KUMMER SURFACES, ISOGENIES AND THETA FUNCTIONS

ADRIAN CLINGHER, ANDREAS MALMENDIER, AND TONY SHASKA

Abstract. The paper discusses geometric and computational aspects associated with (n, n)-isogenies for principally polarized Abelian surfaces and related Kummer surfaces. We start by reviewing the comprehensive Theta function framework for classifying genus-two curves, their principally polarized Jacobians, as well as for establishing explicit quartic normal forms for associated Kummer surfaces. This framework is then used for practical isogeny computations. A particular focus of the discussion is the (n, n)-Split isogeny case. We also explore possible extensions of Richelot's $(2, 2)$-isogenies to higher order cases, with a view towards developing efficient isogeny computation algorithms.

1. Introduction

Abelian varieties, as projective algebraic groups, generalize elliptic curves to higher dimensions. They are important objects in both algebraic geometry and number theory. Among these, Abelian surfaces—two-dimensional Abelian varieties— are of particular interest, due to their intricate geometric and arithmetic structures, which often lead to important practical applications in applied computational fields such as cryptography. This paper explores computational aspects associated with isogenies between Abelian surfaces, with particular focus on (n, n)-isogenies with $n \in \mathbb{N}_{\geq 2}$. The present work may be seen as a continuation of [14], concentrating primarily to Jacobians of genus 2 curves and their associated Kummer surfaces, with a view towards applications to isogeny-based cryptography.

Kummer surface, defined as minimal resolutions for the quotient of an Abelian surface by its inversion involution, provides a powerful geometric platform for studying isogenies. In the case of Jacobians of genus-two curves, the associated Kummer surface may be explicitly described via various birational models given by projective quartic surfaces. The quartic underlying polynomials are usually referred to as *normal forms* and carry various names – Hudson, Göpel, Rosenhain, Cassels-Flynn, Baker. A common theme for all these normal forms is that they can be derived from the theory of Theta functions and their coefficients can be described in terms of special Theta constants called Theta-nulls.

In the realm of cryptography, isogeny-based protocols like the Supersingular Isogeny Diffie-Hellman (SIDH) leverage the computational hardness of finding isogenies—surjective homomorphisms with finite kernels—as a foundation for secure systems. Extending this paradigm from elliptic curves to Abelian surfaces introduces significant advantages: the n^4-torsion groups of Abelian surfaces are substantially larger than the n^2-torsion groups of elliptic curves, potentially enhancing security, while their richer endomorphism algebras may enable more efficient protocols. However, computing (n, n)-isogenies for $n > 2$ presents formidable challenges due to the increased complexity of the kernel, requiring methods beyond classical Richelot $(2, 2)$-isogenies. Moreover, cryptographic security hinges on addressing vulnerabilities, particularly from split Jacobians—Jacobians isogenous to products of elliptic curves—which can reduce the complexity of isogeny problems.

Building on prior work, this paper provides a methodology for computing (n, n)-isogenies, generalizing Richelot's $(2, 2)$-isogenies to arbitrary odd n with the Lubicz-Robert formula, achieving $O(n^2)$ complexity. Our approach leverages the geometry of Kummer surfaces (for various realizations as projective hypersurfaces) and the associated Shioda-Inose surface—a K3 surface derived as a two-isogeny of the Kummer surface—which provides a Hodge-theoretic connection between the Jacobian and its K3 counterpart, enriching the geometric framework for isogeny computations. We relate our methods to classical constructions,

2020 *Mathematics Subject Classification.* 14J28, 14K02, 14K25.

Key words and phrases. Abelian surfaces, Kummer surfaces, isogenies, Theta function.

A.M. acknowledges support from the Simons Foundation through grant no. 202367.

such as those of Dolgachev-Lehavi, enhancing their applicability through projective embeddings and n-tuple techniques.

We also investigate the loci $\mathcal{L}_n$ of (n,n)-Split Jacobians, characterizing their geometric properties and linking them to Humbert surfaces, which are critical for understanding cryptographic vulnerabilities. Recent advances in artificial intelligence and machine learning [56] and [46] enhance this exploration. The former employs supervised models trained on datasets of genus 2 curves to detect $\mathcal{L}_n$ for arbitrary n, while the latter leverages arithmetic insights in positive characteristic to refine cryptanalysis over finite fields.

The paper is structured as follows. Sections 2–4 lay the theoretical groundwork, detailing Abelian surfaces, their endomorphism rings, Theta functions, the geometry of genus 2 curves and their Jacobians, and the structure of Kummer surfaces, including their embeddings and (16,6)-configurations. Section 5 examines the loci $\mathcal{L}_n$, connecting split Jacobians to Humbert surfaces and highlighting their geometric and cryptographic significance. Section 6 presents our computational methods for (n,n)-isogenies, emphasizing a Kummer surface-based approach with the Lubicz-Robert formula, and comparisons to Dolgachev-Lehavi's techniques. Section 7 applies these results to cryptography, analyzing attacks on the superspecial isogeny problem that exploit $\mathcal{L}_n$ and their implications for protocols like the Castryck-Decru-Smith hash.

2. Abelian varieties

Let $\mathcal{A}$, $\mathcal{B}$ be Abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ by $\mathrm{Hom}(\mathcal{A},\mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$. In the context of linear algebra, it is often more convenient to work with the $\mathbb{Q}$-vector spaces $\mathrm{Hom}^0(\mathcal{A},\mathcal{B}) := \mathrm{Hom}(\mathcal{A},\mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathrm{End}^0\,\mathcal{A} := \mathrm{End}\,\mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Q}$. For an Abelian variety $\mathcal{A}$ defined over a number field K, computing $\mathrm{End}_K(\mathcal{A})$ is a harder problem than computing $\mathrm{End}_{\bar{K}}(\mathcal{A})$; see [40, Lemma 5.1] for details.

Lemma 1. *If there exists an algorithm to compute* $\mathrm{End}_K(\mathcal{A})$ *for any Abelian variety of dimension* $g \geq 1$ *defined over a number field* K*, then there is an algorithm to compute* $\mathrm{End}_{\bar{K}}(\mathcal{A})$.

Proof. Since $K \subseteq \bar{K}$, any endomorphism of $\mathcal{A}$ over $\bar{K}$ restricts to an endomorphism over K after base change, but the converse requires additional structure. An algorithm for $\mathrm{End}_K(\mathcal{A})$ determines the $\mathbb{Z}$-module of K-rational endomorphisms. Extending scalars to $\bar{K}$, we compute $\mathrm{End}_{\bar{K}}(\mathcal{A}) = \mathrm{End}_K(\mathcal{A}) \otimes_{\mathbb{Z}} \bar{K}$, leveraging the finite generation of $\mathrm{End}_K(\mathcal{A})$ and the algebraic closure of $\bar{K}$. The lemma follows from the existence of such an extension procedure. □

2.1. Isogenies of Abelian varieties.

A homomorphism $f\colon \mathcal{A} \longrightarrow \mathcal{B}$ is called an **isogeny** if $\mathrm{Im} f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \longrightarrow \mathcal{B}$ exists, we say that $\mathcal{A}$ and $\mathcal{B}$ are isogenous. This relation is symmetric, as shown in Lemma 3. The degree of an isogeny $f\colon \mathcal{A} \longrightarrow \mathcal{B}$ is defined as the degree of the function field extension

$$\deg f := [K(\mathcal{A}) : f^\star K(\mathcal{B})]. \tag{1}$$

This equals the order of the group scheme $\ker(f)$. The group of $\bar{k}$-rational points has order $\#(\ker f)(\bar{k}) = [K(\mathcal{A}) : f^\star K(\mathcal{B})]^{sep}$, where $[K(\mathcal{A}) : f^\star K(\mathcal{B})]^{sep}$ is the degree of the maximal separable subextension. An isogeny f is **separable** if and only if

$$\#\ker f(\bar{k}) = \deg f, \tag{2}$$

equivalently, if $\ker f$ is étale.

Lemma 2. *For any Abelian variety* $\mathcal{A}/k$*, there is a one-to-one correspondence between finite subgroup schemes* $\mathcal{K} \leq \mathcal{A}$ *and isogenies* $f\colon \mathcal{A} \longrightarrow \mathcal{B}$*, where* $\mathcal{B}$ *is determined up to isomorphism. Moreover,* $\mathcal{K} = \ker f$*,* $\mathcal{B} = \mathcal{A}/\mathcal{K}$*,* f *is separable if and only if* $\mathcal{K}$ *is étale, and then* $\deg f = \#\mathcal{K}(\bar{k})$.

Proof. Given a finite subgroup scheme $\mathcal{K} \leq \mathcal{A}$, the quotient $\mathcal{B} = \mathcal{A}/\mathcal{K}$ is an Abelian variety over k, and the natural projection $f\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an isogeny with $\ker f = \mathcal{K}$. Conversely, for an isogeny $f\colon \mathcal{A} \longrightarrow \mathcal{B}$, the kernel $\mathcal{K} = \ker f$ is finite, and $\mathcal{B} \cong \mathcal{A}/\mathcal{K}$ by the quotient structure. The map $\mathcal{K} \mapsto \mathcal{A}/\mathcal{K}$ is injective (distinct kernels yield distinct quotients) and surjective (every isogeny arises this way), establishing the bijection. Separability of f implies $\ker f$ is étale, and $\deg f = \#\mathcal{K}(\bar{k})$ holds in this case due to the étale order matching the field extension degree. □

Isogenous Abelian varieties have commensurable endomorphism rings: if $\mathcal{A}$ and $\mathcal{B}$ are isogenous, then $\mathrm{End}^0(\mathcal{A}) \cong \mathrm{End}^0(\mathcal{B})$. This follows from the existence of isogenies $f\colon \mathcal{A} \to \mathcal{B}$ and $g\colon \mathcal{B} \to \mathcal{A}$ such that $g \circ f = [n]$, inducing an isomorphism on rational endomorphism algebras.

Theorem 1 (Poincaré-Weil)**.** *Let $\mathcal{A}$ be an Abelian variety. Then $\mathcal{A}$ is isogenous to*

$$\mathcal{A}_1^{n_1} \times \mathcal{A}_2^{n_2} \times \cdots \times \mathcal{A}_r^{n_r}, \tag{3}$$

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

Proof. Since $\mathcal{A}$ is an Abelian variety, its isogeny class contains a product of powers of simple Abelian varieties. Let $\mathcal{A} \cong \prod_{i=1}^{r} \mathcal{A}_i^{n_i}$, where $\mathcal{A}_i$ are simple and pairwise non-isogenous. The uniqueness follows from the Jordan-Hölder theorem for Abelian varieties: any two such decompositions have isomorphic factors with equal multiplicities, up to permutation, due to the indecomposability of simple varieties and the structure of $\mathrm{End}^0(\mathcal{A})$. □

Corollary 1. *If $\mathcal{A}$ is an absolutely simple Abelian variety, then every endomorphism not equal to 0 is an isogeny.*

Proof. For $\mathcal{A}$ absolutely simple, $\mathrm{End}^0(\mathcal{A})$ is a division algebra. A non-zero endomorphism ϕ has trivial kernel (since $\ker \phi \neq \mathcal{A}$ and $\mathcal{A}$ has no proper subvarieties as a simple variety), hence is an isogeny. □

Fix a field k and an Abelian variety $\mathcal{A}$ over k. Let H be a finite subgroup of $\mathcal{A}$. From a computational perspective, we consider: (i) finding all Abelian varieties $\mathcal{B}$ over k such that there exists an isogeny $\mathcal{A} \longrightarrow \mathcal{B}$ with kernel isomorphic to H; (ii) given $\mathcal{A}$ and H, determining $\mathcal{B} := \mathcal{A}/H$ and the isogeny $\mathcal{A} \longrightarrow \mathcal{B}$; (iii) given $\mathcal{A}$ and $\mathcal{B}$, determining if they are isogenous and computing a rational expression for an isogeny $\mathcal{A} \longrightarrow \mathcal{B}$. For a survey and conjectures, see [25].

The scalar multiplication by n map $[n]\colon \mathcal{A} \longrightarrow \mathcal{A}$ is an isogeny with kernel a group scheme of order $n^{2\dim \mathcal{A}}$; see [48]. We denote $\mathcal{A}[n] = \ker[n](\bar{k})$, whose elements are the n-**torsion points** of $\mathcal{A}$.

Lemma 3. *Let $f\colon \mathcal{A} \longrightarrow \mathcal{B}$ be an isogeny of degree n. Then there exists an isogeny $\hat{f}\colon \mathcal{B} \longrightarrow \mathcal{A}$ such that*

$$f \circ \hat{f} = \hat{f} \circ f = [n]. \tag{4}$$

*The isogeny $\hat{f}$ is called the **dual** of f.*

Proof. Define $\hat{f}$ via the dual Abelian variety and the polarization induced by f. Since f is an isogeny, there exists a unique $\hat{f}\colon \mathcal{B} \longrightarrow \mathcal{A}$ such that $f \circ \hat{f} = [n]$ on $\mathcal{B}$ and $\hat{f} \circ f = [n]$ on $\mathcal{A}$, satisfying the duality condition due to the finite kernel's order matching $\deg f = n$. □

Theorem 2. *Let $\mathcal{A}/k$ be an Abelian variety, $p = \mathrm{char}\, k$, 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, and there exists an integer $0 \leq i \leq g$ such that

$$\mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i, \text{ for all } m \geq 1. \tag{5}$$

Proof. If $p \nmid n$, $[n]$ is separable as its derivative is non-zero, and $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ follows from the étale nature of the kernel over $\bar{k}$. If $p \mid n$, $[n]$ includes a power of the Frobenius, making it inseparable, and the p-torsion structure depends on the p-rank i, determined by the dimension of the p-divisible group. □

If $i = g$, $\mathcal{A}$ is **ordinary**; if $\mathcal{A}[p^s](\bar{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$, it has p-**rank** t. For $\dim \mathcal{A} = 1$, it is **supersingular** if p-rank is 0; $\mathcal{A}$ is **supersingular** if isogenous to a product of supersingular elliptic curves.

2.2. **Theta functions.** Let $\mathcal{A}$ be an Abelian variety of dimension g over an algebraically closed field k, which we take as $\mathbb{C}$ for simplicity; the arguments here extend to fields of characteristic p coprime to relevant integers via algebraic Theta functions (see [48]). We consider an algebraic variety $\mathcal{A}$ that can be represented as $\mathbb{C}^g/\Lambda$, where $\Lambda = \mathbb{Z}^g + \tau\mathbb{Z}^g$ is a lattice, and τ is a symmetric $g \times g$ matrix in the Siegel upper half-space $\mathbb{H}_g$, satisfying ${}^t\tau = \tau$ and $\mathrm{Im}(\tau) > 0$.

A *Theta function* with characteristic $[a, b]$, where $a, b \in \mathbb{Q}^g$, is defined as

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n+a)^t \tau (n+a) + 2\pi i (n+a)^t (z+b)\right), \tag{6}$$

for $z \in \mathbb{C}^g$. The series converges absolutely due to the positive definiteness of $\mathrm{Im}(\tau)$, ensuring that $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau)$ is holomorphic on $\mathbb{C}^g$. These functions are quasi-periodic with respect to the lattice Λ: for $m \in \mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + m, \tau) = \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau),$$

and for $n \in \mathbb{Z}^g$,

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + \tau n, \tau) = \exp\left(-\pi i n^t \tau n - 2\pi i n^t (z+b)\right) \theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z, \tau).$$

When $a, b \in \{0, 1/2\}^g$, the characteristic is half-integer, and the parity is even if $4a^t b$ is even, odd if $4a^t b$ is odd, reflecting the function's symmetry properties.

Proof of Quasi-Periodicity. For the first property, substitute $z + m$ into the definition:

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + m, \tau) = \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i (n+a)^t \tau (n+a) + 2\pi i (n+a)^t (z+m+b)\right).$$

Since $(n+a)^t m = n^t m + a^t m$ and $n, m \in \mathbb{Z}^g$, the exponential term $\exp(2\pi i n^t m) = 1$, and $a^t m$ is rational, so the sum reindexes to itself, yielding equality. For the second, let $z' = z + \tau n$:

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z + \tau n, \tau) = \sum_{k \in \mathbb{Z}^g} \exp\left(\pi i (k+a)^t \tau (k+a) + 2\pi i (k+a)^t (z+\tau n+b)\right).$$

Set $k = n - m$, adjust the sum, and compute the difference in exponents, then factoring out the term $\exp\left(-\pi i n^t \tau n - 2\pi i n^t (z+b)\right)$ due to the symmetry ${}^t\tau = \tau$, confirm the multiplier. □

Abelian varieties of the form $\mathcal{A} = \mathbb{C}^g/\Lambda$ are in fact *principally polarized*. In fact, the *canonical principal polarization* of $\mathcal{A}$ is given by the positive definite Hermitian form $\mathbf{h}$ on $\mathbb{C}^g$ such that $\alpha = \mathrm{Im}\,\mathbf{h}(\Lambda, \Lambda)$ is the canonical Riemann form on $\mathbb{Z}^g \oplus \tau\,\mathbb{Z}^g$. In turn, this Hermitian form determines a line bundle $\mathscr{L} \to \mathcal{A}$ in the Néron-Severi lattice $\mathrm{NS}(\mathcal{A})$. We call $\mathscr{L}$ the line bundle associated with the principal polarization, and $\mathscr{L}^n = \mathscr{L}^{\otimes n}$ is its n-th tensor powers. Theta functions are sections of these line bundles over $\mathcal{A}$.

A *level n Theta structure* is given by the functions $\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](z, \tau/n)$, where $b \in (\mathbb{Z}/n\mathbb{Z})^g$. It turns out that these form a basis for the space of sections $\Gamma(\mathcal{A}, \mathscr{L}^n)$. The dimension of this space is n^g, reflecting the number of distinct characteristics $b \in (\mathbb{Z}/n\mathbb{Z})^g$. This basis of sections induces a morphism

$$\varphi_n \colon \mathcal{A} \longrightarrow \mathbb{P}^{n^g - 1}, \quad z \mapsto \left(\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](z, \tau/n)\right)_{b \in (\mathbb{Z}/n\mathbb{Z})^g}. \tag{7}$$

For $n \geq 3$, φ_n is an embedding, realizing $\mathcal{A}$ as a projective variety (see [60], Chapter II).

Theorem 3 (Embedding Theorem)**.** *For an Abelian variety $\mathcal{A}$ of dimension g over $\mathbb{C}$ with a principal polarization, the morphism $\varphi_n \colon \mathcal{A} \longrightarrow \mathbb{P}^{n^g - 1}$ is an embedding for $n \geq 3$.*

Proof. The line bundle $\mathscr{L}^n$ is ample for $n \geq 1$, and for $n \geq 3$, it is very ample, meaning it separates points and tangent vectors. For distinct points $x, y \in \mathcal{A}$, there exists $b \in (\mathbb{Z}/n\mathbb{Z})^g$ such that $\theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](x, \tau/n) \neq \theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](y, \tau/n)$, as the functions span a space large enough to distinguish cosets modulo Λ. For a point x and tangent vector $v \in T_x\mathcal{A}$, the directional derivative $D_v \theta\left[\begin{smallmatrix} 0 \\ b \end{smallmatrix}\right](x, \tau/n) \neq 0$ for some b, due to the completeness of the basis. Thus, φ_n is injective with injective differential, embedding $\mathcal{A}$ into $\mathbb{P}^{n^g - 1}$. □

A key result is the transformation law under the symplectic group $\mathrm{Sp}(2g, \mathbb{Z})$, which acts on $\mathbb{H}_g$. For $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}(2g, \mathbb{Z})$, define the transformed period matrix $\tau' = (A\tau + B)(C\tau + D)^{-1}$ and $z' = z(C\tau + D)^{-1}$. Shimura ([60], Chapter III) provides the functional equation:

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z', \tau') = \kappa(\gamma) \det(C\tau + D)^{1/2} \exp\left(\pi i z (C\tau + D)^{-1} C z^t\right) \theta\left[\begin{smallmatrix} a' \\ b' \end{smallmatrix}\right](z, \tau), \tag{8}$$

where $\kappa(\gamma)$ is a constant, and a', b' are transformed characteristics. This law governs the behavior of Theta functions under automorphisms of $\mathcal{A}$.

Theorem 4 (Riemann Theta Relation)**.** *For $z_1, z_2 \in \mathbb{C}^g$, the Theta functions satisfy*

$$\theta(z_1+z_2)\theta(z_1-z_2) = \sum_{m\in(\mathbb{Z}/2\mathbb{Z})^g} \theta\left[\begin{smallmatrix} m/2 \\ 0 \end{smallmatrix}\right](2z_1)\theta\left[\begin{smallmatrix} m/2 \\ 0 \end{smallmatrix}\right](2z_2), \tag{9}$$

where $\theta(z) = \theta\left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z,\tau)$.

Proof. Consider the product $\theta(z_1+z_2)\theta(z_1-z_2)$ as a sum over $n, m \in \mathbb{Z}^g$. Pair terms with $n+m$ and $n-m$, adjust indices, and use the periodicity properties. The right-hand side arises from a Fourier expansion of the product, with the half-integer characteristics $m/2$ accounting for the doubling $2z_1, 2z_2$. The identity holds by the analytic continuation and symmetry of Theta functions (see [60], Chapter II). □

The values $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\tau)$, called *Theta constants* or Theta-nulls, are significant. For a principally polarized $\mathcal{A}$, they determine τ up to the action of $\mathrm{Sp}(2g,\mathbb{Z})$, parameterizing the moduli space $\mathcal{A}_g$. When $a, b \in \{0, 1/2\}^g$, there are 2^{2g} such constants, half even and half odd, reflecting the 2-torsion structure $\mathcal{A}[2]$.

Lemma 4. *The Theta constants $\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](0,\tau)$ for $a, b \in \{0, 1/2\}^g$ are zero if and only if the characteristic $[a, b]$ is odd.*

Proof. The parity depends on $4a^t b \mod 2$. If odd, the summand $\exp(\pi i(n+a)^t\tau(n+a))$ at $z=0$ pairs terms n and $-n-2a$, with opposite signs due to the linear term $2\pi i(n+a)^t b$, canceling to zero. If even, no such cancellation occurs, and the constant is non-zero generically. □

These results underpin the geometric and analytic properties of Abelian varieties, with Theta functions serving as both coordinates and invariants (see [60] for a comprehensive treatment).

2.3. **Jacobian Varieties.** Jacobian varieties are special algebraic varieties that arise as the connected component of the identity in the Picard group of non-singular algebraic curves.

Let $\mathcal{X}$ be a curve of positive genus over k, and assume there exists a k-rational point $P_0 \in \mathcal{X}(k)$ with attached prime divisor $\mathfrak{p}_0 = (P_0)$. There exists an Abelian variety $\mathrm{Jac}_k(\mathcal{X})$ over k and a uniquely determined embedding

$$\phi_{P_0} \colon \mathcal{X} \longrightarrow \mathrm{Jac}_k(\mathcal{X}) \ \text{ with } \ \phi_{P_0}(P_0) = 0_{\mathrm{Jac}_k(\mathcal{X})}, \tag{10}$$

satisfying:

(1) For all extension fields L of k, $\mathrm{Jac}_L\,\mathcal{X} = \mathrm{Pic}^0_{\mathcal{X}_L}(L)$, with this equality given functorially.
(2) For any Abelian variety $\mathbb{A}$ and morphism $\eta\colon \mathcal{X} \longrightarrow \mathbb{A}$ sending P_0 to $0_{\mathbb{A}}$, there exists a unique homomorphism $\psi\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathbb{A}$ such that $\psi \circ \phi_{P_0} = \eta$.

This universal object $\mathrm{Jac}(\mathcal{X})$, called the *Jacobian variety* of $\mathcal{X}$, maps a prime divisor $\mathfrak{p}$ of degree 1 on $\mathcal{X}_L$ to $[\mathfrak{p} - \mathfrak{p}_0]$ in $\mathrm{Pic}^0_{\mathcal{X}_L}(L)$.

Lemma 5. *The Jacobian $\mathrm{Jac}(\mathcal{X})$ is unique up to isomorphism among Abelian varieties satisfying the above properties.*

Proof. Suppose $\mathcal{J}_1$ and $\mathcal{J}_2$ satisfy the conditions with embeddings $\phi_1\colon \mathcal{X} \longrightarrow \mathcal{J}_1$ and $\phi_2\colon \mathcal{X} \longrightarrow \mathcal{J}_2$. By property (2), there exist homomorphisms $\psi_{12}\colon \mathcal{J}_1 \longrightarrow \mathcal{J}_2$ and $\psi_{21}\colon \mathcal{J}_2 \longrightarrow \mathcal{J}_1$ such that $\psi_{12}\circ\phi_1 = \phi_2$ and $\psi_{21}\circ\phi_2 = \phi_1$. Composing, $\psi_{21}\circ\psi_{12}\circ\phi_1 = \phi_1$. Since $\phi_1(\mathcal{X})$ generates $\mathcal{J}_1$ as a group (by the Abel-Jacobi theorem), and $\mathcal{J}_1$ is Abelian, $\psi_{21}\circ\psi_{12}$ acts as the identity on a dense subset, hence $\psi_{21}\circ\psi_{12} = \mathrm{id}_{\mathcal{J}_1}$. Similarly, $\psi_{12}\circ\psi_{21} = \mathrm{id}_{\mathcal{J}_2}$, establishing an isomorphism $\mathcal{J}_1 \cong \mathcal{J}_2$. □

Let L/k be a finite algebraic extension. Then $\mathrm{Jac}_L\,\mathcal{X}$ is the scalar extension of $\mathrm{Jac}\,\mathcal{X}$ with L, forming a fiber product with projection $p\colon \mathrm{Jac}_L\,\mathcal{X} \longrightarrow \mathrm{Jac}\,\mathcal{X}$. The norm map is p_*, and the conorm map is p^*. If $f\colon \mathcal{X} \longrightarrow \mathcal{D}$ is a surjective morphism of curves sending P_0 to Q_0, there exists a unique surjective homomorphism $f_*\colon \mathrm{Jac}\,\mathcal{X} \longrightarrow \mathrm{Jac}\,\mathcal{D}$ such that $f_*\circ\phi_{P_0} = \phi_{Q_0}$. If $\mathrm{Jac}\,\mathcal{X}$ is simple and $\eta\colon \mathcal{X} \longrightarrow \mathcal{D}$ is a separable cover of degree > 1, then $\mathcal{D} \cong \mathbb{P}^1$, as any non-trivial quotient of a simple Abelian variety is trivial.

2.4. **Endomorphism rings of Abelian varieties.** The endomorphism ring of an Abelian variety is a fundamental invariant that encodes its algebraic symmetries and arithmetic structure. For an Abelian variety $\mathcal{A}$ of dimension g over a field k, we define $\mathrm{End}(\mathcal{A})$ as the ring of regular morphisms $\phi : \mathcal{A} \to \mathcal{A}$ that preserve the group operation, satisfying $\phi(x+y) = \phi(x) + \phi(y)$ for all $x, y \in \mathcal{A}(k')$ over any extension field k'. Equipped with addition and composition, and with the identity map as the unit, $\mathrm{End}(\mathcal{A})$ forms a $\mathbb{Z}$-module, but its full complexity emerges in the rational endomorphism algebra $\mathrm{End}^0(\mathcal{A}) = \mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$, a finite-dimensional $\mathbb{Q}$-algebra. Over an algebraically closed field such as $\mathbb{C}$ or $\overline{\mathbb{Q}}$, this algebra provides insight into the variety's isogeny class and geometric properties.

An endomorphism $\phi \in \mathrm{End}(\mathcal{A})$ is an isogeny if it is surjective with a finite kernel, its degree $\deg \phi$ being the order of $\ker \phi$ as a group scheme. Such a ϕ has a dual isogeny $\hat{\phi}\colon \mathcal{A} \longrightarrow \mathcal{A}$ such that $\phi \circ \hat{\phi} = [\deg \phi]$, where $[n]\colon \mathcal{A} \longrightarrow \mathcal{A}$ denotes multiplication by n. A key property across all dimensions is that $\mathrm{End}^0(\mathcal{A})$ is invariant under isogeny: if $\mathcal{A}$ and $\mathcal{B}$ are isogenous Abelian varieties, meaning there exists an isogeny $f\colon \mathcal{A} \longrightarrow \mathcal{B}$, then their rational endomorphism algebras are isomorphic. To see this, consider f with dual $\hat{f}$ satisfying $f \circ \hat{f} = [n]$. The map $\Phi\colon \mathrm{End}(\mathcal{B}) \longrightarrow \mathrm{End}(\mathcal{A})$ given by $\Phi(\phi) = f \circ \phi \circ \hat{f}$ is a ring homomorphism, and extending it to $\mathrm{End}^0(\mathcal{B})$ via $\Phi'(\phi) = \frac{1}{n} f \circ \phi \circ \hat{f}$ yields an isomorphism, as Φ' is injective (if $f \circ \phi \circ \hat{f} = 0$, then $\phi = 0$ since f and $\hat{f}$ are isogenies) and surjective via the inverse map adjusted by scalars (see [48], Chapter III, §19). This invariance underpins the study of endomorphism algebras across isogeny classes.

For an Abelian variety $\mathcal{A}$, the structure of $\mathrm{End}^0(\mathcal{A})$ depends on its decomposition. The Poincaré-Weil theorem asserts that $\mathcal{A}$ is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, where the $\mathcal{A}_i$ are simple (having no non-trivial Abelian subvarieties) and pairwise non-isogenous, with the factors uniquely determined up to permutation and isogeny ([48], Chapter III, §15). If $\mathcal{A}$ is simple, $\mathrm{End}^0(\mathcal{A})$ is a division algebra over its center Z, and $[Z : \mathbb{Q}] \cdot [\mathrm{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = g^2$. If $\mathcal{A}$ is not simple, $\mathrm{End}^0(\mathcal{A})$ is a product of the endomorphism algebras of its factors, adjusted for isogenies.

When we narrow our focus to Abelian surfaces, where $\dim \mathcal{A} = 2$, the classification of $\mathrm{End}^0(\mathcal{A})$ becomes more precise, especially over $\overline{\mathbb{Q}}$. Here, an endomorphism ϕ acts on a 2-dimensional variety, and the possible structures of $\mathrm{End}^0(\mathcal{A})$ are richly detailed by Albert's classification, as refined in [51]. For a principally polarized Abelian surface $\mathcal{A}$—where a polarization $\lambda\colon \mathcal{A} \longrightarrow \hat{\mathcal{A}}$ to the dual has degree 1—the algebra $\mathrm{End}^0_{\overline{\mathbb{Q}}}(\mathcal{A})$ can be one of several types: $\mathbb{Q}$, a real quadratic field (e.g., $\mathbb{Q}(\sqrt{d})$, $d > 0$ square-free), a CM field of degree 4 over $\mathbb{Q}$ (a totally imaginary quadratic extension of a real quadratic field), a non-split quaternion algebra over $\mathbb{Q}$ (e.g., $\left(\frac{a,b}{\mathbb{Q}}\right)$, $a, b \in \mathbb{Q}^\times$), a direct sum $F_1 \oplus F_2$ where each F_i is $\mathbb{Q}$ or an imaginary quadratic field (e.g., $\mathbb{Q}(\sqrt{-d})$), or a matrix algebra from the Mumford-Tate group with center F being $\mathbb{Q}$ or an imaginary quadratic field.

Theorem 5 (Albert's Classification for Abelian Surfaces)**.** *Let $\mathcal{A}$ be a principally polarized Abelian surface over $\overline{\mathbb{Q}}$. Then $\mathrm{End}^0(\mathcal{A})$ is isomorphic to one of:*

(1) $\mathbb{Q}$,
(2) a real quadratic field,
(3) a CM field of degree 4 over $\mathbb{Q}$,
(4) a non-split quaternion algebra over $\mathbb{Q}$,
(5) $F_1 \oplus F_2$ where $F_i = \mathbb{Q}$ or an imaginary quadratic field,
(6) a matrix algebra over a center $F = \mathbb{Q}$ or an imaginary quadratic field.

Proof. Since $\mathcal{A}$ is an Abelian surface over $\overline{\mathbb{Q}}$, its dimension is 2, and by the Poincaré-Weil theorem (Theorem 1), $\mathcal{A}$ is isogenous to a product $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, where the $\mathcal{A}_i$ are simple Abelian varieties, pairwise non-isogenous, and the decomposition is unique up to permutation and isogeny. Given $\dim \mathcal{A} = 2$, only two cases arise: (i) $\mathcal{A}$ is simple ($r = 1$, $n_1 = 1$), or (ii) $\mathcal{A} \cong E_1 \times E_2$, where $\dim E_1 = \dim E_2 = 1$. The rational endomorphism algebra $\mathrm{End}^0(\mathcal{A}) = \mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is semi-simple due to the principal polarization's Rosati involution, and its structure depends on this decomposition.

Case 1: $\mathcal{A}$ is simple. If $\mathcal{A}$ is simple, $\mathrm{End}^0(\mathcal{A})$ is a division algebra over its center Z, a number field over $\mathbb{Q}$, and the dimension formula holds: $[Z : \mathbb{Q}] \cdot [\mathrm{End}^0(\mathcal{A}) : Z] = (\dim \mathcal{A})^2 = 4$. Since $\mathcal{A}$ is principally polarized, the Rosati involution $\phi \mapsto \phi^\dagger$ (where $\phi^\dagger = \hat{\lambda}^{-1} \circ \hat{\phi} \circ \lambda$, $\lambda\colon \mathcal{A} \longrightarrow \hat{\mathcal{A}}$ the polarization) is positive

definite, fixing Z and constraining $\mathrm{End}^0(\mathcal{A})$ to be a division algebra with involution. We consider possible dimensions of Z:

(1) If $Z = \mathbb{Q}$, then $[Z : \mathbb{Q}] = 1$, and $[\mathrm{End}^0(\mathcal{A}) : \mathbb{Q}] = 4$. Possible division algebras over $\mathbb{Q}$ of dimension 4 include:
   (a) $\mathbb{Q}$ itself, dimension 1, where $\mathrm{End}^0(\mathcal{A}) = \mathbb{Q}$, and every non-zero endomorphism is an isogeny (multiplication by a rational).
   (b) A real quadratic field, e.g., $\mathbb{Q}(\sqrt{d})$, $d > 0$ square-free, dimension 2, where $\mathrm{End}^0(\mathcal{A})$ embeds into $M_2(\mathbb{R})$ via real multiplication, satisfying the dimension constraint with $[\mathrm{End}^0(\mathcal{A}) : Z] = 2$.
   (c) A CM field of degree 4, e.g., $\mathbb{Q}(\sqrt{d}, i)$, a totally imaginary quadratic extension of a real quadratic field, dimension 4, with $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, compatible with complex multiplication and the involution (conjugation).
   (d) A non-split quaternion algebra over $\mathbb{Q}$, e.g., $\left(\frac{a,b}{\mathbb{Q}}\right)$, $a, b \in \mathbb{Q}^\times$, dimension 4, with $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, where the standard involution (conjugation) is positive definite under the polarization.

(2) If Z is a quadratic field (real or imaginary), $[Z : \mathbb{Q}] = 2$, then $[\mathrm{End}^0(\mathcal{A}) : Z] = 2$. Here, $\mathrm{End}^0(\mathcal{A})$ is a division algebra over a quadratic field:
   (a) For $Z = \mathbb{Q}(\sqrt{d})$, $d > 0$, $\mathrm{End}^0(\mathcal{A})$ could be a quaternion algebra over Z (dimension 4 over Z, but 8 over $\mathbb{Q}$), exceeding 4, so this is not possible unless $\mathrm{End}^0(\mathcal{A}) = Z$, already covered.
   (b) For $Z = \mathbb{Q}(\sqrt{-d})$, similar constraints apply; a CM field over an imaginary quadratic field has dimension 8 over $\mathbb{Q}$, ruling it out.

(3) If Z is quartic, $[Z : \mathbb{Q}] = 4$, then $[\mathrm{End}^0(\mathcal{A}) : Z] = 1$, so $\mathrm{End}^0(\mathcal{A}) = Z$, a CM field, as above.

Thus, for simple $\mathcal{A}$, $\mathrm{End}^0(\mathcal{A})$ is $\mathbb{Q}$, a real quadratic field, a CM field of degree 4, or a non-split quaternion algebra over $\mathbb{Q}$.

Case 2: $\mathcal{A} \cong E_1 \times E_2$. If $\mathcal{A}$ is not simple, it is isogenous to $E_1 \times E_2$, where E_1 and E_2 are elliptic curves over $\overline{\mathbb{Q}}$. Then $\mathrm{End}^0(\mathcal{A}) = \mathrm{End}^0(E_1) \oplus \mathrm{End}^0(E_2)$, as endomorphisms respect the product structure (no cross-terms exist unless $E_1 \cong E_2$). For an elliptic curve E_i over $\overline{\mathbb{Q}}$:

(1) $\mathrm{End}^0(E_i) = \mathbb{Q}$ if E_i has no complex multiplication (CM), dim= 1.
(2) $\mathrm{End}^0(E_i) = \mathbb{Q}(\sqrt{-d})$, an imaginary quadratic field, if E_i has CM, dim= 2.

Thus, $\mathrm{End}^0(\mathcal{A}) = F_1 \oplus F_2$, where $F_i = \mathrm{End}^0(E_i)$, yielding dimensions 1+1 = 2 or 2+2 = 4 over $\mathbb{Q}$. If $E_1 \cong E_2$, $\mathrm{End}^0(\mathcal{A}) \cong M_2(F)$, where $F = \mathrm{End}^0(E_1)$, a matrix algebra over $\mathbb{Q}$ (dimension 4) or an imaginary quadratic field (dimension 8), but the principal polarization constrains this to a division algebra unless adjusted by the Hodge structure.

When $\mathcal{A}$'s Hodge structure (over $\mathbb{C}$) defines a Mumford-Tate group, $\mathrm{End}^0(\mathcal{A})$ may be a matrix algebra over a center F. For $\dim \mathcal{A} = 2$, $F = \mathbb{Q}$ gives $M_2(\mathbb{Q})$ (dimension 4), or $F = \mathbb{Q}(\sqrt{-d})$ gives a division algebra (dimension 4 over F, 8 over $\mathbb{Q}$), but the polarization restricts to $M_2(\mathbb{Q})$ or reduces to prior cases ([51], §4; [60], Chapter IV).

The dimension bound 4 and semi-simplicity (via Rosati) limit $\mathrm{End}^0(\mathcal{A})$ to these types. Higher-degree fields or algebras (e.g., dimension 8) exceed $\dim \mathcal{A}^2 = 4$, and the polarization excludes non-division or non-positive cases, completing the classification. □

A principal polarization $\lambda \colon \mathcal{A} \longrightarrow \hat{\mathcal{A}}$ induces the Rosati involution $\phi \mapsto \phi^\dagger = \hat{\lambda}^{-1} \circ \hat{\phi} \circ \lambda$, fixing the center and ensuring $\mathrm{End}^0(\mathcal{A})$ is semi-simple. The trace form $\langle \phi, \psi \rangle = \mathrm{tr}(\phi^\dagger \circ \psi)$ is positive definite: for $\phi \neq 0$, $\mathrm{tr}(\phi^\dagger \circ \phi) > 0$, as $\phi^\dagger \circ \phi$ is a non-zero symmetric endomorphism, and the polarization's positivity on $\hat{\mathcal{A}}$ guarantees this (see [48], Chapter IV, §21). Thus, $\mathrm{End}^0(\mathcal{A})$ decomposes into simple algebras matching Albert's types.

The dimension of $\mathrm{End}^0(\mathcal{A})$ for an Abelian surface is at most 4, reflecting $g = 2$. If $\mathcal{A}$ is simple, it is 1, 2, or 4; if a product, it sums to 2 or 4. For a Jacobian $\mathrm{Jac}(\mathcal{X})$, $\mathrm{End}^0_{\mathbb{Q}}(\mathrm{Jac}\,\mathcal{X})$ is typically $\mathbb{Q}$ unless $\mathcal{X}$ has special symmetries, yielding richer structures as detailed in [51].

3. Genus 2 Curves and their Jacobians

Let $\mathcal{X}$ be a genus 2 curve defined over a field k. A curve of genus 2 is a smooth, projective, geometrically irreducible algebraic curve with genus $g = 2$, meaning its geometric genus—computed as the dimension of the

space of holomorphic differentials over an algebraically closed field—is 2. The gonality of $\mathcal{X}$, denoted $\gamma_{\mathcal{X}}$, is the minimal degree of a non-constant morphism from $\mathcal{X}$ to $\mathbb{P}^1$, and for genus 2 curves, $\gamma_{\mathcal{X}} = 2$. This implies that $\mathcal{X}$ is hyperelliptic, admitting a degree 2 covering $\pi\colon \mathcal{X} \to \mathbb{P}^1$, which we call the hyperelliptic projection. By Hurwitz's formula, applied to this double cover, the number of branch points $r = 6$. These 6 branch points in $\mathbb{P}^1(\bar{k})$ are the images of the Weierstrass points of $\mathcal{X}$, points where the hyperelliptic involution $\imath$ (an automorphism of order 2) fixes the curve. The moduli space of genus 2 curves, denoted $\mathcal{M}_2$, classifies such curves up to isomorphism and has dimension $r - 3 = 3$, reflecting the three degrees of freedom in their configuration after projective transformations.

The arithmetic structure of $\mathcal{M}_2$ was profoundly studied by Igusa [31], building on earlier work by Clebsch, Bolza, and others. The isomorphism classes of genus two curves correspond to the equivalence classes of binary sextics and therefore determined by their invariants. These invariants are homogeneous polynomials in the coefficients of a defining equation, with degrees 2, 4, 6, 8, and 10, respectively, and we refer to [3] for a comprehensive treatment of their properties and relations. Two genus 2 curves $\mathcal{X}$ and $\mathcal{X}'$ are isomorphic over $\bar{k}$ if and only if there exists $l \in \bar{k}^\star$ such that $J_{2i}(\mathcal{X}) = l^{2i} J_{2i}(\mathcal{X}')$ for $i = 1, \dots, 5$, a condition reflecting the projective weighting of the invariants. When char $k \neq 2$, the invariant J_8 is redundant, expressible in terms of J_2, J_4, J_6, and J_{10}, simplifying the classification.

Henceforth, we assume char $k \neq 2$, ensuring a standard form for the curve's equation. Then, $\mathcal{X}$ can be represented by an affine Weierstrass equation

$$y^2 = f(x) = a_6 x^6 + \cdots + a_1 x + a_0, \tag{11}$$

over $\bar{k}$, where $f(x)$ is a monic polynomial of degree 6 with distinct roots, and the discriminant $\Delta_f = J_{10} \neq 0$ guarantees smoothness. Thus, we will be considering the weighted projective space $\mathbb{P}_{(2,4,6,10)}(k)$ using the invariants J_2, J_4, J_6, J_{10} and the space $\mathbb{P}_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}$, where $J_{10} \neq 0$ excludes singular curves. From now on, by invariants of a genus 2 curve, we mean J_2, J_4, J_6, J_{10}, and by a genus 2 curve, we refer to its isomorphism class, represented as a moduli point $[J_2 : J_4 : J_6 : J_{10}] \in \mathbb{P}_{(2,4,6,10)}(k)$.

3.1. **Principal polarizations and Torelli theorem.** The Jacobian $\mathrm{Jac}(\mathcal{X})$ of a genus 2 curve $\mathcal{X}$ is an Abelian surface, a 2-dimensional principally polarized Abelian variety, constructed as the Picard group $\mathrm{Pic}^0(\mathcal{X})$ of degree 0 divisor classes on $\mathcal{X}$. Given a k-rational point $P_0 \in \mathcal{X}(k)$, the embedding $\phi_{P_0}\colon \mathcal{X} \longrightarrow \mathrm{Jac}(\mathcal{X})$, defined by $P \mapsto [P - P_0]$, maps $\mathcal{X}$ into $\mathrm{Jac}(\mathcal{X})$ with $\phi_{P_0}(P_0) = 0$. This embedding is canonical up to translation, and $\mathrm{Jac}(\mathcal{X})$ is functorial; see Lemma 5. The hyperelliptic involution $\imath\colon \mathcal{X} \longrightarrow \mathcal{X}$, swapping sheets of the cover π, induces an involution $\imath_*\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Jac}(\mathcal{X})$ with $\imath_*(D) = -D$, which, on the level of the Abelian surface, we denote by $-\mathbb{I}$ and which is central to the construction of Kummer surfaces.

A map $f\colon \mathcal{X} \longrightarrow \mathcal{D}$ between curves induces homomorphisms $f^*\colon \mathrm{Jac}(\mathcal{D}) \longrightarrow \mathrm{Jac}(\mathcal{X})$ (pullback) and $f_*\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Jac}(\mathcal{D})$ (pushforward), reflecting the functorial nature of the Jacobian. When f is a maximal covering, i.e., not factoring through an isogeny, it reveals the Jacobian's structure. For an Abelian surface $\mathcal{A}$, a polarization is an isogeny $\lambda\colon \mathcal{A} \to \hat{\mathcal{A}}$ to the dual, and $\mathcal{A}$ is principally polarized if $\deg \lambda = 1$. The Theta divisor $\Theta \subset \mathrm{Jac}(\mathcal{X})$, image of ϕ_{P_0}, provides such a polarization, making $\mathrm{Jac}(\mathcal{X})$ a principal case.

Let us explain the construction of a principal polarization on $\mathrm{Jac}(\mathcal{X})$ in more and explicit detail: The Siegel three-fold is the quasi-projective variety of dimension three, obtained from the Siegel upper half-plane $\mathbb{H}_2$ of degree two[1] divided by the action of the modular transformations $\Gamma_2 := \mathrm{Sp}_4(\mathbb{Z})$, i.e.,

$$\mathbb{A}_2 = \mathbb{H}_2/\Gamma_2. \tag{12}$$

Each $\tau = \left(\begin{smallmatrix} \tau_{11} & \tau_{12} \\ \tau_{12} & \tau_{22} \end{smallmatrix}\right) \in \mathbb{H}_2$ determines a complex Abelian surface $\mathcal{A} = \mathbb{C}^2/\Lambda$ obtained from the lattice $\Lambda = \langle \mathbb{Z}^2 \oplus \tau\, \mathbb{Z}^2 \rangle$ with the period matrix $(\mathbb{I}_2, \tau) \in \mathrm{Mat}(2, 4; \mathbb{C})$.

We consider two Abelian surfaces $\mathcal{A}$ and $\widetilde{\mathcal{A}}$ isomorphic if and only if there is an $M \in \Gamma_2$ such that $\widetilde{\tau} = M(\tau)$. The *canonical principal polarization* of $\mathcal{A}$ is given by the positive definite Hermitian forms $\mathbf{h}$ on $\mathbb{C}^2$ such that $\alpha = \mathrm{Im}\, \mathbf{h}(\Lambda, \Lambda) \subset \mathbb{Z}$ where α is the Riemann form $\alpha(x_1 + x_2\tau, y_1 + y_2\tau) = x_1^t \cdot y_2 - y_1^t \cdot x_2$ on $\mathbb{Z}^2 \oplus \tau\, \mathbb{Z}^2$. Similarly, we define the subgroup $\Gamma_2(2n) = \{M \in \Gamma_2 |\, M \equiv \mathbb{I} \mod 2n\}$ and Igusa's congruence subgroups $\Gamma_2(2n, 4n) = \{M \in \Gamma_2(2n) |\, \mathrm{diag}(B) = \mathrm{diag}(C) \equiv \mathbb{I} \mod 4n\}$ with corresponding Siegel modular threefolds $\mathbb{A}_2(2)$, $\mathbb{A}_2(2, 4)$, and $\mathbb{A}_2(4, 8)$ such that

$$\Gamma_2/\Gamma_2(2) \cong S_6, \quad \Gamma_2(2)/\Gamma_2(2, 4) \cong (\mathbb{Z}/2\mathbb{Z})^4, \quad \Gamma_2(2, 4)/\Gamma_2(4, 8) \cong (\mathbb{Z}/2\mathbb{Z})^9, \tag{13}$$

[1] By definition $\mathbb{H}_2$ is the set of two-by-two symmetric matrices over $\mathbb{C}$ whose imaginary part is positive definite

where S_6 is the permutation group of six elements. The geometric meaning of $\mathbb{A}_2(2), \mathbb{A}_2(2,4)$, and $\mathbb{A}_2(4,8)$ will be discussed below.

The Hermitian form determines a line bundle $\mathscr{L} \to \mathcal{A}$ in the Néron-Severi lattice $\mathrm{NS}(\mathcal{A})$. A general fact from linear algebra asserts that one can always choose a basis of Λ such that α is given by the matrix $\left(\begin{smallmatrix} 0 & D \\ -D & 0 \end{smallmatrix}\right)$ with $D = \left(\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right)$ where $d_1, d_2 \in \mathbb{N}$, $d_1, d_2 \geq 0$, and d_1 divides d_2. For a principal polarization one has $(d_1, d_2) = (1,1)$. Since transformations in Γ_2 preserve the Riemann form α, it follows that the Siegel three-fold is also the set of isomorphism classes of principally polarized Abelian surfaces, i.e., Abelian surfaces with a polarization of type $(1,1)$.

For a principally polarized Abelian variety $\mathcal{A}$ the line bundle $\mathscr{L}$ defining its principal polarization is ample and satisfies $h^0(\mathscr{L}) = 1$. There exists an effective divisor Θ such that $\mathscr{L} = \mathcal{O}_{\mathcal{A}}(\Theta)$, uniquely defined only up to translations. The divisor $\Theta \in \mathrm{NS}(\mathcal{A})$ is precisely the Theta divisor associated with the polarization. It is known that the Abelian surface $\mathcal{A}$ is not the product of two elliptic curves if and only if Θ is an irreducible divisor. Torelli's theorem states that the map sending a curve $\mathcal{X}$ to its Jacobian $\mathrm{Jac}(\mathcal{X})$, that is $\mathcal{X} \mapsto (\mathrm{Jac}(\mathcal{X}), \Theta)$, is injective and defines a birational map $\mathcal{M}_2 \dashrightarrow \mathbb{A}_2$.

Conversely, if the period matrix τ of a principally polarized Abelian variety $\mathcal{A}$ is not equivalent to a point with $\tau_{12} = 0$ relative to Γ_2, then a Θ divisor on $\mathcal{A}$ is given by a non-singular curve $\mathcal{X}$ of genus-two, i.e., $\Theta = [\mathcal{X}]$ such that $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$. Thus, a principally polarized Abelian surface is either the Jacobian of a smooth curve of genus two with a Theta divisor or the product of two complex elliptic curves, with the product polarization.

Igusa proved [34,35] that the ring of modular forms is generated by the Siegel modular forms ψ_4, ψ_6, χ_{10}, χ_{12} and by one more cusp form χ_{35} of odd weight 35[2] whose square is the following polynomial [34, p. 849] in the even generators

$$
\begin{aligned}
\chi_{35}^2 = \frac{1}{2^{12}\,3^9}\,\chi_{10}\,\big(&2^{24}\,3^{15}\,\chi_{12}^5 - 2^{13}\,3^9\,\psi_4^3\,\chi_{12}^4 - 2^{13}\,3^9\,\psi_6^2\,\chi_{12}^4 + 3^3\,\psi_4^6\,\chi_{12}^3 \\
&- 2\cdot 3^3\,\psi_4^3\,\psi_6^2\,\chi_{12}^3 - 2^{14}\,3^8\,\psi_4^2\,\psi_6\,\chi_{10}\,\chi_{12}^3 - 2^{23}\,3^{12}\,5^2\,\psi_4\,\chi_{10}^2\,\chi_{12}^3 + 3^3\,\psi_6^4\,\chi_{12}^3 \\
&+ 2^{11}\,3^6\,37\,\psi_4^4\,\chi_{10}^2\,\chi_{12}^2 + 2^{11}\,3^6\,5\cdot 7\,\psi_4\,\psi_6^2\,\chi_{10}^2\,\chi_{12}^2 - 2^{23}\,3^9\,5^3\,\psi_6\,\chi_{10}^3\,\chi_{12}^2 \\
&- 3^2\,\psi_4^7\,\chi_{10}^2\,\chi_{12} + 2\cdot 3^2\,\psi_4^4\,\psi_6^2\,\chi_{10}^2\,\chi_{12} + 2^{11}\,3^5\,5\cdot 19\,\psi_4^3\,\psi_6\,\chi_{10}^3\,\chi_{12} \\
&+ 2^{20}\,3^8\,5^3\,11\,\psi_4^2\,\chi_{10}^4\,\chi_{12} - 3^2\,\psi_4\,\psi_6^4\,\chi_{10}^2\,\chi_{12} + 2^{11}\,3^5\,5^2\,\psi_6^3\,\chi_{10}^3\,\chi_{12} \\
&- 2\,\psi_4^6\,\psi_6\,\chi_{10}^3 - 2^{12}\,3^4\,\psi_4^5\,\chi_{10}^4 + 2^2\,\psi_4^3\,\psi_6^3\,\chi_{10}^3 + 2^{12}\,3^4\,5^2\,\psi_4^2\,\psi_6^2\,\chi_{10}^4 \\
&+ 2^{21}\,3^7\,5^4\,\psi_4\,\psi_6\,\chi_{10}^5 - 2\,\psi_6^5\,\chi_{10}^3 + 2^{32}\,3^9\,5^5\,\chi_{10}^6\big)\,.
\end{aligned}
\tag{14}
$$

Hence, the expression $Q := 2^{12}\,3^9\,\chi_{35}^2/\chi_{10}$ is a polynomial of degree 60 in the even generators. Igusa also proved that each Siegel modular form (with trivial character) of odd weight is divisible by the form χ_{35}.

Igusa [34, p. 848] proved that the relations between the Igusa invariants of a binary sextic $y^2 = f(x)$ defining a smooth genus-two curve $\mathcal{X}$ and the even Siegel modular forms for the associated principally polarized Abelian surface $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ with period matrix τ are as follows:

$$
\begin{aligned}
J_2(f) &= -2^3\cdot 3\,\frac{\chi_{12}(\tau)}{\chi_{10}(\tau)}\,, \\
J_4(f) &= \quad 2^2\,\psi_4(\tau)\,, \\
J_6(f) &= -\frac{2^3}{3}\,\psi_6(\tau) - 2^5\,\frac{\psi_4(\tau)\,\chi_{12}(\tau)}{\chi_{10}(\tau)}\,, \\
J_{10}(f) &= -2^{14}\,\chi_{10}(\tau) \neq 0\,.
\end{aligned}
\tag{15}
$$

Here, the Igusa invariant J_{10} is the discriminant of the sextic $f(x)$ and we are using the same normalization as in [43, 45]. It follows that the moduli space $\mathcal{M}_2$ has a compactification $\mathbb{A}_2^\star$ as the weighted projective space $\mathbb{P}_{(2,4,6,10)}(k)$ using the invariants J_2, J_4, J_6, J_{10} and

$$
\mathbb{A}_2 \cong \mathbb{P}_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}. \tag{16}
$$

[2]For a detailed introduction to Siegel modular forms relative to Γ_2, Humbert surfaces, and the Satake compactification of the Siegel modular threefold we refer to Freitag's book [24].

3.2. **Göpel groups and Theta divisors.** For an Abelian surface $\mathcal{A}$, such as the Jacobian $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ of a genus 2 curve $\mathcal{X}$ over a field k, the group of 2-torsion points $\mathcal{A}[2]$ consists of elements $x \in \mathcal{A}(\bar{k})$ satisfying $2x = 0$, forming a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2g} = (\mathbb{Z}/2\mathbb{Z})^4$ over $\bar{k}$ when $\mathrm{char}\, k \neq 2$. Translation by a 2-torsion point is an isomorphism of $\mathcal{A}$, mapping $\mathcal{A}[2]$ to itself, preserving its structure under the Weil pairing, which defines an alternating bilinear form on $\mathcal{A}[2]$. A subspace $G \leq \mathcal{A}[2]$ is isotropic if the Weil pairing vanishes on $G \times G$, and a maximal isotropic subspace, or Göpel group, has dimension 2 (containing 4 points, as $2^2 = 4$).

Let us explain the construction of Göpel groups in more and explicit detail: consider the Jacobian $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ of a genus-two curve $\mathcal{X}$ in Rosenhain form

$$\mathcal{X}\colon \quad y^2 = xz(x-z)(x-\lambda_1 z)(x-\lambda_2 z)(x-\lambda_3 z), \tag{17}$$

with roots at $\lambda_1, \lambda_2, \lambda_3, \lambda_4 = 0, \lambda_5 = 1, \lambda_6 = \infty$. Every nontrivial order-two point on $\mathcal{A}$ can be considered the difference of Weierstrass points $P_i \in \mathcal{X}$ for $1 \leq i \leq 6$. In fact, the sixteen order-two points of $\mathcal{A}$ are obtained using the embedding of the curve into the connected component of the identity in the Picard group, i.e., $\mathcal{X} \hookrightarrow \mathrm{Jac}\,(\mathcal{X}) \cong \mathrm{Pic}^0(\mathcal{X})$. We obtain the 15 elements $P_{ij} = [P_i + P_j - 2\,P_6] \in \mathcal{A}[2]$ with $1 \leq i < j \leq 6$ and set $P_0 = P_{66} = [0]$. For $\{i,j,k,l,m,n\} = \{1,\ldots,6\}$, the group law on $\mathcal{A}[2]$ is given by the relations

$$P_0 + P_{ij} = P_{ij}\,, \quad P_{ij} + P_{ij} = P_0\,, \quad P_{ij} + P_{kl} = P_{mn}, \quad P_{ij} + P_{jk} = P_{ik}\,. \tag{18}$$

The subgroup $\Gamma_2(2) = \{M \in \Gamma_2 |\, M \equiv \mathbb{I} \mod 2\}$ with $\Gamma_2/\Gamma_2(2) \cong S_6$ where S_6 is the permutation group of six elements is now realized as the permutations of the roots of the right hand side of Equation (17) when we have identification $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$. Accordingly, $\mathbb{A}_2(2)$ is the three-dimensional moduli space of principally polarized Abelian surfaces with level-two structure.

The space $\mathcal{A}[2]$ of order-two points admits a symplectic bilinear form, the aforementioned Weil pairing such that the two-dimensional, maximal isotropic subspace of $\mathcal{A}[2]$ with respect to the Weil pairing are the Göpel groups. It is then easy to check that there are exactly 15 inequivalent Göpel groups, and they are of the form

$$\{P_0, P_{ij}, P_{kl}, P_{mn}\} \tag{19}$$

such that $\{i,j,k,l,m,n\} = \{1,\ldots,6\}$. The standard Theta divisor $\Theta = \Theta_6 = \{[P - P_6] \mid P \in \mathcal{X}\}$ contains the six order-two points P_0, P_{i6} for $1 \leq i \leq 5$. Likewise for $1 \leq i \leq 5$, the five translates $\Theta_i = P_{i6} + \Theta$ contain P_0, P_{i6}, P_{ij} with $j \neq i, 6$, and the ten translates $\Theta_{ij6} = P_{ij} + \Theta$ for $1 \leq i < j \leq 5$ contain $P_{ij}, P_{i6}, P_{j6}, P_{kl}$ with $k, l \neq i, j, 6$ and $k < l$. Conversely, each order-two point lies on exactly six of the divisors, namely

$$P_0 \in \Theta_i \qquad \text{for } i = 1,\ldots,6, \tag{20}$$

$$P_{i6} \in \Theta_i, \Theta_6, \Theta_{ij6} \quad \text{for } i = 1,\ldots,5 \text{ with } j \neq i, 6, \tag{21}$$

$$P_{ij} \in \Theta_i, \Theta_j, \Theta_{kl6} \quad \text{for } 1 \leq i < j \leq 5 \text{ with } k, l \neq i, j, 6 \text{ and } k < l. \tag{22}$$

Hence, we have a configuration of sixteen elements $P_0, P_{ij} \in \mathcal{A}[2]$ and sixteen Theta divisors $\Theta, \Theta_i, \Theta_{ijk}$, where each Theta divisor contains six order-two points, and where each order-two point is contained in six Theta divisors. This configuration is called the 16_6 *configuration on the Abelian surface* $\mathcal{A}$.

Moreover, we call the divisors $\{\Theta_i\}$ and $\{\Theta_{jk6}\}$ with $1 \leq i \leq 6$ and $1 \leq j < k < 6$, the six *odd* and the ten *even* Theta divisors, respectively. In this way, the odd Theta divisors are the six translates of the curve $\mathcal{X}$ by P_{i6} with $1 \leq i \leq 6$, and thus with the six Weierstrass points P_i on the curve $\mathcal{X}$. Furthermore, there is a one-to-one correspondence between pairs of odd Theta divisors and two-torsion points on $\mathcal{A}[2]$ since $\Theta_i \cap \Theta_j = \{P_0, P_{ij}\}$, and, in turn, unordered pairs $\{P_i, P_j\}$ of Weierstrass points since $P_{ij} = P_{i6} + P_{j6}$.

3.3. **Theta constants of genus two.** For $\left(\begin{smallmatrix} a_1 & a_2 \\ b_1 & b_2 \end{smallmatrix}\right) \in \mathbb{F}_2^4$ – where $\mathbb{F}_2$ denotes the finite field with two elements – there are sixteen corresponding Theta functions. We always identify $\left(\begin{smallmatrix} a_1 & a_2 \\ b_1 & b_2 \end{smallmatrix}\right) \in \mathbb{F}_2^4$ with the corresponding characteristic $\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right]$, $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$. The Theta functions with characteristics $[a, b]$, $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$, are defined as

$$\theta\left[\begin{smallmatrix} a \\ b \end{smallmatrix}\right](z,\tau) = \sum_{m \in \mathbb{Z}^2} \exp\left(\pi i (m+a)^t \tau (m+a) + 2\pi i (m+a)^t (z+b)\right). \tag{23}$$

We note that this definition is obtained by specializing the situation of Section 2.2 to $g = 2$. Among the Theta functions, 10 are even and 6 are odd functions according to

$$\theta\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}(-z,\tau) = (-1)^{a^t\cdot b}\,\theta\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}(z,\tau). \tag{24}$$

A *level-n Theta structure* is given by the functions $\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](z,\tau/n)$, where $b \in (\mathbb{Z}/n\mathbb{Z})^2$. For a period matrix $\tau \in \mathbb{H}_2$, the values of the Theta functions $\theta\left[\begin{smallmatrix}a\\ b\end{smallmatrix}\right](z,\tau/2)$, with $a, b \in (\mathbb{Z}/2\mathbb{Z})^2$ at $z = 0$, are called *theta constants* or *theta null points*. In particular, we set $\theta_i = \theta\left[\begin{smallmatrix}a_i\\ b_i\end{smallmatrix}\right](0,\tau)$, where corresponding to either

$$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right) \in \mathbb{F}_2, \tag{25}$$

or, equivalently, the characteristics $a = 0$, $b = [0,0]$, $[1/2,1/2]$ $[1/2,0]$, $[0,1/2]$, we have labeled the functions $\theta_1, \theta_2, \theta_3, \theta_4$.

We will also introduce Theta functions that are evaluated at 2τ. Under duplication of the modular variable, the Theta functions $\theta_1, \theta_5, \theta_7, \theta_8$ play a role dual to $\theta_1, \theta_2, \theta_3, \theta_4$. We renumber the former and use the symbol Θ to mark the fact that they are evaluated at the isogenous Abelian variety. That is, Theta constants $\{\Theta_1^2, \Theta_2^2, \Theta_3^2, \Theta_4^2\}$ and $\{\theta_1^2, \theta_2^2, \theta_3^2, \theta_4^2\}$ correspond to the following Theta characteristics

$$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right), \text{ and } \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right). \tag{26}$$

Thomae's formula is a formula introduced by Thomae relating Theta constants to the branch points of a genus 2 curve. The three λ parameters appearing in the Rosenhain normal form in Equation (17) are ratios of even Theta constants. There are 720 choices for such expressions since the forgetful map to $\mathcal{M}_2$ is a Galois covering of degree $720 = |S_6|$ where S_6 acts on the roots of $\mathcal{X}$ by permutations. Any of the 720 choices may be used, we choose the one also used in [27, 52]:

Lemma 6. *For any period point $\tau \in \mathbb{A}_2(2)$, there is a genus-two curve $\mathcal{X} \in \mathcal{M}_2$ with level-two structure and Rosenhain roots $\lambda_1, \lambda_2, \lambda_3$ such that*

$$\lambda_1 = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \lambda_2 = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \lambda_3 = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}. \tag{27}$$

Similarly, the following expressions are perfect squares of Theta constants:

$$\begin{aligned} \lambda_1 - 1 &= \frac{\theta_7^2\theta_9^2}{\theta_2^2\theta_4^2}, & \lambda_2 - 1 &= \frac{\theta_5^2\theta_9^2}{\theta_4^2\theta_{10}^2}, & \lambda_3 - 1 &= \frac{\theta_5^2\theta_7^2}{\theta_2^2\theta_{10}^2}, \\ \lambda_2 - \lambda_1 &= \frac{\theta_3^2\theta_6^2\theta_9^2}{\theta_2^2\theta_4^2\theta_{10}^2}, & \lambda_3 - \lambda_1 &= \frac{\theta_1^2\theta_6^2\theta_7^2}{\theta_2^2\theta_4^2\theta_{10}^2}, & \lambda_3 - \lambda_2 &= \frac{\theta_5^2\theta_6^2\theta_8^2}{\theta_2^2\theta_4^2\theta_{10}^2}. \end{aligned} \tag{28}$$

Conversely, given a smooth genus-two curve $\mathcal{X} \in \mathcal{M}_2$ with three distinct complex numbers $(\lambda_1, \lambda_2, \lambda_3)$ different from $0, 1, \infty$, there is complex Abelian surface $\mathcal{A}$ with period matrix $(\mathbb{I}_2, \tau)$ and $\tau \in \mathbb{A}_2(2)$ such that $\mathcal{A} = \operatorname{Jac}\mathcal{X}$ and the fourth powers of the even Theta constants are given by

$$\begin{aligned} \theta_1^4 &= R\,\lambda_3\lambda_1(\lambda_2-1)(\lambda_3-\lambda_1), & \theta_2^4 &= R\,\lambda_2(\lambda_2-1)(\lambda_3-\lambda_1), \\ \theta_3^4 &= R\,\lambda_2\lambda_1(\lambda_2-\lambda_1)(\lambda_3-\lambda_1), & \theta_4^4 &= R\,\lambda_3(\lambda_3-1)(\lambda_2-\lambda_1), \\ \theta_5^4 &= R\,\lambda_1(\lambda_2-1)(\lambda_3-1)(\lambda_3-\lambda_2), & \theta_6^4 &= R\,(\lambda_3-\lambda_2)(\lambda_3-\lambda_1)(\lambda_2-\lambda_1), \\ \theta_7^4 &= R\,\lambda_2(\lambda_3-1)(\lambda_1-1)(\lambda_3-\lambda_1), & \theta_8^4 &= R\,\lambda_2\lambda_3(\lambda_3-\lambda_2)(\lambda_1-1), \\ \theta_9^4 &= R\,\lambda_3(\lambda_2-1)(\lambda_1-1)(\lambda_2-\lambda_1), & \theta_{10}^4 &= R\,\lambda_1(\lambda_1-1)(\lambda_3-\lambda_2), \end{aligned} \tag{29}$$

where $R \in \mathbb{C}^*$ is a non-zero constant.

According to [52, Sec. 3] we have the following *Frobenius identities* relating Theta constants:

$$\begin{aligned} \theta_5^2\theta_6^2 &= \theta_1^2\theta_4^2 - \theta_2^2\theta_3^2, & \theta_5^4 + \theta_6^4 &= \theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4, \\ \theta_7^2\theta_9^2 &= \theta_1^2\theta_3^2 - \theta_2^2\theta_4^2, & \theta_7^4 + \theta_9^4 &= \theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4, \\ \theta_8^2\theta_{10}^2 &= \theta_1^2\theta_2^2 - \theta_3^2\theta_4^2, & \theta_8^4 + \theta_{10}^4 &= \theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4. \end{aligned} \tag{30}$$

The following identities are called the *second principal transformations of degree two* [32, 33] for Theta constants:

$$\begin{aligned} \theta_1^2 &= \Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2, & \theta_2^2 &= \Theta_1^2 + \Theta_2^2 - \Theta_3^2 - \Theta_4^2, \\ \theta_3^2 &= \Theta_1^2 - \Theta_2^2 - \Theta_3^2 + \Theta_4^2, & \theta_4^2 &= \Theta_1^2 - \Theta_2^2 + \Theta_3^2 - \Theta_4^2. \end{aligned} \tag{31}$$

We also have the following identities:

$$
\begin{aligned}
\theta_5^2 &= 2\,(\Theta_1\Theta_3 + \Theta_2\Theta_4)\,, & \theta_6^2 &= 2\,(\Theta_1\Theta_3 - \Theta_2\Theta_4)\,,\\
\theta_7^2 &= 2\,(\Theta_1\Theta_4 + \Theta_2\Theta_3)\,, & \theta_8^2 &= 2\,(\Theta_1\Theta_2 + \Theta_3\Theta_4)\,,\\
\theta_9^2 &= 2\,(\Theta_1\Theta_4 - \Theta_2\Theta_3)\,, & \theta_{10}^2 &= 2\,(\Theta_1\Theta_2 - \Theta_3\Theta_4)\,.
\end{aligned}
\tag{32}
$$

The characterization of the Siegel modular threefolds $\mathbb{A}_2(2)$, $\mathbb{A}_2(2,4)$, and $\mathbb{A}_2(4,8)$ as projective varieties and their Satake compactifications was given in [36]*Prop. 2.2:

Proposition 1.

(1) The holomorphic map $\Xi_{2,4}\colon \mathbb{H}_2 \longrightarrow \mathbb{P}^3$ given by $\tau \mapsto [\Theta_1 : \Theta_2 : \Theta_3 : \Theta_4]$ is an isomorphism between the Satake compactification $\overline{\mathbb{A}_2(2,4)}$ and $\mathbb{P}^3$.

(2) The holomorphic map $\Xi_{4,8}\colon \mathbb{H}_2 \longrightarrow \mathbb{P}^9$ given by $\tau \mapsto [\theta_1 : \cdots : \theta_{10}]$ is an isomorphism between the Satake compactification $\overline{\mathbb{A}_2(4,8)}$ and the closure of $\Xi_{4,8}$ in $\mathbb{P}^9$.

(3) We have the following commutative diagram:

$$
\begin{array}{ccccc}
\overline{\mathbb{A}_2(4,8)} & & \xrightarrow{\quad\Xi_{4,8}\quad} & & \mathbb{P}^9 \\
\Big\downarrow{\scriptstyle \pi} & & & & \Big\downarrow{\scriptstyle \mathrm{Sq}} \\
\overline{\mathbb{A}_2(2,4)} & & \xrightarrow{\Xi_{2,4}} \mathbb{P}^3 & \xrightarrow{\mathrm{Ver}} & \mathbb{P}^9 \\
\Big\downarrow{\scriptstyle \mathrm{Ros}} & & & & \\
\overline{\mathbb{A}_2(2)} & & & &
\end{array}
$$

Here, π is the covering map with deck transformations $\Gamma_2(2,4)/\Gamma_2(4,8) \cong (\mathbb{Z}/2\mathbb{Z})^9$, the map Sq *is the square map $[\theta_1 : \cdots : \theta_{10}] \mapsto [\theta_1^2 : \cdots : \theta_{10}^2]$, the map* Ver *is the Veronese type map defined by the quadratic relations (31) and (32), and the map* Ros *is the covering map with the deck transformations $\Gamma_2(2)/\Gamma_2(2,4) \cong (\mathbb{Z}/2\mathbb{Z})^3$ given by plugging the quadratic relations (31) and (32) into Equations (27).*

3.4. **Richelot isogenies.** Richelot isogenies provide a classical framework for studying (2,2)-isogenies between principally polarized Abelian surfaces, particularly Jacobians of genus 2 curves. Note that the Abelian surfaces are here in general *not* split. It is well-known that the quotient $\hat{\mathcal{A}} = \mathcal{A}/G$ by a Göpel group G is again a principally polarized Abelian surface, as detailed in [49]*Sec. 23. The natural projection $\Psi\colon \mathcal{A} \longrightarrow \hat{\mathcal{A}}$ is an isogeny with kernel G, called a *(2,2)-isogeny* because $\deg \Psi = |G| = 4 = 2^2$, reflecting a kernel of rank 2 over $\mathbb{Z}/2\mathbb{Z}$.

Analytically, over $\mathbb{C}$, if $\mathcal{A} = \mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$ and $\tau \in \mathbb{H}_2$, a Göpel group $G \leq \mathcal{A}[2]$ corresponds to a 2-dimensional subspace of $\frac{1}{2}\Lambda/\Lambda$. The quotient $\hat{\mathcal{A}} = \mathcal{A}/G$ can be represented as $\mathbb{C}^2/\hat{\Lambda}$, where $\hat{\Lambda} = \mathbb{Z}^2 \oplus 2\tau\mathbb{Z}^2$, adjusting the lattice to double the period in one direction. The isogeny is then

$$
\begin{aligned}
\Psi\colon \quad \mathcal{A} = \mathbb{C}^2/\langle \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2 \rangle &\longrightarrow \hat{\mathcal{A}} = \mathbb{C}^2/\langle \mathbb{Z}^2 \oplus 2\tau\mathbb{Z}^2 \rangle \\
(z, \tau) &\mapsto (z, 2\tau),
\end{aligned}
\tag{33}
$$

mapping points modulo the coarser lattice, with kernel G generated by representatives of $\mathcal{A}[2]$ spanning a rank-2 subgroup.

For $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$, where $\mathcal{X}$ is a smooth genus 2 curve, we explore whether $\hat{\mathcal{A}} = \mathrm{Jac}(\hat{\mathcal{X}})$ for another genus 2 curve $\hat{\mathcal{X}}$, and how their moduli relate. Richelot addressed this geometrically in [54], with modern treatments in [8]. Over $\mathbb{C}$, $\mathcal{A}[2]$ has $2^{2g} = 16$ points, and there are 15 Göpel groups (computed as the number of 2-dimensional isotropic subspaces in $(\mathbb{Z}/2\mathbb{Z})^4$ under the symplectic form induced by the Weil pairing). Each corresponds to a (2,2)-isogeny, and Richelot's construction identifies $\hat{\mathcal{X}}$ explicitly. Given $\mathcal{X}$ with equation $Y^2 = f_6(X, Z)$, a sextic in homogeneous coordinates, any factorization $f_6 = A \cdot B \cdot C$ into three quadratic polynomials A, B, C defines a curve $\hat{\mathcal{X}}$ via

$$
\Delta_{ABC} \cdot Y^2 = [A, B][A, C][B, C],
\tag{34}
$$

where $[A, B] = A'B - AB'$ with $A' = \frac{dA}{dx}$ (assuming a dehomogenized coordinate $x = X/Z$), and Δ_{ABC} is the determinant of the coefficients of A, B, C in the basis $\{x^2, xz, z^2\}$. It was shown in [8] that $\mathrm{Jac}(\mathcal{X})$ and

$\mathrm{Jac}(\hat{\mathcal{X}})$ are (2,2)-isogenous, and there are exactly 15 such factorizations (corresponding to partitions of 6 roots into 3 pairs), yielding all distinct (2,2)-isogenous Abelian surfaces to $\mathrm{Jac}(\mathcal{X})$.

The geometric insight stems from the isomorphism $S_6 \cong \mathrm{Sp}(4, \mathbb{F}_2)$, where S_6 permutes the 6 Weierstrass points of $\mathcal{X}$ (or Theta divisors containing a fixed order-two point), and $\mathrm{Sp}(4, \mathbb{F}_2)$ acts on $\mathcal{A}[2]$.

3.4.1. *An explicit model using Theta constants.* To compute Richelot isogenies explicitly, we adopt a Theta function approach, following [52]. For $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$, consider Göpel groups $G = \{P_0, P_{15}, P_{23}, P_{46}\}$ and $G' = \{P_0, P_{12}, P_{34}, P_{56}\}$, where $\mathcal{A}[2] = \{P_{ij}\}_{i<j}$ labels the 2-torsion points, with $P_0 = P_{66}$ the identity. These satisfy $G + G' = \mathcal{A}[2]$ and $G \cap G' = \{P_0\}$, as $|G + G'| = 4 \cdot 4/1 = 16$. Set $\hat{\mathcal{A}} = \mathcal{A}/G$, and let $\hat{G}$ be the image of G' in $\hat{\mathcal{A}}$. We aim to relate the Rosenhain roots of $\mathcal{X}$:

$$\mathcal{X}\colon \quad y^2 = xz(x-z)(x-\lambda_1 z)(x-\lambda_2 z)(x-\lambda_3 z), \tag{35}$$

where $\lambda_4 = 0$, $\lambda_5 = 1$, $\lambda_6 = \infty$, to those of $\hat{\mathcal{X}}$ with

$$\hat{\mathcal{X}}\colon \quad y^2 = x(x-1)(x-\Lambda_1)(x-\Lambda_2)(x-\Lambda_3). \tag{36}$$

Theta constants give explicit equations for the moduli of $\mathrm{Jac}(\mathcal{X})$ and $\mathrm{Jac}(\hat{\mathcal{X}})$: for a period matrix $\tau \in \mathbb{H}_2$, we use θ_i for $\mathcal{X}$ and Θ_i for $\hat{\mathcal{X}}$, with characteristics forming Göpel groups. That is, we let $G = \{P_0, P_{15}, P_{23}, P_{46}\}$ correspond to the Göpel group in $\mathbb{F}_2^4$ formed by the characteristics

$$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right), \tag{37}$$

yielding the Theta constants $\theta_1, \theta_2, \theta_3, \theta_4$. They determine the moduli $\lambda_1, \lambda_2, \lambda_3$ in Equation (27) by plugging in the quadratic relations (31) and (32).

The isogeny $\Psi\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Jac}(\hat{\mathcal{X}})$ modifies the lattice, and the dual Theta constants Θ_i for $\hat{\mathcal{X}}$ relate to θ_i via the isogeny's action in (26). Results in [52] and [13] give

$$\Lambda_1 = \frac{\Theta_1^2\Theta_3^2}{\Theta_2^2\Theta_4^2}, \quad \Lambda_2 = \frac{\Theta_3^2\Theta_8^2}{\Theta_4^2\Theta_{10}^2}, \quad \Lambda_3 = \frac{\Theta_1^2\Theta_8^2}{\Theta_2^2\Theta_{10}^2}. \tag{38}$$

For G the corresponding Richelot isogeny is obtained by factoring $f_6 = xz(x-z)(x-\lambda_1 z)(x-\lambda_2 z)(x-\lambda_3 z)$ into

$$A = (x-\lambda_1 z)(x-z), \quad B = (x-\lambda_2 z)(x-\lambda_3 z), \quad C = xz, \tag{39}$$

adjusting for homogeneity (e.g., $C = xz$ at infinity). Applying (34), we compute $\hat{\mathcal{X}}$ and its Igusa invariants, which are rational functions of $\{\theta_1, \theta_2, \theta_3, \theta_4\}$. A quadratic twist $\hat{\mathcal{X}}^{(\mu)}$ with

$$\mu = \frac{(\theta_1\theta_2 - \theta_3\theta_4)^2(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)}{4\theta_1\theta_2\theta_3\theta_4(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)}$$

adjusts the roots to

$$\begin{aligned}
\Lambda_1 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)}, \\
\Lambda_2 &= \frac{(\theta_1^2 - \theta_2^2 - \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 - \theta_2^2 + \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)}, \\
\Lambda_3 &= \frac{(\theta_1^2 + \theta_2^2 + \theta_3^2 + \theta_4^2)(\theta_1^2\theta_2^2 + \theta_3^2\theta_4^2 + 2\theta_1\theta_2\theta_3\theta_4)}{(\theta_1^2 + \theta_2^2 - \theta_3^2 - \theta_4^2)(\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2)},
\end{aligned} \tag{40}$$

matching the Richelot construction's invariants, verifying isomorphism. Similarly, for the Göpel group $G' = \{P_0, P_{12}, P_{34}, P_{56}\}$, the dual isogeny $\hat{\Psi}\colon \hat{\mathcal{A}} \longrightarrow \mathcal{A} = \hat{\mathcal{A}}/\hat{G}$ uses $\hat{A} = [B, C]$, $\hat{B} = [A, C]$, $\hat{C} = [A, B]$ to recover $\mathcal{X}$. These Richelot isogenies realize the pair of dual $(2,2)$-isogenies, given by

$$\mathcal{A} = \mathrm{Jac}(\mathcal{X}) \xrightarrow{\Psi} \hat{\mathcal{A}} = \mathrm{Jac}(\hat{\mathcal{X}}) \cong \mathcal{A}/G \xrightarrow{\hat{\Psi}} \mathcal{A} \cong \hat{\mathcal{A}}/\hat{G}, \tag{41}$$

for the complementary maximal isotropic subgroups G, G'. If we introduce new rescaled moduli

$$\lambda_1' = \frac{\lambda_1 + \lambda_2\lambda_3}{l}, \quad \lambda_2' = \frac{\lambda_2 + \lambda_1\lambda_3}{l}, \quad \lambda_3' = \frac{\lambda_3 + \lambda_1\lambda_2}{l},$$

with $l^2 = \lambda_1\lambda_2\lambda_3$, and similarly for Λ_i', then these relate symmetrically, as shown in [13]:

Proposition 2. *The moduli of $\mathcal{X}$ in (35) and $\hat{\mathcal{X}}$ in (36) satisfy*

$$
\begin{aligned}
\Lambda_1' &= 2\frac{2\lambda_1' - \lambda_2' - \lambda_3'}{\lambda_2' - \lambda_3'}, & \lambda_1' &= 2\frac{2\Lambda_1' - \Lambda_2' - \Lambda_3'}{\Lambda_2' - \Lambda_3'}, \\
\Lambda_2' - \Lambda_1' &= -\frac{4(\lambda_1' - \lambda_2')(\lambda_1' - \lambda_3')}{(\lambda_1' + 2)(\lambda_2' - \lambda_3')}, & \lambda_2' - \lambda_1' &= -\frac{4(\Lambda_1' - \Lambda_2')(\Lambda_1' - \Lambda_3')}{(\Lambda_1' + 2)(\Lambda_2' - \Lambda_3')}, \\
\Lambda_3' - \Lambda_1' &= -\frac{4(\lambda_1' - \lambda_2')(\lambda_1' - \lambda_3')}{(\lambda_1' - 2)(\lambda_2' - \lambda_3')}, & \lambda_3' - \lambda_1' &= -\frac{4(\Lambda_1' - \Lambda_2')(\Lambda_1' - \Lambda_3')}{(\Lambda_1' - 2)(\Lambda_2' - \Lambda_3')}.
\end{aligned} \tag{42}
$$

4. Kummer Surfaces

Given an Abelian surface $\mathcal{A}$ over a field k, the *singular Kummer surface* is the quotient $\mathcal{K}_\mathcal{A} = \mathcal{A}/\langle -\mathbb{I}\rangle$, where the involution $-\mathbb{I}\colon \mathcal{A} \longrightarrow \mathcal{A}$ acts by $P \mapsto -P$. $\mathcal{K}_\mathcal{A}$ is a singular algebraic variety of dimension two with 16 ordinary double points, each corresponding to an order-two point in $\mathcal{A}[2] = \{P \in \mathcal{A}(\bar{k}) \mid 2P = 0\}$, the set of which has cardinality $2^{2\cdot 2} = 16$ over an algebraically closed field.

The quotient construction of $\mathcal{K}_\mathcal{A}$ leverages the group structure of $\mathcal{A}$: the involution $-\mathbb{I}$ is an automorphism of order two, and its fixed points, the 2-torsion points, map to singularities on $\mathcal{K}_\mathcal{A}$. Each singularity is locally isomorphic to the quotient of $\mathbb{C}^2$ by the action $z \mapsto -z$, an A_1 singularity, characterized by a quadratic cone. The minimal resolution is denoted the *Kummer surface* $\mathrm{Kum}(\mathcal{A})$ and is a smooth K3 surface, obtained by blowing up each double point by gluing in an exceptional (-2)-curve; see [62] and [44] for details. Conversely, there is a map $\mathrm{Kum}(\mathcal{A}) \longrightarrow \mathcal{K}_\mathcal{A}$ contracting the (-2) curves.

4.1. Kummer surfaces with principal polarizations.

For an Abelian surface $\mathcal{A}$ equipped with a principal polarization $\mathscr{L} = \mathcal{O}_\mathcal{A}(\Theta)$, one can always choose the Theta divisor to satisfy $(-\mathbb{I})^*\Theta = \Theta$, that is, to be a *symmetric Theta divisor*. The Abelian surface $\mathcal{A}$ then maps to the complete linear system $|2\Theta|$. The rational map $\varphi_2\colon \mathcal{A} \longrightarrow \mathbb{P}^3$ associated with the line bundle $\mathscr{L}^2$ induces a map to projective space $\mathbb{P}^3$, its image $\varphi_2(\mathcal{A})$ is a quartic hypersurface, reflecting the degree of the line bundle $\mathscr{L}^2$ associated with the doubled principal polarization, and φ_2 factors via an embedding through the projection $\mathcal{A} \longrightarrow \mathcal{A}/\langle -\mathbb{I}\rangle$; see [4]. We identify the singular Kummer variety $\mathcal{A}/\langle -\mathbb{I}\rangle$ with its image $\mathcal{K}_\mathcal{A}$ in $\mathbb{P}^3$. We will give explicit algebraic equations for the image in Section 4.3.

For the principally polarized Abelian surface $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ associated with a smooth genus 2 curve $\mathcal{X}$ with the standard Theta divisor $\Theta \cong [\mathcal{X}]$, we will now construct the morphism to $\mathbb{P}^3$ explicitly, using the Theta functions from Section 2.2. In fact, the level-two Theta functions directly give the map φ_2 into $\mathbb{P}^3$ when we identify $\mathscr{L}$ with the line bundle that was introduced in Section 2.2. Specifically, assume that $\mathcal{A}$ is not a product of elliptic curves, for $\mathcal{A} = \mathbb{C}^2/\Lambda$ with a period matrix $\tau \in \mathbb{H}_2$, the functions $\varphi_2(z) = (\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](z, \tau/2))_{b\in(\mathbb{Z}/2\mathbb{Z})^2}$ satisfy $\varphi_2(z) = \varphi_2(-z)$ and induce the morphism $\mathcal{K}_\mathcal{A} \longrightarrow \mathbb{P}^3$; see Section 3.3 and [4, Thm. 4.8.1]). This morphism φ_2 is in fact an embedding and its image is a quartic surface in $\mathbb{P}^3$ with Theta constants determining its equation. We have the following:

Lemma 7. *Let $\mathcal{A}$ be a principally polarized Abelian surface over $\mathbb{C}$, not isomorphic to a product of elliptic curves. The map $\varphi_2\colon \mathcal{K}_\mathcal{A} \longrightarrow \mathbb{P}^3$ defined by $\varphi_2(z) = (\theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](z, \tau/2))_{b\in(\mathbb{Z}/2\mathbb{Z})^2}$ is an embedding.*

Proof. The Theta functions $\theta_i(z) = \theta\left[\begin{smallmatrix}0\\ b\end{smallmatrix}\right](z, \tau/2)$ for $b \in (\mathbb{Z}/2\mathbb{Z})^2$ are even, satisfying $\theta_i(-z) = \theta_i(z)$ due to the characteristic's symmetry under the involution ι. Thus, $\varphi_2\colon \mathcal{A} \longrightarrow \mathbb{P}^3$ factors through the quotient $\pi\colon \mathcal{A} \longrightarrow \mathcal{K}_\mathcal{A}$, inducing a well-defined map $\overline{\varphi_2}\colon \mathcal{K}_\mathcal{A} \longrightarrow \mathbb{P}^3$. For $\mathcal{A}$ principally polarized, the line bundle $\mathscr{L}^2$ corresponds to 2Θ, where Θ is the Theta divisor. The space of sections $\Gamma(\mathcal{A}, \mathscr{L}^2)$ is four-dimensional, spanned by the θ_i. If $\mathcal{A}$ is not a product $E_1 \times E_2$, the polarization ensures $\mathscr{L}^2$ is very ample on $\mathrm{Kum}(\mathcal{A})$, separating points and tangent vectors. Specifically, for distinct points $x, y \in \mathcal{K}_\mathcal{A}$ (not both in $\mathcal{A}[2]$), there exists i such that $\theta_i(x) \neq \theta_i(y)$, and for a point x with tangent direction v, some θ_i has non-zero derivative along v. Thus, $\overline{\varphi_2}$ embeds $\mathcal{K}_\mathcal{A}$ as a quartic surface with 16 nodes at the images of $\mathcal{A}[2]$. □

The image of each order-two point of $\mathcal{A}$ is a singular point on the Kummer surface $\mathcal{K}_\mathcal{A}$ and called a *node*. That is, nodes are the images of the order-two points $P_{ij} \in \mathcal{A}[2]$. Similarly, any Theta divisor of $\mathcal{A}$ is mapped to the intersection of the singular Kummer surface with a plane. We call such a singular plane a *trope*. In the complete linear system $|2\Theta|$ on $\mathrm{Jac}(\mathcal{X})$, the odd symmetric Theta divisors Θ_i on $\mathrm{Jac}(\mathcal{X})$ are

mapped to six tropes T_i, and the even symmetric Theta divisors Θ_{ijk} on $\mathrm{Jac}(\mathcal{X})$ are mapped to the tropes T_{ijk}. The ten tropes T_{ijk} with $1 \le i < j < k \le 6$ correspond to partitions of $\{1,\dots,6\}$ into two unordered sets of three, say $\{i,j,k\}$ $\{l,m,n\}$. We use the formulas for T_{ijk} from [10, Sec. 3.7] paying careful attention to the fact that we have moved the root λ_6 to infinity. Hence, a configuration of sixteen nodes and sixteen tropes is induced on $\mathcal{K}_{\mathcal{A}}$, where each trope contains six nodes and each node is contained in six tropes. This configuration is called the 16_6 *configuration on the singular Kummer surface* $\mathcal{K}_{\mathcal{A}}$.

4.2. **Kummer surfaces from odd characteristics.** The Jacobian $\mathrm{Jac}\,(\mathcal{X})$ of a smooth genus two curve $\mathcal{X}$ is birational to the symmetric product $\mathrm{Sym}^2(\mathcal{X})$. Let us consider the function field of $\mathrm{Sym}^2(\mathcal{X}) = (\mathcal{X}\times\mathcal{X})/\langle\sigma\rangle$ where σ interchanges the copies of $\mathcal{X}$. For a smooth genus-two curve $\mathcal{X}$ in Rosenhain form (17), the function field of the variety $\mathrm{Sym}^2(\mathcal{X})/\langle\imath\times\imath\rangle$ – where $\imath\times\imath$ is the involution on $\mathrm{Sym}^2(\mathcal{X})$ induced by the hyperelliptic involution $\imath$ on $\mathcal{X}$ – is generated by $z_1 = z^{(1)}z^{(2)}$, $z_2 = x^{(1)}z^{(2)} + x^{(2)}z^{(1)}$, $z_3 = x^{(1)}x^{(2)}$, and $\tilde{z}_4 = y^{(1)}y^{(2)}$, subject to the relation

$$\tilde{z}_4^2 = z_1 z_3 (z_1 - z_2 + z_3) \prod_{i=1}^{3} (\lambda_i^2\, z_1 - \lambda_i\, z_2 + z_3)\,. \tag{43}$$

Equation (43) is a special case of a *double sextic surface*, i.e., the double cover of $\mathbb{P}^2$ branched on the union of six lines (and hence over a sextic curve). The minimal resolution of a double sextic surface is always a K3 surface; see [2]. Equation (43) is known as *Shioda sextic* associated with $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$; see [61]. It follows that the minimal resolution of $\mathcal{W}$ is isomorphic to the Kummer surface $\mathrm{Kum}(\mathcal{A})$.

In Equation (43) the double cover of $\mathbb{P}^2 = \mathbb{P}(z_1, z_2, z_3)$ is branched along the following six lines T_i with $1 \le i \le 6$, given by

$$\lambda_i^2\, z_1 - \lambda_i\, z_2 + z_3 = 0 \text{ with } 1 \le i \le 3, \quad z_1 = 0, \quad z_1 - z_2 + z_3 = 0, \quad z_3 = 0\,. \tag{44}$$

These six lines are precisely the aforementioned odd tropes and tangent to the common conic $K_2 = z_2^2 - 4\, z_1 z_3 = 0$. Conversely, it is easy to see that any six lines tangent to a common conic can always be brought into the form of Equations (44) using a projective transformation. Thus, we can rewrite Equation (43) as

$$\tilde{z}_4^2 = \mathsf{T}_1\mathsf{T}_2\mathsf{T}_3\mathsf{T}_4\mathsf{T}_5\mathsf{T}_6\,. \tag{45}$$

Moreover, one easily checks that Moreover, there are fifteen linear relations between the odd tropes, and a generating set is given by

$$\begin{aligned}
\mathsf{T}_1 &= (1-\lambda_1)\mathsf{T}_4 + \lambda_1\mathsf{T}_5 + \lambda_1(\lambda_1-1)\mathsf{T}_6,\\
\mathsf{T}_2 &= (1-\lambda_2)\mathsf{T}_4 + \lambda_2\mathsf{T}_5 + \lambda_2(\lambda_2-1)\mathsf{T}_6,\\
\mathsf{T}_3 &= (1-\lambda_3)\mathsf{T}_4 + \lambda_3\mathsf{T}_5 + \lambda_3(\lambda_3-1)\mathsf{T}_6.
\end{aligned} \tag{46}$$

Humbert proved that the Kummer plane $(\mathbb{P}^2; \mathsf{T}_1, \dots, \mathsf{T}_6)$ inherits essential information of the principally polarized Abelian surface $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ itself; see [30].

We consider the blow up $p\colon \widehat{\mathcal{A}} \longrightarrow \mathcal{A}$, replacing the sixteen order-two points with the exceptional curves $E_1, \dots, E_{16}$. The linear system $|4p^*\Theta - \sum E_i|$ determines a morphism of degree two from $\widehat{\mathcal{A}}$ to a complete intersection of three quadrics in $\mathbb{P}^5$. The net spanned by these quadrics is isomorphic to $\mathbb{P}^2$ with a discriminant locus corresponding to the union of six lines (44). In [13] we showed the following:

Theorem 6. *The Kummer surface* $\mathrm{Kum}(\mathcal{A})$ *associated with the Jacobian* $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ *of a genus-two curve* $\mathcal{X}$ *in Rosenhain normal form (17) is the complete intersection of three quadrics in* $\mathbb{P}^5 = \mathbb{P}(\mathsf{t}_1 : \cdots : \mathsf{t}_6)$ *given by*

$$\begin{aligned}
\mathsf{t}_1^2 &= (1-\lambda_1)\mathsf{t}_4^2 + \lambda_1\mathsf{t}_5^2 + \lambda_1(\lambda_1-1)\mathsf{t}_6^2,\\
\mathsf{t}_2^2 &= (1-\lambda_2)\mathsf{t}_4^2 + \lambda_2\mathsf{t}_5^2 + \lambda_2(\lambda_2-1)\mathsf{t}_6^2,\\
\mathsf{t}_3^2 &= (1-\lambda_3)\mathsf{t}_4^2 + \lambda_3\mathsf{t}_5^2 + \lambda_3(\lambda_3-1)\mathsf{t}_6^2.
\end{aligned} \tag{47}$$

Proof. The Shioda sextic is given by the double cover of $\mathbb{P}^2$ branched along the reducible sextic that is the union of the six lines given by the tropes $\mathsf{T}_1, \dots, \mathsf{T}_6$. The tropes $\mathsf{T}_1, \dots, \mathsf{T}_6$ satisfy fifteen linear relations of rank three equivalent to Equations (46). Introducing $\mathsf{T}_i = \mathsf{t}_i^2$ such that $\tilde{z}_4 = \mathsf{t}_1\mathsf{t}_2\mathsf{t}_3\mathsf{t}_4\mathsf{t}_5\mathsf{t}_6$, the (smooth)

Kummer surface $\mathrm{Kum}(\mathcal{A}) = \widehat{\mathcal{A}}/\langle -\mathbb{I}\rangle$ is the complete intersection of three quadrics in $\mathbb{P}^5 \ni [\mathsf{t}_1 : \mathsf{t}_2 : \mathsf{t}_3 : \mathsf{t}_4 : \mathsf{t}_5 : \mathsf{t}_6]$ given by Equations (47). □

The following fact is well known:

Remark 1. *For the principally polarized Abelian surface $(\mathcal{A}, \mathscr{L})$, a basis of sections for $\mathscr{L}^4$, called the Theta functions of level $(2,2)$, is given by the odd genus 2 Theta functions that we denote by $\theta_i(z)$ for $11 \le i \le 16$.*

In [13, Lemma 4.11] it was shown that Thomae's formula provides an explicit relation between tropes and the Theta functions used in Theorem 6. In particular, it was shown that the following holds:

Remark 2. *There is a bijection between the six tropes $\mathsf{T}_1, \ldots, \mathsf{T}_6$ and the squares of the odd Theta functions $\theta_{11}^2(z), \ldots, \theta_{16}^2(z)$ such that Equations (44) are induced by the Mumford relations for Theta functions.*

The Shioda sextic is closely related to two quartic equations, known as the *Baker quartic* and *Cassels-Flynn quartic*. The Baker quartic is obtained directly from the Shioda sextic in Equation (44), using parameters

$$\begin{array}{rclcrcl} L_4 &=& 1+\lambda_1+\lambda_2+\lambda_3\,, & & L_3 &=& \lambda_1+\lambda_2+\lambda_3+\lambda_1\lambda_2+\lambda_2\lambda_3+\lambda_1\lambda_3\,, \\ L_1 &=& \lambda_1\lambda_2\lambda_3\,, & & L_2 &=& \lambda_1\lambda_2+\lambda_2\lambda_3+\lambda_1\lambda_3+\lambda_1\lambda_2\lambda_3\,, \end{array} \tag{48}$$

and the variable transformation given by

$$\begin{array}{l} \mathbf{W} = K_2\, z_1\,, \qquad \mathbf{X} = K_2\, z_2\,, \qquad \mathbf{Y} = K_2\, z_3\,, \\ \mathbf{Z} = 2\tilde{z}_4 - \big(L_1 z_1^2 z_2 - 2L_2 z_1^2 z_3 + L_3 z_1 z_2 z_3 - 2L_4 z_1 z_3^2 + z_2 z_3^2\big)\,. \end{array} \tag{49}$$

Equation (43) is then equivalent to the quartic surface in $\mathbb{P}^3 = \mathbb{P}(\mathbf{W}, \mathbf{X}, \mathbf{Y}, \mathbf{Z})$ given by the vanishing locus of the following *Baker determinant*, i.e.,

$$\begin{vmatrix} 0 & L_1\mathbf{W} & -\mathbf{Z} & \mathbf{Y} \\ L_1\mathbf{W} & 2L_2\mathbf{W}+2\mathbf{Z} & L_3\mathbf{W}-\mathbf{Y} & \mathbf{X} \\ -\mathbf{Z} & L_3\mathbf{W}-\mathbf{Y} & 2L_4\mathbf{W}-2\mathbf{X} & \mathbf{W} \\ \mathbf{Y} & \mathbf{X} & \mathbf{W} & 0 \end{vmatrix} = 0\,. \tag{50}$$

The Baker determinant was first derived in [1].

In addition to K_2 introduced above, let us also define homogeneous polynomials $K_l = K_l(z_1, z_2, z_3)$ of degree $4-l$ for $l = 0, 1$ with

$$\begin{array}{l} K_2 = z_2^2 - 4z_1 z_3\,, \qquad K_1 = -2z_2 z_3^2 - 2L_1 z_1^2 z_2 + 4L_2 z_1^2 z_3 - 2L_3 z_1 z_2 z_3 + 4L_4 z_1 z_3^2\,, \\ K_0 = L_1^2 z_1^4 - 2L_1 L_3 z_1^3 z_3 + (2L_1 - 4L_2 L_4 + L_3^2) z_1^2 z_3^2 + 4L_1 L_4 z_1^2 z_2 z_3 \\ \qquad + 3(-2L_1 z_2^2 z_3 + 2L_2 z_2 z_3^2 - L_3 z_3^3) z_1 + z_3^4\,. \end{array} \tag{51}$$

A variable transformation in Equation (43), given by

$$\tilde{z}_4 = \frac{1}{4}\,(K_2 z_4 + 2K_1)\,, \tag{52}$$

or, equivalently, the variable transformation in Equation (50), given by

$$\mathbf{W} = K_2\, z_1\,, \qquad \mathbf{X} = K_2\, z_2\,, \qquad \mathbf{Y} = K_2\, z_3\,, \qquad \mathbf{Z} = K_2 z_4 + K_1\,, \tag{53}$$

yields the quartic projective surface $\mathcal{K}$ in $\mathbb{P}^3 = \mathbb{P}(z_1, z_2, z_3, z_4)$ given by

$$K_2(z_1, z_2, z_3)\; z_4^2 \;+\; K_1(z_1, z_2, z_3)\; z_4 \;+\; K_0(z_1, z_2, z_3) = 0\,. \tag{54}$$

The quartic appeared in Cassels and Flynn [10, Sec. 3] and is called the *Cassels-Flynn quartic*. Recall from Proposition 1 that $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$ is the rational function field of the moduli space $\mathbb{A}_2(2)$. In summary, for the principally polarized Abelian surface $\mathcal{A}$ with the standard Theta divisor $\Theta \cong [\mathcal{X}]$ and polarizing line bundle $\mathscr{L} = \mathcal{O}_{\mathcal{A}}(\Theta)$ we have the following; see [9]:

Proposition 3. *Assume that $\lambda_1, \lambda_2, \lambda_3$ are the Rosenhain roots of a smooth genus-two curve $\mathcal{X}$ in Equation (17). The surfaces in Equations (43) and (50) are birational equivalent over $\mathbb{Q}(\lambda_1, \lambda_2, \lambda_3)$. In particular, the quartic hypersurfaces are isomorphic to the singular Kummer variety $\mathcal{K}_{\mathcal{A}}$ associated with the principally polarized Abelian surface $(\mathcal{A}, \mathscr{L})$.*

4.3. **Kummer surfaces from even characteristics.** In this section we give explicit algebraic equations for the singular Kummer variety $\mathcal{K}_{\mathcal{A}} = \mathcal{A}/\langle -\mathbb{I}\rangle$, associated with a principally polarized Abelian variety $(\mathcal{A}, \mathscr{L})$: they are called the *Hudson quartic*, *Göpel quartic*, and *Rosenhain quartic*; see results in [4].

Let $\mathscr{L}$ again be the symmetric ample line bundle of an Abelian surface $\mathcal{A}$ defining its principal polarization and consider the rational map $\varphi_2 \colon \mathcal{A} \longrightarrow \mathbb{P}^3$ associated with the line bundle $\mathscr{L}^2$. Its image $\varphi_2(\mathcal{A})$ is a quartic surface in $\mathbb{P}^3$ which in projective coordinates $[w : x : y : z]$ can be written as

$$\begin{aligned} 0 = \xi_0\,(w^4 + x^4 + y^4 + z^4) + \xi_4\, wxyz \\ +\xi_1\,(w^2z^2 + x^2y^2) + \xi_2\,(w^2x^2 + y^2z^2) + \xi_3\,(w^2y^2 + x^2z^2), \end{aligned} \tag{55}$$

with $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$. Any general member of the family (55) is smooth. As soon as the surface is singular at a general point, it must have sixteen singular nodal points because of its symmetry. The discriminant turns out to be a homogeneous polynomial of degree eighteen in the parameters $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$ and was determined in [4, Sec. 7.7 (3)]. Thus, the Kummer surfaces form an open set among the hypersurfaces in Equation (55) with parameters $[\xi_0 : \xi_1 : \xi_2 : \xi_3 : \xi_4] \in \mathbb{P}^4$, namely the ones that make the only irreducible factor of degree three in the discriminant vanish, i.e.,

$$\xi_0\,(16\xi_0^2 - 4\xi_1^2 - 4\xi_2^2 - 4\xi_3^3 + \xi_4^2) + 4\,\xi_1\xi_2\xi_3 = 0. \tag{56}$$

Setting $\xi_0 = 1$ and using the affine moduli $\xi_1 = -A$, $\xi_2 = -B$, $\xi_3 = -C$, $\xi_4 = 2D$, we obtain the normal form of a nodal quartic surface. Thus, we say that a *Hudson quartic* is the surface in $\mathbb{P}^3 = \mathbb{P}(w, x, y, z)$ given by

$$\begin{aligned} 0 = w^4 + x^4 + y^4 + z^4 + 2Dwxyz \\ -A(w^2z^2 + x^2y^2) - B(w^2x^2 + y^2z^2) - C(w^2y^2 + x^2z^2)\,, \end{aligned} \tag{57}$$

where $A, B, C, D \in \mathbb{C}$ such that

$$D^2 = A^2 + B^2 + C^2 + ABC - 4\,. \tag{58}$$

The Hudson quartic in Equation (57) is invariant under the transformations changing signs of two coordinates, generated by

$$[w : x : y : z] \to [-w : -x : y : z], \quad [w : x : y : z] \to [-w : x : -y : z],$$

and under the permutations of variables, generated by $[w : x : y : z] \to [x : w : z : y]$ and $[w : x : y : z] \to [y : z : w : x]$.

A different quartic hypersurface equation is due to Kummer [38] and Borchardt [7]. We say that a *Göpel quartic* is the surface in $\mathbb{P}^3 = \mathbb{P}(P, Q, R, S)$ given by

$$\Phi^2 - 4\,\delta^2 SPQR = 0\,, \tag{59}$$

with

$$\Phi = P^2 + Q^2 + R^2 + S^2 - \alpha\,(PS + QR) - \beta\,(PQ + RS) - \gamma\,(PR + QS)\,, \tag{60}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ such that

$$\delta^2 = \alpha^2 + \beta^2 + \gamma^2 + \alpha\beta\gamma - 4\,. \tag{61}$$

We have the following:

Proposition 4. *The Hudson quartic in Equation (57) is isomorphic to the Göpel quartic in Equation (59), for suitable sets of parameters (A, B, C, D) satisfying Equation (58) and $(\alpha, \beta, \gamma, \delta)$ satisfying Equation (61). In particular, the quartic hypersurfaces are isomorphic to the singular Kummer variety $\mathcal{K}_{\mathcal{A}}$ associated with the principally polarized Abelian surface $(\mathcal{A}, \mathscr{L})$.*

Proof. We first introduce complex numbers $[w_0 : x_0 : y_0 : z_0] \in \mathbb{P}^3$ such that

$$\begin{aligned} A = \frac{w_0^4 - x_0^4 - y_0^4 + z_0^4}{w_0^2z_0^2 - x_0^2y_0^2}, \quad B = \frac{w_0^4 + x_0^4 - y_0^4 - z_0^4}{w_0^2x_0^2 - y_0^2z_0^2}, \quad C = \frac{w_0^4 - x_0^4 + y_0^4 - z_0^4}{w_0^2y_0^2 - x_0^2z_0^2}, \\ D = \frac{w_0x_0y_0z_0 \prod_{\epsilon,\epsilon' \in \{\pm 1\}} (w_0^2 + \epsilon x_0^2 + \epsilon' y_0^2 + \epsilon\epsilon' z_0^2)}{(w_0^2z_0^2 - x_0^2y_0^2)(w_0^2x_0^2 - y_0^2z_0^2)(w_0^2y_0^2 - x_0^2z_0^2)}, \end{aligned} \tag{62}$$

and

$$\alpha = 2\,\frac{w_0^2\,y_0^2 + x_0^2\,z_0^2}{w_0^2\,y_0^2 - x_0^2\,z_0^2}, \quad \beta = 2\,\frac{w_0^2\,x_0^2 + y_0^2\,z_0^2}{w_0^2\,x_0^2 - y_0^2\,z_0^2}, \quad \gamma = 2\,\frac{w_0^2\,z_0^2 + x_0^2\,y_0^2}{w_0^2\,z_0^2 - x_0^2\,y_0^2},$$

$$\delta^2 = 16\,\frac{w_0^4 x_0^4 y_0^4 z_0^4 \prod_{\epsilon,\epsilon'\in\{\pm 1\}}(w_0^2 + \epsilon x_0^2 + \epsilon' y_0^2 + \epsilon\epsilon' z_0^2)}{\left(w_0^2\,y_0^2 - x_0^2\,z_0^2\right)^2\left(w_0^2\,x_0^2 - y_0^2\,z_0^2\right)^2\left(w_0^2\,z_0^2 - x_0^2\,y_0^2\right)^2}. \tag{63}$$

Then, the linear transformation given by

$$\begin{aligned} P &= w_0\,w + x_0\,x + y_0\,y + z_0\,z\,,\\ Q &= w_0\,w + x_0\,x - y_0\,y - z_0\,z\,,\\ R &= w_0\,w - x_0\,x - y_0\,y + z_0\,z\,,\\ S &= w_0\,w - x_0\,x + y_0\,y - z_0\,z\,, \end{aligned} \tag{64}$$

transforms Equation (59) into Equation (57). □

Lemma 8. *Using the same notation as in Equation (62), the sixteen nodes of the Hudson quartic (57) are given by*

$$\begin{gathered} [w_0 : x_0 : y_0 : z_0], [-w_0 : -x_0 : y_0 : z_0], [-w_0 : x_0 : -y_0 : z_0], [-w_0 : x_0 : y_0 : -z_0],\\ [x_0 : w_0 : z_0 : y_0], [-x_0 : -w_0 : z_0 : y_0], [-x_0 : w_0 : -z_0 : y_0], [-x_0 : w_0 : z_0 : -y_0],\\ [y_0 : z_0 : w_0 : x_0], [-y_0 : -z_0 : w_0 : x_0], [-y_0 : z_0 : -w_0 : x_0], [-y_0 : z_0 : w_0 : -x_0],\\ [z_0 : y_0 : x_0 : w_0], [-z_0 : -y_0 : x_0 : w_0], [-z_0 : y_0 : -x_0 : w_0], [-z_0 : y_0 : x_0 : -w_0]. \end{gathered}$$

In particular, for generic parameters (A, B, C, D), no node is contained in the coordinate planes $w = 0$, $x = 0$, $y = 0$, or $z = 0$.

We also set

$$\begin{aligned} p_0^2 &= w_0^2 + x_0^2 + y_0^2 + z_0^2, \quad q_0^2 = w_0^2 + x_0^2 - y_0^2 - z_0^2,\\ r_0^2 &= w_0^2 - x_0^2 + y_0^2 - z_0^2, \quad s_0^2 = w_0^2 - x_0^2 - y_0^2 + z_0^2. \end{aligned} \tag{65}$$

We have the following:

Lemma 9. *The nodes of the Göpel quartic (59) are given by*

$$\begin{gathered} [p_0^2 : q_0^2 : r_0^2 : s_0^2], [q_0^2 : p_0^2 : s_0^2 : r_0^2], [r_0^2 : s_0^2 : r_0^2 : q_0^2], [s_0^2 : r_0^2 : q_0^2 : p_0^2],\\ [w_0x_0 + y_0z_0 : w_0x_0 - y_0z_0 : 0 : 0], [w_0x_0 - y_0z_0 : w_0x_0 + y_0z_0 : 0 : 0],\\ [0 : 0 : w_0x_0 + y_0z_0 : w_0x_0 - y_0z_0], [0 : 0 : w_0x_0 - y_0z_0 : w_0x_0 + y_0z_0],\\ [w_0z_0 + x_0y_0 : 0 : w_0z_0 - x_0y_0 : 0], [0 : w_0z_0 + x_0y_0 : 0 : w_0z_0 - x_0y_0],\\ [w_0z_0 - x_0y_0 : 0 : w_0z_0 + x_0y_0 : 0], [0 : w_0z_0 - x_0y_0 : 0 : w_0z_0 + x_0y_0],\\ [w_0y_0 + x_0z_0 : 0 : 0 : w_0y_0 - x_0z_0], [0 : w_0y_0 + x_0z_0 : w_0y_0 - x_0z_0 : 0],\\ [0 : w_0y_0 - x_0z_0 : w_0y_0 + x_0z_0 : 0], [w_0y_0 - x_0z_0 : 0 : 0 : w_0y_0 + x_0z_0]. \end{gathered}$$

In [4, Prop. 10.3.2] yet another normal form for a nodal quartic surfaces was established. We say that a *Rosenhain quartic* is the surface in $\mathbb{P}^3 = \mathbb{P}(Y_0, \ldots, Y_3)$ given by

$$\begin{aligned} &a^2(Y_0^2Y_1^2 + Y_2^2Y_3^2) + b^2(Y_0^2Y_2^2 + Y_1^2Y_3^2) + c^2(Y_0^2Y_3^2 + Y_1^2Y_2^2)\\ &+2ab(Y_0Y_1 - Y_2Y_3)(Y_0Y_2 + Y_1Y_3) - 2ac(Y_0Y_1 + Y_2Y_3)(Y_0Y_3 + Y_1Y_2)\\ &+2bc(Y_0Y_2 - Y_1Y_3)(Y_0Y_3 - Y_1Y_2) + d^2Y_0Y_1Y_2Y_3 = 0, \end{aligned} \tag{66}$$

with $[a : b : c : d] \in \mathbb{P}^3$. Equation (66) is invariant under the Cremona transformation

$$[Y_0 : Y_1 : Y_2 : Y_3] \;\mapsto\; [Y_1Y_2Y_3 : Y_0Y_2Y_3 : Y_0Y_1Y_3 : Y_0Y_1Y_2]\,. \tag{67}$$

The following was proved in [4, Prop. 10.3.2]:

Proposition 5. *For generic parameters $[a : b : c : d] \in \mathbb{P}^3$, the Rosenhain quartic in Equation (66) is isomorphic to the singular Kummer variety $\mathcal{K}_{\mathcal{A}}$ associated with the principally polarized Abelian surface $(\mathcal{A}, \mathscr{L})$.*

We also have the following:

Lemma 10. *The Rosenhain quartic in Equation (66) is isomorphic to the Hudson quartic in Equation (57).*

Proof. Using the same notation as in the proof of Proposition 4, we set

$$\begin{aligned} a &= 4(w_0^2 z_0^2 - x_0^2 y_0^2)(w_0 y_0 + x_0 z_0), \\ b &= (w_0^2 + x_0^2 - y_0^2 - z_0^2)(w_0^2 - x_0^2 + y_0^2 - z_0^2)(w_0 x_0 - y_0 z_0), \\ c &= (w_0^2 - x_0^2 - y_0^2 + z_0^2)(w_0^2 + x_0^2 + y_0^2 + z_0^2)(w_0 x_0 + y_0 z_0), \end{aligned} \tag{68}$$

and a polynomial expression for d^2 of degree twelve that we do not write out explicitly. Then, the linear transformation given by

$$\begin{aligned} Y_0 &= w_0\, w + x_0\, x + y_0\, y + z_0\, z\,, \\ Y_1 &= w_0\, w + x_0\, x - y_0\, y - z_0\, z\,, \\ Y_2 &= z_0\, w + y_0\, x + x_0\, y + w_0\, z\,, \\ Y_3 &= z_0\, w + y_0\, x - x_0\, y - w_0\, z\,, \end{aligned} \tag{69}$$

transforms Equation (66) into Equation (57). □

4.4. **An explicit model using Theta functions.** We provide an explicit model for the quartic hypersurfaces in terms of Theta functions.

In addition to the identities from Section 3.3, we have the following identities for Theta functions with non-vanishing elliptic argument [32, 33]:

$$\begin{aligned} \theta_1\,\theta_1(z) &= \Theta_1(z)^2 + \Theta_2(z)^2 + \Theta_3(z)^2 + \Theta_4(z)^2\,, \\ \theta_2\,\theta_2(z) &= \Theta_1(z)^2 + \Theta_2(z)^2 - \Theta_3(z)^2 - \Theta_4(z)^2\,, \\ \theta_3\,\theta_3(z) &= \Theta_1(z)^2 - \Theta_2(z)^2 - \Theta_3(z)^2 + \Theta_4(z)^2\,, \\ \theta_4\,\theta_4(z) &= \Theta_1(z)^2 - \Theta_2(z)^2 + \Theta_3(z)^2 - \Theta_4(z)^2\,, \end{aligned} \tag{70}$$

and

$$\begin{aligned} 4\,\Theta_1\,\Theta_1(2z) &= \theta_1(z)^2 + \theta_2(z)^2 + \theta_3(z)^2 + \theta_4(z)^2\,, \\ 4\,\Theta_2\,\Theta_2(2z) &= \theta_1(z)^2 + \theta_2(z)^2 - \theta_3(z)^2 - \theta_4(z)^2\,, \\ 4\,\Theta_3\,\Theta_3(2z) &= \theta_1(z)^2 - \theta_2(z)^2 - \theta_3(z)^2 + \theta_4(z)^2\,, \\ 4\,\Theta_4\,\Theta_4(2z) &= \theta_1(z)^2 - \theta_2(z)^2 + \theta_3(z)^2 - \theta_4(z)^2\,. \end{aligned} \tag{71}$$

The following is a well-known fact:

Remark 3. *For the principally polarized Abelian surface $(\mathcal{A}, \mathscr{L})$, a basis of sections for $\mathscr{L}^2$, called Theta functions of level two, is given by $\Theta_i(2z)$ or, alternatively, $\theta_i^2(z)$ for $1 \le i \le 4$ using Equations (71).*

We have the following:

Proposition 6. *For the surface in $\mathbb{P}^3$ given by Equation (59), the coordinates are given by*

$$[P : Q : R : S] = \left[\theta_1(z)^2 : \theta_2(z)^2 : \theta_3(z)^2 : \theta_4(z)^2\right]\,, \tag{72}$$

and the parameters are

$$\begin{aligned} \alpha &= \frac{\theta_1^4 - \theta_2^4 - \theta_3^4 + \theta_4^4}{\theta_1^2\theta_4^2 - \theta_2^2\theta_3^2}, \quad \beta = \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2}, \quad \gamma = \frac{\theta_1^4 - \theta_2^4 + \theta_3^4 - \theta_4^4}{\theta_1^2\theta_3^2 - \theta_2^2\theta_4^2}, \\ \delta &= \frac{\theta_1\theta_2\theta_3\theta_4 \prod_{\epsilon,\epsilon' \in \{\pm 1\}} (\theta_1^2 + \epsilon\theta_2^2 + \epsilon'\theta_3^2 + \epsilon\epsilon'\theta_3^2)}{(\theta_1^2\,\theta_2^2 - \theta_3^2\,\theta_4^2)\,(\theta_1^2\,\theta_3^2 - \theta_2^2\,\theta_4^2)\,(\theta_1^2\,\theta_4^2 - \theta_2^2\,\theta_3^2)}. \end{aligned} \tag{73}$$

Proof. A direct computation shows that the non-vanishing elliptic variables $[P:Q:R:S] = [\theta_1(z)^2 : \theta_2(z)^2 : \theta_3(z)^2 : \theta_4(z)^2]$ satisfy Equation (59), with

$$\alpha = 2\,\frac{\Theta_1^2\Theta_3^2+\Theta_2^2\Theta_4^2}{\Theta_1^2\Theta_3^2-\Theta_2^2\Theta_4^2},\quad \beta = 2\,\frac{\Theta_1^2\Theta_2^2+\Theta_3^2\Theta_4^2}{\Theta_1^2\Theta_2^2-\Theta_3^2\Theta_4^2},\quad \gamma = 2\,\frac{\Theta_1^2\Theta_4^2+\Theta_2^2\Theta_3^2}{\Theta_1^2\Theta_4^2-\Theta_2^2\Theta_3^2}. \tag{74}$$

The parameters can be re-written

$$\alpha = \frac{\theta_1^4-\theta_2^4-\theta_3^4+\theta_4^4}{\theta_1^2\theta_4^2-\theta_2^2\theta_3^2},\quad \beta = \frac{\theta_1^4+\theta_2^4-\theta_3^4-\theta_4^4}{\theta_1^2\theta_2^2-\theta_3^2\theta_4^2},\quad \gamma = \frac{\theta_1^4-\theta_2^4+\theta_3^4-\theta_4^4}{\theta_1^2\theta_3^2-\theta_2^2\theta_4^2}. \tag{75}$$

such that over $\mathbb{A}_2(4,8)$ the modulus δ is given as

$$\delta = \frac{\theta_1\theta_2\theta_3\theta_4\prod_{\epsilon,\epsilon'\in\{\pm1\}}(\theta_1^2+\epsilon\theta_2^2+\epsilon'\theta_3^2+\epsilon\epsilon'\theta_3^2)}{(\theta_1^2\,\theta_2^2-\theta_3^2\,\theta_4^2)\,(\theta_1^2\,\theta_3^2-\theta_2^2\,\theta_4^2)\,(\theta_1^2\,\theta_4^2-\theta_2^2\,\theta_3^2)}.$$

□

Remark 4. *The transformation $[w:x:y:z]\to[-w:x:y:z]$ is an isomorphism between a Hudson quartic in Equation (57) with moduli (A,B,C,D) and the one with $(A,B,C,-D)$. Moreover, the two quartics coincide exactly along the coordinate planes $w=0$, $x=0$, $y=0$, or $z=0$.*

We also provide an explicit model for the Hudson quartic in terms of Theta functions. In terms of Theta functions, the relation between Equation (57) and Equation (59) was first determined by Borchardt [7]. We have the following:

Proposition 7. *For the surface in $\mathbb{P}^3$ given by Equation (57), the coordinates are given by*

$$[w:x:y:z] = [\Theta_1(2z):\Theta_2(2z):\Theta_3(2z):\Theta_4(2z)]\,, \tag{76}$$

and the parameters are

$$A = \frac{\Theta_1^4-\Theta_2^4-\Theta_3^4+\Theta_4^4}{\Theta_1^2\Theta_4^2-\Theta_2^2\Theta_3^2},\quad B = \frac{\Theta_1^4+\Theta_2^4-\Theta_3^4-\Theta_4^4}{\Theta_1^2\Theta_2^2-\Theta_3^2\Theta_4^2},\quad C = \frac{\Theta_1^4-\Theta_2^4+\Theta_3^4-\Theta_4^4}{\Theta_1^2\Theta_3^2-\Theta_2^2\Theta_4^2},$$
$$D = \frac{\Theta_1\Theta_2\Theta_3\Theta_4\prod_{\epsilon,\epsilon'\in\{\pm1\}}(\Theta_1^2+\epsilon\Theta_2^2+\epsilon'\Theta_3^2+\epsilon\epsilon'\Theta_4^2)}{(\Theta_1^2\Theta_2^2-\Theta_3^2\Theta_4^2)(\Theta_1^2\Theta_3^2-\Theta_2^2\Theta_4^2)(\Theta_1^2\Theta_4^2-\Theta_2^2\Theta_3^2)}. \tag{77}$$

Proof. Comparing Equations (74) and (63), we find a solution in terms of Theta function given by

$$[w_0:x_0:y_0:z_0] = [\Theta_1:\Theta_2:\Theta_3:\Theta_4]\,. \tag{78}$$

Equations (64) are equivalent to

$$\begin{aligned}
\theta_1^2(z) &= \Theta_1\,\Theta_1(2z)+\Theta_2\,\Theta_2(2z)+\Theta_3\,\Theta_3(2z)+\Theta_4\,\Theta_4(2z),\\
\theta_2^2(z) &= \Theta_1\,\Theta_1(2z)+\Theta_2\,\Theta_2(2z)-\Theta_3\,\Theta_3(2z)-\Theta_4\,\Theta_4(2z),\\
\theta_3^2(z) &= \Theta_1\,\Theta_1(2z)-\Theta_2\,\Theta_2(2z)-\Theta_3\,\Theta_3(2z)+\Theta_4\,\Theta_4(2z),\\
\theta_4^2(z) &= \Theta_1\,\Theta_1(2z)-\Theta_2\,\Theta_2(2z)+\Theta_3\,\Theta_3(2z)-\Theta_4\,\Theta_4(2z).
\end{aligned} \tag{79}$$

Comparing Equations (64) with Equations (79), the coordinates can be expressed in terms of Theta functions with non-vanishing elliptic arguments as

$$[w:x:y:z] = [\Theta_1(2z):\Theta_2(2z):\Theta_3(2z):\Theta_4(2z)].$$

□

The map $\pi\colon \mathbb{P}(w,x,y,z)\longrightarrow\mathbb{P}(P,Q,R,S)$ with $P=w^2,\ldots,S=z^2$ is $8:1$ outside the coordinate planes. The map π induces a covering of a reducible octic surface in $\mathbb{P}^3$ given by

$$(\Phi'-2Dwxyz)\,(\Phi'+2Dwxyz)=0\,, \tag{80}$$

with

$$\Phi' = w^4+x^4+y^4+z^4-A(w^2y^2+y^2z^2)-B(w^2z^2+x^2y^2)-C(w^2x^2+y^2z^2),$$

onto the Göpel quartic in Equation (59) with $\alpha = A$, $\beta = B$, $C = \gamma$, and $D = \delta$. We can assume that the Hudson quartic and Göpel quartic are the singular Kummer varieties associated with two principally polarized Abelian varieties, say $\mathcal{A}$ and $\hat{\mathcal{A}}$, respectively. We have the following:

Proposition 8. *The map $\pi\colon \mathbb{P}(w,x,y,z) \longrightarrow \mathbb{P}(P,Q,R,S)$ with $P = w^2, \ldots, S = z^2$ restricted to the Hudson quartic onto the Göpel quartic with $\alpha = A$, $\beta = B$, $C = \gamma$, and $D = \delta$, is induced by a $(2,2)$-isogeny $\Psi\colon \mathcal{A} \longrightarrow \hat{\mathcal{A}}$.*

Proof. The rational map π is 4:1 from the Hudson quartic onto the Göpel quartic. In fact, the map $\pi\colon \mathbb{P}(w,x,y,z) \longrightarrow \mathbb{P}(P,Q,R,S)$ maps the sixteen nodes on the Göpel-Hudson quartic in Lemma 8 to four nodes on the Göpel quartic in Lemma 9. □

Similarly, we have for the Rosenhain quartic (66):

Proposition 9. *For the surface in $\mathbb{P}^3$ given by Equation (66), the coordinates are given by*

$$[Y_0 : Y_1 : Y_2 : Y_3] = \left[\theta_1(z)^2 : \theta_2(z)^2 : \theta_7(z)^2 : \theta_{12}(z)^2\right] \ , \tag{81}$$

and the parameters are

$$\begin{aligned}
a &= (2\,\Theta_1\Theta_4 - 2\,\Theta_2\Theta_3)\,(2\,\Theta_1\Theta_4 + 2\,\Theta_2\Theta_3)\,(2\,\Theta_1\Theta_3 + 2\,\Theta_2\Theta_4)\,,\\
b &= \left(\Theta_1^2 + \Theta_2^2 - \Theta_3^2 - \Theta_4^2\right)\left(\Theta_1^2 - \Theta_2^2 + \Theta_3^2 - \Theta_4^2\right)(2\,\Theta_1\Theta_2 - 2\,\Theta_3\Theta_4)\,,\\
c &= \left(\Theta_1^2 - \Theta_2^2 - \Theta_3^2 + \Theta_4^2\right)\left(\Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2\right)(2\,\Theta_1\Theta_2 + 2\,\Theta_3\Theta_4)\,,\\
d^2 &= 256\,\Theta_1\Theta_2\Theta_4\Theta_3\left(\Theta_1^2\Theta_4^2 - \Theta_2^2\Theta_3^2\right)\left(\Theta_1^4 - \Theta_2^4 - \Theta_3^4 + \Theta_4^4\right)\\
&+8\left(\Theta_1^2 + \Theta_4^2\right)\left(\Theta_2^2 + \Theta_3^2\right)\left(\Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2\right)^2\left(\Theta_1^2 - \Theta_2^2 - \Theta_3^2 + \Theta_4^2\right)^2\\
&+8\left(\Theta_1^2 - \Theta_4^2\right)\left(\Theta_2^2 - \Theta_3^2\right)\left(\Theta_1^2 + \Theta_2^2 - \Theta_3^2 - \Theta_4^2\right)^2\left(\Theta_1^2 - \Theta_2^2 + \Theta_3^2 - \Theta_4^2\right)^2\\
&-32\left(\Theta_1^2\Theta_2^2 + \Theta_3^2\Theta_4^2\right)\left(\Theta_1^2 + \Theta_2^2 + \Theta_3^2 + \Theta_4^2\right)\left(\Theta_1^2 - \Theta_2^2 + \Theta_3^2 - \Theta_4^2\right)\\
&\times\left(\Theta_1^2 - \Theta_2^2 - \Theta_3^2 + \Theta_4^2\right)\left(\Theta_1^2 + \Theta_2^2 - \Theta_3^2 - \Theta_4^2\right).
\end{aligned}$$

The Rosenhain roots of the genus 2 curve $\mathcal{X}$ in Equation (35) generate the rational function field $\mathbb{Q}(\lambda_1,\lambda_2,\lambda_3)$ of the moduli space $\mathbb{A}_2(2)$ of principally polarized Abelian surfaces $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ with level-two structure. The moduli A, B, C, D of the Hudson quartic (57) are then given by the rational functions

$$\begin{gathered}
A = 2\,\frac{\lambda_1+1}{\lambda_1-1}, \quad B = 2\,\frac{\lambda_1\lambda_2 + \lambda_1\lambda_3 - 2\lambda_2\lambda_3 - 2\lambda_1 + \lambda_2 + \lambda_3}{(\lambda_2-\lambda_3)(\lambda_1-1)}, \quad C = 2\,\frac{\lambda_3+\lambda_2}{\lambda_3-\lambda_2},\\
D = 4\,\frac{\lambda_1 - \lambda_2\lambda_3}{(\lambda_2-\lambda_3)(\lambda_1-1)}\ .
\end{gathered} \tag{82}$$

Similarly, the Rosenhain roots of the genus 2 curve $\hat{\mathcal{X}}$ in Equation (36) generate the rational function field $\mathbb{Q}(\Lambda_1,\Lambda_2,\Lambda_3)$ of the moduli space $\hat{\mathbb{A}}_2(2)$ of $(2,2)$-isogenous principally polarized Abelian surfaces with level-2 structure. In turn, the moduli $\alpha, \beta, \gamma, \delta$ of the Göpel quartic (59) are given by the rational functions

$$\begin{gathered}
\alpha = 2\,\frac{\Lambda_1+1}{\Lambda_1-1},\ \beta = 2\,\frac{\Lambda_1\Lambda_2 + \Lambda_1\Lambda_3 - 2\Lambda_2\Lambda_3 - 2\Lambda_1 + \Lambda_2 + \Lambda_3}{(\Lambda_2-\Lambda_3)(\Lambda_1-1)},\ \gamma = 2\,\frac{\Lambda_3+\Lambda_2}{\Lambda_3-\Lambda_2},\\
\delta = \frac{4(\Lambda_1 - \Lambda_2\Lambda_3)}{(\Lambda_1-1)(\Lambda_3-\Lambda_2)}.
\end{gathered} \tag{83}$$

Recalling the statement of Proposition 1, we conclude the following:

Theorem 7. *For the Jacobian $\mathrm{Jac}(\mathcal{X})$ of a smooth genus-two curve $\mathcal{X}$ in Rosenhain normal form given by Equation (35) we have the following:*

1. *The Hudson quartic (57) is the image of $[\Theta_1(2z) : \Theta_2(2z) : \Theta_3(2z) : \Theta_4(2z)]$ in $\mathbb{P}^3$ with moduli (82) defined over $\mathbb{A}_2(2)$.*
2. *The Göpel quartic (59) is the image of $[\theta_1^2(z) : \theta_2^2(z) : \theta_3^2(z) : \theta_4^2(z)]$ in $\mathbb{P}^3$ with moduli (83) defined over $\hat{\mathbb{A}}_2(2)$.*
3. *The Rosenhain quartic (66) is the image of $[\theta_1^2(z) : \theta_2^2(z) : \theta_7^2(z) : \theta_{12}^2(z)]$ in $\mathbb{P}^3$ with moduli defined over $\mathbb{A}_2(2,4)$.*

Tetrahedra in $\mathbb{P}^3$ whose faces are tropes are called *Rosenhain tetrahedra* if all vertices are nodes; they are called *Göpel tetrahedra* if none of the vertices are nodes. It turns out that Rosenhain tetrahedra have an odd number of odd tropes, namely one or three, whereas Göpel tetrahedra have an even number of odd tropes, namely zero or two. In [13] it was shown that Thomae's formula provides an explicit relation between tropes and the Theta functions used in Theorem 7. In particular, in [13] it was shown that tropes can be chosen so that the following holds:

Remark 5.

(1) *The tropes of the Göpel tetrahedron* $\{\mathsf{T}_{256}, \mathsf{T}_{136}, \mathsf{T}_{356}, \mathsf{T}_{126}\}$ *can be chosen to coincide with the Theta functions* $[\theta_1^2(z) : \theta_2^2(z) : \theta_3^2(z) : \theta_4^2(z)]$.

(2) *The tropes of the Rosenhain tetrahedron* $\{\mathsf{T}_{256}, \mathsf{T}_{136}, \mathsf{T}_{246}, \mathsf{T}_{2}\}$*, can be chosen to coincide with the Theta functions* $[\theta_1^2(z) : \theta_2^2(z) : \theta_7^2(z) : \theta_{12}^2(z)]$.

4.5. **Shioda-Inose Surfaces.** Given an Abelian surface $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$, one can construct an associate *Shioda-Inose surface* $\mathcal{Y} := \mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$, which is a K3 surface that shares a similar Hodge structure with $\mathcal{A}$, on its transcendental lattice.

The surface, $\mathcal{Y}$, is obtained (see [12]) as a geometric two-isogeny of $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$. Namely, one has a diagram as below, involving rational double-cover maps:

$$\mathrm{Jac}(\mathcal{X}) \overset{\pi}{\dashrightarrow} \mathrm{Kum}(\mathrm{Jac}(\mathcal{X})) \underset{p}{\overset{r}{\rightleftarrows}} \mathcal{Y} = \mathrm{SI}(\mathrm{Jac}(\mathcal{X})) \tag{84}$$

The Shioda-Inose terminology for $\mathcal{Y}$ is motivated by the existence of a Shioda-Inose structure on this surface. In turn, such a structure induces an isomorphism of integral Hodge structures between the transcendental lattices of $\mathrm{Jac}(\mathcal{X})$ and $\mathcal{Y}$ (see [62]). More specifically, $\mathcal{Y}$ admits an involution fixing the holomorphic (2,0)-form, with quotient $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$, and the rational degree-two map $p\colon \mathcal{Y} \longrightarrow \mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ determined a Hodge isometry between $T(\mathcal{Y})(2)$ and $T(\mathrm{Kum}(\mathrm{Jac}(\mathcal{X})))$; see [44].

Lemma 11. *In the situation above the Shioda-Inose structure induces an isomorphism between the transcendental lattices* $T(\mathrm{Jac}(\mathcal{X}))$ *and* $T(\mathcal{Y})$*, up to scaling.*

Proof. The transcendental lattice $T(\mathrm{Jac}(\mathcal{X}))$ is the orthogonal complement of the Néron-Severi group in the cohomology lattice $H^2(\mathrm{Jac}(\mathcal{X}), \mathbb{Z})$. The map $\pi\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ contracts the 2-torsion cycles, and the map $p\colon \mathcal{Y} \to \mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$ doubles the lattice, with the involution on $\mathcal{Y}$ preserving the (2,0)-form. The Hodge structure on $T(\mathcal{Y})$ aligns with $T(\mathrm{Jac}(\mathcal{X}))$, and the scaling by 2 in $T(\mathcal{Y})(2)$ matches the degree of the cover, ensuring an isometry of integral lattices. □

The Shioda-Inose surfaces can be constructed explicitly as minimal resolutions of some special projective quartic surfaces. Namely, consider the following family of quartics in $\mathbb{P}^3$:

$$y^2zw - 4x^3z + 3\alpha xzw^2 + \beta zw^3 + \gamma xz^2w - \frac{1}{2}(\delta z^2w^2 + w^4) = 0. \tag{85}$$

Then, under the condition $(\gamma, \delta) \neq (0, 0)$, the minimal resolution of the above quartic is a K3 surface $\mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$ of Shioda-Inose type. Moreover, the connection with the associated genus-two curve can be determined via the fact that the coefficients $(\alpha, \beta, \gamma, \delta)$ can be computed in terms of genus-two Siegel modular forms. Namely, one has (see [12]):

$$[\alpha : \beta : \gamma : \delta] \;=\; \left[\psi_4 :\; \psi_6 :\; 2^{12}3^5\chi_{10} :\; 2^{12}3^6\chi_{12}\right] \tag{86}$$

The right-hand term above involves the Igusa modular forms of Section 3.1 and the identity should be seen as an equality of points in the weighted-projective space $\mathbb{P}_{(2,3,5,6)}$. From here, one can compute directly the Igusa invariants of the associated genus-two curve as:

$$[J_2 : J_4 : J_6 : J_{10}] \;=\; \left[2^3 3\delta :\; 2^2 3^2 \alpha\gamma^2 :\; 2^3 3^2 (4\alpha\delta + \beta\gamma)\gamma^2 : 2^2\gamma^6\right]. \tag{87}$$

It is also important to note the connection between the quartic form (85) and the Hudson quartic (57) which describes $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$. The Kummer surface carries a special Jacobian elliptic fibration $\pi\colon \mathrm{Kum}(\mathrm{Jac}(\mathcal{X})) \to \mathbb{P}^1$ which, in the generic case, has a Mordell-Weil isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and a configuration of singular fibers consisting of a fiber of Kodaira type I_5^*, five fibers of type I_2 and one fiber of

type I_1. The generator of the Mordell-Weil group is associated with a section of order two. Deriving from the Hudson quartic description, the fibration π can also be described explicitly via an equation of type:

$$Y^2 = X\left(X^2 + \mathcal{P}(t)X + \mathcal{Q}(t)\right) \tag{88}$$

where $\mathcal{P}(t)$ and $\mathcal{Q}(t)$ are polynomials of degrees 4 and 6 with coefficients involving the Hudson quartic parameters $A.B, C, D$ (see [12] for the explicit formulas). The section of order two may be seen in this model as $X = 0$. Translations by this order-two section, within the smooth fibers, extend to a global Nikulin involution on $\mathrm{Kum}(\mathrm{Jac}(\mathcal{X}))$. After taking the quotient by this involution and resolving the eight occurring singularities, one obtains a new K3 surface - the Shioda-Inose surface $\mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$. The quotient map $r\colon \mathrm{Kum}(\mathrm{Jac}(\mathcal{X})) \dashrightarrow \mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$ may be seen in the context of (88) as:

$$(X, Y) \mapsto (x, y) = \left(\frac{\mathcal{Q}(t)}{X},\ -\frac{\mathcal{Q}(t)Y}{X^2}\right)\ , \tag{89}$$

with the two-isogenous elliptic fibration on $\mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$ being given by:

$$y^2 = X\left(x^2 + \tilde{\mathcal{P}}(t)x + \tilde{\mathcal{Q}}(t)\right)\ , \tag{90}$$

with $\tilde{\mathcal{P}}(t) = -2\mathcal{P}(t)$ and $\tilde{\mathcal{Q}}(t) = \mathcal{P}(t)^2 - 4\mathcal{Q}(t)$. This dual elliptic fibration (90), whose underlying surface is the Shioda-Inose surface $\mathrm{SI}(\mathrm{Jac}(\mathcal{X}))$, also has Mordell-Weil group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and carries a singular fiber of Kodaira type I_{10}^*. As it turns out, (90) matches the elliptic fibration obtained by projection to $[x\colon w]$ in the context of the Shioda-Inose quartic (85). This allows one to obtain explicit formulas relating the parameters $(\alpha, \beta, \gamma, \delta)$ to the Hudson coefficients $A.B, C, D$. We refer to [12] for the actual formulas.

5. (n, n)-Split Jacobians

We have seen above that sets of Abelian surfaces with the same endomorphism ring form sub-varieties within $\mathbb{A}_2$. In fact, we showed that the endomorphism ring of principally polarized Abelian surface tensored with $\mathbb{Q}$ is either a quartic CM field, an indefinite quaternion algebra, a real quadratic field or in the generic case $\mathbb{Q}$. Irreducible components of the corresponding subsets in $\mathbb{A}_2$ have dimensions $0, 1, 2$ and are known as *CM points*, *Shimura curves*, and *Humbert surfaces*, respectively. The latter can be related to a fascinating aspect of genus 2 Jacobians, namely their potential *decomposability*.

Let $\psi\colon \mathcal{X} \longrightarrow E_1$ be a maximal degree n covering to an elliptic curve E_1, meaning $\deg\psi = n$ and ψ does not factor through an isogeny of E_1. Then, there exists another elliptic curve $E_2 := \mathrm{Jac}(\mathcal{X})/E_1$, defined as the quotient by the connected component of $\ker(\psi_*)$, such that $\mathrm{Jac}(\mathcal{X})$ is isogenous to $E_1 \times E_2$ via an isogeny of degree n^2. We then call $\mathrm{Jac}(\mathcal{X})$ (n, n)**-decomposable** or (n, n)**-Split**, a property studied in [26]. The locus of such curves in $\mathcal{M}_2$ forms a 2-dimensional irreducible subvariety, with explicit computations for $n = 2, 3, 5$ given in [57], [59], and [42], respectively.

Consider an irreducible, smooth, projective curve $\mathcal{X}$ of genus 2 and a maximal covering $\psi_1\colon \mathcal{X} \longrightarrow E_1$ of degree n. The induced map $\psi_1^*\colon E_1 \longrightarrow \mathrm{Jac}(\mathcal{X})$ is injective, embedding E_1 as a subvariety, and $\psi_{1,*}\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow E_1$ has kernel $\ker(\psi_{1,*})$, an elliptic curve E_2 since $\dim \mathrm{Jac}(\mathcal{X}) = 2$ and $\dim E_1 = 1$ (see [58]). Fixing a Weierstrass point $P \in \mathcal{X}$, the embedding

$$\begin{aligned} i_P\colon \mathcal{X} &\longrightarrow \mathrm{Jac}(\mathcal{X}) \\ x &\mapsto\ [(x) - (P)] \end{aligned} \tag{91}$$

maps $\mathcal{X}$ into $\mathrm{Jac}(\mathcal{X})$. Let $g\colon E_2 \longrightarrow \mathrm{Jac}(\mathcal{X})$ be the natural inclusion, with dual $g^*\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow E_2$. Define $\psi_2 = g^* \circ i_P\colon \mathcal{X} \longrightarrow E_2$, a morphism to E_2. This yields exact sequences:

$$0 \longrightarrow E_2 \xrightarrow{g} \mathrm{Jac}(\mathcal{X}) \xrightarrow{\psi_{1,*}} E_1 \to 0, \tag{92}$$

and its dual

$$0 \longrightarrow E_1 \xrightarrow{\psi_1^*} \mathrm{Jac}(\mathcal{X}) \xrightarrow{g^*} E_2 \longrightarrow 0. \tag{93}$$

If $\deg(\psi_1) = 2$ or odd, $\psi_2\colon \mathcal{X} \longrightarrow E_2$ is unique up to elliptic curve isomorphism, as shown in [59]. The Hurwitz space $\mathbb{H}_\sigma$ of such covers embeds as a 2-dimensional subvariety $\mathcal{L}_n \subset \mathcal{M}_2$, with equations in terms of J_2, J_4, J_6, J_{10} given in [57] (for $n = 2$), [59] (for $n = 3$), and [42] (for $n = 5$). We say $\mathcal{X}$ has an (n, n)-decomposable Jacobian if $\mathrm{Jac}(\mathcal{X})$ admits such a structure, with E_1 and E_2 as its components.

5.1. **Humbert surfaces.** The Humbert surface H_Δ with invariant Δ is the space of principally polarized Abelian surfaces admitting a symmetric endomorphism with discriminant Δ. It turns out that Δ always is a positive integer satisfying $\Delta \equiv 0, 1 \mod 4$ and uniquely determined H_Δ. In fact, H_Δ is the image inside $\mathbb{A}_2$ under the projection of the rational divisor associated with the equation

$$a\,\tau_{11} + b\,\tau_{12} + c\,\tau_{22} + d\,(\tau_{12}^2 - \tau_{11}\,\tau_{22}) + e = 0\,, \tag{94}$$

with integers a, b, c, d, e satisfying $\Delta = b^2 - 4\,a\,c - 4\,d\,e$ and $\tau = \left(\begin{smallmatrix} \tau_{11} & \tau_{12} \\ \tau_{12} & \tau_{22} \end{smallmatrix}\right) \in \mathbb{H}_2$. The following was proven by Birkenhake and Lange in [5]:

Theorem 8. *For $n \in \mathbb{N}$ the Humbert surface H_{n^2} is the locus of principally polarized Abelian surfaces $(\mathcal{A}, \mathscr{L}) \in \mathbb{A}_2$ admitting an isogeny of degree n^2, given by*

$$\hat{\Psi}\colon \quad \big(E_1 \times E_2,\ \mathcal{O}_{E_1}(n) \boxtimes \mathcal{O}_{E_2}(n)\big) \ \longrightarrow\ \big(\mathcal{A}, \mathscr{L}\big)\,, \tag{95}$$

where $\mathcal{O}_{E_l}(n)$ is a line bundle of degree n on an elliptic curve $\mathcal{E}_l$ for $l = 1, 2$.

For example, inside of $\mathbb{A}_2$ sit the Humbert surfaces H_1 and H_4 that are defined as the images under the projection of the rational divisor associated to $\tau_{12} = 0$ and $\tau_{11} - \tau_{22} = 0$, respectively. In fact, the singular locus of $\mathbb{A}_2$ has H_1 and H_4 as its two connected components. As analytic spaces, H_1 and H_4 are each isomorphic to the Hilbert modular surface

$$\big((\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})) \rtimes \mathbb{Z}_2\big)\backslash\big(\mathbb{H} \times \mathbb{H}\big)\,. \tag{96}$$

In terms of Siegel modular forms in Section 3.1 we have the following characterization, see [28]:

Proposition 10. *The vanishing divisor of the cusp form χ_{10} in $\mathbb{A}_2$ is the Humbert surface H_1, i.e., a period point τ is equivalent to a point with $\tau_{12} = 0$ relative to Γ_2 if and only if $\chi_{10}(\tau) = 0$. The vanishing divisor of Q in $\mathbb{A}_2$ is the Humbert surface H_4, i.e., a period point τ is equivalent to a point with $\tau_{11} = \tau_{22}$ relative to Γ_2 if and only if $Q = 0$.*

It is known that one has $\chi_{10}(\tau) = 0$ if and only if the principally polarized Abelian surface $\mathcal{A}$ is a product of two elliptic curves $\mathcal{A} = E_{\tau_{11}} \times E_{\tau_{22}}$ with the transcendental lattice $\mathrm{T}_\mathcal{A} = H \oplus H$; see [43]. Here, H denotes the lattice $\mathbb{Z}^2$ with quadratic form $q(\vec{v}) = 2v_1v_2$. Moreover, for $Q(\tau) = 0$ the transcendental lattice of the corresponding Abelian surface $\mathcal{A}$ is given by $\mathrm{T}_\mathcal{A} = H \oplus \langle 2\rangle \oplus \langle -2\rangle$. Here, $\langle m\rangle$ denotes the rank-one lattice $\mathbb{Z}v$ with $q(v) = m$. Similarly, for $\tau \in H_{n^2}$, the transcendental lattice of $\mathcal{A}$ is given by $\mathrm{T}_\mathcal{A} = H \oplus \langle n\rangle \oplus \langle -n\rangle$.

Considering $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ as above, the isogeny in the above theorem is precisely $\hat{\Psi} = \psi_1^* \times \psi_2^*$. The Humbert hypersurface H_Δ then parameterizes curves $\mathcal{X}$ whose Jacobians admit an optimal action by the order $\mathcal{O}_\Delta$, a condition tied to embeddings of quadratic fields (see [29]). In particular, H_{n^2} correspond to curves with (n, n)-Split Jacobians, reflecting isogenies to products of elliptic curves. A point in $H_{m^2} \cap H_{n^2}$ $(m \neq n)$ indicates either a simple Abelian surface with quaternionic multiplication by an indefinite quaternion algebra over $\mathbb{Q}$, or a self-product E^2 where E is an elliptic curve, a phenomenon prominent on Shimura curves.

Proposition 11. $\mathrm{Jac}(\mathcal{X})$ *is a geometrically simple Abelian variety if and only if it is not (n, n)-decomposable for some $n > 1$. Equivalently, if $\mathrm{Jac}(\mathcal{X})$ is split over k, then there exists an integer $n \geq 2$ such that $\mathrm{Jac}(\mathcal{X})$ is (n, n)-Split.*

Proof. Suppose $\mathrm{Jac}(\mathcal{X})$ is geometrically simple, i.e., simple over $\bar{k}$. By the Poincaré-Weil theorem, $\mathrm{Jac}(\mathcal{X})$ is isogenous to $\mathcal{A}_1^{n_1} \times \cdots \times \mathcal{A}_r^{n_r}$, and simplicity over $\bar{k}$ implies $r = 1$, $n_1 = 1$, with $\mathcal{A}_1 = \mathrm{Jac}(\mathcal{X})$. If $\mathrm{Jac}(\mathcal{X})$ were (n, n)-decomposable, there would exist a maximal degree n covering $\psi\colon \mathcal{X} \longrightarrow E_1$, inducing an isogeny $\mathrm{Jac}(\mathcal{X}) \longrightarrow E_1 \times E_2$ of degree n^2, where E_1, E_2 are elliptic curves. Over $\bar{k}$, this isogeny splits $\mathrm{Jac}(\mathcal{X})$ into a product of 1-dimensional varieties, contradicting simplicity unless $n = 1$, which is trivial (as $\deg \psi = 1$ implies $\mathcal{X} \cong E_1$, contradicting $g = 2$). Thus, $\mathrm{Jac}(\mathcal{X})$ is not (n, n)-decomposable for any $n > 1$.

Conversely, if $\mathrm{Jac}(\mathcal{X})$ is not (n, n)-decomposable for any $n > 1$, suppose it is not geometrically simple. Then over $\bar{k}$, $\mathrm{Jac}(\mathcal{X}) \cong E_1 \times E_2$, with $\dim E_i = 1$. By the theory of maximal coverings ([26]), there exists a degree $n > 1$ map $\psi : \mathcal{X} \to E_1$ (e.g., projection via a correspondence), making $\mathrm{Jac}(\mathcal{X})$ isogenous to $E_1 \times E_2$, hence (n, n)-Split, a contradiction. Thus, $\mathrm{Jac}(\mathcal{X})$ must be simple over $\bar{k}$.

For the equivalent statement, if $\mathrm{Jac}(\mathcal{X})$ is split over k (isogenous to $E_1 \times E_2$ over k), there exists a maximal covering $\psi\colon \mathcal{X} \longrightarrow E_1$ of degree $n \geq 2$, as genus 2 curves admit non-trivial maps to elliptic curves, inducing the (n, n)-Split structure (see [58], §3). □

This characterization connects the geometric simplicity of $\mathrm{Jac}(\mathcal{X})$ to its indecomposability, a key property for later isogeny studies. In terms of the Kummer plane introduced in Section 4.2 we have the following:

Remark 6. *In* [5] *the geometry of the Kummer plane was determined over several Humbert surfaces* H_Δ. *In particular, the following statement were proven* [5, Cor. 7.2] *and* [5, Cor. 7.3]*:*

$\Delta = 4$: *if* $(\mathcal{A},\mathscr{L}) \in H_4$ *if and only if (numbering the six lines on its Kummer plane* $(\mathbb{P}^2;\mathsf{T}_1,\dots,\mathsf{T}_6)$ *suitably) the three points* $\mathsf{T}_1\cap\mathsf{T}_2$, $\mathsf{T}_3\cap\mathsf{T}_4$, $\mathsf{T}_5\cap\mathsf{T}_6$ *are collinear.*

$\Delta = 16$: *if* $(\mathcal{A},\mathscr{L}) \in H_{16}$ *then its Kummer plane* $(\mathbb{P}^2;\mathsf{T}_1,\dots,\mathsf{T}_6)$ *admits a cubic passing smoothly through three of the 15 points* $\mathsf{T}_m\cap\mathsf{T}_n$ *and touching the singular lines* T_n *in the remaining intersection points with even multiplicity. Conversely, if* $(\mathbb{P}^2;\mathsf{T}_1,\dots,\mathsf{T}_6)$ *admits such a curve, then* $(\mathcal{A},\mathscr{L}) \in H_\Delta$ *with* $\Delta \in \{4,8,12,16,20\}$.

For the transcendental lattice it follows $\mathrm{T}_{\mathrm{Kum}(\mathcal{A})} \cong \mathrm{T}_{\mathcal{A}}(2)$ [47, Thm. 10]. *In particular we have*

$$\mathrm{T}_{\mathrm{Kum}(\mathcal{A})} = H(2)\oplus\langle 4\rangle\oplus\langle -4\rangle \text{ for } (\mathcal{A},\mathscr{L}) \in H_4\,. \tag{97}$$

Generally, for $\mathcal{A} \in H_{n^2}$ *it follows from* [47] *that* $\mathrm{Kum}(\mathcal{A})$ *has Picard rank 18, and the transcendental lattice is given by*

$$\mathrm{T}_{\mathrm{Kum}(\mathcal{A})} \cong \mathrm{T}_{\mathcal{A}}(2) = H(2)\oplus\langle 2n\rangle\oplus\langle -2n\rangle\,. \tag{98}$$

5.2. **The case of $(2,2)$-Split Jacobians.** The case of a smooth genus 2 curve $\mathcal{X}$ with a $(2,2)$-Split Jacobian was described by Bolza [6] explicitly. In particular, he proved that the Jacobian $\mathrm{Jac}(\mathcal{X})$ for a smooth genus-two curve $\mathcal{X}$ is $(2,2)$-Split if and only if $Q(\tau)=0$; see Proposition 10. Next we will provide several explicit models for the algebraic curves involved in this case.

5.2.1. *Bolza's representation.* Bolza also proved that one can always represent this extra involution as $[X:Y:Z]\mapsto[-X:Y:Z]$ if the genus 2 curve is given in the from

$$\mathcal{X}\colon\quad Y^2 = X^6 + s_1X^4Z^2 + s_2X^2Z^4 + Z^6\,. \tag{99}$$

One uses Equations (15) and Equation (14) to check that $Q = 2^{12}\,3^9\,\chi_{35}^2/\chi_{10}$ always vanishes for such a genus-two curve.

Given the elliptic involution, its composition with the hyperelliptic involution defines a second elliptic involution. The two involutions define two elliptic subfields of degree two for the function field of $\mathcal{X}$. We introduce the elliptic curves E_l in $\mathbb{P}^2=\mathbb{P}(x_l,y_l,z_l)$ for $l=1,2$, given by

$$E_1\colon\ y_1^2z_1 = x_1^3 + s_2x_1^2z_1 + s_1x_1z_1^2 + z_1^3\,,\quad E_2\colon\ y_2^2z_2 = x_2^3 + s_1x_2^2z_2 + s_2x_2z_2^2 + z_2^3\,, \tag{100}$$

where E_1 and E_2 have the j-invariants $j_1=j(E_1)$ and $j_2=j(E_2)$ with

$$j_1 = \frac{2^8\left(3s_1-s_2^2\right)^3}{4(s_1^3+s_2^3)-(s_1s_2)^2-18s_1s_2+27}\,,\quad j_2 = \frac{2^8\left(3s_2-s_1^2\right)^3}{4(s_1^3+s_2^3)-(s_1s_2)^2-18s_1s_2+27}\,, \tag{101}$$

respectively. Here, we use the standard normalization of the j-invariant where the square torus with the complex structure i satisfies $j=1728=12^3$. The degree-two quotient maps $\psi_l\colon\mathcal{X}\longrightarrow E_l$ associated with the involutions are given by

$$\psi_1\colon\quad \mathcal{X}\ \longrightarrow\ E_1\,,\qquad \big[X:Y:Z\big]\ \mapsto\ \big[x_1:y_1:z_1\big] = \big[XZ^2:Y:X^3\big]\,, \tag{102}$$

and

$$\psi_2\colon\quad \mathcal{X}\ \longrightarrow\ E_2\,,\qquad \big[X:Y:Z\big]\ \mapsto\ \big[x_2:y_2:z_2\big] = \big[X^2Z:Y:Z^3\big]\,, \tag{103}$$

respectively, for $XZ\neq 0$.

5.2.2. *Pringsheim's representation.* One can also start with a smooth genus-two curve $\mathcal{X}$ in Rosenhain form given by Equation (17). We use the aforementioned relations between the Igusa invariants and the Siegel modular forms to expand the generators of the ring of modular forms in terms of the Rosenhain roots. We obtain

$$
\begin{aligned}
-\frac{2^{22}\chi_{35}^2(\tau)}{\chi_{10}^4(\tau)} &= (\lambda_1-\lambda_2\lambda_3)^2(\lambda_2-\lambda_1\lambda_3)^2(\lambda_3-\lambda_1\lambda_2)^2 \\
\times\ & (\lambda_1-\lambda_2-\lambda_3+\lambda_2\lambda_3)^2(-\lambda_1+\lambda_2-\lambda_3+\lambda_1\lambda_3)^2(-\lambda_1-\lambda_2+\lambda_3+\lambda_1\lambda_2)^2 \\
\times\ & (\lambda_1\lambda_2+\lambda_1\lambda_3-\lambda_2\lambda_3-\lambda_1)^2(\lambda_1\lambda_2+\lambda_2\lambda_3-\lambda_1\lambda_3-\lambda_2)^2(\lambda_1\lambda_3+\lambda_2\lambda_3-\lambda_1\lambda_2-\lambda_3)^2 \\
\times\ & \left\{ \begin{array}{l} (\lambda_1\lambda_2-\lambda_1\lambda_3-\lambda_1+\lambda_3)^2(\lambda_1\lambda_3-\lambda_2\lambda_3-\lambda_1+\lambda_3)^2(\lambda_1\lambda_2-\lambda_2\lambda_3-\lambda_1+\lambda_2)^2 \\ (\lambda_1\lambda_2-\lambda_1\lambda_3+\lambda_1-\lambda_2)^2(\lambda_1\lambda_3-\lambda_2\lambda_3+\lambda_2-\lambda_3)^2(\lambda_1\lambda_2-\lambda_2\lambda_3-\lambda_2+\lambda_3)^2\,. \end{array} \right.
\end{aligned}
\tag{104}
$$

The vanishing divisor of Equation (104) defines fifteen components in $\mathbb{H}_2/\Gamma_2(2)$ of discriminant $\Delta = 4$. Notice that each line in Equation (104) is arranged to be invariant under permutations of the three roots $\lambda_1, \lambda_2, \lambda_3$. Pringsheim proved the following statement[3] in [53]:

Proposition 12 (Pringsheim)**.** *There are exactly 15 components in $\mathbb{H}_2/\Gamma_2(2)$ covering H_4. Each of the component is equivalent to $\tau_{11} = \tau_{22}$ relative to the modular group Γ_2. Moreover, there is a transposition of the six roots $(\lambda_1, \lambda_2, \lambda_3, 0, 1, \infty)$ in $\Gamma_2/\Gamma_2(2) \cong S_6$ that permutes each pair of components.*

We will use component $\lambda_1 = \lambda_2\lambda_3$ in Proposition 12 to construct a smooth genus-two curve in Rosenhain normal form admitting an elliptic involution. That is, we consider the smooth genus-two curve $\mathcal{X}$, given by

$$
\mathcal{X}\colon \quad Y^2 = XZ\,(X-Z)\,(X-\lambda_2\lambda_3 Z)\,(X-\lambda_2 Z)\,(X-\lambda_3 Z)\,,
\tag{105}
$$

with a discriminant given by

$$
\lambda_2^6\lambda_3^6(\lambda_2-1)^4(\lambda_3-1)^4(\lambda_2\lambda_3-1)^4(\lambda_2-\lambda_3)^2\,.
\tag{106}
$$

Let us denote by $\Lambda_l \in \mathbb{P}^1\backslash\{0,1,\infty\}$ the modular parameter for the elliptic curves E_l in $\mathbb{P}^2 = \mathbb{P}(x_l, y_l, z_l)$ for $l = 1, 2$ defined by the *Legendre normal form*

$$
E_l\colon \quad y_l^2 z_l = x_l\big(x_l - z_l\big)\big(x_l - \Lambda_l z_l\big)\,,
\tag{107}
$$

with the hyperelliptic involution given by $\imath_l : [x_l : y_l : z_l] \mapsto [x_l : -y_l : z_l]$. One easily checks the following:

Lemma 12. *The function field of the smooth genus-two curve $\mathcal{X}$ contains the subfields given by the function fields of the elliptic curves $\mathcal{E}_l$ for $l = 1, 2$ if*

$$
\Lambda_1\Lambda_2 = \frac{(\lambda_2+\lambda_3)^2 - 4\lambda_2\lambda_3}{(1-\lambda_2)^2(1-\lambda_3)^2}\,, \qquad \Lambda_1+\Lambda_2 = -\frac{2(\lambda_2+\lambda_3)}{(1-\lambda_2)(1-\lambda_3)}\,.
\tag{108}
$$

We then have the following:

Proposition 13. *Assume that $\lambda_2, \lambda_3 \in \mathbb{P}^1\backslash\{0,1,\infty\}$ satisfy $\lambda_2 \neq \lambda_3^{\pm 1}$, and the moduli of the curves $\mathcal{X}$ and E_l in Equations (105) and (107) satisfy Equations (108). Quotient maps $\psi_l\colon \mathcal{X} \longrightarrow E_l$ for $l = 1, 2$ are given by*

$$
\psi_l\colon \quad \mathcal{X} \ \longrightarrow\ E_l\,, \qquad \big[X : Y : Z\big] \mapsto \big[x_l : y_l : z_l\big] \ \text{ for } l = 1, 2,
\tag{109}
$$

with

$$
\big[x_l : y_l : z_l\big] \ = \ \big[r(X-\lambda_2 Z)(X-\lambda_3 Z)\,XZ :\ (X-(-1)^l q Z)\,Y :\ r^3X^2Z^2\big]\,,
\tag{110}
$$

for $XZ \neq 0$, and $[x_l : y_l : z_l] = [1 : 0 : 0]$ otherwise. Here, q, r are square roots of $q^2 = \lambda_2\lambda_3$ and $r^2 = (1-\lambda_2)(1-\lambda_3)$, respectively. The elliptic involutions $\jmath_l$ on $\mathcal{X}$, given by

$$
\jmath_l\colon \quad \big[X : Y : Z\big] \mapsto \big[\lambda_2\lambda_3 Z :\ (-1)^{l+1}\lambda_2\lambda_3 q Y :\ X\big]\,,
\tag{111}
$$

satisfy $\psi_l \circ \jmath_l = \psi_l$ for $l = 1, 2$.

[3] We corrected two minor typos in the statement of the main theorem.

Proof. The genus-two curve $\mathcal{X}$ in Equation (105) is assumed to be smooth. Thus, one must have $\lambda_2, \lambda_3 \in \mathbb{P}^1\backslash\{0,1,\infty\}$ and $\lambda_2 \neq \lambda_3^{\pm 1}$. The remainder of the proof follows by explicit computation. We note that a choice of square root for r is changed by composing ψ_l with the elliptic involution on E_l. The choice of square root for q is changed by interchanging $\psi_1 \leftrightarrow \psi_2$. □

Remark 7. *Using a covering space of $c\lambda_1 = \lambda_2\lambda_3$ in Proposition 12, given by the set of tuples (k_1, k_2) with $\lambda_l = k_l^2$ for $l = 2, 3$ and $\lambda_1 = (k_2 k_3)^2$, we obtain for the modular parameters of the elliptic-curve quotients E_l in Lemma 12 the following algebraic solutions of Equation (108):*

$$\Lambda_1 = -\frac{(k_2 - k_3)^2}{(1-k_2^2)(1-k_3^2)}\,, \qquad \Lambda_2 = -\frac{(k_2 + k_3)^2}{(1-k_2^2)(1-k_3^2)}\,. \tag{112}$$

A change of square roots $(k_2, k_3) \mapsto (\pm k_2, \pm k_3)$ leaves Equations (112) invariant, whereas the change $(k_2, k_3) \mapsto (\pm k_2, \mp k_3)$ interchanges Λ_1 and Λ_2. This means that the elliptic curves E_l with level-two structure can be constructed over $\mathbb{Q}(k_2, k_3)$ as a finite field extension of $\mathbb{Q}(\Lambda_1, \Lambda_2)$.

5.2.3. *Legendre's gluing construction.* The Weierstrass points P_i of the curve $\mathcal{X}$ in Equation (105), given by

$$\begin{aligned} P_1 &: [\lambda_2\lambda_3 : 0 : 1]\,, \quad P_2 : [\lambda_2 : 0 : 1]\,, \quad P_3 : [\lambda_3 : 0 : 1]\,, \\ P_4 &: [0 : 0 : 1]\,, \quad P_5 : [1 : 0 : 1]\,, \quad P_6 : [1 : 0 : 0]\,, \end{aligned} \tag{113}$$

are the fixed points of the hyperelliptic involution. The two elliptic involutions $\jmath_l$ in Equation (111) for $l = 1, 2$ (each) pairwise interchange the Weierstrass points, i.e.,

$$\jmath_l\colon \quad P_2 \leftrightarrow P_3\,, \quad P_1 \leftrightarrow P_5\,, \quad P_4 \leftrightarrow P_6\,. \tag{114}$$

The points $Q_{l,\pm}$, given by

$$\begin{aligned} Q_{1,\pm}\colon &\quad [-q : \pm i q^{\frac{3}{2}}(k_2k_3 + 1)(k_2 + k_3) : 1]\,, \\ Q_{2,\pm}\colon &\quad [\ \ q : \pm\, q^{\frac{3}{2}}(k_2k_3 - 1)(k_2 - k_3) : 1]\,, \end{aligned} \tag{115}$$

are the ramification points of ψ_l in Equation (109) for $l = 1$ and $l = 2$, respectively. The involution $\jmath_1$ fixes the points $Q_{1,+}$ and $Q_{1,-}$, and interchanges the points $Q_{2,+} \leftrightarrow Q_{2,-}$. An analogous statements holds for the involution $\jmath_2$. The hyperelliptic involution of the curve $\mathcal{X}$ interchanges the elements of the two pairs simultaneously, i.e., $Q_{l,+} \leftrightarrow Q_{l,-}$ for $l = 1, 2$.

The pairs $\{P_2, P_3\}$, $\{P_1, P_5\}$, $\{Q_{2,+}, Q_{2,-}\}$, and $\{P_5, P_6\}$ are mapped by ψ_1 to the two-torsion points $p_0 : [x_1 : y_1 : z_1] = [0 : 0 : 1]$, $p_1 : [1 : 0 : 1]$, $p_{\Lambda_1} : [\Lambda_1 : 0 : 1]$, and the identity $p_\infty : [1 : 0 : 0]$ in E_1. Similarly, the pairs $\{P_2, P_3\}$, $\{P_1, P_5\}$, $\{Q_{1,+}, Q_{1,-}\}$, and $\{P_5, P_6\}$ are mapped by ψ_2 to the two-torsion points $p_0 : [x_2 : y_2 : z_2] = [0 : 0 : 1]$, $p_1 : [1 : 0 : 1]$, $p_{\Lambda_2} : [\Lambda_2 : 0 : 1]$, and the identity $p_\infty : [1 : 0 : 0]$ in E_2.

We associate with the branch locus of ψ_1 and ψ_2 the effective divisor of degree two $B_1 = [\psi_1(Q_{1,+}) + \psi_1(Q_{1,-})]$ on E_1 and $B_2 = [\psi_2(Q_{2,+}) + \psi_2(Q_{2,-})]$ on E_2, respectively. One checks that for $\psi_1(Q_{1,\pm})$ one has $[x_1 : z_1] = [\Lambda_2 : 1]$, and for $\psi_2(Q_{2,\pm})$ one has $[x_2 : z_2] = [\Lambda_1 : 1]$. Because of $\mathrm{Pic}^0(E_l) \cong E_l$ the line bundle $\mathcal{O}_{E_l}(B_l)$ associated with the branch locus B_l is equivalent to the line bundle $\mathcal{O}_{E_l}(2p_\alpha)$ if and only if

$$\psi_l(Q_{l,+}) \oplus \psi_l(Q_{l,-}) = 2p_\alpha = p_\alpha \oplus p_\alpha\,, \tag{116}$$

where $\oplus$ refers to the addition with respect to the elliptic curve group law on E_l. Using the properties for ψ_l in Equation (109) one finds that

$$\psi_l(Q_{l,+}) \oplus \psi_l(Q_{l,-}) = 0\,, \tag{117}$$

and $p_\alpha \in E_l[2]$ is a two-torsion point. Thus, there are four line bundle $\mathcal{L}_l \to E_l$ such that $\mathcal{L}_l^{\otimes 2} \cong \mathcal{O}_{E_l}(B_l)$, namely $\mathcal{L}_l \cong \mathcal{O}_{E_l}(p_\alpha)$. It follows $h^0(\mathcal{E}_l, \mathcal{L}_l) = 1$ by the Riemann-Roch theorem. Conversely, the preimage of the vanishing locus of a section of $\mathcal{L}_l \to \mathcal{E}_l$ determines a unique double cover $\psi_l\colon \mathcal{X} \longrightarrow E_l$. The composition on $\mathcal{X}$ of the elliptic involution with the hyperelliptic involution defines a second elliptic involution, and a second elliptic-curve quotient is obtained. Thus, the data $(E_l, \mathcal{L}_l, B_l)$ for either $l = 1$ or $l = 2$ determines the curve $\mathcal{X}$ uniquely. As we have seen, this data is equivalent to an (unordered) pair $\{\Lambda_1, \Lambda_2\}$ of modular parameters $\Lambda_1, \Lambda_2 \in \mathbb{P}^1\backslash\{0,1,\infty\}$ with $\Lambda_1 \neq \Lambda_2$. Legendre constructed an explicit model for $\mathcal{X}$ over $\mathbb{Q}(\Lambda_1, \Lambda_2)$; this is often referred to as *Legendre's gluing method*. Following Serre's explanation [55, Sec. 27] of Legendre's gluing method we obtain:

Proposition 14. *Assume that $\Lambda_1, \Lambda_2 \in \mathbb{P}^1\backslash\{0,1,\infty\}$ satisfy $\Lambda_1 \neq \Lambda_2$, and the moduli of $\mathcal{X}$ and E_l in Equations (105) and (107) satisfy Equations (108). The smooth genus-two curve, given by*

$$\widetilde{\mathcal{X}}\colon \quad Y^2 = \left(X^2 - Z^2\right)\left(X^2 - \frac{\Lambda_1}{\Lambda_2}Z^2\right)\left(X^2 - \frac{1-\Lambda_1}{1-\Lambda_2}Z^2\right), \tag{118}$$

is isomorphic to $\mathcal{X}$ over a finite field extension of $\mathbb{Q}(\lambda_2, \lambda_3)$. The curve is also isomorphic to each of the curves obtained by replacing $\{\Lambda_1, \Lambda_2\}$ in Equation (118) by one of the following pairs:

$$\left\{\frac{1}{1-\Lambda_1}, \frac{1}{1-\Lambda_2}\right\}, \left\{\frac{\Lambda_1-1}{\Lambda_1}, \frac{\Lambda_2-1}{\Lambda_2}\right\}, \left\{\frac{1}{\Lambda_1}, \frac{1}{\Lambda_2}\right\}, \left\{\frac{\Lambda_1}{\Lambda_1-1}, \frac{\Lambda_2}{\Lambda_2-1}\right\}, \left\{1-\Lambda_1, 1-\Lambda_2\right\}. \tag{119}$$

Proof. Using Remark 7 and denoting the Igusa-Clebsch invariants of any pairs genus-two curves in the statement of the proposition by $[J_2 : J_4 : J_6 : J_{10}]$ and $[J_2' : J_4' : J_6' : J_{10}']$, respectively, one checks that

$$[J_2 : J_4 : J_6 : J_{10}] = [s^2 J_2' \ : \ s^4 J_4' \ : \ s^6 J_6' \ : \ s^{10} J_{10}'] = [J_2' : J_4' : J_6' : J_{10}'] \tag{120}$$

with $s \in \mathbb{Q}(\lambda_2, \lambda_3, \sqrt{\lambda_2\lambda_3})$. □

The six pairs, given by $\{\Lambda_1, \Lambda_2\}$ and Equation (119), correspond to the orbit of the data $(E_l, \mathcal{L}_l, B_l)$ under $\Gamma/\Gamma(2)$, i.e., the orbit under simultaneous action of the *anharmonic group* on an elliptic curve in Legendre form. The anharmonic group is generated by the two transformations $\Lambda \mapsto 1-\Lambda, \Lambda/(\Lambda-1)$.

Since the Picard group $\mathrm{Pic}^0(\mathcal{X}) \cong \mathrm{Jac}\,(\mathcal{X})$ consists of elements of the from $[P+Q-2P_0]$ for $P, Q \in \mathcal{X}$, an isogeny Ψ of Abelian surfaces is defined by setting

$$\Psi\colon \ \mathrm{Jac}\,\mathcal{X} \longrightarrow E_1 \times E_2\,, \quad [P+Q-2P_6] \mapsto \big(\psi_1(P) \oplus \psi_1(Q),\ \psi_1(P) \oplus \psi_2(Q)\big)\,. \tag{121}$$

It follows from the construction of the line bundles $\mathcal{L}_l \to E_l$ in Section 5.2.3 that the line bundle $\mathscr{L} \to \mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ associated with the principal polarization of $\mathcal{A}$ satisfies $\mathscr{L} \cong \Psi^*(\mathcal{L}_1 \boxtimes \mathcal{L}_2)$. Ψ is the dual isogeny to $\hat{\Psi}$ in Theorem 8. The elliptic involutions $\jmath_l$ on $\mathcal{X}$ extend to involutions on the Jacobian $\mathcal{A} = \mathrm{Jac}\,(\mathcal{X})$ that coincide on $\mathcal{A}[2]$. We denote this induced involution on $\mathcal{A}[2]$ by $\jmath\colon \mathcal{A}[2] \longrightarrow \mathcal{A}[2]$.

Given the marking $(P_1, \ldots, P_6) = (\lambda_1 = \lambda_2\lambda_3, \lambda_2, \lambda_3, 0, 1, \infty)$ of the Weierstrass points for the curve $\mathcal{X}$ as before, we have the following:

Proposition 15. *In the situation above, the kernel of $\Psi\colon \mathcal{A} = \mathrm{Jac}\,(\mathcal{X}) \longrightarrow E_1 \times E_2$ is given by the Göpel group*

$$\ker\Psi \ = \ \big\{P_0, P_{15}, P_{23}, P_{46}\big\} \ \cong \ (\mathbb{Z}/2\mathbb{Z})^2 \ \subset \ \mathcal{A}[2]\,. \tag{122}$$

In particular, Ψ is a $(2,2)$-isogeny and $\hat{\mathcal{A}} = \mathcal{A}/\ker\Psi \cong E_1 \times E_2$ with $\mathrm{T}_{\hat{\mathcal{A}}} = H \oplus H$.

Proof. The induced actions of the two elliptic involutions $\jmath_l$ on $\mathrm{Jac}\,(\mathcal{X})$ fix the divisors P_{15}, P_{23}, P_{46}, and $[Q_{l,+} + Q_{l,-} - 2P_0]$. It follows from the explicit formulas for ψ_l in Proposition that $(P, Q) \in \ker\Psi$ if and only if $P, Q \in \mathcal{A}[2]$ and $\jmath_l(P) = Q$ for $l = 1, 2$. □

5.3. **Loci of (n,n)-Split Jacobians.** The locus $\mathcal{L}_n \subset \mathcal{M}_2$ of genus 2 curves over $\overline{\mathbb{Q}}$ whose Jacobians are (n,n)-Split, i.e., isogenous to a product $E_1 \times E_2$ via an (n,n)-isogeny with kernel an isotropic subgroup of order n^2, is an irreducible two-dimensional subvariety. We have computed $\mathcal{L}_n$ for $n = 2, 3, 5, 7, 11$, providing explicit equations in terms of Igusa invariants J_2, J_4, J_6, J_{10} (see [57], [59], [42] for $n = 2, 3, 5$). For $n = 2$, $\mathcal{L}_2$ was determined explicitly in Section 5.2; for odd n, $\mathcal{L}_n$ is a Hurwitz space of degree-n coverings, irreducible due to automorphism group transitivity, with dimension 2 from $\mathcal{M}_2$'s 3 minus the isotropy codimension.

In cryptography, identifying $\mathcal{L}_n$ is critical. Over finite fields (e.g., $\mathbb{F}_{p^2}$), a split $\mathrm{Jac}(\mathcal{X}) \in \mathcal{L}_n$ reduces the superspecial isogeny problem's complexity from $\tilde{O}(p)$ to elliptic curve subproblems ($\tilde{O}(\sqrt{p})$), as exploited by Costello et al. [15]. Their algorithm detects (n,n)-splittings using Kumar's parameterizations [37]—matching our $\mathcal{L}_n$—speeding up attacks by factors of 16–159 for p from 50 to 1000 bits. This weakens protocols like the Castryck-Decru-Smith hash [11], where split Jacobians enable faster collision finding, suggesting key selection avoid $\mathcal{L}_n$ to bolster security.

6. Computing higher (n,n)-Isogenies

The Richelot isogenies treated in Section 3.4 represent the simplest instance of a broader class of isogenies between Abelian surfaces, specifically (2,2)-isogenies with kernels of order 4. Here, we generalize to (n,n)-isogenies with $n \in \mathbb{N}_{>2}$, where the kernel has order n^2, focusing on computational methods for Jacobians of genus 2 curves, leveraging their Kummer surfaces.

To start, we consider an isogeny

$$\Phi\colon \quad \mathrm{Jac}(\mathcal{X}) \to \mathrm{Jac}(\mathcal{Y}), \tag{123}$$

with kernel $G \leq \mathrm{Jac}(\mathcal{X})[n]$ of order n^2, where $\mathcal{X}$ and $\mathcal{Y}$ are smooth genus 2 curves over a field k with char $k \neq 2$, and $\mathrm{Jac}(\mathcal{X})$ and $\mathrm{Jac}(\mathcal{Y})$ are their Jacobian varieties, each a principally polarized Abelian surface. Over $\mathbb{C}$, represent $\mathrm{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$ with $\Lambda = \mathbb{Z}^2 \oplus \tau\mathbb{Z}^2$, where $\tau \in \mathbb{H}_2$ is the period matrix. The n-torsion subgroup $\mathrm{Jac}(\mathcal{X})[n] = \{P \in \mathrm{Jac}(\mathcal{X}) \mid [n]P = 0\}$ has order $n^{2g} = n^4$ for $g = 2$, and an isotropic subgroup $G \subset \mathrm{Jac}(\mathcal{X})[n]$ under the Weil pairing has order n^2. Let $\Theta_{\mathcal{X}}$ and $\Theta_{\mathcal{Y}}$ denote the Theta divisors on $\mathrm{Jac}(\mathcal{X})$ and $\mathrm{Jac}(\mathcal{Y})$, respectively, where $\Theta_{\mathcal{X}}$ is the image of $\mathcal{X}$ under an embedding such as $\phi_{P_0}\colon \mathcal{X} \to \mathrm{Jac}(\mathcal{X})$, $P \mapsto [P - P_0]$, for a base point $P_0 \in \mathcal{X}(k)$. An (n,n)-isogeny requires determining both the codomain $\mathrm{Jac}(\mathcal{Y})$ and the map Φ.

One easily checks that the isogeny Φ satisfies $\Phi(\Theta_{\mathcal{X}}) \in |n\Theta_{\mathcal{Y}}|$, the linear system of divisors linearly equivalent to n times $\Theta_{\mathcal{Y}}$. On the other hand, the singular Kummer surface $\mathcal{K}_{\mathrm{Jac}(\mathcal{Y})} = \mathrm{Jac}(\mathcal{Y})/\langle -\mathbb{I}\rangle$ embeds in $\mathbb{P}^3$ via level-two Theta functions, and on it $\Phi(\Theta_{\mathcal{X}})$ descends to a curve of degree $2n$, genus 0, and arithmetic genus $\frac{1}{2}(n^2-1)$, computable without explicitly determining Φ, as shown in [22]. It is precisely this curve that can provide a deeper inside into the (n,n)-isogeny itself.

6.1. The n-tuple embedding of Dolgachev-Lehavi.

For $\mathcal{X}$, given as the binary sextic

$$y^2 = f(x,z) = a_6x^6 + \cdots + a_1xz^5 + a_0z^6, \tag{124}$$

with $\Delta_f = J_{10} \neq 0$, the divisor at infinity is

$$D_\infty := [1 : \sqrt{f(1,0)} : 0] + [1 : -\sqrt{f(1,0)} : 0], \tag{125}$$

assuming a normalization where infinity points are $[1 : y : 0]$. The Weierstrass points of $\mathcal{X}$ are denoted $P_i\colon [x_i : 0 : z_i]$ for $i = 1, \ldots, 6$, with $f(x_i, z_i) = 0$, forming the Weierstrass divisor

$$W_{\mathcal{X}} := \sum_{i=1}^{6} [x_i : 0 : z_i]\,. \tag{126}$$

A canonical divisor on $\mathcal{X}$ is

$$K_{\mathcal{X}} = W_{\mathcal{X}} - 2D_\infty, \tag{127}$$

as $\deg W_{\mathcal{X}} = 6$, $\deg D_\infty = 2$, and $2g - 2 = 2$. A divisor $D \in \mathrm{Jac}(\mathcal{X})$ of the form $D = [P + Q - D_\infty]$, with $P\colon [x_P : y_P : 1]$ and $Q\colon [x_Q : y_Q : 1]$, corresponds to an ideal $(a(x,z), y - b(x,z))$, where $a(x,z) = (x - x_Pz)(x - x_Qz)$ is a monic polynomial of degree $d \leq 2$ –quadratic if $P \neq Q$, linear if $P = Q$– and $b(x,z)$ is a cubic polynomial interpolating y_P, y_Q.

We embed $\mathcal{X}$ via the n-tuple map

$$\rho_{2n}\colon \quad \mathbb{P}^2_{(1,2,1)} \to \mathbb{P}^{2n}, \quad [x : y : z] \mapsto [z^{2n} : xz^{2n-1} : \cdots : x^{2n-1}z : x^{2n}], \tag{128}$$

with image $\mathcal{R}_{2n}$, a rational normal curve of degree $2n$. Any $2n+1$ distinct points on $\mathcal{R}_{2n}$ are linearly independent, as the space of degree $2n$ homogeneous polynomials has dimension $2n+1$. For $n \geq 3$, the 6 points $\rho_{2n}(P_i)$ are independent ($6 < 7$ for $n = 3$), and

$$W := \langle \rho_{2n}(W_{\mathcal{X}}) \rangle \subset \mathbb{P}^{2n} \tag{129}$$

is 5-dimensional. The secant line $\mathcal{L}_{P,Q}$ is

$$\mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2n}(P), \rho_{2n}(Q) \rangle & \text{if } P \notin \{Q, \imath(Q)\}, \\ T_{\rho_{2n}(P)}(\mathcal{R}_{2n}) & \text{otherwise,} \end{cases} \tag{130}$$

where $\imath$ is the hyperelliptic involution on $\mathcal{X}$. Dolgachev and Lehavi ([22]) proved:

Theorem 9 (Dolgachev-Lehavi)**.** *Let $\mathcal{X}$ be a genus 2 curve, $G \subset \mathrm{Jac}(\mathcal{X})[n]$ an isotropic subgroup of order n^2, and $\rho_{2n}\colon \mathcal{X} \longrightarrow \mathcal{R}_{2n} \subset \mathbb{P}^{2n}$ the n-tuple embedding. There exists a hyperplane $H \subset \mathbb{P}^{2n}$ such that:*

(i) H contains $W = \langle \rho_{2n}(W_{\mathcal{X}}) \rangle$,

(ii) the intersections $H \cap \mathcal{L}_e$ for each non-zero $e \in G$ span a subspace $N \subset H$ of codimension 3.

The projection $\mathbb{P}^{2n} \to \mathbb{P}^3$ from N maps $\rho_{2n}(W_{\mathcal{X}})$ to a conic $\mathcal{C} \subset \mathbb{P}^3$, and the double cover of $\mathcal{C}$ ramified at these 6 points is a genus 2 curve $\mathcal{Y}$ with $\mathrm{Jac}(\mathcal{Y}) \cong \mathrm{Jac}(\mathcal{X})/G$.

Proof. The linear system $|n\Theta_{\mathcal{X}}|$ on $\mathrm{Jac}(\mathcal{X})$ has dimension $n^2 - 1$ (projective dimension of divisors modulo scalars), and for an isotropic subgroup G of order n^2, $\mathrm{Jac}(\mathcal{Y}) = \mathrm{Jac}(\mathcal{X})/G$ is principally polarized with Theta divisor $\Theta_{\mathcal{Y}}$. Since $\deg \Theta_{\mathcal{X}} = 2$, $\Phi(\Theta_{\mathcal{X}}) \in |n\Theta_{\mathcal{Y}}|$ has degree $2n$ and projects to a genus-zero curve on the singular Kummer surface $\mathcal{K}_{\mathrm{Jac}(\mathcal{Y})} = \mathrm{Jac}(\mathcal{Y})/\langle -\mathbb{I} \rangle$ with arithmetic genus $\frac{1}{2}(2n-1)(2n-2) = n^2 - 1$ by the adjunction formula. Embed $\mathcal{X}$ via ρ_{2n}, where W has dimension 5 (6 points minus 1). The secant variety over G (order n^2) requires a hyperplane H (dimension $2n-1$) containing W. The $n^2 - 1$ secants $\mathcal{L}_e$ intersect H in points spanning a subspace N of dimension $n^2 - 2$, codimension 3 in H (since $n^2 - 2 = 2n - 1 - 3$ for $n \geq 2$). Projection from N to $\mathbb{P}^3$ maps the 6 points to a conic $\mathcal{C}$ (5 points determine a conic in $\mathbb{P}^3$), and the double cover ramified at 6 points has genus $1 + \frac{1}{2}(6-2) = 2$ by Riemann-Hurwitz, with $\mathrm{Jac}(\mathcal{Y}) \cong \mathrm{Jac}(\mathcal{X})/G$ ([22], Theorem 1). □

For $n = 2$, this aligns with Richelot isogenies ($W \subset \mathbb{P}^4$, N a point). Smith ([63]) developed an algorithm using this theorem, effective for $n = 3$ ($|G| = 9$), refined in [16], [18], [19], and [20]. For $n = 3$, $W \subset \mathbb{P}^6$, H is 5-dimensional, N is 2-dimensional, and the projection yields a conic in $\mathbb{P}^3$. Improvements over [20] include optimized secant computations and invariant recovery. For larger n, the algorithm scales, solving linear systems for H and N.

6.2. **The Lubicz-Robert Formula for (n,n)-Isogenies.** The Lubicz-Robert formula provides an efficient method to compute (n,n)-isogenies directly on the Kummer surface $\mathrm{Kum}(\mathrm{Jac}\,\mathcal{X})$, leveraging Theta coordinates to bypass high-dimensional embeddings like ρ_{2n}. The Lubicz-Robert formula achieves this by expressing Theta coordinates in terms of sums over G. This approach is particularly effective for odd n and builds on the foundational work of Lubicz and Robert in [41], offering a higher-dimensional analog to Vélu's formulas for elliptic curves.

The Lubicz-Robert formula addresses two tasks: computing the Theta null points of $\mathrm{Jac}(\mathcal{Y})$ and evaluating Φ at points in $\mathrm{Jac}(\mathcal{X})$. For an isotropic G, one represents $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$ (by Lagrange's four-square theorem, with $r \leq 4$) and chooses generators $g_1, g_2 \in G$ such that $G = \langle a_1 g_1, a_2 g_1, a_3 g_2, a_4 g_2 \rangle$ in a suitable basis. The **Lubicz-Robert Formula** then comprises:

(1) Theta null points of $\mathrm{Jac}(\mathcal{Y})$, given by

$$\hat{\theta}_i = \sum_{g \in G} \prod_{u=1}^{r} \theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (g, \tau)_{\alpha_u i},$$

where $\theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (g, \tau)$ are level-two Theta functions at $g \in G$, and $\alpha_u i$ adjusts indices to align with the basis (e.g., a permutation or selection).

(2) Point evaluations for $P \in \mathrm{Jac}(\mathcal{X})$, given by

$$\Phi(P)_i = \sum_{g \in G} \prod_{u=1}^{r} \theta \left[\begin{smallmatrix} a_u \\ b_u \end{smallmatrix} \right] (P + g, \tau)_{\alpha_u i}.$$

We have the following:

Theorem 10 (Lubicz-Robert)**.** *For an isotropic subgroup $G \subset \mathrm{Jac}(\mathcal{X})[n]$ of order n^2, the Theta coordinates $\hat{\theta}_i$ and $\Phi(P)_i$ computed via the above formulas define the codomain $\mathrm{Jac}(\mathcal{Y}) = \mathrm{Jac}(\mathcal{X})/G$ and the isogeny $\Phi\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Jac}(\mathcal{Y})$, respectively, with complexity $O(n^2)$ field operations for a general $n = a_1^2 + \cdots + a_r^2$.*

Proof. Represent $\mathrm{Jac}(\mathcal{X}) = \mathbb{C}^2/\Lambda$, and $\mathrm{Jac}(\mathcal{Y}) = \mathbb{C}^2/\hat{\Lambda}$, where $\hat{\Lambda} = \mathbb{Z}^2 \oplus n\tau\mathbb{Z}^2 + G$. The Theta functions on $\mathrm{Jac}(\mathcal{Y})$ are derived from $\mathrm{Jac}(\mathcal{X})$ by summing over G, adjusting the lattice periodicity. For the null points, $\hat{\theta}_i$ aggregates contributions from G, with the product $\prod_{u=1}^{r} \theta_{j_u}(g)$ reflecting the kernel's structure via $n = \sum a_u^2$. With $|G| = n^2$ and $r \leq 4$, the sum has n^2 terms, each a product of $O(1)$ evaluations, totaling

$O(n^2)$ operations. For $\Phi(P)$, the sum ensures $\Phi(P+g') = \Phi(P)$ for $g' \in G$, as $\theta_{j_u}(P+g+g') = \theta_{j_u}(P+g)$, defining the quotient map. Isotropy preserves the principal polarization, as the Weil pairing vanishes on G, and the resulting $\hat{\theta}_i$ define $\mathrm{Jac}(\mathcal{Y})$'s Theta structure ([41], Theorem 4.1). □

On $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$, $\hat{\theta}_i$ determine $\mathcal{K}_{\mathrm{Jac}(\mathcal{Y})}$'s quartic equation, and $\Phi(P)_i$ maps Kummer points, preserving the (16,6)-configuration on $\mathrm{Jac}(\mathcal{X})$. For $\mathcal{X} : y^2 = f(x)$, choose $G \subset \mathrm{Jac}(\mathcal{X})[n]$, e.g., for $n = 3$, G of order 9 from combinations of 3-torsion points of the form $(x_i, 0)$. Compute $\theta_i(g)$ using the curve's equation, then $\hat{\theta}_i$ over G. The map Φ respects $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})} \longrightarrow \mathcal{K}_{\mathrm{Jac}(\mathcal{Y})}$, maintaining geometric properties ([48], Chapter III).

Proposition 16. *The Lubicz-Robert formula on $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$ determines $\mathcal{Y}$'s equation via Theta nulls $\hat{\theta}_i$, and Φ's action on $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$ preserves the (16,6)-configuration of tropes and nodes.*

Proof. The $\hat{\theta}_i$ define $\mathcal{K}_{\mathrm{Jac}(\mathcal{Y})}$'s quartic in $\mathbb{P}^3$, from which $\mathcal{Y}$'s Rosenhain form is derived via Igusa invariants ([41], §5). The (16,6)-configuration maps under Φ to $\mathrm{Jac}(\mathcal{Y})[2]$, preserving isotropy and structure, as the formula respects the Weil pairing's symmetry ([48], Chapter III). □

6.3. **Isogenies for the (n,n)-Split case.** The Lubicz-Robert method also intersects with the geometric classification of genus 2 curves. Recall that the loci $\mathcal{L}_n$ were described in Section 5 as irreducible two-dimensional subvarieties of $\mathcal{M}_2$ where $\mathrm{Jac}(\mathcal{X})$ is (n,n)-Split. They can be computationally probed using the Lubicz-Robert formula: by computing $\hat{\theta}_i$ for a given $\mathcal{X}$ and an isotropic subgroup G, one can determine if $[\mathcal{X}] \in \mathcal{L}_n$, aligning with detection algorithms by Costello et al. [15]. This method contrasts with Dolgachev-Lehavi's approach, operating in $\mathbb{P}^3$ with $O(n^2)$ complexity, enhancing efficiency for odd n. While $\mathcal{L}_n$ does not drive computation –the isogeny Φ is computed agnostically from G– it verifies splitting post-hoc, aligning with detection by Costello et al. [15]. Their use of $\mathcal{L}_n$ to accelerate attacks (e.g., 25x for 100-bit p) underscores its cryptographic role, not in computing ϕ, but in assessing security by identifying weak split Jacobians.

Thus, our explicit computations for $n = 2, 3, 5, 7, 11$ provide test cases, that can be used to validate the formula's efficiency and offer a bridge between geometric loci and cryptographic applications. While $\mathcal{L}_n$ does not directly aid in computing Φ, it provides a geometric testbed. Given $[\mathcal{X}] \in \mathcal{L}_n$, the Lubicz-Robert formula must yield $\mathrm{Jac}(\mathcal{Y}) \cong E_1 \times E_2$, verifiable via invariants. But the computation proceeds independently of this property, relying solely on G, benchmarking algorithms like Lubicz-Robert. This dual role enhances both geometric classification and cryptanalysis.

6.3.1. *The $(2,2)$-Split case via Kummer surfaces.* As explained in Section 5.2.3, Legendre's gluing method provides a method of constructing a smooth genus-two curve $\mathcal{X}$ with $[\mathcal{X}] \in \mathcal{L}_2$ such that $\mathrm{Jac}(\mathcal{X})$ is $(2,2)$-isogenous to the product of two non-isogenous elliptic curves $E_1 \times E_2$. In Theorem 11 we will construct the quartic Kummer surface $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$ that is the surface analogue of Legendre's gluing method.

On the other hand, the Kummer surface $\mathrm{Kum}(E_1 \times E_2)$ is the minimal resolution of quotient surface of the product Abelian surface $E_1 \times E_2$ by the inversion automorphism where the elliptic curves E_l for $l = 1, 2$ are not mutually isogenous. Oguiso proved that these surfaces admit eleven distinct Jacobian elliptic fibrations [50]. Kuwata and Shioda furthered Oguiso's work in [39] and computed their Weierstrass models, reducible fibers, and Mordell-Weil lattices.

For $\mathrm{Kum}(E_1 \times E_2)$ a simple model is obtained as follows: let us define a double quadric surface closely related to $E_1 \times E_2$ for the elliptic curves given by Equation (107). In general, a *double quadric surface* is obtained as the double cover branched along a locus of bi-degree $(4,4)$ in $\mathbb{P}^1 \times \mathbb{P}^1$; see [2]. It is well known that the minimal resolution of any double quadric is a K3 surface. In our situation, we identify $\mathbb{P}^1 = \mathbb{P}(x_l, z_l)$ for $l = 1, 2$ and define the special double quadric surface $\mathcal{K}_{E_1 \times E_2}$, given by

$$\mathcal{K}_{E_1 \times E_2} : \quad y_{1,2}^2 = x_1 z_1 (x_1 - z_1)(x_1 - \Lambda_1 z_1)\, x_2 z_2 (x_2 - z_2)(x_2 - \Lambda_2 z_2)\,. \tag{131}$$

There is a natural projection map $\pi \colon \mathcal{E}_1 \times \mathcal{E}_2 \dashrightarrow \mathcal{K}_{E_1 \times E_2}$ given by $y_{1,2} = z_1 z_2 y_1 y_2$, invariant under the action of $\imath_1 \times \imath_2$. It follows that the minimal resolution of $\mathcal{K}_{E_1 \times E_2}$ is the Kummer surface $\mathrm{Kum}(\mathcal{E}_1 \times \mathcal{E}_2)$.

A $(2,2)$-isogeny $\Psi \colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathcal{E}_1 \times \mathcal{E}_2$ was constructed in Equation (121). In fact, Legendre's gluing method in Section 5.2.3 determines the smooth genus-two curve $\mathcal{X}$ in Equation (118) explicitly, admitting an elliptic involution with elliptic-curve quotients E_1 and E_2. The quotient maps determine the $(2,2)$-isogeny $\Psi \colon \mathrm{Jac}(\mathcal{X}) \longrightarrow E_1 \times E_2$ in Equation (121). General results in [4, Sec. 1] and Theorem 8 show that there is

a dual $(2,2)$-isogeny $\hat{\Psi}$ in Equation (95) with

$$\hat{\Psi}\colon\ \mathcal{E}_1 \times \mathcal{E}_2 \ \longrightarrow\ \mathrm{Jac}\,(\mathcal{X})\,. \tag{132}$$

Up to isomorphisms, the composition $\Psi \circ \hat{\Psi}$ is given by multiplication by two on each factor of $E_1 \times E_2$, i.e., $[2] \times [2]$. Thus, the $(2,2)$-isogeny and its dual $(2,2)$-isogeny fit in the following diagram:

$$E_1 \times E_2 \xrightarrow{\hat{\Psi}} \mathrm{Jac}\,(\mathcal{X}) \xrightarrow{\Psi} E_1 \times E_2 \qquad \text{(dashed } [2]\times[2]\text{)} \tag{133}$$

and induce rational maps on the level of Kummer surfaces

$$\mathrm{Kum}\,(E_1 \times E_2) \xrightarrow{\hat{\Psi}_*} \mathrm{Kum}(\mathrm{Jac}\,\mathcal{X}) \xrightarrow{\Psi_*} \mathrm{Kum}\,(E_1 \times E_2)$$

In Theorem 12 we will construct the corresponding rational maps relating the singular Kummer surfaces $\mathcal{K}_{\mathrm{Jac}\,(\mathcal{X})}$ and $\mathcal{K}_{E_1\times E_2}$. This construction can be considered **an application of the Lubicz-Robert formula to the $(2,2)$-Split case**. However, we provide an entirely geometric construction of the induced isogenies, following the work in [9].

We start with the two elliptic curves E_l for $l = 1, 2$ in Legendre form in Equation (107); we notice that they can be represented as a complete quadric intersection in $\mathbb{P}^3$. Let I_1 be the complete intersection of the two quadric surfaces in $\mathbb{P}^3 = \mathbb{P}(\mathbf{X}_{00}, \mathbf{X}_{01}, \mathbf{X}_{10}, \mathbf{X}_{11})$, given by

$$I_1\colon\quad \begin{cases} \mathbf{X}_{01}^2 &=& \mathbf{X}_{10}^2 + \mathbf{X}_{11}^2\,, \\ \mathbf{X}_{00}^2 &=& \mathbf{X}_{10}^2 + (1-\Lambda_1)\mathbf{X}_{11}^2\,, \end{cases} \tag{134}$$

and I_2 be the complete intersection in $\mathbb{P}^3 = \mathbb{P}(\mathbf{Y}_{00}, \mathbf{Y}_{01}, \mathbf{Y}_{10}, \mathbf{Y}_{11})$, given by

$$I_2\colon\quad \begin{cases} \mathbf{Y}_{01}^2 &=& \mathbf{Y}_{10}^2 + \mathbf{Y}_{11}^2\,, \\ \mathbf{Y}_{00}^2 &=& \mathbf{Y}_{10}^2 + (1-\Lambda_2)\mathbf{Y}_{11}^2\,. \end{cases} \tag{135}$$

We have the following:

Lemma 13. *E_l is birational equivalent to I_l for $l = 1, 2$ over $\mathbb{Q}(\Lambda_l)$.*

Proof. A rational map $E_1 \hookrightarrow \mathbb{P}^3, [x_1 : y_1 : z_1] \mapsto [\mathbf{X}_{00}, \mathbf{X}_{01}, \mathbf{X}_{10}, \mathbf{X}_{11}]$ is given by

$$\big[\mathbf{X}_{00} : \mathbf{X}_{01} : \mathbf{X}_{10} : \mathbf{X}_{11}\big] = \big[x_1^2 - 2\Lambda_1 x_1 z_1 + \Lambda_1 z_1^2 : x_1^2 - \Lambda_1 z_1^2 : x_1^2 - 2x_1 z_1 + \Lambda_1 z_1^2 : \pm 2 y_1 z_1\big]\,. \tag{136}$$

It has a rational inverse $I_1 \dashrightarrow E_1, [\mathbf{X}_{00}, \mathbf{X}_{01}, \mathbf{X}_{10}, \mathbf{X}_{11}] \mapsto [x_1 : y_1 : z_1]$, given by

$$\big[x_1 : y_1 : z_1\big] \ =\ \big[\Lambda_1(\mathbf{X}_{1,0} - \mathbf{X}_{0,0}) :\ \pm\Lambda_1(\Lambda_1 - 1)\mathbf{X}_{1,1} :\ (1-\Lambda_1)\mathbf{X}_{0,1} + \Lambda_1\mathbf{X}_{1,0} - \mathbf{X}_{0,0}\big]\,. \tag{137}$$

Thus, we obtain a birational equivalence between E_1 and I_1. An analogous argument holds for E_2 and I_2. □

There is a well defined map $\tilde{\pi}\colon I_1 \times I_2 \dashrightarrow \mathbb{P}^3$ with $\mathbb{P}^3 = \mathbb{P}(\mathbf{Z}_{00}, \mathbf{Z}_{01}, \mathbf{Z}_{10}, \mathbf{Z}_{11})$ induced by

$$\big[\mathbf{Z}_{00} : \mathbf{Z}_{01} : \mathbf{Z}_{10} : \mathbf{Z}_{11}\big] \ =\ \big[\mathbf{X}_{00}\mathbf{Y}_{00} :\ \mathbf{X}_{01}\mathbf{Y}_{01} :\ \mathbf{X}_{10}\mathbf{Y}_{10} :\ \mathbf{X}_{11}\mathbf{Y}_{11}\big]\,. \tag{138}$$

In fact, we have the following:

Theorem 11. *Let $\Lambda_1, \Lambda_2 \in \mathbb{P}^1\backslash\{0, 1, \infty\}$ and $\Lambda_1 \neq \Lambda_2$. The image $\tilde{\pi}(I_1 \times I_2)$ in $\mathbb{P}^3 = \mathbb{P}(\mathbf{Z}_{00}, \mathbf{Z}_{01}, \mathbf{Z}_{10}, \mathbf{Z}_{11})$ is the quartic projective surface, given by*

$$\begin{aligned} &\mathbf{Z}_{00}^4 + (1-\Lambda_1)(1-\Lambda_2)\mathbf{Z}_{01}^4 + \Lambda_1\Lambda_2\mathbf{Z}_{10}^4 + \Lambda_1\Lambda_2(1-\Lambda_1)(1-\Lambda_2)\mathbf{Z}_{11}^4 \\ &-(2-\Lambda_1-\Lambda_2)\big(\mathbf{Z}_{00}^2\mathbf{Z}_{01}^2 + \Lambda_1\Lambda_2\mathbf{Z}_{10}^2\mathbf{Z}_{11}^2\big) - (2\Lambda_1\Lambda_2 - \Lambda_1 - \Lambda_2)\big(\mathbf{Z}_{00}^2\mathbf{Z}_{11}^2 + \mathbf{Z}_{01}^2\mathbf{Z}_{10}^2\big) \\ &-(\Lambda_1+\Lambda_2)\big(\mathbf{Z}_{00}^2\mathbf{Z}_{10}^2 + (1-\Lambda_1)(1-\Lambda_2)\mathbf{Z}_{01}^2\mathbf{Z}_{11}^2\big) \ =\ 0\,. \end{aligned} \tag{139}$$

The quartic hypersurface is birational equivalent over $\mathbb{Q}(\lambda_2\lambda_3, \lambda_2 + \lambda_3)$ to the singular Kummer variety $\mathcal{K}_{\mathcal{A}}$ associated with the principally polarized Abelian surface $\mathcal{A} = \mathrm{Jac}(\mathcal{X})$ with $\mathcal{X}$ in Equation (118) and parameters satisfying (108). The minimal resolution is isomorphic to a Kummer surface of Picard rank 18.

Proof. We multiply (pairwise) Equations (134) and (134) and use the variables in Equation (138). We obtain Equation (139). For elliptic moduli K_l and complementary elliptic moduli K_l' with $\Lambda_l = K_l^2 = 1-(K_l')^2 \in \mathbb{P}^1\backslash\{0,1,\infty\}$ for $l=1,2$, Equation (139) is isomorphic over $\mathbb{Q}(\sqrt{K_1K_2},\sqrt{K_1'K_2'})$ to the equation in $\mathbb{P}^3=\mathbb{P}(w,x,y,z)$ given by

$$\begin{aligned} 0 \;=\; & w^4+x^4+y^4+z^4-\frac{(K_1')^2+(K_2')^2}{K_1'K_2'}\big(w^2z^2+x^2y^2\big) \\ & -\frac{K_1^2+K_2^2}{K_1K_2}\big(w^2y^2+x^2z^2\big)+\frac{(K_1K_2')^2+(K_1'K_2)^2}{K_1K_2K_1'K_2'}\big(w^2x^2+y^2z^2\big)\,. \end{aligned} \tag{140}$$

In fact, in Equation (139) we can rescale

$$\mathbf{Z}_{00}=x\,,\quad \mathbf{Z}_{01}=\frac{y}{\sqrt{K_1'K_2'}}\,,\quad \mathbf{Z}_{10}=\frac{z}{\sqrt{K_1K_2}}\,,\quad \mathbf{Z}_{11}=\frac{w}{\sqrt{K_1K_2}\sqrt{K_1'K_2'}}\,, \tag{141}$$

and obtain Equation (140). We check that the latter is a Hudson quartic in Equation (57) with $D=0$. Accordingly, its minimal resolution is a Jacobian Kummer surface of Picard rank 18.

For parameters satisfying Equations (108), the map, given by

$$[\mathbf{Z}_{00}:\mathbf{Z}_{01}:\mathbf{Z}_{10}:\mathbf{Z}_{11}] \;\mapsto\; [\mathbf{W}:\mathbf{X}:\mathbf{Y}:\mathbf{Z}]\,,$$

$$\begin{aligned} \text{with}\qquad \mathbf{W} &= \mathbf{Z}_{0,1}-\mathbf{Z}_{1,0}-\mathbf{Z}_{1,1}\,, \\ \mathbf{X} &= -(1-\lambda_2)(1-\lambda_3)\mathbf{Z}_{0,0}+(1+\lambda_2\lambda_3)\mathbf{Z}_{0,1}-(\lambda_2+\lambda_3)\mathbf{Z}_{1,0}\,, \\ \mathbf{Y} &= \lambda_2\lambda_3(\mathbf{Z}_{0,1}-\mathbf{Z}_{1,0}+\mathbf{Z}_{1,1})\,, \\ \mathbf{Z} &= -\lambda_2\lambda_3((1-\lambda_2)(1-\lambda_3)\mathbf{Z}_{0,0}+(1+\lambda_2\lambda_3)\mathbf{Z}_{0,1}-(\lambda_2+\lambda_3)\mathbf{Z}_{1,0})\,, \end{aligned} \tag{142}$$

is an isomorphism, defined over $\mathbb{Q}(\lambda_2\lambda_3,\lambda_2+\lambda_3)$, between the quartic surface in Equation (139) and the Baker quartic introduced in Equation (50) with $\lambda_1=\lambda_2\lambda_3$. Substituting Equations (142) into Equation (50), we obtain Equation (139) up to a non-vanishing scale factor. Inverting Equations (142) yields

$$\begin{aligned} \mathbf{Z}_{0,0} &= \lambda_2\lambda_3\mathbf{X}+\mathbf{Z}\,, \\ \mathbf{Z}_{0,1} &= \lambda_2\lambda_3(\lambda_2+\lambda_3)\mathbf{W}-\lambda_2\lambda_3\mathbf{X}+(\lambda_2+\lambda_3)\mathbf{Y}+\mathbf{Z}\,, \\ \mathbf{Z}_{1,0} &= \lambda_2\lambda_3(\lambda_2\lambda_3+1)\mathbf{W}-\lambda_2\lambda_3\mathbf{X}+(\lambda_2\lambda_3+1)\mathbf{Y}+\mathbf{Z}\,, \\ \mathbf{Z}_{1,1} &= -\lambda_2\lambda_3(1-\lambda_2)(1-\lambda_3)\mathbf{W}+(1-\lambda_2)(1-\lambda_3)\mathbf{Y}\,. \end{aligned} \tag{143}$$

Moreover, Equations (52) and (53) provide a birational equivalence between Equation (139) and the Cassels-Flynn quartic. It is easy to see that for $\lambda_1=\lambda_2\lambda_3$ in Equations (48) this equivalence is well defined over $\mathbb{Q}(\lambda_2\lambda_3,\lambda_2+\lambda_3)$ □

On the other hand, the double quadric $\mathcal{K}_{E_1\times E_2}$ in Equation (131) is related to the surface in Equation (139) as follows:

Lemma 14. *In the commutative diagram*

$$\begin{array}{ccc} \mathcal{E}_1\times\mathcal{E}_2 & \xrightarrow{\cong} & \mathcal{I}_1\times\mathcal{I}_2 \\ \pi\downarrow & & \downarrow\tilde{\pi} \\ \mathcal{K}_{E_1\times E_2} & \xrightarrow{\hat{\psi}_\pm} & \mathcal{K}_{\mathrm{Jac}(\mathcal{X})} \end{array} \tag{144}$$

the maps $\hat{\psi}_\pm\colon \mathcal{K}_{E_1\times E_2} \dashrightarrow \mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$ *are rational maps of degree two given by*

$$\begin{aligned} \hat{\psi}_\pm:\qquad & (x_1,z_1,x_2,z_2,y_{1,2}) \;\mapsto\; [\mathbf{Z}_{00}:\mathbf{Z}_{01}:\mathbf{Z}_{10}:\mathbf{Z}_{11}]\,, \\ \textit{with}\qquad \mathbf{Z}_{00} &= \big(x_1^2-2\Lambda_1x_1z_1+\Lambda_1z_1^2\big)\big(x_2^2-2\Lambda_2x_2z_2+\Lambda_2z_2^2\big)\,, \\ \mathbf{Z}_{01} &= \big(x_1^2-\Lambda_1z_1^2\big)\big(x_2^2-\Lambda_2z_2^2\big)\,, \\ \mathbf{Z}_{10} &= \big(x_1^2-2x_1z_1+\Lambda_1z_1^2\big)\big(x_2^2-2x_2z_2+\Lambda_2z_2^2\big)\,, \\ \mathbf{Z}_{11} &= \pm 4y_{1,2}\,, \end{aligned} \tag{145}$$

such that $\hat{\psi}_\pm\circ\pi\circ\imath_l=\hat{\psi}_\mp\circ\pi$ *for* $l=1,2$ *and* $\imath_l$ *the hyperelliptic involution on* E_l.

Proof. Equation (145) follows immediately from Lemma 13 (with a choice ± 1 for the relative sign of y_1 and y_2) and the fact that $\pi\colon E_1 \times E_2 \longrightarrow \mathcal{K}_{E_1\times E_2}$ is given by $y_{1,2} = z_1 z_2 y_1 y_2$. The fact that the map is a rational map of degree two follows directly from the fact that Equation (131) is a double quadric surface. □

For the elliptic curve E_l with $\Lambda_l \in \mathbb{P}^1\backslash\{0,1,\infty\}$ for $l = 1, 2$, multiplication by two $[2]\colon E_1 \longrightarrow E_1$ (with respect to the elliptic-curve group law) is given by

$$\begin{aligned} x_l &\mapsto 2(x_l^2 - \Lambda_l z_l)^2 y_l z_l \,, \\ y_l &\mapsto (x_l^2 - 2\Lambda_l x_l z_l + \Lambda_l z_l^2)(x_l^2 - 2x_l z_l + \Lambda_l z_l^2)(x_l^2 - \Lambda_l z_l^2) \,, \\ z_l &\mapsto 8 y_l^3 z_l^3 \,. \end{aligned} \tag{146}$$

The map can be expressed as rational map originating from the complete intersection of quadrics I_1 in Equation (134) (resp. I_2 in Equation (135)), i.e.,

$$[\mathbf{X}_{00}, \mathbf{X}_{01}, \mathbf{X}_{10}, \mathbf{X}_{11}] \;\mapsto\; [x_1 : y_1 : z_1] = [\mathbf{X}_{0,1}^2 \mathbf{X}_{1,1} : \mathbf{X}_{0,0}\mathbf{X}_{0,1}\mathbf{X}_{1,0} : \mathbf{X}_{1,1}^3] \,. \tag{147}$$

The induced map for their Cartesian products factors into rational maps between $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$ to $\mathcal{K}_{E_1\times E_2}$. We have the following:

Proposition 17. *Rational maps $\psi_\pm\colon \mathcal{K}_{\mathrm{Jac}(\mathcal{X})} \dashrightarrow \mathcal{K}_{E_1\times E_2}$ of degree two are*

$$\begin{aligned} \psi_\pm :\quad & [\mathbf{Z}_{00} : \mathbf{Z}_{01} : \mathbf{Z}_{10} : \mathbf{Z}_{11}] \;\mapsto\; (x_1, z_1, x_2, z_2, y_{1,2}) \,, \\ \textit{with}\quad & x_1 = Q \,, \qquad z_1 = (\Lambda_1 - \Lambda_2)\mathbf{Z}_{1,1}^2 \,, \\ & x_2 = (\Lambda_1 - \Lambda_2)\mathbf{Z}_{0,1}^2 \,, \qquad z_2 = Q \,, \\ & y_{1,2} = \pm(\Lambda_1 - \Lambda_2)^2 Q^2 \mathbf{Z}_{0,0}\mathbf{Z}_{0,1}\mathbf{Z}_{1,0}\mathbf{Z}_{1,1} \,, \end{aligned} \tag{148}$$

where we have set

$$Q = \mathbf{Z}_{0,0}^2 - (1-\Lambda_1)\mathbf{Z}_{0,1}^2 - \Lambda_1 \mathbf{Z}_{1,0}^2 + \Lambda_1(1-\Lambda_2)\mathbf{Z}_{1,1}^2 \,, \tag{149}$$

and they satisfy that the composition $\psi_\pm \circ \hat{\psi}_\pm\colon \mathcal{K}_{E_1\times E_2} \dashrightarrow \mathcal{K}_{E_1\times E_2}$ is induced by the diagonal action of multiplication by two on $E_1 \times E_2$ in Equation (146).

Proof. The composition of elliptic-curve isogenies is given by

$$\left(\begin{array}{c} [\mathbf{X}_{00} : \mathbf{X}_{01} : \mathbf{X}_{10} : \mathbf{X}_{11}] \\ [\mathbf{Y}_{00} : \mathbf{Y}_{01} : \mathbf{Y}_{10} : \mathbf{Y}_{11}] \end{array} \right) \mapsto \left(\begin{array}{c} [x_1 : z_1 : y_1] = [\mathbf{X}_{0,1}^2 \mathbf{X}_{1,1} : \mathbf{X}_{1,1}^3 : \mathbf{X}_{0,0}\mathbf{X}_{0,1}\mathbf{X}_{1,0}] \\ [x_2 : z_2 : y_2] = [\mathbf{Y}_{0,1}^2 \mathbf{Y}_{1,1} : \mathbf{Y}_{1,1}^3 : \mathbf{Y}_{0,0}\mathbf{Y}_{0,1}\mathbf{Y}_{1,0}] \end{array} \right) . \tag{150}$$

The relation, given by

$$\big[\mathbf{Z}_{00} : \mathbf{Z}_{01} : \mathbf{Z}_{10} : \mathbf{Z}_{11}\big] \;=\; \big[\mathbf{X}_{00}\mathbf{Y}_{00} :\; \mathbf{X}_{01}\mathbf{Y}_{01} :\; \mathbf{X}_{10}\mathbf{Y}_{10} :\; \mathbf{X}_{11}\mathbf{Y}_{11}\big] \,, \tag{151}$$

induces a correspondence between $\mathcal{K}_{E_1\times E_2}$ and $\mathcal{K}_{\mathrm{Jac}(\mathcal{X})}$, given by

$$\begin{gathered} x_1 x_2 = \mathbf{Z}_{0,1}^2 \,, \qquad z_1 z_2 = \mathbf{Z}_{1,1}^2 \,, \qquad y_{1,2} = \mathbf{Z}_{0,0}\mathbf{Z}_{0,1}\mathbf{Z}_{1,0}\mathbf{Z}_{1,1} \,, \\ (\Lambda_1 - \Lambda_2) x_1 z_2 = Q \,, \qquad (\Lambda_2 - \Lambda_1) x_2 z_1 = R \,, \qquad QR = -(\Lambda_1 - \Lambda_2)^2 \mathbf{Z}_{0,1}^2 \mathbf{Z}_{1,1}^2 \,, \end{gathered} \tag{152}$$

with $Q = (\Lambda_1 - \Lambda_2)\mathbf{X}_{01}^2\mathbf{Y}_{11}^2$ and $R = (\Lambda_2 - \Lambda_1)\mathbf{X}_{11}^2\mathbf{Y}_{01}^2$. One then obtains

$$\begin{aligned} Q &= \mathbf{Z}_{0,0}^2 - (1-\Lambda_1)\mathbf{Z}_{0,1}^2 - \Lambda_1\mathbf{Z}_{1,0}^2 + \Lambda_1(1-\Lambda_2)\mathbf{Z}_{1,1}^2 \,, \\ R &= \mathbf{Z}_{0,0}^2 - (1-\Lambda_2)\mathbf{Z}_{0,1}^2 - \Lambda_2\mathbf{Z}_{1,0}^2 + \Lambda_2(1-\Lambda_1)\mathbf{Z}_{1,1}^2 \,. \end{aligned} \tag{153}$$

When solving for an equivalence class, given by

$$(x_1, z_1, x_2, z_2, y_{1,2}) \;\sim\; (\mu x_1,\; \mu z_1,\; \nu x_2,\; \nu z_2,\; \mu^2\nu^2 y_{1,2}) \text{ with } \mu, \nu \in \mathbb{C}^\times \,, \tag{154}$$

we obtain Equations (148). Using the relation $QR = -(\Lambda_1 - \Lambda_2)^2\mathbf{Z}_{0,1}^2\mathbf{Z}_{1,1}^2$ the solution can also be written as

$$\begin{gathered} x_1 = (\Lambda_2 - \Lambda_1)\mathbf{Z}_{0,1}^2 \,, \quad z_1 = R \,, \quad x_2 = R \,, \quad z_2 = (\Lambda_2 - \Lambda_1)\mathbf{Z}_{1,1}^2 \,, \\ y_{1,2} = (\Lambda_1 - \Lambda_2)^2 R^2 \mathbf{Z}_{0,0}\mathbf{Z}_{0,1}\mathbf{Z}_{1,0}\mathbf{Z}_{1,1} \,. \end{gathered} \tag{155}$$

Equation (146) provides an explicit formula for the (diagonal) action of multiplication by two on $E_1 \times E_2$. We apply the projection map $\pi\colon E_1 \times E_2 \longrightarrow \mathcal{K}_{E_1\times E_2}$ given by $y_{1,2} = z_1 z_2 y_1 y_2$ to obtain the induced action

on the the double quadric in Equation (131). We check that this agrees with the composition of maps $\psi_\pm \circ \hat{\psi}_\pm$. □

In summary, the construction of isogenies descends directly to the level of Kummer surfaces and yield the following Kummer sandwich theorem, see [9, Thm. 2.38] for details:

Theorem 12. *The rational maps $\hat{\psi}_\pm, \psi_\pm$ in Equations (145) and (148) fit into the following Kummer sandwich:*

$$\mathcal{K}_{E_1 \times E_2} \xrightarrow{\hat{\psi}_\pm} \mathcal{K}_{\mathrm{Jac}(\mathcal{X})} \xrightarrow{\psi_\pm} \mathcal{K}_{E_1 \times E_2}$$

The maps $\hat{\psi}_\pm, \psi_\pm$ are defined over $\mathbb{Q}(\Lambda_1, \Lambda_2)$ and induced (up to the action of the minus identity involution) by the $(2,2)$-isogeny in Equation (95) and its dual $(2,2)$-isogeny in Equation (121).

7. Cryptography Applications

The computational methods for (n,n)-isogenies and the geometric classification of the loci $\mathcal{L}_n$, developed in Sections 2 through 6, enable applications to isogeny-based cryptography in genus 2.

Let $\mathcal{S}_2(p)$ denote the isomorphism classes of superspecial principally polarized Abelian surfaces over $\mathbb{F}_{p^2}$. The superspecial isogeny problem seeks an isogeny $\phi\colon \mathrm{Jac}(\mathcal{X}) \longrightarrow \mathrm{Jac}(\mathcal{Y})$ between superspecial genus 2 Jacobians over $\mathbb{F}_{p^2}$, for some prime p. The Costello-Smith algorithm [17] addresses this by navigating the Richelot isogeny graph $\Gamma_2(2;p)$, whose vertices are superspecial principally polarized Abelian surfaces in $\mathcal{S}_2(p)$, to reach products $E_1 \times E_2 \in \mathcal{E}_2(p)$. The Richelot isogeny graph $\Gamma_2(2;p)$, while not Ramanujan [23], exhibits sufficient expansion properties to support efficient random walks from $\mathcal{S}_2(p)$ to $\mathcal{E}_2(p)$, a key feature leveraged in both the original algorithm and the optimized attack. Subsequent elliptic isogeny computations, leveraging the Delfs-Galbraith algorithm [21] in $\tilde{O}(\sqrt{p})$ time, yield a complexity of $\tilde{O}(p)$ bit operations, given $\#\mathcal{S}_2(p) = O(p^3)$ and $\#\mathcal{E}_2(p) = O(p^2)$.

An attack by Costello et al. [15] optimizes this approach by detecting (n,n)-splittings for $n \leq 11$, using equations of $\mathcal{L}_n$, derived in [42, 57, 59]. The attack inspects approximately n^3 neighbors per step (e.g., 40 for $n=3$) through invariant computations, bypassing full isogeny evaluations. This reduces the cost from 1176 multiplications in $\mathbb{F}_p$ per Richelot step to as few as 35, as reported in Table 5 of [15], achieving speedups of 16 to 159 times for primes p from 50 to 1000 bits. The asymptotic complexity remains $\tilde{O}(p/n^3)$, but the reduced constants significantly enhance cryptanalytic efficiency.

The attack's reliance on precomputed $\mathcal{L}_n$ equations limits its scope to small n. Recent work in [56] introduces machine learning-based methods, to detect whether a curve lies in $\mathcal{L}_n$ for arbitrary n. This enables the attack to target larger n, potentially increasing its efficacy. Additionally, rational points on $\mathcal{L}_n$ in $\mathbb{P}_{(2,4,6,10)}(\mathbb{Q})$ over fields of positive characteristic studied in [46], provide arithmetic insights for assessing protocol vulnerabilities by informing secure key selection.

The Costello et al. attack impacts protocols reliant on the superspecial isogeny problem, such as the CDS hash function [11], which maps inputs via Richelot isogenies in $\Gamma_2(2;p)$. For a Jacobian $\mathrm{Jac}(\mathcal{X}) \in \mathcal{L}_n$, the attack accelerates traversal to $\mathcal{E}_2(p)$, facilitating collision finding by identifying distinct paths to the same product, as noted by Florit and Smith [23]. For a 100-bit prime, a 25-fold speedup reduces security from $\tilde{O}(2^{100})$ to below 2^{96}, posing risks to under parameterized systems. For 512-bit primes, a 100-fold speedup yields $\tilde{O}(2^{509})$, remaining secure classically but with a reduced margin.

In a hypothetical genus 2 SIDH scheme, where the secret is an (n^k, n^k)-isogeny, the attack finds a path to $\mathcal{E}_2(p)$ if $\mathrm{Jac}(\mathcal{Y}) \in \mathcal{L}_n$, but does not recover the kernel S, limiting its threat to key exchange compared to hash functions. The larger n^4-torsion groups and complex endomorphism structures of genus 2 Jacobians offer potential security advantages over elliptic curve protocols like SIDH. Explicit computation of $\mathcal{L}_n$ enables protocol designers to avoid vulnerable Jacobians suggesting that careful key selection can mitigate attack risks.

Achieving a complete break of genus 2 isogeny-based cryptography, reducing it to polynomial time or practical insecurity, requires advances beyond the current attack. A method to recover the secret kernel $S \subset \mathrm{Jac}(\mathcal{X})[n^k]$ from public data, such as images of torsion points under ϕ, is essential but challenged by the n^4-dimensional torsion group and polarization complexities. A sub-exponential algorithm or polynomial-time solution for the isogeny problem remains elusive, potentially requiring improved expansion of the non-Ramanujan graph $\Gamma_2(n;p)$ or endomorphism ring computations. A quantum algorithm achieving polynomial

time, surpassing the current $\tilde{O}(\sqrt{p}/n^{3/2})$ via Grover's search, is undeveloped. Protocol-specific vulnerabilities, such as degree conversion from $(2^m n, 2^m n)$ to (n^k, n^k) or torsion leakage, could suffice, but no such methods exist.

Our computational methods, particularly the Lubicz-Robert formula with $O(n^2)$ complexity, enhance the efficiency of (n, n)-isogeny computations, directly supporting genus 2 cryptographic protocols. By computing isogenies via sums of Theta functions on the Kummer surface the formula leverages the geometric embedding of Kummer surfaces into $\mathbb{P}^3$ achieving $O(n^2)$ complexity through efficient operations in low-dimensional projective space. This generalizes Richelot's constructions, achieving practical advantages over traditional approaches. Future research may optimize $\mathcal{L}_n$ detection for larger n, possibly through new parameterizations, to refine cryptanalysis.

References

[1] H. F. Baker, *On a system of differential equations leading to periodic functions*, Acta Math. **27** (1903), no. 1, 135–156. MR1554977

[2] Wolf Barth, *Even sets of eight rational curves on a K3-surface*, Complex geometry (Göttingen, 2000), 2002, pp. 1–25. MR1922094

[3] L. Beshaj, R. Hidalgo, S. Kruk, A. Malmendier, S. Quispe, and T. Shaska, *Rational points in the moduli space of genus two*, Higher genus curves in mathematical physics and arithmetic geometry, [2018] ©2018, pp. 83–115. MR3782461

[4] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, Second, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR2062673

[5] Christina Birkenhake and Hannes Wilhelm, *Humbert surfaces and the Kummer plane*, Trans. Amer. Math. Soc. **355** (2003), no. 5, 1819–1841. MR1953527

[6] Oskar Bolza, *On binary sextics with linear transformations into themselves*, Amer. J. Math. **10** (1887), no. 1, 47–70. MR1505464

[7] C. W. Borchardt, *über die Darstellung der Kummerschen Fläche vierter Ordnung mit sechzehn Knotenpunkten durch die Göpelsche biquadratische Relation zwischen vier Thetafunctionen mit zwei Variabeln*, J. Reine Angew. Math. **83** (1877), 234–244. MR1579732

[8] Jean-Benoit Bost and Jean-Francois Mestre, *Moyenne arithmetico-géometrique et periodes des courbes de genre* 1 *et* 2, Gaz. Math. **38** (1988), 36–64. MR970659

[9] Noah Braeger, Adrian Clingher, Andreas Malmendier, and Shantel Spatig, *Isogenies of certain K3 surfaces of rank 18*, Res. Math. Sci. **8** (2021), no. 4, Paper No. 57, 60. MR4323344

[10] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090

[11] Wouter Castryck, Thomas Decru, and Benjamin Smith, *Hash functions from superspecial genus-2 curves using richelot isogenies*, Journal of Mathematical Cryptology **14** (2020), no. 1, 268–292. Preprint available at Cryptology ePrint Archive, Paper 2019/296, https://eprint.iacr.org/2019/296.

[12] Adrian Clingher and Charles F. Doran, *Lattice polarized K3 surfaces and Siegel modular forms*, Adv. Math. **231** (2012), no. 1, 172–212. MR2935386

[13] Adrian Clingher and Andreas Malmendier, *Normal forms for Kummer surfaces*, Integrable systems and algebraic geometry. Vol. 2, 2020, pp. 119–174. MR4421430

[14] Adrian Clingher, Andreas Malmendier, and Tony Shaska, *On isogenies among certain abelian surfaces*, Michigan Mathematical Journal **71** (2022May), no. 2, 227–269. Received: 29 August 2019; Revised: 22 June 2020; Published: May 2022.

[15] Maria Corte-Real Santos, Craig Costello, and Sam Frengley, *An algorithm for efficient detection of (n, n)-splittings and its application to the isogeny problem in dimension 2*, Public-key cryptography – pkc 2024, 2024, pp. 157–189.

[16] Romain Cosset and Damien Robert, *Computing* (ℓ, ℓ)*-isogenies in polynomial time on Jacobians of genus* 2 *curves*, Math. Comp. **84** (2015), no. 294, 1953–1975. MR3335899

[17] Craig Costello and Benjamin Smith, *The supersingular isogeny problem in genus 2 and beyond*, Post-Quantum Cryptography (PQCrypto 2020) **12100** (2020), 151–168. MR4139650.

[18] ———, *The supersingular isogeny problem in genus 2 and beyond*, Post-quantum cryptography, [2020] ©2020, pp. 151–168. MR4139650

[19] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost, *Explicit isogenies in quadratic time in any characteristic*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 267–282. MR3540960

[20] Thomas Decru and Sabrina Kunzweiler, *Efficient computation of* $(3^n, 3^n)$*-isogenies*, Progress in cryptology—AFRICACRYPT 2023, [2023] ©2023, pp. 53–78. MR4638168

[21] Christina Delfs and Steven D. Galbraith, *Computing isogenies between supersingular elliptic curves over* $\mathbb{F}_p$, Designs, Codes and Cryptography **78** (2016), no. 1, 329–346.

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

[23] Enric Florit and Benjamin Smith, *Random and zig-zag sampling for genus-2 isogeny graphs*, 2022. Accessed via ePrint.

[24] E. Freitag, *Siegelsche Modulfunktionen*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 254, Springer-Verlag, Berlin, 1983. MR871067

[25] Gerhard Frey, *Isogenies in theory and praxis*, Open problems in mathematics and computational science, 2014, pp. 37–68. MR3330877

[26] Gerhard Frey and Ernst Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, 2011, pp. 1–19.

[27] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, J. Math. Cryptol. **1** (2007), no. 3, 243–265. MR2372155

[28] V. A. Gritsenko and V. V. Nikulin, *Igusa modular forms and "the simplest" Lorentzian Kac-Moody algebras*, Mat. Sb. **187** (1996), no. 11, 27–66. MR1438983

[29] 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

[30] Georges Humbert, *Sur les fonctionnes abéliennes singulières. I, II, III*, J. Math. Pures Appl. serie 5 (1901), V, 233–350 (1899); VI, 279–386 (1900); VII, 97–123 (1901).

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

[32] ———, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200. MR0141643

[33] Jun-Ichi Igusa, *On Siegel modular forms genus two. II*, Amer. J. Math. **86** (1964), 392–412. MR0168805

[34] Jun-ichi Igusa, *Modular forms and projective invariants*, Amer. J. Math. **89** (1967), 817–855. MR0229643

[35] ———, *On the ring of modular forms of degree two over* $\mathbf{Z}$, Amer. J. Math. **101** (1979), no. 1, 149–183. MR527830

[36] Kenji Koike, *On Jacobian Kummer surfaces*, J. Math. Soc. Japan **66** (2014), no. 3, 997–1016. MR3238326

[37] 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

[38] E. E. Kummer, *Über die Flächen vierten Grades, auf welchen Schaaren von Kegelschnitten liegen*, J. Reine Angew. Math. **64** (1865), 66–76. MR1579281

[39] Masato Kuwata and Tetsuji Shioda, *Elliptic parameters and defining equations for elliptic fibrations on a Kummer surface*, Algebraic geometry in East Asia—Hanoi 2005, 2008, pp. 177–215. MR2409557

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

[41] David Lubicz and Damien Robert, *Arithmetic on abelian and Kummer varieties*, Finite Fields Appl. **39** (2016), 130–158. MR3475546

[42] 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

[43] A. Malmendier and T. Shaska, *The Satake sextic in F-theory*, J. Geom. Phys. **120** (2017), 290–305. MR3712162

[44] ———, *From hyperelliptic to superelliptic curves*, Albanian J. Math. **13** (2019), no. 1, 107–200. MR3978315

[45] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17. MR3731039

[46] J. Mello, S. Salami, E. Shaska, and T. Shaska, *Rational points and zeta functions of Humbert surfaces with square discriminant* (2025), available at 2504.19268.

[47] D. R. Morrison, *On K3 surfaces with large Picard number*, Invent. Math. **75** (1984), no. 1, 105–121. MR728142

[48] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

[49] ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

[50] Keiji Oguiso, *On Jacobian fibrations on the Kummer surfaces of the product of nonisogenous elliptic curves*, J. Math. Soc. Japan **41** (1989), no. 4, 651–680. MR1013073

[51] Frans Oort, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, 1988, pp. 469–502. MR977774

[52] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218

[53] Alfred Pringsheim, *Zur Transformation zweiten Grades der hyperelliptischen Functionen erster Ordnung*, Math. Ann. **9** (1876), no. 4, 445–475. MR1509868

[54] Fried. Jul. Richelot, *De transformatione integralium Abelianorum primi ordinis commentatio. Caput secundum. De computatione integralium Abelianorum primi ordinis*, J. Reine Angew. Math. **16** (1837), 285–341. MR1578135

[55] Jean-Pierre Serre, *Rational points on curves over finite fields*, notes by F. Gouvea of lectures at Harvard University (1985).

[56] Elira Shaska and Tanush Shaska, *Machine learning for moduli space of genus two curves and an application to isogeny-based cryptography*, J. Algebraic Combin. **61** (2025), no. 2, 23. MR4870337

[57] Tanush Shaska and Helmut 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

[58] Tony Shaska, *Curves of genus 2 with* $\langle n, n\rangle$ *decomposable jacobians*, Journal of Symbolic Computation **31** (2001), no. 5, 603–617. MR1828706

[59] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Mathematicum **16** (2004), no. 2, 263–280. MR2039100

[60] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1971. Reprinted by Princeton University Press, 1994.

[61] Tetsuji Shioda, *Classical Kummer surfaces and Mordell-Weil lattices*, Algebraic geometry, 2007, pp. 213–221. MR2296439

[62] Tetsuji Shioda and Katsumi Inose, *On singular k3 surfaces*, Complex Analysis and Algebraic Geometry (1977), 119–136. A collection of papers dedicated to K. Kodaira.
[63] Benjamin Smith, *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, 2012, pp. 159–170. MR2961408

Department of Mathematics and Statistics, University of Missouri - St. Louis, St. Louis, MO 63121
Email address: clinghera@umsl.edu

Department of Mathematics & Statistics, Utah State University, Logan, UT 84322
Email address: andreas.malmendier@usu.edu

Department of Mathematics and Statistics, Oakland University, Rochester, MI 48309
Email address: shaska@oakland.edu