\pi : \mathcal{C} \to \mathbb{P}^1$ there is an associated Weierstrass model $\overline{\pi} : \overline{\mathcal{C}} \to \mathbb{P}^1$ with a corresponding distinguished section $\overline{S}_0$ obtained by contracting all fibers not meeting $S_0$. The fibers of $\overline{\mathcal{C}}$ are all irreducible whose singularities are all rational double points, and $\mathcal{C}$ is the minimal desingularization. If we choose some $t \in \mathcal{C}$ as a local affine coordinate on $\mathbb{P}^1$, we can present $\overline{\mathcal{C}}$ in the Weierstrass normal form

$$Y^2 = 4X^3 - g_2(t)X - g_3(t),$$

where $g_2(t)$ and $g_3(t)$ are polynomials of degree respectively 4 and 6 in $t$.

## 3. $(n, n)$ reducible Jacobians surfaces

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, many rational points, nice examples of descent [23], 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 [4]. A detailed account of applications of such curves in cryptography is provided in [9].

Let $\mathcal{C}$ be a genus 2 curve defined over an algebraically closed field $k$, $\operatorname{char} k = 0$, $K$ the function field of $\mathcal{C}$, and $\psi_1 : \mathcal{C} \longrightarrow E_1$ a degree $n$ covering from $\mathcal{C}$ to an elliptic curve $E$; see [21] for the basic definitions. The covering $\psi_1 : \mathcal{C} \longrightarrow E$ is called a *maximal covering* if it does not factor through a nontrivial isogeny. We call $E$ a *degree $n$ elliptic subcover* of $\mathcal{C}$. 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 $\mathrm{Jac}(\mathcal{C})$ and the product $E_1 \times E_2$. Such curve $\mathcal{C}$ is said to have $(n, n)$-decomposable (or $(n, n)$-split) Jacobian. The focus of this paper is on isogenies among the elliptic curves $E_1$ and $E_2$.

The locus of genus 2 curves $\mathcal{C}$ with $(n, n)$-decomposable Jacobian it is denoted by $\mathcal{L}_n$. When $n = 2$ or $n$ an odd integer, $\mathcal{L}_n$ is a 2-dimensional algebraic subvariety of the moduli space $\mathcal{M}_2$ of genus two curves; see [21] 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 [27] for $\mathcal{L}_2$, [24] for $\mathcal{L}_3$, and [17] for $\mathcal{L}_5$. There is a more recent paper on the subject [13] where results of [17, 24] are confirmed and equations for $n > 5$ are studied.

3.1. $(2,2)$ **reducible Jacobians surfaces.** Let $\mathcal{C}/k$ as above and $\mathbb{F} = k(\mathcal{C})$ its function field. We assume that $k$ is algebraically closed and $\operatorname{char} k \neq 2$. Since degree 2 coverings correspond to Galois extensions of function fields, the elliptic subcover is fixed by an involution in $\operatorname{Aut}(\mathbb{F}/k)$. There is a group theoretic aspect of the $n = 2$ case which was discussed in detail in [27]. The number of elliptic subcovers in this case correspond to the number of non-hyperelliptic involutions in $\operatorname{Aut}(\mathbb{F}/k)$, which are called *elliptic involutions*. The equation of $\mathcal{C}$ is given by

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

and in [1,2] it was shown that when defined over $\mathbb{F}$ 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 $\mathcal{C}_{(s_1,s_2)}$ and two corresponding elliptic subcovers. Two such curves $(\mathcal{C}_{(s_1,s_2)}, \varepsilon_{s_1,s_2})$ and $(\mathcal{C}_{(s_1',s_2')}, \varepsilon_{s_1',s_2'})$ are isomorphic if and only if their dihedral invariants $u$ and $v$ are the same; [27]. Thus, the points $(s_1, s_2) \in k^2$ correspond to elliptic involutions of $\operatorname{Aut} \mathcal{C}$ while the points $(u, v) \in k^2$ correspond to elliptic involutions of the reduced automorphism group $\overline{\operatorname{Aut}}\, \mathcal{C}$.

Let $\mathcal{C}$ be a genus 2 curve, $\operatorname{Aut}(\mathcal{C})$ its automorphism group, $\sigma_0$ the hyperelliptic involution, and $\overline{\operatorname{Aut}}(\mathcal{C}) := \operatorname{Aut}(\mathcal{C})/\langle \sigma_0 \rangle$ the reduced automorphism group. If $\operatorname{Aut}(\mathcal{C})$ has another involution $\sigma_1$, then the quotient space $\mathcal{C}/\langle \sigma_1 \rangle$ 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 $\psi_i : \mathcal{C} \to \mathcal{C}/\langle \sigma_i \rangle$, $i = 1, 2$, are the maximal covers as above and $E_i := \mathcal{C}/\langle \sigma_i \rangle$ the elliptic subcovers of $\mathcal{C}$ 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 $\mathcal{L}_2$. The following was proved in [27].

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

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

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

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

In [27] it was shown that $\mathcal{C}$ is determined up to a coordinate change by the subgroup $H \cong D_3$ of $SL_2(k)$ generated by $\tau_1 : X \to \varepsilon_6 X$ and $\tau_2 : X \to \frac{1}{X}$, where $\varepsilon_6$ is a primitive 6-th root of unity. Let $\varepsilon_3 := \varepsilon_6^2$. The coordinate change by $\tau_1$ replaces $s_1$ by $\varepsilon_3 s_2$ and $s_2$ by $\varepsilon_3^2 s_2$. The coordinate change by $\tau_2$ switches $s_1$ and $s_2$. Invariants of this $H$-action are:

$$u := s_1 s_2, \quad v := s_1^3 + s_2^3 \tag{5}$$

which are known in the literature as *dihedral invariants*. 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 $\operatorname{char}(k) \neq 3$. 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 $\langle \tau_1, \tau_2 \rangle$.

If $\mathrm{char}(k) = 3$ then $u = u'$ and $v = v'$ implies $s_1^3 s_2^3 = s_1'^3 s_2'^3$ and $s_1^3 + s_2^3 = s_1'^3 + s_2'^3$, hence $(s_1^3, s_2^3) = (s_1'^3, s_2'^3)$ or $(s_1^3, s_2^3) = (s_2'^3, s_1'^3)$. But this implies $(s_1, s_2) = (s_1', s_2')$ or $(s_1, s_2) = (s_2', s_1')$.

For $(s_1, s_2) \in k^2$ with $\Delta \neq 0$, equation Eq. (4) defines a genus 2 field $\mathbb{F}_{s_1,s_2} = k(X,Y)$. Its reduced automorphism group contains the elliptic involution $\varepsilon_{s_1,s_2} : X \mapsto -X$. Two such pairs $(\mathbb{F}_{s_1,s_2}, \varepsilon_{s_1,s_2})$ and $(\mathbb{F}_{s_1',s_2'}, \varepsilon_{s_1',s_2'})$ 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 Eq. (5)). 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 [27].

**Proposition 2.** *i) The $(u, v) \in k^2$ with $\Delta \neq 0$ bijectively parameterize the isomorphism classes of pairs $(\mathbb{F}, \varepsilon)$ where $\mathbb{F}$ is a genus 2 field and $\varepsilon$ an elliptic involution of $\overline{\mathrm{Aut}}\,(\mathbb{F})$.*

*ii) The $(u, v)$ satisfying additionally*

$$(v^2 - 4u^3)(4v - u^2 + 110u - 1125) \neq 0 \tag{6}$$

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

Our goal is to investigate when the pairs of elliptic subfields $\mathbb{F}_{s_1,s_2}$ (respectively isomorphism classes $(\mathbb{F}, \varepsilon)$) are isogenous. We want to find if that happens when $\mathcal{C}$ is defined over a number field $K$. Hence, the following result is crucial.

**Proposition 3.** *Let $K$ be a number field and $\mathcal{C}/K$ be a genus 2 curve with $(2,2)$ geometrically reducible Jacobian and $E_i$, $i = 1, 2$ its elliptic components. Then its dihedral invariants $u, v \in K$ and $\mathcal{C}$ is isomorphic (over $\bar{K}$) to a twist whose polynomials are given as polynomials in $u$ and $v$. Moreover, $E_i$, for $i = 1, 2$ are defined over $K$ if and only if*

$$\begin{aligned} S_2(u,v) :=& v^4 - 18(u+9)v^3 - (4u^3 - 297u^2 - 1458u - 729)v^2 \\ & - 216u^2(7u+27)v + 4u^3(2u^3 - 27u^2 + 972u + 729) \end{aligned} \tag{7}$$

*is a complete square in $K$.*

*Proof.* Let $j_1$ and $j_2$ denote the $j$-invariants of the elliptic components $E_1$ and $E_2$ from Lem. 1. The $j$-invariants $j_1$ and $j_2$ of the elliptic components are given in terms of the coefficients $s_1, s_2$ by the following

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

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

It is shown in [27] that they satisfy the quadratic

$$j^2 - \left(256 \frac{v^2 - 2u^3 + 54u^2 - 9uv - 27v}{\Delta}\right) j + 65536 \frac{u^2 + 9u - 3v}{\Delta^2} = 0 \tag{8}$$

where $\Delta = \Delta(u,v) = u^2 - 4v + 18u - 27$. The discriminant of this quadratic is $S(u,v)$ as claimed. When $S(u,v)$ is a complete square in $K$, then $j_1$ and $j_2$ have values in $K$. Since for elliptic curves the field of moduli is a field of definition, elliptic curves $E_1$ and $E_2$ are defined over $K$. $\square$

See [25] for details, where an explicit equation of $\mathcal{C}$ is provided with coefficients as rational functions in $u$ and $v$, or [19] for a more general setup. Hence, we have the following.

**Lemma 2.** *Let $\mathcal{C}$ be a genus 2 curve with $(2,2)$ geometrically reducible Jacobian and $E_i$, $i=1,2$ its elliptic components and $K$ its field of moduli. Then* $\mathrm{Jac}(\mathcal{C})$ *is $(2,2)$ reducible over $K$ if and only if $S_2(u,v)$ is a complete square in $K$.*

*Proof.* The elliptic components $E_1$ and $E_2$ are defined over $K$ when their $j$-invariants are in $K$. This happens when the discriminant of the above quadratic is a complete square. The discriminant of the quadratic is exactly $S(u,v)$ as above. □

We define the following surface

$$\mathcal{S}_2: \; y^2 = S_2(u,v), \tag{9}$$

where $S_2(u,v)$ is as Eq. (7). Coefficients of Eq. (8) can be expressed in terms of the Siegel modular forms or equivalently in terms of the Igusa arithmetic invariants; see [22] or [27]. They were discovered independently in [3], where they are called *modular invariants.* There is a degree 2 covering $\Phi: \mathcal{S}_2 \to \mathcal{L}_2$, where $(u,v,\pm y) \to (u,v)$. Then we have the following.

**Proposition 4.** *Let $K$ be a number field. There is a 2:1 correspondence between the set of $K$-rational points on the elliptic surface $\mathcal{E}$ and the set of Jacobians* $\mathrm{Jac}(\mathcal{C})$ *which are $(2,2)$ reducible over $K$.*

*Proof.* Every pair of $K$-rational points $(u,v,\pm y)$ in $\mathcal{E}$ gives the dihedral invariants $(u,v) \in K^2$ which determine the field of moduli of the genus 2 curve $\mathcal{C}$. Since $\mathcal{C}$ has extra involutions then $\mathcal{C}$ is defined over the field of moduli. Hence, $\mathcal{C}$ is defined over $\mathcal{K}$. The fact that $(u,v,\pm y)$ is $K$ rational means that the $j$-invariants $j_1$ and $j_2$ of elliptic components take values $\pm y$. Hence, $j_1, j_2 \in K$ and $E_1$ and $E_2$ are defined over $K$.

The $(2,2)$ isogeny

$$\mathrm{Jac}\,\mathcal{C} \to E_1 \times E_2$$

is defined by $D \to (\psi_{1,\star}(D), \psi_{2,\star}(D))$ where $\psi_i: \mathcal{C} \to E_i$, $i=1,2$ are as in Eq. (3). Since $\psi_i$ are defined over $K$, then the $(2,2)$ isogeny is defined over $K$. □

Next we turn our attention to isogenies between $E_1$ and $E_2$.

**Proposition 5.** *Let $\mathcal{C}$ 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 $\mathcal{C}$ defined over $K$ such that there is a degree $N$ isogeny $E_1 \to E_2$ and $K$-rational points on the modular curve $X_0(N)$ given in terms of $u$ and $v$.*

*Proof.* If $\mathcal{C}$ is defined over $K$ then the corresponding $(u,v) \in K^2$ since they are in the field of moduli of $\mathcal{C}$, which is contained in $K$. Conversely, if $u$ and $v$ satisfy the equation of $X_0(N)$ then we can determine the equation of $\mathcal{C}$ in terms of $u$ and $v$ as in [25]. □

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

**Proposition 6.** *For $N=2,3,5,7$ there are only finitely many curves $\mathcal{C}$ defined over $K$ with $(2,2)$-decomposable Jacobian and* $\mathrm{Aut}\,(\mathcal{C}) \cong V_4$ *such that $E_1$ is $N$-isogenous to $E_2$.*

*Proof.* Let us now check if elliptic components 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 described in the preliminaries. 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

$$\begin{aligned} f_1 = &-16v^3 - 81216v^2 - 892296v - 2460375 + 3312uv^2 + 707616vu + 3805380u+ \\ &18360vu^2 - 1296162u^2 - 1744u^3v - 140076u^3 + 801u^4 + 256u^5 \end{aligned} \tag{10}$$

$$\begin{aligned} f_2 = &\, 4096u^7 + 256016u^6 - 45824u^5v + 4736016u^5 - 2126736vu^4 + 23158143u^4 \\ &- 25451712u^3v - 119745540u^3 + 5291136v^2u^2 - 48166488vu^2 - 2390500350u^2 \\ &- 179712uv^3 + 35831808uv^2 + 1113270480vu + 9300217500u - 4036608v^3 \\ &- 1791153000v - 8303765625 - 1024v^4 + 163840u^3v^2 - 122250384v^2 + 256u^2v^3 \end{aligned} \tag{11}$$

Notice that each one of these components has genus $g \geq 2$. From Falting's theorem [6] there are only finitely many $K$-rational points.

Let $N = 3$. Then, from equation Eq. (6) and $\phi_3(j_1, j_2) = 0$ we have:

$$(4v - u^2 + 110u - 1125) \cdot g_1(u, v) \cdot g_2(u, v) = 0 \tag{12}$$

where $g_1$ and $g_2$ are

$$\begin{aligned} g_1 = &-27008u^6 + 256u^7 - 2432u^5v + v^4 + 7296u^3v^2 - 6692v^3u - 1755067500u \\ &+ 2419308v^3 - 34553439u^4 + 127753092vu^2 + 16274844vu^3 - 1720730u^2v^2 \\ &- 1941120u^5 + 381631500v + 1018668150u^2 - 116158860u^3 + 52621974v^2 \\ &+ 387712u^4v - 483963660vu - 33416676v^2u + 922640625 \end{aligned} \tag{13}$$

$$\begin{aligned} g_2 = &\, 291350448u^6 - v^4u^2 - 998848u^6v - 3456u^7v + 4749840u^4v^2 + 17032u^5v^2 \\ &+ 4v^5 + 80368u^8 + 256u^9 + 6848224u^7 - 10535040v^3u^2 - 35872v^3u^3 + 26478v^4u \\ &- 77908736u^5v + 9516699v^4 + 307234984u^3v^2 - 419583744v^3u - 826436736v^3 \\ &+ 27502903296u^4 + 28808773632vu^2 - 23429955456vu^3 + 5455334016u^2v^2 \\ &- 41278242816v + 82556485632u^2 - 108737593344u^3 - 12123095040v^2 \\ &+ 41278242816vu + 3503554560v^2u + 5341019904u^5 - 2454612480u^4v \end{aligned} \tag{14}$$

Thus, there is a isogeny of degree 3 between $E_1$ and $E_2$ if and only if $u$ and $v$ satisfy equation Eq. (12). The vanishing of the first factor is equivalent to $G \cong D_6$. So, if $Aut(\mathcal{C}) \cong D_6$ then $E_1$ and $E_2$ are isogenous of degree 3. The other factors are curves of genus $g \geq 2$ and from [6] have only finitely many $K$-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. Using [6] we conclude the proof. □

Next we consider the case when $|\operatorname{Aut}(\mathcal{C})| > 4$. First notice that the invariants $j_1$ and $j_2$ are roots of the quadratic Eq. (8). If $G \cong D_4$, then $\sigma_1$ and $\sigma_2$ 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. (8), 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 $\overline{G} \cong V_4$ 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 $\mathcal{C}$ are $\tau_1 : X \to -X$, $\tau_2 : X \to \frac{1}{X}$, $\tau_3 : X \to -\frac{1}{X}$. Since $\tau_1$ and $\tau_3$ 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 $\tau_1$ is the double root of Eq. (8), namely

$$j = 256\frac{v^3}{v+1}. \tag{15}$$

To find the $j$-invariant of the elliptic subfields fixed by $\tau_3$ 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 $\phi$ are $q_i = \pm\frac{2i\sqrt{a}}{\sqrt{a-1}}$. From Lem. 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

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

Then, we have the following result.

**Proposition 7.** *Let $\mathcal{C}$ be a genus 2 curve with $\mathrm{Aut}\,(\mathcal{C}) \cong D_4$ 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 $\mathcal{C}$ defined over $K$ 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

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

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

3.2. $(3, 3)$ **reducible Jacobian surfaces.** In this section we focus on genus 2 curves with $(3, 3)$-split Jacobians. This case was studied in detail in[24], where it was proved that if $\mathbb{F}$ is a genus 2 field over $k$ and $e_3(\mathbb{F})$ the number of $\mathrm{Aut}\,(\mathbb{F}/k)$-classes of elliptic subfields of $\mathbb{F}$ of degree 3, then

i) $e_3(\mathbb{F}) = 0, 1, 2$, or 4

ii) $e_3(\mathbb{F}) \geq 1$ if and only if the classical invariants of $\mathbb{F}$ satisfy the irreducible equation $f(J_2, J_4, J_6, J_{10}) = 0$ displayed in [24, Appendix A].

There are exactly two genus 2 curves (up to isomorphism) with $e_3(\mathbb{F}) = 4$. The case $e_3(\mathbb{F}) = 1$ (resp., 2) occurs for a 1-dimensional (resp., 2-dimensional) family of genus 2 curves. We are interested on the 2-dimensional family, since the case $e_3(\mathbb{F}) = 1$ is the singular locus of the case $e_3(\mathbb{F}) = 2$.

We let $\mathcal{C}$ be a genus 2 curve define over $k = \bar{k}$, $\mathrm{char}\, k \neq 2, 3$, and $\mathbb{F} := k(\mathcal{C})$ its function field.

**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

$$Y^2 = (\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1)\,(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1), \tag{17}$$

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

$$\begin{aligned}
U_1 &= \frac{\mathfrak{v} X^2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1},\\
U_2 &= \frac{(\mathfrak{v} X + 3)^2\,(\mathfrak{v}(4\mathfrak{u} - \mathfrak{v} - 9) X + 3\mathfrak{u} - \mathfrak{v})}{\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)},\\
V_1 &= Y\,\frac{\mathfrak{v}^2 X^3 - \mathfrak{v} X - 2}{\mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1},\\
V_2 &= (27 - \mathfrak{v})^{\frac{3}{2}}\,Y\,\frac{\mathfrak{v}^2(\mathfrak{v} - 4\mathfrak{u} + 8) X^3 + \mathfrak{v}(\mathfrak{v} - 4\mathfrak{u}) X^2 - \mathfrak{v} X + 1}{(4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1)^2}
\end{aligned} \tag{18}$$

and the elliptic curves have equations:

$$\begin{aligned}
\mathcal{E}_1 :&\quad V_1^2 = R\,U_1^3 - (12\mathfrak{u}^2 - 2\mathfrak{u}\mathfrak{v} - 18\mathfrak{v}) U_1^2 + (12\mathfrak{u} - \mathfrak{v}) U_1 - 4\\
\mathcal{E}_2 :&\quad V_2^2 = c_3 U_2^3 + c_2 U_2^2 + c_1 U_2 + c_0
\end{aligned} \tag{19}$$

where

$$\begin{aligned}
c_0 &= -(9\mathfrak{u} - 2\mathfrak{v} - 27)^3\\
c_1 &= (4\mathfrak{u} - \mathfrak{v} - 9)\,(729\mathfrak{u}^2 + 54\mathfrak{u}^2\mathfrak{v} - 972\mathfrak{u}\mathfrak{v} - 18\mathfrak{u}\mathfrak{v}^2 + 189\mathfrak{v}^2 + 729\mathfrak{v} + \mathfrak{v}^3)\\
c_2 &= -\mathfrak{v}\,(4\mathfrak{u} - \mathfrak{v} - 9)^2\,(54\mathfrak{u} + \mathfrak{u}\mathfrak{v} - 27\mathfrak{v})\\
c_3 &= \mathfrak{v}^2\,(4\mathfrak{u} - \mathfrak{v} - 9)^3
\end{aligned} \tag{20}$$

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.

We define the following invariants of two cubic polynomials. For $F(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0$ and $G(X) = b_3 X^3 + b_2 X^2 + b_1 X + b_0$ define

$$H(F, G) := a_3 b_0 - \frac{1}{3} a_2 b_1 + \frac{1}{3} a_1 b_2 - a_0 b_3$$

We denote by $R(F, G)$ the resultant of $F$ and $G$ and by $D(F)$ the discriminant of $F$. Also, $r_1(F, G) = \frac{H(F,G)^3}{R(F,G)}$, $r_2(F, G) = \frac{H(F,G)^4}{D(F)\,D(G)}$, and $r_3 = \frac{H(F,G)^2}{J_2(F\,G)}$. Invariants $r_1, r_2$, and $r_3$ form a complete system of invariants for unordered pairs of cubics. For $F = \mathfrak{v}^2 X^3 + \mathfrak{u}\mathfrak{v} X^2 + \mathfrak{v} X + 1$ and $G = 4\mathfrak{v}^2 X^3 + \mathfrak{v}^2 X^2 + 2\mathfrak{v} X + 1$ as in Eq. (17) we have

$$\begin{aligned}
\chi &:= r_1 = 3^3 \cdot \frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^3}{4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3}\\
\psi &:= r_2 = -2^4 \cdot 3^4\,\frac{\mathfrak{v}(\mathfrak{v} - 9 - 2\mathfrak{u})^4}{(\mathfrak{v} - 27)(4\mathfrak{v}^2 - 18\mathfrak{u}\mathfrak{v} + 27\mathfrak{v} - \mathfrak{u}^2\mathfrak{v} + 4\mathfrak{u}^3)},
\end{aligned}$$

It was shown in [24] that the function field of the locus $\mathcal{L}_3$, genus 2 curves with $(3, 3)$ reducible Jacobians, is exactly $k(\chi, \psi)$.

**Lemma 3.** $k(\mathcal{L}_3) = k(\chi, \psi)$.

By eliminating $\mathfrak{u}$ and $\mathfrak{v}$ we have rational expressions of absolute invariants $i_1, i_2, i_3$ in terms of $\chi$ and $\psi$ as in [24, Eq. (19)]. We can take

$$[J_2 : J_4 : J_6 : J_{10}] = \left[1 : \frac{1}{144} i_1 : \left(\frac{1}{5184} i_2 + \frac{1}{432} i_1\right) : \frac{1}{486} i_3\right]$$

Hence, we have

$$\begin{aligned}
J_2 =& \chi \left(\chi^2 + 96\,\chi\,\psi - 1152\,\psi^2\right)\\
J_4 =& \frac{\chi}{2^6} \left(\chi^5 + 192\,\chi^4\psi + 13824\,\chi^3\psi^2 + 442368\,\chi^2\psi^3 + 5308416\,\chi\,\psi^4\right.\\
&\left. + 786432\,\chi\,\psi^3 + 9437184\,\psi^4\right)\\
J_6 =& \frac{\chi}{2^9} \left(3\,\chi^8 + 864\,\chi^7\psi + 94464\,\chi^6\psi^2 + 4866048\,\chi^5\psi^3 + 111476736\,\chi^4\psi^4\right.\\
&+ 509607936\,\chi^3\psi^5 - 12230590464\,\chi^2\psi^6 + 1310720\,\chi^4\psi^3 + 155713536\,\chi^3\psi^4\\
&\left. - 1358954496\,\chi^2\psi^5 - 18119393280\,\chi\,\psi^6 + 4831838208\,\psi^6\right)\\
J_{10} =& - 2^{30}\chi^3\psi^9
\end{aligned}$$

It would be an interesting problem to determine for what values of $\chi$ and $\psi$ the curve $\mathcal{C}$ is defined over the field of moduli.

3.2.1. *Elliptic components.* We express the j-invariants $j_i$ of the elliptic components $\mathcal{E}_i$ of $\mathcal{A}$, from Eq. (19), in terms of $u$ and $v$ as follows:

$$\begin{aligned}
j_1 &= 16\mathfrak{v}\,\frac{(\mathfrak{v}\mathfrak{u}^2 + 216\mathfrak{u}^2 - 126\mathfrak{v}\mathfrak{u} - 972\mathfrak{u} + 12\mathfrak{v}^2 + 405\mathfrak{v})^3}{(\mathfrak{v}-27)^3(4\mathfrak{v}^2 + 27\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{v}\mathfrak{u} - \mathfrak{v}\mathfrak{u}^2)^2}\\
j_2 &= -256\,\frac{(\mathfrak{u}^2 - 3\mathfrak{v})^3}{\mathfrak{v}(4\mathfrak{v}^2 + 27\mathfrak{v} + 4\mathfrak{u}^3 - 18\mathfrak{v}\mathfrak{u} - \mathfrak{v}\mathfrak{u}^2)}
\end{aligned} \tag{21}$$

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 $\chi$ and $\psi$ invariants as follows:

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

$$j^2 - s\,j + t = 0 \tag{22}$$

*where*

$$\begin{aligned}
s =& \frac{1}{16777216\psi^3\chi^8} \left(1712282664960\psi^3\chi^6 + 1528823808\psi^4\chi^6 + 49941577728\psi^4\chi^5\right.\\
&- 38928384\psi^5\chi^5 - 258048\psi^6\chi^4 + 12386304\psi^6\chi^3 + 901736973729792\psi\chi^{10}\\
&+ 966131712\psi^5\chi^4 + 16231265527136256\chi^{10} + 480\psi^8\chi + 101376\psi^7\chi^2\\
&+ 479047767293952\psi\chi^8 + 7827577896960\psi^2\chi^9 + 2705210921189376\chi^9\\
&+ 21641687369515008\chi^{12} + 32462531054272512\chi^{11} + \psi^9\\
&+ 619683250176\psi^3\chi^7 + 1408964021452800\psi\chi^9 + 45595641249792\psi^2\chi^8\\
&\left. + 7247757312\psi^3\chi^8 + 37572373905408\psi^2\chi^7\right)\\
t =& - \frac{1}{68719476736\chi^12\psi^3} (84934656\chi^5 + 1179648\chi^4\psi - 5308416\chi^4\\
&-442368\chi^3\psi - 13824\chi^2\psi^2 - 192\chi\psi^3 - \psi^4)^3
\end{aligned} \tag{23}$$

*Proof.* Substitute $j_1$ and $j_2$ as in Eq. (21) in equation Eq. (22). $\square$

**Remark 1.** *The computation of the above equation is rather involved; see [24] or [26] for details. Notice that if $\mathcal{C}$ is defined over a field $K$ then $\chi, \psi \in K$. The converse is not necessarily true.*

Invariants $s$ and $t$ are *modular invariants* similar to the $n = 2$ case and can be expressed in terms of the Siegel modular forms or equivalently in terms of the Igusa arithmetic invariants.

Let $K$ be the field of moduli of $\mathcal{C}$. The discriminant of the quadratic in Eq. (22) is given by

$$\begin{aligned}\Delta(\chi,\psi) = \frac{1}{2^{48}\,\chi^{16}\psi^6}\,\big(&48922361856\,\chi^8 + 48922361856\,\chi^7 + 2293235712\,\psi\,\chi^6\\ &+ 31850496\,\psi^2\chi^5 + 110592\,\psi^3\chi^4 + 12230590464\,\chi^6 + 1528823808\,\psi\,\chi^5\\ &+79626240\,\psi^2\chi^4 + 2211840\,\psi^3\chi^3 + 34560\,\psi^4\chi^2 + 288\,\psi^5\chi + \psi^6\big)^2\\ &\big(195689447424\,\chi^8 + 195689447424\,\chi^7 - 2038431744\,\psi\,\chi^6 + 48922361856\,\chi^6\\ &- 113246208\,\psi^2\chi^5 + 5096079360\,\psi\,\chi^5 - 753664\,\psi^3\chi^4 + 217645056\,\psi^2\chi^4\\ &+4866048\,\psi^3\chi^3 + 59904\,\psi^4\chi^2 + 384\,\psi^5\chi + \psi^6\big)\end{aligned} \tag{24}$$

Notice that this is a perfect square if and only if the second factor is a perfect square in $K$. Similarly with the case $n = 2$ we define the following;

$$\mathcal{S}_3: \qquad y^2 = S_3(\chi,\psi), \tag{25}$$

where

$$\begin{aligned}S_3(\chi,\psi) :=&2^{28}\cdot 3^6\chi^8 + 2^{28}\cdot 3^6\chi^7 - 2^{23}\cdot 3^5(\psi-24)\chi^6 - 2^{22}\cdot 3^3\psi(\psi-45)\chi^5\\ &- 2^{15}\psi^2(23\psi - 6642)\chi^4 + 2^{14}\cdot 3^3\cdot 11\psi^3\chi^3 + 2^9\cdot 3^2\cdot 13\psi^4\chi^2\\ &+ 2^7\cdot 3\psi^5\chi + \psi^6\end{aligned} \tag{26}$$

is the second factor in the discriminant $\Delta(\chi,\psi)$. Even in this case there is a degree 2 covering

$$\begin{aligned}\Phi : \mathcal{S}_3 &\mapsto \mathcal{L}_3\\ (\chi,\psi,\pm y) &\to (\chi,\psi)\end{aligned}$$

from $\mathcal{S}_3$ to the space of genus 2 curves with $(3,3)$-reducible Jacobians.

**Lemma 5.** *Let $\mathcal{C}$ be a genus 2 curve with $(3,3)$ reducible Jacobian. The elliptic components of $\mathrm{Jac}(\mathcal{C})$ are defined over the field of moduli $K$ of $\mathcal{C}$ only when $S_3(\chi,\psi)$ is a complete square in $K$ or equivalently when the surface $y^2 = \mathcal{S}_3(\chi,\psi)$, has $K$-rational point.*

*Proof.* The proof is similar to that of the case $n = 2$. Invariants $\chi, \psi$ are in the field of moduli $K$ of $\mathcal{C}$; see [24]. When the surface $y^2 = \mathcal{S}_3(\chi,\psi)$, has $K$-rational point that means that $j_1, j_2 \in K$ and therefore $E_1$ and $E_2$ are defined over $K$. □

Notice that in this case the curve $\mathcal{C}$ is not necessarily defined over its field of moduli $K$. In [19] we determine exact conditions when this happens.

3.2.2. *Isogenies between the elliptic components.* Now let us consider the case when $n = 3$. 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 8.** *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 $\mathcal{C}$ defined over $\mathcal{K}$ 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. (23). We get a curve in $\chi$, $\psi$ of genus 169. From Faltings theorem there are only finitely many $K$-rational points $(\chi,\psi)$. Since, $K(\chi,\psi)$ is the field of moduli of $\mathcal{C}$, then $\mathcal{C}$ can not be defined over $K$ if $\chi,\psi$ are not in $K$. This completes the proof. $\square$

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 $\chi,\psi$ 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

(27)

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

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.

**Proposition 9.** *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 $\mathcal{C}$ defined over $K$ such that $E_1$ is $N$-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 [17]. One can possibly even investigate cases for $n>5$ by using results of [13]. However, the computations will be much more complicated.

We summarize our results in the following theorem.

**Theorem 1.** *Let $\mathcal{C}$ be e genus 2 curve, defined over a number field $K$, and $\mathcal{A} :=$ $\mathrm{Jac}(\mathcal{C})$ with canonical principal polarization $\iota$, such that $\mathcal{A}$ is geometrically $(n,n)$ reducible to $E_1 \times E_2$. Then the following hold:*

**i):** *If $n = 2$ and $\mathrm{Aut}\,(\mathcal{A}, \iota) \cong V_4$ then there are finitely many elliptic components $E_1, E_2$ defined over $K$ and $N = 2, 3, 5, 7$-isogenous to each other*

**ii):** *If $n = 2$ and $\mathrm{Aut}\,(\mathcal{A}, \iota) \cong D_4$ then*

*a) there are infinitely many elliptic components $E_1, E_2$ defined over $K$ and $N = 2$-isogenous to each other*

*b) there are finitely many elliptic components $E_1, E_2$ defined over $K$ and $N = 3, 5, 7$-isogenous to each other*

**iii):** *If $n = 3$ then*

*a) there are finitely many elliptic components $E_1, E_2$ defined over $K$ and $N = 5$-isogenous to each other*

*b) there are possible infinitely many elliptic components $E_1, E_2$ defined over $K$ and $N = 2, 3, 7$-isogenous to each other*

*Proof.* From [9, Thm. 32] or [29] we have that $\mathrm{Aut}\,(\mathcal{C}) \cong \mathrm{Aut}\,(\mathcal{A}, \iota)$. Consider now the case when $n = 2$ and $\mathrm{Aut}\,(\mathcal{C}) \cong V_4$. From Prop. 6 we have the result. If $\mathrm{Aut}\,(\mathcal{A}, \iota) \cong D_4$ then from Prop. 7 we have the result ii).

Part iii) a) follows from Prop. 8 and part iii) b) from Prop. 9. □

**Corollary 1.** *Let $\mathcal{A}$ be a 2-dimensional Jacobian variety, defined over a number field $K$, and $(3, 3)$ isogenous to the product of elliptic curves $E_1 \times E_2$. Then there are infinitely many curves $E_1, E_2$ defined over $K$ and $N = 2, 3, 7$-isogenous to each other.*

*Proof.* We computationally check that the corresponding conic has a $K$-rational point. □

As a final remark we would like to add that we are not aware of any other methods, other than computational ones, to determine for which pairs $(n, N)$ we have many $K$-rational elliptic components.

## 4. Kummer and Shioda-Inose surfaces of reducible Jacobians

Consider $\mathcal{C}$ a genus two curve with $(n, n)$-decomposable Jacobian and $E_1$, $E_2$ its elliptic components. We continue our discussion of Kummer $\mathrm{Kum}(\mathrm{Jac}(\mathcal{C}))$ and Shioda-Inose $\mathrm{SI}(\mathrm{Jac}(\mathcal{C}))$ surfaces of $\mathrm{Jac}\,\mathcal{C}$ started in Section 2.3.

Malmendier and Shaska in [18] proved that as a genus two curve $\mathcal{C}$ varies the Shioda-Inose K3 surface $\mathrm{SI}(\mathrm{Jac}(\mathcal{C}))$ fits into the following forur parameter family in $\mathbb{P}^3$ given in terms of the variables $[W : X : Y : Z] \in \mathbb{P}^3$ by the equation

$$Y^2 ZW - 4\, X^3 Z + 3\alpha\, XZW^2 + \beta\, ZW^3 + \gamma\, XZ^2 W - \frac{1}{2}(\delta\, Z^2 W^2 + W^4) = 0, \tag{28}$$

where the parameters $(\alpha, \beta, \gamma, \delta)$ can be given in terms of the Igusa-Clebsch invariants by

$$(\alpha, \beta, \gamma, \delta) = \left( \frac{1}{4} I_4, \frac{1}{8} I_2 I_4 - \frac{3}{8} I_6, -\frac{243}{4} I_{10}, \frac{243}{32} I_2 I_{10} \right) \tag{29}$$

Denote by $\mathcal{S}$ the moduli space of the Shioda-Inose surfaces given in Eq. (29) and $\mathcal{L}_n$ the locus in $\mathcal{M}_2$ of $(n, n)$-reducible genus 2 curves. Then there is a map

$$\phi_n : \mathcal{L}_n \to \mathcal{S}$$

such that every curve $[\mathcal{C}] \in \mathcal{L}_n$ goes to the corresponding $\mathrm{SI}(\mathrm{Jac}(\mathcal{C}))$. Then we have the following:

**Proposition 10.** *For $n=2,3$ the map $\phi_n$ is given as follows:*

*i) If $n=2$ then the Shioda-Inose surface is given by Eq. (28) for*

$$
\begin{aligned}
\alpha &= u^2 - 126\,u + 12\,v + 405\\
\beta &= -u^3 - 729\,u^2 + 36\,uv - 4131\,u + 1404\,v + 3645\\
\gamma &= -3888\,\left(u^2+18\,u-4\,v-27\right)^2\\
\delta &= 7776\,(15+u)\left(u^2+18\,u-4\,v-27\right)^2
\end{aligned}
\tag{30}
$$

*ii) if $n=3$ then the Shioda-Inose surface is given by Eq. (28) for*

$$
\begin{aligned}
\alpha =& \frac{1}{256}\cdot\chi\cdot\left(\chi^5+192\,\chi^4\psi+13824\,\chi^3\psi^2+442368\,\chi^2\psi^3+5308416\,\chi\,\psi^4+\right.\\
&\left.+786432\,\chi\,\psi^3+9437184\,\psi^4\right)\\
\beta =& \frac{1}{512}\cdot\chi^2\cdot\left(\chi^2+96\,\chi\,\psi-1152\,\psi^2\right)\cdot\left(\chi^5+192\,\chi^4\psi+13824\,\chi^3\psi^2+\right.\\
&\left.+442368\,\chi^2\psi^3+5308416\,\chi\,\psi^4+786432\,\chi\,\psi^3+9437184\,\psi^4\right)\\
\gamma =& -\frac{3}{4096}\chi\cdot\left(3\,\chi^8+864\,\chi^7\psi+94464\,\chi^6\psi^2+4866048\,\chi^5\psi^3+111476736\,\chi^4\psi^4+\right.\\
&+509607936\,\chi^3\psi^5-12230590464\,\chi^2\psi^6+1310720\,\chi^4\psi^3+155713536\,\chi^3\psi^4-\\
&\left.-1358954496\,\chi^2\psi^5-18119393280\,\chi\,\psi^6+4831838208\,\psi^6\right)\\
\delta =& -2^{25}\,3^5\,\chi^4\left(\chi^2+96\,\chi\,\psi-1152\,\psi^2\right)\psi^9
\end{aligned}
\tag{31}
$$

*Proof.* Case i) is a direct substitution of $J_2,\dots,J_{10}$, given in terms of $u$ and $v$ in [27], in Eq. (29). To prove case ii) we first express the Igusa invariants $J_2,\dots,J_{10}$ in terms of $\chi$ and $\psi$. Then using Eq. (29) we have the desired result. $\square$

**Remark 2.** *It was shown in [27] (resp. [24]) that invariants $u$ and $v$ (resp. $\chi$ and $\psi$) are modular invariants given explicitly in terms of the genus 2 Siegel modular forms.*

**Corollary 2.** *Let $\mathcal{C}$ be e genus 2 curve, defined over a number field $K$, with canonical principal polarization $\iota$, such that $\mathrm{Jac}(\mathcal{C})$ is geometrically $(n,n)$ reducible to $E_1\times E_2$ and $E_1$ is $N$-isogenous to $E_2$. There are only finitely many $\mathrm{SI}(\mathrm{Jac}(\mathcal{C})$ surfaces defined over $K$ such that*

**i):** *$n=2$, $\mathrm{Aut}\,(\mathrm{Jac}(\mathcal{C}),\iota)\cong V_4$, and $N=2,3,5,7$.*
**ii):** *$n=2$, $\mathrm{Aut}\,(\mathrm{Jac}(\mathcal{C}),\iota)\cong D_4$, and $N=3,5,7$.*
**iii):** *$n=3$ and $N=5$*

*Proof.* The Eq. (28) of the surface $\mathrm{SI}(\mathrm{Jac}(\mathcal{C})$ is defined over $k$ when $u$ and $v$ (resp. $\chi$ and $\psi$) are defined over $k$. From Thm. 1 we know that there are only finitely many $k$-rational ordered pairs $(u,v)$ (resp. $(\chi,\psi)$). $\square$

If the elliptic curves are defined by the equations

$$E_1:\ y^2=x^3+ax+b,\qquad E_2:\ y^2=x^3+cx+d$$

then an affine singular model of the $\mathrm{Kum}(\mathrm{Jac}(\mathcal{C}))$ is given as follows

$$x_2^3+cx_2+d=t_2^2(x_1^3+ax_1+b). \tag{32}$$

The map $\mathrm{Kum}(\mathrm{Jac}(\mathcal{C}))\to\mathbb{P}^1$, such that $(x_1,x_2,t_2)\to t_2$, is an elliptic fibration, which in the literature it is known as Kummer pencil. This elliptic fibration has geometric sections that are defined only over the extension $k(E_1[2],E_2[2])/k$.

Take a parameter $t_6$ such that $t_2 = t_6^3$ and consider Eq. (32) as a family of cubic curves in $\mathbb{P}^2$ over the field $k(t_6)$. This family has a rational point $(1 : t_6^2 : 0)$ and using this rational point we can get the Weierstrass form of the Eq. (32) as follows

$$Y^2 = X^3 - 3acX + \frac{1}{64}\left(\Delta_{E_1} t_6^6 + 864bd + \frac{\Delta_{E_2}}{t_6^6}\right)$$

where $\Delta_{E_1}$ and $\Delta_{E_2}$ are respectively the discriminant of the elliptic curves $E_1$ and $E_2$. Note that if we choose other equations of $E_1$ and $E_2$ then we get an isomorphic equation for the Kummer surface. Setting $t_1 = t_6^6$ in the above equation we get an elliptic curve which will be denoted with $F^{(1)}_{E_1,E_2}$ and the Néron-Severi model of this elliptic curve over $k(t_1)$ is called the *Inose surface* associated with $E_1$ and $E_2$, see [14] for more details.

**Definition 2.** *For $s = 1, \dots, 6$ let $t_s$ be a parameter satisfying $t_s^s = t_1$. Define the elliptic curve $F^{(s)}_{E_1,E_2}$ over $k(t_s)$ by*

$$F^{(s)}_{E_1,E_2} : Y^2 = X^3 - 3acX + \frac{1}{64}\left(\Delta_{E_1} t_s^s + 864bd + \frac{\Delta_{E_2}}{t_s^s}\right) \tag{33}$$

Note that the Kodaira-Néron model of $F^{(s)}_{E_1,E_2}$ is a K3 surface for $s = 1, \dots, 6$ but not for $s \geq 7$. The following proposition is a direct consequence of [14, Prop. 2.9] and Thm. 1.

**Lemma 6.** *Let $\mathcal{A} := \operatorname{Jac}\mathcal{C}$ be an $(n,n)$-decomposable Jacobian and $E_1$, $E_2$ its elliptic components. For $n = 2, 3$ there are infinitely many values for $t_5$ and $t_6$ such that the Mordell-Weil groups $F^{(5)}_{E_1,E_2}(\bar{k}(t_5))$ and $F^{(6)}_{E_1,E_2}(\bar{k}(t_6))$ have rank 18.*

*Proof.* From Thm. 1 we know that for $n = 2, 3$ there are infinitely many curves $E_1$ that are isogenous to $E_2$. From [14, Prop. 2.9] we have that if $E_1$ is isogenous to $E_2$ and they have complex multiplication, then the rank of $F^{(5)}$ and $F^{(6)}$ is 18. ☐

**Corollary 3.** *The field of definition of the Mordell-Weil group of $F^{s}_{E_1,E_2}(\bar{k}(t))$ is contained in $k(E_1[s] \times E_2[s])$, for almost all $t$.*

*Proof.* From Thm. 1 we know that for almost all $(n,n)$-Jacobians, $n = 2, 3$, $E_1$ is not isogenous to $E_2$. The result follows as a consequence of [14, Thm.2.10 (i)]. ☐

4.1. **Kummer surfaces in positive characteristic and applications to cryptography.** Supersingular isogeny based cryptography currently uses elliptic curves that are defined over a quadratic extension field $L$ of a non-binary field $K$ and such that its entire 2-torsion is $L$-rational. More specifically implementations of supersingular isogeny Diffie Hellman (SIDH) fix a large prime field $K = \mathbb{F}_p$ with $p = 2^i 3^j - 1$ for $i > j > 100$, construct $L = \mathbb{F}_{p^2}$ and work with supersingular isogeny elliptic curves over $\mathbb{F}_{p^2}$ whose group structures are all isomorphic to $\mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$. Hence, all such elliptic curves have full rational 2-torsion and can be written in Montgomery form.

What is the relation between the Abelian surfaces $\operatorname{Jac}(\mathcal{C})$ defined over $\mathbb{F}_p$ when the elliptic components are supersingular Montgomery curves defined over $\mathbb{F}_{p^2}$? This is relevant in supersingular isogeny based cryptography since computing isogenies in the Kummer surface associated to supersingular Jacobians is much more efficient than computing isogenies in the full Jacobian group.

In [4] are studied $(2,2)$-reducible Jacobians and it is pointed out that most of the literature on the topic studies the splitting of $\mathrm{Jac}(\mathcal{C})$ over the algebraic closure $\bar{K}$. However, form our Lem. 2 we get necessary and sufficient conditions when $\mathrm{Jac}(\mathcal{C})$ splits over $K$. From [27] we know that for a curve $\mathcal{C} \in \mathcal{L}_2$, we can choose the curve to have equation

$$y^2 = (x^2-\lambda_1)(x^2-\lambda_2)\left(x^2 - \frac{1}{\lambda_1\lambda_2}\right)$$

and its elliptic subcovers have equations $y^2 = (x-\lambda_1)(x-\lambda_2)\left(x^2 - \frac{1}{\lambda_1\lambda_2}\right)$ and $y^2 = x(x-\lambda_1)(x-\lambda_2)\left(x^2 - \frac{1}{\lambda_1\lambda_2}\right)$.

We can reverse the above construction as follows. Let $p \equiv 3 \mod 4$ and $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ for $i^2=-1$. Consider the following supersingular Montgomery curve

$$E_\alpha : y^2 = x(x-\alpha)\left(x - \frac{1}{\alpha}\right), \tag{34}$$

for $\alpha \notin \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^2}$ such that $\alpha = \alpha_0 + \alpha_1 i$, for some $\alpha_0, \alpha_1 \in \mathbb{F}_p$. Then by lifting to a genus 2 curve we get a genus two curve $\mathcal{C}$ given as follows

$$\mathcal{C} : y^2 = f_1(x)\, f_2(x)\, f_3(x).$$

where

$$\begin{aligned}
f_1(x) &= x^2 + \frac{2\alpha_0}{\alpha_1}\, x - 1\\
f_2(x) &= x^2 - \frac{2\alpha_0}{\alpha_1}\, x - 1\\
f_3(x) &= x^2 - \frac{2\alpha_0(\alpha_0^2+\alpha_1^2-1)}{\alpha_1(\alpha_0^2+\alpha_1^2+1)}\, x - 1
\end{aligned} \tag{35}$$

Then, Thus, $\mathrm{Jac}\,\mathcal{C}$ is $(2,2)$-reducible with elliptic components the above curves.

The Weil restriction of the 1-dimensional variety $E_\alpha(\mathbb{F}_{p^2})$ is the the variety

$$W_\alpha := \mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha) = V(W_0(x_0,x_1,y_0,y_1), W_1(x_0,x_1,y_0,y_1))$$

where

$$\begin{aligned}
W_0 =& (\alpha_0^2+\alpha_1^2)(\alpha_0(x_0^2-x_1^2) - 2\alpha_1 x_0 x_1 + \delta_0(y_0^2-y_1^2) - 2\delta_1 y_0 y_1\\
&- x_0(x_0^2-3x_1^2+1)) + \alpha_0(x_0^2-x_1^2) + 2\alpha_1 x_0 x_1\\
W_1 =& (\alpha_0^2+\alpha_1^2)(\alpha_1(x_0^2-x_1^2) - 2\alpha_0 x_0 x_1 + \delta_1(y_0^2-y_1^2) - 2\delta_0 y_0 y_1\\
&- x_0(x_0^2-3x_1^2+1)) + \alpha_1(x_0^2-x_1^2) + 2\alpha_0 x_0 x_1
\end{aligned}$$

are obtained by putting $x = x_0 + x_1 i$, $y = y_0 + y_1 i$, $\delta = \delta_0 + \delta_1 i$, and $x_i, y_i, \alpha_i, \delta_i \in \mathbb{F}_p$ for $i = 0, 1$. In [4] it was proved the following:

**Lemma 7.** *Let $E_\alpha$ and $\mathcal{C}$ be as defined above. Then, the Weil restriction of $E_\alpha(\mathbb{F}_{p^2})$ is $(2,2)$-isogenous to the Jacobian $\mathrm{Jac}_{\mathbb{F}_p}(\mathcal{C})$ i.e.*

$$\mathrm{Jac}_{\mathbb{F}_p}(\mathcal{C}) \cong Res_{\mathbb{F}_p}^{F_p^2}(E_\alpha)$$

*Moreover, since $E_\alpha$ is supersingular then $\mathrm{Jac}(\mathcal{C})$ is supersingular.*

From our results in the previous section we have that

**Corollary 4.** *Let $C$ be defined over $\mathbb{F}_p$. Then, $\mathrm{Jac}(\mathcal{C})$ is $(2,2)$ reducible over $\mathbb{F}_p$ if and only if $S_2(u,v)$ is a complete square in $\mathbb{F}_p$ or equivalently $\mathcal{S}_2$ has $\mathbb{F}_p$ points.*

*Proof.* Since the equation of both elliptic components is defined over their field of moduli that means that their minimal field of definition is determined by their $j$-invariants. Such invariants are defined over $\mathbb{F}_p$ if and only if when $\mathcal{S}(u, v)$ in Eq. (7) is a complete square in $\mathbb{F}_p$. $\square$

What about $(3,3)$-reducible Jacobians? The situation is slightly different. The main reason is that a curve $\mathcal{C} \in \mathcal{L}_3$ is not necessarily defined over its field of moduli. However, if we start with a curve $\mathcal{C} \in \mathcal{L}_3$ defined over $\mathbb{F}_p$, then from Lem. 5 we can determine precisely when $\mathrm{Jac}(\mathcal{C})$ splits over $\mathbb{F}_p$. The above construction via the Weils restriction is a bit more complicated for curves in $\mathcal{L}_3$.

The case for the Kummer approach in supersingular isogeny-based cryptography would be much stronger if it were able to be applied efficiently for both parties. There has been some explicit work done in the case of (3, 3) [24] and (5, 5)-isogenies [17], but those situations are much more complicated than the case of Richelot isogenies.

As pointed out by Costello in the last paragraph of [4]: *One hope in this direction is the possibility of pushing odd degree l-isogeny maps from the elliptic curve setting to the Kummer setting. This was difficult in the case of 2-isogenies because the maps themselves are (2, 2)- isogenies, but in the case of odd degree isogenies there is nothing obvious preventing this approach.*

## References


[1] L. Beshaj, *Minimal integral Weierstrass equations for genus 2 curves*, Higher genus curves in mathematical physics and arithmetic geometry, 2018, pp. 63–82. MR3782460

[2] Lubjana Beshaj, *Absolute reduction of binary forms*, Albanian J. Math. **12** (2018), no. 1, 36–77. MR3914348

[3] Adrian Clingher and Charles F. Doran, *Modular invariants for lattice polarized k3 surfaces*, Michigan Mathematical Journal **215** (2007), no. 2.

[4] Craig Costello, *Computing supersingular isogenies on kummer surfaces* (2018).

[5] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, 2008, pp. 51–69. MR2457735

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR718935

[7] Gerhard Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus* 2, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 1995, pp. 79–98. MR1363496

[8] Gerhard Frey and Ernst Kani, *Curves of genus 2 with elliptic differentials and associated Hurwitz spaces*, Arithmetic, geometry, cryptography and coding theory, 2009, pp. 33–81. MR2555986

[9] Gerhard Frey and Tony Shaska, *Curves, Jacobians, and Cryptography*, Algebraic curves and their applications, 2019, pp. 280–350.

[10] Ki-ichiro Hashimoto and Naoki Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296. MR1329525

[11] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649. MR0114819

[12] K. Kodaira, *On compact analytic surfaces. II, III*, Ann. of Math. (2) 77 (1963), 563–626; ibid. **78** (1963), 1–40. MR0184257

[13] 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

[14] Abhinav Kumar and Masato Kuwata, *Elliptic K3 surfaces associated with the product of two elliptic curves: Mordell-Weil lattices and their fields of definition*, Nagoya Math. J. **228** (2017), 124–185. MR3721376

[15] Davide Lombardo, *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv (2016).

[16] David Lubicz and Damien Robert, *Computing separable isogenies in quasi-optimal time*, LMS J. Comput. Math. **18** (2015), no. 1, 198–216. MR3349315
[17] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800
[18] A. Malmendier and T. Shaska, *The Satake sextic in F-theory*, J. Geom. Phys. **120** (2017), 290–305. MR3712162
[19] ______, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17. MR3731039
[20] ______, *From hyperelliptic to superelliptic curves*, Albanian J. Math. **13** (2019), no. 1, 107–200. MR3978315
[21] T. Shaska, *Curves of genus 2 with* $(N, N)$ *decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706
[22] ______, *Curves of genus two covering elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2001. Thesis (Ph.D.)–University of Florida. MR2701993
[23] ______, *Genus 2 curves with* $(3, 3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), 2002, pp. 205–218. MR2041085
[24] ______, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100
[25] ______, *Genus two curves covering elliptic curves: a computational approach*, Computational aspects of algebraic curves, 2005, pp. 206–231. MR2182041
[26] ______, *Genus two curves with many elliptic subcovers*, Comm. Algebra **44** (2016), no. 10, 4450–4466. MR3508311
[27] 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
[28] T. Shioda and H. Inose, *On singular* $K3$ *surfaces* (1977), 119–136. MR0441982
[29] Yuri G. Zarhin, *Families of absolutely simple hyperelliptic Jacobians*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 1, 24–54. MR2578467

Depart. of Mathematical Sciences, United States Military Academy at West Point
*E-mail address*: Lubjana.Beshaj@usma.edu

Depart. of Mathematics and Statistics, American University,, Washington DC, 20016.
*E-mail address*: aelezi@american.edu

Depart.of Mathematics and Statistics, Oakland University Rochester, MI, 48309.
*E-mail address*: shaska@oakland.edu