ABELIAN SURFACES ADMITTING AN \((l,l)\)-ENDOMORPHISM

REINIER BRÖKER, KRISTIN LAUTER, AND MARCO STRENG

Abstract. We give a classification of all principally polarized abelian surfaces that admit an \((l,l)\)-isogeny to themselves, and show how to compute all the abelian surfaces that occur. We make the classification explicit in the simplest case \(l = 2\). As part of our classification, we also show how to find all principally polarized abelian surfaces with multiplication by a given imaginary quadratic order.

1. Introduction

For a prime \(l\), the \(l\)-th modular polynomial \(\Phi_l \in \mathbb{Z}[X,Y]\) is a model for the modular curve \(Y_0(l)\) parametrizing elliptic curves together with an isogeny of degree \(l\). This polynomial is used in various algorithms, including the ‘Schoof-Atkin-Elkies’ algorithm (see [14]) to count the number of points on an elliptic curve \(E/F_p\). If we specialize \(\Phi_l\) in \(Y = X\) we get a univariate polynomial \(\Phi_l(X,X) \in \mathbb{Z}[X]\) whose roots are the \(j\)-invariants of the elliptic curves \(E/\mathbb{C}\) that admit an endomorphism of degree \(l\). There is a close link between \(\Phi_l(X,X)\) and the Hilbert class polynomials \(H_O\) of imaginary quadratic orders \(O\). More precisely, we have

\[
\Phi_l(X,X) = \prod_O H_O(X)^{e(O)}
\]

where the product ranges over all imaginary quadratic orders \(O\) that contain an element of norm \(l\). The exponent

\[
e(O) = \# \left( \{\alpha \in O \text{ of norm } l\} / O^* \right) \in \mathbb{Z}_{>0}
\]

measures how many elements of norm \(l\) there are in \(O\). One of the applications of (1.1) is a proof that \(H_O(X)\) has integral coefficients.

In this article we investigate an analogue of equation (1.1) for abelian surfaces. The appropriate analogue of an isogeny of degree \(l\) is an \((l,l)\)-isogeny. If \(A\) and \(B\) are abelian surfaces with principal polarizations \(\varphi_A\) and \(\varphi_B\), then an \((l,l)\)-isogeny

\[
\lambda : (A, \varphi_A) \to (B, \varphi_B)
\]

is an isogeny \(\lambda : A \to B\) such that we have \(\varphi_A \circ [l] = \hat{\lambda} \circ \varphi_B \circ \lambda\), with \(\hat{\lambda}\) the dual of \(\lambda\). Let \(\mathcal{M}_2^{(l,l)} \subset A_2\) be the reduced subvariety of principally polarized abelian surfaces \((A, \varphi_A)\) admitting an \((l,l)\)-isogeny \((A, \varphi_A) \to (A, \varphi_A)\). The variety \(\mathcal{M}_2^{(l,l)}\) is the natural analogue of the zero set of \(\Phi(X,X)\). The goal in this article is to identify the irreducible subvarieties of \(\mathcal{M}_2^{(l,l)}\), which is the natural analogue of equality (1.1).

2000 Mathematics Subject Classification. Primary 14J10.

The research for this paper was done during an internship of the third-named author at Microsoft Research.
While the moduli space of elliptic curves is 1-dimensional, the moduli space $\mathcal{A}_2$ of principally polarized abelian surfaces is 3-dimensional. Its function field is generated by three Igusa invariants

$$j_i : \mathcal{A}_2 \to \mathbb{P}^1(\mathbb{C})$$

as e.g. defined in [6]. One can define three modular polynomials $P_l$, $Q_l$, $R_l \in \mathbb{Q}(X_1, X_2, X_3)[Y]$ for abelian surfaces using these Igusa functions, see e.g. [4, Sec. 4].

As a first idea, one might let $W_i \subset \mathbb{C}[X_1, X_2, X_3, Y_1, Y_2, Y_3]$ be the ideal generated by the numerators of

$$P_l(X_1, X_2, X_3, Y_1), \quad Y_2 - Q_l(X_1, X_2, X_3, Y_1), \quad Y_3 - R_l(X_1, X_2, X_3, Y_1)$$

and view this as the analogue of $\Phi_l$. However, the functions $j_i$ do not give a bijection

$$\mathcal{A}_2 \to \mathbb{P}^1(\mathbb{C})^3,$$

even when we restrict the domain to the moduli space of Jacobians of curves and consider the resulting map to $\mathbb{C}^3$. Because of this and other reasons, the space described by $W_i$ is very unnatural. However, the space $W_i$ can be very useful in computational applications, as its intersection with $X_i = Y_i$, pulled back to $\mathcal{A}_2$, contains $\mathcal{M}_2^{(i,l)}$. We use generators for $W_2$ computed by Dupont in his thesis [5] in Section 7.

We will show that $\mathcal{M}_2^{(i,l)}$ consists of a finite set of explicitly computable Humbert surfaces, Shimura curves and CM-points. In particular, the space $\mathcal{M}_2^{(i,l)}$ is 2-dimensional. The CM-points are a direct analogue of the Hilbert class polynomials for genus 1. Our main result, proved in Section 4.4, is the following.

**Theorem 1.1.** Let $l$ be a prime number. The variety $\mathcal{M}_2^{(i,l)}$ is the union of the following list of varieties:

1. Either one or two irreducible Humbert surfaces, depending on whether $l \equiv 3 \mod 4$ or not as in Corollary 4.2.
2. For every imaginary quadratic integer $x$ of norm $l$ and trace less than $2\sqrt{l}$, all Shimura curves corresponding to $\mathbb{Z}[x]$. The correspondence between $\mathbb{Z}[x]$ and Shimura curves is given in Theorem 3.6.
3. For every imaginary quadratic integer $x$ of norm $l$ and trace less than $2\sqrt{l}$, all CM-points corresponding to $\mathbb{Z}[x]$. The correspondence between $\mathbb{Z}[x]$ and CM-points is given in Theorem 3.6.
4. For every algebraic integer $x$ of degree 4 with the property that all complex absolute values of $x$ are equal to $\sqrt{l}$, the CM-points corresponding to the order $\mathbb{Z}[x, \pi] \subset K = \mathbb{Q}[x]$. This correspondence is given in Theorem 3.6.
5. For every pair of integers $t_1$, $t_2$ such that $-2\sqrt{l} < t_2 < t_1 < 2\sqrt{l}$, the points corresponding to finitely many principally polarized abelian surfaces that are $(n,n)$-isogenous to $E_1 \times E_2$. Here, $n$ divides $t_1 - t_2$ and $E_i$ is an elliptic curve whose endomorphism ring contains the quadratic order of discriminant $t_i^2 - 4l$.

We can make Theorem 1.1 more explicit in the simplest case $l = 2$. It turns out for instance that the Shimura curves listed as case (2) in fact lie on the Humbert surface of case (1). More precisely, we will prove the following theorem.

**Theorem 1.2.** The variety $\mathcal{M}_2^{(2,2)}$ is the union of the Humbert surface of discriminant 8, which is irreducible, and a finite set of CM-points listed in Section 7.
The organization of this article is as follows. Section 2 gives background on abelian surfaces and isogenies. Section 3 describes the moduli space of abelian surfaces with endomorphism ring structure. Section 4 gives the proof of Theorem 1.1. Section 5 examines the endomorphism rings for each of the cases occurring in the Theorem. Section 6 recalls explicit glueing techniques that are used in Section 7 where we compute all irreducible components of $\mathcal{M}_2^{(2,2)}$ in terms of Igusa invariants.

2. Background

In this section we recall some background on complex abelian surfaces and $(l,l)$-isogenies. We state the results in terms of Riemann forms, but note that most can be generalized to fields of arbitrary characteristic.

Let $V$ be a 2-dimensional complex vector space, and let $\Lambda \subset V$ be a full lattice. Any form $E : \Lambda \times \Lambda \to \mathbb{Z}$ can be extended to a form $E : V \times V \to \mathbb{R}$, and we call $E$ a Riemann form if the form $H(x, y) = E(ix, y) + iE(x, y)$ is Hermitian and positive definite. We say that the quotient $V/\Lambda$ is a (complex) abelian surface if $\Lambda \subset V$ admits a Riemann form.

For an abelian surface $A = V/\Lambda$, we define its dual as $A^\vee = V^\vee/\Lambda^\vee$ with $V^\vee = \{ f : V \to \mathbb{C} \mid f(\alpha v) = \alpha f(v), f(v + w) = f(v) + f(w) \}$, $\Lambda^\vee = \{ f \in V^\vee \mid \text{Im}(f(\Lambda)) \subset \mathbb{Z} \}$.

A Riemann form $E$ on $A$ determines a homomorphism

$$\varphi_E : A \to A^\vee$$

by $\varphi_E(x) = H(x, \cdot)$ for $x \in V$. The map $\varphi_E$ is called a polarization and the pair $(E, \varphi_E)$ a polarized abelian variety. We say that the quotient $V/\Lambda$ is a (complex) abelian surface if $\Lambda \subset V$ admits a Riemann form.

Lemma 2.1. Let $A = V/\Lambda$ be an abelian surface with Riemann form $E$. Then there is exactly one map $' : \text{End}(A) \to \text{End}(A)$ with the property $E'(yu, v) = f(yu, v)$ for all $u, v$. This map is a ring involution.

Proof. This follows immediately from the defining properties of $E$. □

Definition 2.2. The map $'$ in Lemma 2.1 is called the Rosati-involution associated to the polarization $\varphi_E$.

A surjective morphism $f : A \to B$ between abelian surfaces is called an isogeny if it has finite kernel. The polarization $\varphi_E$ occurring in (2.1) is an example of an isogeny. If $E'$ is a Riemann form on $B$, then an isogeny $f : A \to B$ induces a Riemann form

$$f^*E' : (u, v) \mapsto E'(f(u), f(v))$$
on $A$.

Definition 2.3. For a positive integer $n$, an $(n, n)$-isogeny $f : (A, E) \to (B, E')$ is an isogeny $A \to B$ such that

1. $f^*E' = nE$ holds and
2. the kernel of $f$ is contained in $A[n]$.

For prime $n$, the second item is automatic from the first, and the definition is easily seen to be equivalent to the definition given in the introduction.
Lemma 2.4. Let \((A, \varphi_E)\) be a principally polarized abelian surface that admits an \((n, n)\)-isogeny \(x\) to itself. Then we have \(x'x = [n]\).

Proof. This follows immediately from [2, Prop. 5.1.2] and [2, Lemma 5.1.4].

The kernel of an \((n, n)\)-isogeny \(x : (A, E) \to (B, E')\) is a subgroup of the \(n\)-torsion \(A[n]\) with additional structure. To analyze it, we define the Weil pairing \(e_n : A[n] \times A[n] \to \mathbb{C}^*[n]\) by

\[ e_n(u, v) = \exp(2\pi i E(u, v)) \]

for \(u, v \in \frac{1}{n} A \subset V\). We say that a subgroup \(G \subset A[n]\) is isotropic (with respect to the Weil pairing) if \(e_n\) restricts to the trivial form on \(G \times G\). We say that \(G\) is maximally isotropic if it is not strictly contained in another isotropic subgroup.

Lemma 2.5. Let \(x : (A, E) \to (B, E')\) be an \((n, n)\)-isogeny. Then the kernel of \(x\) is maximally isotropic with respect to the Weil pairing. Furthermore, every maximally isotropic subgroup \(G \subset A[n]\) arises as the kernel of an \((n, n)\)-isogeny.

If \(n\) is prime, then there are exactly \((n^4 - 1)/(n - 1)\) such subgroups.

Proof. The first two statements follow from [16, Prop. 16.8]. The last statement follows from the proof of [4, Lemma 6.1].

We will need a few properties of the analytic and rational representation of an \((n, n)\)-isogeny. We recall the basic concepts in the remainder of this section. Let \(A_1 = \mathbb{C}^2/A_1\) and \(A_2 = \mathbb{C}^2/A_2\) be two principally polarized abelian surfaces, and let \(f : A_1 \to A_2\) be a homomorphism. We can uniquely lift \(f\) to a \(\mathbb{C}\)-linear map \(F : \mathbb{C}^2 \to \mathbb{C}^2\) with \(F(A_1) \subseteq A_2\). The natural map

\[ \rho_a : \text{Hom}(A_1, A_2) \to \text{Hom}(\mathbb{C}, \mathbb{C}^2) \]

sending \(f\) to \(F\) is called the analytic representation of \(\text{Hom}(A_1, A_2)\). By restricting \(F\) to the lattice \(A_1\), we get a \(\mathbb{Z}\)-linear map \(F_{A_1}\) that induces \(F\). The natural map

\[ \rho_r : \text{Hom}(A_1, A_2) \to \text{Hom}(\mathbb{Z}, A_1, A_2) \]

sending \(f\) to \(F_{A_1}\) is called the rational representation of \(\text{Hom}(A_1, A_2)\). We use the same notation and terminology for the \(\mathbb{Q}\)-linear extension of \(\rho_a\) and \(\rho_r\).

For \(f \in \text{End}_\mathbb{Q}(A) = \text{End}(A) \otimes \mathbb{Q}\), let \(P_f^a\) be the characteristic polynomial of the analytic representation \(\rho_a(f)\) of \(f\). Likewise, we get \(P_f^r\) for the rational representation of \(f\). Explicitly, we have

\[ P_f^a = \det(X \text{id}_{\mathbb{C}^2} - \rho_a(f)) \in \mathbb{C}[X] \quad \text{and} \quad P_f^r = \det(X \text{id}_{\mathbb{Z}} - \rho_r(f)) \in \mathbb{Q}[X]. \]

The polynomial \(P_f^a\) is quadratic, and \(P_f^r\) has degree 4. The following lemma gives the relation between the analytic and the rational representation.

Lemma 2.6. Let \(A = \mathbb{C}^2/\Lambda\) be a principally polarized abelian surface, and let \(f \in \text{End}_\mathbb{Q}(A)\) be given. Then we have

(a) \(P_f^a = P_f^r \cdot 
abla_f\)

(b) \(P_f^r = \overline{P_f^r}\)

where \(\nabla\) denotes complex conjugation and \(\ast\) denotes the Rosati-involution. The polynomial \(P_f^r\) has integer coefficients if \(f\) is an endomorphism of \(A\).

Proof. This follows immediately from [2, Prop. 5.1.2] and [2, Lemma 5.1.4].
3. Moduli spaces of abelian surfaces with endomorphism structure

For a principally polarized abelian surface $A = (A, \varphi_E)$ with $(n, n)$-isogeny $x$ to itself, the algebra $K = \mathbb{Q}[x]$ is a subalgebra of the endomorphism algebra $\text{End}_\mathbb{Q}(A)$. We distinguish between the case that $K$ is / is not a field.

3.1. $K$ is not a field. Using Lemma 2.6 we analyze the structure of $K = \mathbb{Q}[x]$ if $K$ is not a field. The result is the following lemma.

Lemma 3.1. Let $x$ be an endomorphism of a principally polarized abelian surface $A/\mathbb{C}$ with $xx' = l$ for some prime $l$. Let $K = \mathbb{Q}[x] \subseteq \text{End}(A) \otimes \mathbb{Q}$ and assume that $K$ is not a field. Then we have $P^2_x = (X - \beta_1)(X - \beta_2)$ for some pair of imaginary quadratic integers $\beta_1, \beta_2 \in \mathbb{C}$ of absolute value $\sqrt{l}$ and non-equal trace. The map

$$x \mapsto (\beta_1, \beta_2)$$

gives an isomorphism $K \cong \mathbb{Q}(\beta_1) \times \mathbb{Q}(\beta_2)$. Furthermore, there exist elliptic curves $E_1, E_2$, a positive integer $n | (\text{Tr} \beta_1 - \text{Tr} \beta_2) \neq 0$ and an $(n, n)$-isogeny

$$\lambda : E_1 \times E_2 \to A$$

with the following properties:

1. the endomorphism ring of $E_i$ contains $\mathbb{Z}[\beta_i]$ for $i = 1, 2$;
2. we have $x \circ \lambda = \lambda \circ (\beta_1, \beta_2)$.

Proof. Choose a basis of $\mathbb{C}^2$ such that the analytic representation of $x$ is upper-triangular, say

$$\rho_a(x) = \left( \begin{array}{cc} \beta_1 & * \\ 0 & \beta_2 \end{array} \right)$$

with $\beta_1, \beta_2$ in $\mathbb{C}$. Note that $\rho_a(x') = \rho_a(lx^{-1})$ is also upper-triangular, say

$$\rho_a(x') = \left( \begin{array}{cc} \gamma_1 & * \\ 0 & \gamma_2 \end{array} \right).$$

As $\beta_1$ and $\beta_2$ are roots of $P^2_x$, they are algebraic integers. We let $g$ be the minimal polynomial of $\beta_1$. We claim that $\gamma_2$ is not an algebraic conjugate of $\beta_1$, i.e., that $g(\gamma_2) \neq 0$ holds. Indeed: otherwise we have $\text{Tr}(g(x)g(x')) = \text{Tr}(g(x)g(x')) = 0$ and because $'$ is positive definite by [2, Thm. 5.1.8], we find $g(x) = 0$, contradicting the assumption that $K$ is not a field.

By Lemma 2.6(b), we have $\{\gamma_1, \gamma_2\} = \{\beta_1, \beta_2\}$, so the claim above yields $\gamma_1 = \beta_1, \gamma_2 = \beta_2$, and that $\beta_1$ and $\beta_2$ are not algebraic conjugates. It follows from $\beta_1\beta_2 = \beta_1\gamma_1 = l$ that $\beta_1$ has absolute value $\sqrt{l}$ for $i = 1, 2$. Since $\beta_1$ and $\beta_2$ are non-conjugate imaginary quadratic integers with the same norm, they have distinct trace. It follows that $x \mapsto (\beta_1, \beta_2)$ gives an isomorphism

$$K = \mathbb{Q}[X]/(P^2_x) \cong \mathbb{Q}(\beta_1) \oplus \mathbb{Q}(\beta_2).$$

To prove the remainder of the lemma, put

$$e = x + x' - \text{Tr} \beta_1 \in \text{End}(A),$$

and let $k = \text{Tr}(\beta_2) - \text{Tr}(\beta_1) \neq 0$. The relation $e^2 = ke$ holds on the two $\beta_i$-eigenspaces $V_i$ of the analytic representation of $x$ in $\mathbb{C}^g$ and hence on $A$. We see that $e/k \in \text{End}_\mathbb{Q}(A)$ satisfies

$$(e/k)' = e/k \quad \text{and} \quad (e/k)^2 = e/k,$$
i.e., $e/k$ is a symmetric idempotent in the endomorphism algebra. Let $n \mid k$ be the smallest positive integer such that $ne/k$ is an endomorphism and let $E_1$ be its image. It is clear that $E_1 = V_2/(V_2 \cap \Lambda)$ is an elliptic curve inside $A = \mathbb{C}^\ell/\Lambda$.

The element $1 - e/k$ is also a symmetric idempotent, and we let $E_2$ be the image of $(1 - e/k) \in \text{End}(A)$. The subvariety $E_2$ is also an elliptic curve, and it is the complementary subvariety of $E_1$ in $A$. We claim that the ‘addition map’

$$
(\lambda, \lambda) \mapsto \lambda + \lambda
$$

is an $(n, n)$-isogeny.

To prove the claim, we note that $\lambda$ is an isogeny by a corollary to Poincaré’s reducibility theorem [2, Cor. 5.3.6]. Using the isomorphism $\text{End}(A) \to \text{NS}(A)$ between the symmetric endomorphisms of $A$ and its Néron-Severi group, see e.g. [2, Thm. 5.2.4], we see that the restriction of the polarization $\varphi_A$ to $E_i$ is the polarization $\varphi_{E_i} \circ [n]$.

It remains to show that $\ker \lambda$ is contained in $(E_1 \times E_2)[n]$. This follows from the argument in [11, Sec. 2] showing that $\ker \lambda$ is isomorphic to both $E_1[n]$ and $E_2[n]$. □

If the ring $\mathbb{Z}[\beta]$ is contained in the endomorphism ring of $E$, then we automatically have $E \cong \mathbb{C}/\mathfrak{a}$ for a $\mathbb{Z}[\beta]$-ideal $\mathfrak{a}$. It is well understood how to compute an algebraic model of $\mathbb{C}/\mathfrak{a}$, we refer to [6] for details. Once the finitely many candidates for $E_1$ and $E_2$ are computed, there are only finitely many possibilities for $n$ and $\lambda$, hence for $A$.

3.2. $K$ is a field. We continue with the case that $K = \mathbb{Q}[x]$ is a field. The following lemma restricts the structure of $K/\mathbb{Q}$.

**Lemma 3.2.** Let $A$ and $K = \mathbb{Q}[x]$ be as above. Suppose that $K$ is a field. Then $K$ is either a quadratic field or a degree-4 CM-field, i.e., a degree-4 number field $K$ such that complex conjugation induces the same automorphism of $K$ for every embedding $K \to \mathbb{C}$. In both cases, the Rosati-involution $\tau$ is complex conjugation on $K$.

**Proof.** See [2, Sec. 5.5]. □

**Example 3.3.** Let $\mathbb{Q}[x]$ be a quadratic field over $\mathbb{Q}$ and suppose that we have $x\tau = l$. Then the trace of $x$ is at most $2\sqrt{l}$. In particular, for $l = 2$, we have $x \in \{ \sqrt{-2}, \frac{1}{2}(1 + \sqrt{-7}), 1 + \sqrt{-1}, \sqrt{2} \}$ up to sign and complex conjugation.

By Lemma 3.2, the field $K$ is quadratic or a degree-4 CM-field. In the former case, let $m(K) = 2$ and in the latter case let $m(K) = 1$. Writing $A = V/\Lambda$, there exists an isomorphism

$$
\Lambda \otimes \mathbb{Q} \cong K^{m(K)}.
$$

The lattice $\Lambda$ has a natural $\mathbb{Z}[x]$-module structure, and, under an isomorphism as above, corresponds to a $\mathbb{Z}[x]$-submodule $\mathcal{M}$ of $K^{m(K)}$ of rank 4 over $\mathbb{Z}$.

**Lemma 3.4.** Let $A, K, \tau, \mathcal{M}$ be as above. Then there exists a matrix $T \in \text{GL}_2(K)$ satisfying $(T')^T = -T$ such that $E(u, v) = \text{Tr}_{K/\mathbb{Q}}(u^T Tv')$ is the Riemann form inducing the principal polarization on $A$.

**Proof.** See [2, Prop. 9.2.3.] and [2, Prop. 9.6.5]. □
Example 3.5. If $K$ is a real quadratic field, then $^tI$ is the identity on $K$. The matrix $T$ therefore equals
\[
\begin{pmatrix}
0 & r \\
-r & 0
\end{pmatrix}
\]
for some $r \in K^*$.

Lemma 3.4 tells us that the surface $A$ yields a pair $(M, T)$ consisting of a $\mathbb{Z}[x]$-submodule $M$ of $K^{m(K)}$ and a matrix $T \in \text{GL}_2(K)$ such that the $\mathbb{Q}$-bilinear form $K^{m(K)} \times K^{m(K)} \rightarrow \mathbb{Q}$ given by $(u, v) \mapsto \text{Tr}_{K/\mathbb{Q}}(u^T T v')$ restricts to a $\mathbb{Z}$-bilinear form $M \times M \rightarrow \mathbb{Z}$ of determinant 1. Conversely, for a fixed algebraic integer $x$ and for a fixed pair $(M, T)$, Shimura gives an explicit complex analytic description [2, Sec. 9.8] of the subspace $S(M, T) \subset A_2$ of principally polarized abelian surfaces belonging to this pair $(M, T)$. The following theorem states that $S(M, T)$ is an irreducible variety and gives its dimension.

Theorem 3.6. Let $K$ be either a quadratic field or a degree-4 CM-field and let $\mathbb{Z}[x]$ be an order in $K$. Let $M$ be a $\mathbb{Z}[x]$-submodule of $K^{m(K)}$ of rank $m(K)$ and $T \in \text{GL}_2(K)$ a matrix satisfying $(T')^T = -T$. Suppose that the $\mathbb{Q}$-bilinear form $K^{m(K)} \times K^{m(K)} \rightarrow \mathbb{Q}$ given by $(u, v) \mapsto \text{Tr}_{K/\mathbb{Q}}(u^T T v')$ restricts to a $\mathbb{Z}$-bilinear form $M \times M \rightarrow \mathbb{Z}$ of determinant 1. Let $S(M, T) \subset A_2$ be the subspace of all principally polarized abelian surfaces that correspond to $(M, T)$. Then the following holds:

- if $K$ is real quadratic, then $S(M, T)$ is an irreducible (Humbert) surface,
- if $K$ is imaginary quadratic and $\det(T) > 0$, then $S(M, T)$ is an irreducible (Shimura) curve. For any abelian surface $A$ in $S(M, T)$, the polynomial $P_x$ is the minimal polynomial of $x$;
- if $K$ is imaginary quadratic and $\det(T) < 0$, then $S(M, T)$ consists of one abelian surface $A$, which is isogenous as an unpolarized surface to a product $E \times E$ of an elliptic curve with itself. In this case we have $\text{End}_\mathbb{Q}(E) = K$ and $P_x = (x - \beta)^2$ for some $\beta \in \mathbb{C}$;
- if $K$ is a degree-4 CM-field, then $S(M, T)$ consists of one abelian surface.

Proof. All cases are special cases of the theory in [2, §9.6], except the real quadratic case, which is a special case of [2, §9.2].

4. Finding All Abelian Surfaces

In this section we show how to explicitly compute the pairs $(M, T)$ that occur in the first four cases of Theorem 1.1. Our computations yield the proof of the Main Theorem as well.

Two pairs $(M_1, T_1)$ and $(M_2, T_2)$ as in Theorem 3.6 are called isomorphic if there exists a matrix $S \in \text{GL}_2(K)$ with
\[
S^{-1} M_1 = M_2 \quad \text{and} \quad S^T T_1 S' = T_2.
\]
Isomorphic pairs yield the same moduli subspace inside $A_2$, and to prove Theorem 1.1, it suffices to show that the number of isomorphism classes of pairs $(M_i, T_i)$ is finite.

If $\sigma$ is an automorphism of $K$, then also $(M, T)$ and $(\sigma M, \sigma T)$ yield the same moduli space. Hence, given $K$ and $x \in K$ we can describe all principally polarized abelian surfaces $A/C$ admitting an endomorphism $x$ with $\mathbb{Q}[x] = K$ by listing the isomorphism classes of pairs $(M_i, T_i)$ up to this action of $\text{Aut}(K)$. 
First assume that $K = \mathbb{Q}[x]$ is a quadratic field. Depending on $K$ and $(\mathcal{M}, T)$ we either get a surface, a curve or a point in the moduli space.

4.1. Real quadratic fields.

**Lemma 4.1.** Let $K = \mathbb{Q}[x]$ be real quadratic and let $\mathcal{O} = \mathbb{Z}[x]$ be an order in $K$. Let $(\mathcal{M}, T)$ be a pair consisting of an $\mathcal{O}$-submodule $\mathcal{M}$ of $K^2$ that is free of rank $4$ as a $\mathbb{Z}$-module and a matrix $T \in \text{GL}_2(K)$ that satisfies the conditions of Lemma 3.4. Then, up to isomorphism, we have

$$\mathcal{M} = \mathcal{O}_1 \oplus \mathcal{O}_1 \quad \text{and} \quad T = \delta(\mathcal{O}_1)^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where $\mathcal{O}_1 \supset \mathcal{O}$ is an order of $K$ and $\delta(\mathcal{O}_1) = 2\alpha - \text{Tr} \alpha$ generates the different of $\mathcal{O}_1 = \mathbb{Z}[\alpha]$.

**Proof.** Let $(\mathcal{M}, T)$ be a pair consisting of an $\mathcal{O}$-module of $\mathbb{Z}$-rank 4 and a matrix $T$ satisfying the conditions of Theorem 3.6. As $\mathcal{O}$ is quadratic, every ideal is generated by 2 elements as a $\mathbb{Z}$-module, hence in particular as an $\mathcal{O}$-module. By Bass [1, Prop. 1.5], this implies that every finitely generated projective $\mathcal{O}$-module is the direct sum of ideals of $\mathcal{O}$. For $\mathcal{M}$ of rank 4 over $\mathbb{Z}$, this implies (after a suitable choice of basis) $\mathcal{M} = a \oplus b$ for fractional (not necessarily invertible) $\mathcal{O}$-ideals $a, b$. By Example 3.5, we know that $T$ is of the form

$$\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix}$$

for some $c \in K^*$. We derive that $a$ has trace dual $a^\dagger = bc$, and as a consequence we see that $a$ and $b$ have the same multiplier ring $\mathcal{O}_1$. An argument similar to [13, Prop. 3.4] shows that we have $abc = \delta(\mathcal{O}_1)^{-1}$, and $b$ therefore equals $(\delta(\mathcal{O}_1)c)\mathcal{O}_1^{-1}$ as $\mathcal{O}_1$-ideal. Without loss of generality, we may therefore assume that we have $a = \mathcal{O}_1$ and hence $bc = \mathcal{O}_1^\dagger = (1/\delta(\mathcal{O}_1))\mathcal{O}_1$. Then after scaling we get $\mathcal{M} = \mathcal{O}_1 \times \mathcal{O}_1$ and $c = 1/\delta(\mathcal{O}_1)$, which proves the lemma.

**Corollary 4.2.** Let $l$ be prime. Then the variety $\mathcal{M}^{(l)}_2$ contains exactly two irreducible Humbert surfaces for $l \equiv 1 \mod 4$ and exactly one irreducible Humbert surface otherwise.

**Proof.** The ring $\mathbb{Z}[\sqrt{l}]$ has index 2 in the maximal order of $K = \mathbb{Q}(\sqrt{l})$ for $l \equiv 1 \mod 4$ and equals the maximal order otherwise. By Lemma 4.1 and Theorem 3.6, we get two surfaces for $l \equiv 1 \mod 4$: one surface for $\mathcal{M} = \mathbb{Z}[\sqrt{l}]^2$ and one for $\mathcal{M} = \mathcal{O}_K^2$. In the other case, we find only one $\mathcal{M}$ and hence only one Humbert surface.

Alternatively, this result is the special case $t = 1$ of [24, Thm. IX.2.4], which states that the Humbert surface $H_D$ of discriminant $D$ is irreducible for every quadratic discriminant $D$. For $D = 4l$ prime with $l \equiv 1 \mod 4$, this gives one component $H_{D/4}$ and one component $H_D$. For $D = 4l$ with $l \not\equiv 1 \mod 4$, we have only the irreducible surface $H_D$. 

4.2. Imaginary quadratic fields. The situation is similar for imaginary quadratic fields $K$: we again have to list all pairs $(\mathcal{M}, T)$ for the order $\mathcal{O} = \mathbb{Z}[x]$. We may proceed analogously to the proof of Lemma 4.1 and write $\mathcal{M} = a \oplus b$ for fractional $\mathbb{Z}[x]$-ideals $a, b$. However, since we have less control over the matrix $T$, we cannot derive that $\mathcal{M} = \mathcal{O}_1 \oplus \mathcal{O}_1$ for an order $\mathcal{O}_1 \supset \mathcal{O}$ in this case.
For $\mathcal{O} = \mathbb{Z}[x]$, let $\delta(\mathcal{O}) = 2x - \text{Tr}(x)$ be the different of $\mathcal{O}$. Then, for the matrix $S = \delta T$, the condition $T^T = -T$ is equivalent to $S^T = S$, in other words, to $S$ being Hermitian. There seems to be a lot of theory related to the classification of pairs $(\mathcal{M}, S)$ that one could try to apply to the problem of enumerating these pairs. For example, Hayashida-Nishi [8] computes the class number of pairs $(\mathcal{M}, S)$ with $S$ positive definite, Shimura [20] computes the class number of pairs where $\mathcal{M}$ is a so-called “maximal lattice”, and we will see below how to associate to $S$ the structure of a quaternion algebra on $\mathcal{M} \otimes \mathbb{Q}$, making $\mathcal{M}$ into an ideal for an order $B$ in this quaternion algebra, and one might hope to use results on class numbers of $B$. However, such results all require $\mathcal{O}$ (or possibly even $B$) to be a maximal order. General results that do not require maximal orders seem to be lacking, hence we will give a more direct approach below.

**Lemma 4.3.** If $\mathcal{M} \supset \mathcal{O} \times \mathcal{O}$, then we have $[\mathcal{M} : \mathcal{O} \times \mathcal{O}] = \pm \det S$.

**Proof.** The determinant of $E : (u, v) \mapsto \text{Tr}_{K/\mathbb{Q}}(u^T T v')$ with respect to a $\mathbb{Z}$-basis of $\mathcal{O} \times \mathcal{O}$ can be computed to be $(\det S)^2$. With respect to a $\mathbb{Z}$-basis of $\mathcal{M}$, it therefore equals $[\mathcal{M} : \mathcal{O} \oplus \mathcal{O}]^{-2}(\det S)^2$. On the other hand, as the polarization is principal, this determinant is known to be 1, which proves Lemma 4.3. □

Applying complex conjugation to $(\mathcal{M}, T)$ if needed, we may assume that $S$ is not negative definite. Write $\Phi(u, v) = u^T S v'$ and $\mu(u) = \Phi(u, u)$. We distinguish two cases: the case where $\mu$ takes the value 0 on $\mathcal{M}$ and the case where it doesn’t.

If $\mu$ does not take the value 0. Take a $K$-basis $b_1, b_2$ of $\mathcal{M} \otimes \mathbb{Q}$ with $b_1, b_2 \in \mathcal{M}$, and choose this basis such that $|\mu(b_1)|$ is minimal over all $b_1 \in \mathcal{M}$, and $|\mu(b_2)|$ is minimal among all $b_2 \in \mathcal{M}$ that satisfy $\Phi(b_1, b_2) = 0$.

Let $a = \mu(b_1)$ and $b = \mu(b_2)$, and identify $\mathcal{M} \otimes \mathbb{Q}$ with $K^2$ via the basis $b_1, b_2$.

**Lemma 4.4.** We have

\[(1) \quad \mathcal{O} \times \mathcal{O} \subset \mathcal{M} \subset (\frac{1}{a}\mathcal{O}) \times (\frac{1}{b}\mathcal{O}),\]

where for both inclusions the index is $|ab|$.

\[(2) \quad 1 \leq |a| \leq \frac{2\text{d}(\mathcal{O})^{1/2}}{\pi} \quad \text{and} \quad |a| \leq |b| \leq 4\text{d}(\mathcal{O})^{3/2}/\pi^2 + \frac{4 + \text{d}(\mathcal{O})}{4},\]

with $t = 1$ if $S$ is indefinite, and $t = 2$ if $S$ is definite.

**Proof.** Note that $b_1 = (1, 0)^T$ and $b_2 = (0, 1)^T$ are in the $\mathcal{O}$-module $\mathcal{M}$, hence $\mathcal{M} \supset \mathcal{O} \times \mathcal{O}$. Now take any element $(u, v)^T$ in $\mathcal{M}$. Then we have $au = \Phi(u, b_1) \in \mathcal{O}$ and $bv = \Phi(u, b_2) \in \mathcal{O}$, which proves the inclusions in (1). The index of both inclusions is $|ab|$ by Lemma 4.3.

The body $V = \{(u, v)^T \in \mathbb{C}^2 : \text{max}\{|a|u\overline{a}, |b|v\overline{v}| \leq B\}$ is closed, convex and symmetric of volume $\pi^2 B^2/|ab|$, which for $B = 2\text{d}(\mathcal{O})^{1/2}/\pi$ is equal to $4[M : \mathcal{O} \times \mathcal{O}]^{-1}\text{d}(\mathcal{O}) = 16\text{covol}(\mathcal{M})$. By Minkowski’s convex body theorem, this implies that $V \cap \mathcal{M}$ contains a non-zero element $z = (u, v)^T$. We find $|\mu(z)| = |au\overline{a} + bv\overline{v}| \leq tB$, hence by choice of $b_1$ also $|a| \leq tB$. 

---

**ABELIAN SURFACES ADMITTING AN $(l,l)$-ENDOMORPHISM**

9
Finally, let

\[ W = \{(u, v)^T \in \mathbb{C}^2 : |\text{Re}(u)| < \frac{1}{|a|}, |\text{Im}(u)| < \frac{d(\mathcal{O})^{1/2}}{2|a|}, |b| v \pi \leq C \}, \]

so

\[ \text{vol}(W) = 2\pi \frac{d(\mathcal{O})^{1/2}}{a^2 |b|}, \]

which for \( C = 2tBd(\mathcal{O})/\pi = 4td(\mathcal{O})^{3/2}/\pi^2 \) is equal to \( 4d(\mathcal{O})/|ab| \cdot tB/|a| \geq 16c\text{vol}(\mathcal{M}) \). By Minkowski’s convex body theorem, this implies that \( V \cap \mathcal{M} \) contains a non-zero element \( z = (u, v)^T \). We find \( |\mu(z)| = |au\pi + bv\pi| \leq C + a\frac{4d(\mathcal{O})}{4\pi^2} \leq C + \frac{4d(\mathcal{O})}{4\pi^2} \), hence by choice of \( b_2 \), the number \( |b| \) is below this bound, which proves part (2).

If \( \mu \) takes the value 0. Let \( b_1 \in \mathcal{M} \) with \( \mu(b_1) = 0 \) be such that \( zb_1 \in \mathcal{M} \) for \( z \in K \) implies \( |z| \geq 1 \). Then take \( b_2 \in \mathcal{M} \) such that \( a = \Phi(b_1, b_2) \in \mathcal{O} \) has minimal absolute value among all \( b_2 \) linearly independent of \( b_1 \), and such that \( b = \mu(b_2) \in \mathbb{Z} \) has minimal absolute value among all \( b_2 \) for the given value of \( a \).

Identify \( \mathcal{M} \otimes \mathbb{Q} \) with \( K^2 \) via the \( K \)-basis \( b_1, b_2 \).

**Lemma 4.5.** We have

1. \( \mathcal{M} \supset \mathcal{O} \times \mathcal{O} \) with index \( N(a) \),
2. \( 1 \leq N(a) \leq \pi^{-2} d(\mathcal{O}) \) and \( |b| \leq \frac{1}{2} |\text{Tr}_{K/\mathbb{Q}}(a)| \leq |a| \)

**Proof.** As the basis elements \( b_1 = (1, 0) \) and \( b_2 = (0, 1) \) are in \( \mathcal{M} \), so is \( \mathcal{O} \times \mathcal{O} \). By Lemma 4.3, the index is \( \pm \text{det} S \). As we have \( -\text{det} S = N(a) > 0 \), this proves (1).

Let \( V = \{(u, v) \in \mathbb{C}^2 : N(u), N(v) < 1 \} \), which has volume \( \pi^2 \) and note that \( \mathcal{M} \subset \mathbb{C}^2 \) has covolume

\[ \frac{d(\mathcal{O})}{4[\mathcal{M} : \mathcal{O} \times \mathcal{O}]} = \frac{d(\mathcal{O})}{4N(a)}. \]

By Minkowski’s convex body theorem, if \( \pi^2 > d(\mathcal{O})/N(a) \), then there exists a non-zero \( z = ub_1 + vb_2 \in \mathcal{M} \) with \( N(u), N(v) < 1 \). Now \( v = 0 \) contradicts minimality of \( b_1 \), hence \( z \) is linearly independent of \( b_1 \) and \( 0 < N(u) < 1 \) contradicts minimality of \( b_2 \). This proves \( \pi^2 \leq d(\mathcal{O})/N(a) \), which gives our upper bound on \( N(a) \).

By translation of \( b_2 \) via a \( \mathbb{Z} \)-multiple of \( b_1 \), we can always get \( |b| \leq \frac{1}{2} |\text{Tr}_{K/\mathbb{Q}}(a)| \).

**Example 4.6.** Let \( K = \mathbb{Q}(\sqrt{-2}) \) and let \( x \in K \) satisfy \( \mathcal{O}_K = \mathbb{Z}[x] \). Since \( \mathcal{O}_K \) has class number 1, the only projective \( \mathbb{Z}[x] \)-submodule of rank 2 of \( K \times K \) up to \( \text{GL}_2(K) \)-equivalence is

\[ \mathcal{M} = \mathcal{O}_K \times \mathcal{O}_K. \]

We want to find a complete set of representatives for the set of matrices \( T \in \text{GL}_2(K) \) that fit into a pair \( (\mathcal{M}, T) \), up to isomorphism and complex conjugation of that pair.

Let \( \delta = (x - \overline{x}) = 2\sqrt{-2} \) denote the different of \( \mathcal{O}_K \). Let \( S = \delta T \) be the Hermitian matrix corresponding to \( T \). In this situation, we can use the technique of [8, §5] instead of the method of the current section. We find that

\[ T_1 = \frac{1}{\delta} \left( \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \quad \text{and} \quad T_2 = \frac{1}{\delta} \left( \begin{array}{cc} 2 & \sqrt{-2} + 1 \\ -\sqrt{-2} + 1 & 2 \end{array} \right) \]
are representatives of the two isomorphism classes for positive definite \( S \). Each corresponds to a point in the moduli space.

We find that there are exactly two isomorphism classes with \( \det S < 0 \), and they are represented by

\[
T_3 = \frac{1}{\delta} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad T_4 = \frac{1}{\delta} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},
\]

each yielding a Shimura curve.

4.3. Degree-4 CM-fields. Let \( K \) be a degree-4 CM-field, and fix an order \( \mathcal{O} \subset K \) with \( \mathcal{O} = \mathcal{O}_0 \).

We want to enumerate the isomorphism classes of pairs \((\mathcal{M}, T)\), where \( \mathcal{M} \subset K \) is an \( \mathcal{O} \)-module of rank 4 over \( \mathbb{Z} \) and \( T = (\xi) \) is a \( 1 \times 1 \)-matrix such that

1. \( \xi \) is totally negative;
2. the bilinear form \( E : \mathcal{M} \times \mathcal{M} \to \mathbb{Q} \) given by \( E(x, y) = \text{Tr}_{K/\mathbb{Q}}(\xi xy) \) has image \( \mathbb{Z} \) and determinant 1.

Recall that we call \((\mathcal{M}_1, \xi_1)\) isomorphic to \((\mathcal{M}_2, \xi_2)\) if and only if there exists \( u \in K^* \) satisfying \( u^{-1} \mathcal{M}_1 = \mathcal{M}_2 \) and \( u\mathcal{O}_1 = \mathcal{O}_2 \).

The fact that the image of the bilinear form is in \( \mathbb{Z} \) is equivalent to the inclusion of \( \mathcal{O} \)-ideals \( \xi\mathcal{M} \subset \mathcal{M}^* \), where \( \mathcal{M}^* \) is the dual of \( \mathcal{M} \) for the trace form \( (x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(xy) \). The determinant of \( E \) is 1 if and only if this inclusion is an equality, so we need to enumerate pairs \((\mathcal{M}, \xi)\) satisfying \( \xi\mathcal{M} = \mathcal{M}^* \), up to isomorphism.

This observation is a generalization of Theorems 3.13 and 3.14 of [22]. After we have listed all pairs \((\mathcal{M}, \xi)\), we can use e.g. the techniques from [25] to construct an algebraic model for the abelian variety corresponding to \((\mathcal{M}, \xi)\).

We now show how to compute the set of pairs \((\mathcal{M}, \xi)\) up to isomorphism. For any fractional \( \mathcal{O} \)-ideal \( \mathcal{M} \), write \( \mathcal{M}_K = \mathcal{M} \otimes_{\mathcal{O}} \mathcal{O}_K \). If \( e \) denotes the exponent of the abelian group \( \mathcal{O}_K/\mathcal{O} \), then for every \( \mathcal{M} \), we have \( e\mathcal{M}_K \subset \mathcal{M} \subset \mathcal{M}_K \). As a first step, we compute a complete set \( C \) of representatives of the class group of the maximal order \( \mathcal{O}_K \) of \( K \). For any \( \mathcal{N} \in C \), it is a finite computation to find all \( \mathcal{M} \) with \( \mathcal{M}_K = \mathcal{N} \). This gives us a complete set of representatives of the ideals \( \mathcal{M} \) up to multiplication by \( K^* \).

The next step is to find all possibilities for \( \xi \) for each \( \mathcal{M} \). Let \( \mathcal{O}(\mathcal{M}) = \{ x \in K : x\mathcal{M} \subseteq \mathcal{M} \} \) be the multiplier ring of \( \mathcal{M} \) and let \( K_0 \) be the real quadratic subfield of \( K \). For every pair \((\mathcal{M}, \xi)\), we have

\[
\xi\mathcal{M}_K \supseteq \xi\mathcal{M} = \mathcal{M}^* \supseteq \mathcal{M}_K^* = \mathcal{M}_K^{-1}\mathcal{D}_K^{-1} \quad \text{and} \quad e\xi\mathcal{M}_K \subseteq \xi\mathcal{M} = \mathcal{M}^* \subseteq e^{-1}\mathcal{M}_K^* = e^{-1}\mathcal{M}_K^{-1}\mathcal{D}_K^{-1} \mathcal{Q},
\]

so for every valuation \( v \) of \( K \), we have

\[
-2v(e) \leq v(\xi\mathcal{M}_K\mathcal{M}_K\mathcal{D}_K/\mathcal{Q}) \leq 0.
\]

This gives finitely many candidate ideals \( \xi\mathcal{O}_K \). For each, we can check whether it is principal and generated by an element \( \xi \in K \) such that \( \xi^2 \) is totally negative.

If so, let \( U \) be a complete set of representatives of those classes \( \mathcal{N} \) in the finite group \( \mathcal{O}^*_K/\mathcal{N}_K/\mathcal{D}_K(\mathcal{O}(\mathcal{M})^*) \) for which \((\mathcal{M}, u\xi)\) satisfies (1) and (2) above. The pairs \((\mathcal{M}, u\xi)\) cover all isomorphism classes.
4.4. The main Theorem. In this section we put all the theory developed up to
now into action and give a proof of Theorem 1.1.

Proof of Theorem 1.1. Fix a prime \( l \), and let \( A \in \mathcal{M}_2^{(l)} \) be a principally
polarized abelian surface. For an \((l,l)\) endomorphism \( x : A \to A \) we write \( K = \mathbb{Q}[x] \).
There are two possibilities: \( K \) is a field or it is not.

If \( K \) is not a field, Lemma 3.1 gives restrictions on \( x \). Using the notation of
this lemma, we note that there are only finitely many pairs \((\beta_1, \beta_2)\) of imaginary
quadratic elements of complex absolute value \( \sqrt{l} \). For each pair, there are finitely
many isomorphism classes of complex elliptic curves \( E_i \) with \( \text{End}(E_i) \supseteq \mathbb{Z}[\beta_i] \).
Finally, for each pair of curves \((E_1, E_2)\) there are finitely many possibilities for the
kernel of \( \lambda \). This means that there are only finitely many choices for \((A, x)\). These choices correspond to case (5) of Theorem 1.1.

Now suppose that \( K \) is a field. First we show that there are only finitely many
possibilities for \( K \). By Lemma 3.2, the degree of \( K/\mathbb{Q} \) divides four and the Rosati
involution equals complex conjugation on \( K \subset \mathbb{C} \). If there exists a real embedding,
then we have \( K = \mathbb{Q}(\sqrt{l}) \). Otherwise, \( K \) is a CM-field of degree two or four. In
both cases, \( x \) is a non-real algebraic integer and \( x + x' \) is in every real absolute
value less than \( 2\sqrt{l} \), which implies that the set of possible \( K \)'s is finite.

Theorem 3.6 associates to every pair \((\mathcal{M}, T)\), consisting of a \( \mathbb{Z}[x]\)-submodule of
\( K^m(K) \) and a matrix \( T \in \text{GL}_2(K) \) with \((T')^T = -T \), a moduli space \( S(\mathcal{M}, T) \subset \mathcal{A}_2 \).
The surface \( A \) is contained in some space \( S(\mathcal{M}, T) \) and, conversely, for every \((\mathcal{M}, T)\)
we have \( S(\mathcal{M}, T) \subset \mathcal{M}_2^{(l,l)} \). Hence, it remains to show that there are only finitely
many isomorphism classes of pairs \((\mathcal{M}, T)\).

For real quadratic \( K \), the number of pairs \((\mathcal{M}, T)\) correspond to the number
of orders \( \mathbb{Z}[x] \subseteq \mathcal{O} \subseteq \mathcal{O}_K \). It is classical that there are only finitely many such
orders \( \mathcal{O} \). This is case (1) of Theorem 1.1 and the proof follows from Theorem 3.6
and Corollary 4.2 above.

For imaginary quadratic \( K \), Lemmas 4.5 and 4.4 bound the index \([\mathcal{M} : \mathbb{Z}[x] \times \mathbb{Z}[x]]\) in terms of the discriminant of \( \mathbb{Z}[x] \). This implies that there are only finitely
many choices for \( \mathcal{M} \). The matrix \( T \) is

\[
\delta^{-1} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{or} \quad \delta^{-1} \begin{pmatrix} 0 & a' \\ a & b \end{pmatrix}
\]

respectively for the cases of Lemmas 4.4 and 4.5. These are cases (2) and (3) of
Theorem 1.1.

Finally, assume that \( K \) is a degree-4 CM-field. This is case (4) of Theorem 1.1.
Section 4.3 gives an algorithm for explicitly computing all pairs \((\mathcal{M}, T) = (\mathcal{M}, (\xi))\)
and we show that this approach terminates in a finite amount of time. Going
through the computations done in the algorithm, we note that since the class group
of \( \mathcal{O}_K \) is finite, there are only finitely many ideal classes \( \mathcal{N} \). For any \( \mathcal{N} \), there are
only finitely many \( \mathcal{M} \) with \( \mathcal{M} \otimes \mathcal{O} \mathcal{O}_K = \mathcal{N} \) because we can restrict to those \( M \)
satisfying \( e \mathcal{N} \subseteq \mathcal{M} \subseteq \mathcal{N} \), where the exponent \( e \) of \( \mathcal{O}_K/\mathcal{O} \) is finite. Hence, there
are only finitely many choices for \( \mathcal{M} \). As explained in Section 4.3, the valuations
of \( \xi \) are bounded, so there are only finitely many choices for the principal \( \mathcal{O}_K \)-ideal
generated by \( \xi \).  \( \square \)
5. Endomorphism rings, and decompositions into elliptic curves

Next, we recall the endomorphism rings corresponding to each of the cases mentioned above. For details, see [19] or [2, Exercises 9.10(3) and (4)].

In some cases, we can use this information to write our abelian surfaces as glueings. In the remaining cases, we can use it to write our Shimura curves as components of intersections of Humbert surfaces.

If \( S \) is definite, then the endomorphism \( \phi \) acts on \( V \) by multiplication by a complex number \( \beta \). Any decomposition of \( M \otimes \Q \) as \( K \times K \) yields a decomposition of \( V = M \otimes \R \) into 1-dimensional complex subspaces \( V_1 \) and \( V_2 \). We find elliptic curves \( E_i = V_i/(V_i \cap M) \) and an isogeny \( E_1 \times E_2 \to A \), which allows us to find \( A \) by glueing (see Section 6) elliptic curves with endomorphism ring containing \( \Z[x] \).

Moreover, we find that \( \text{End}(A) \otimes \Q \) contains \( \text{Mat}_2(K) \), which acts on \( M \subset \K \times \K \).

In fact, the ring \( \text{End}(A) \) equals the set of elements of \( \text{Mat}_2(K) \) that multiply \( M \) into itself. We give an example of this construction in the proof of Lemma 7.1.

If \( S \) is indefinite, then we give \( B = M \otimes \Q \) a quaternion algebra structure induced by \( S \) as defined by e.g. [20]. This quaternion algebra structure is easiest described by choosing a \( K \)-basis of \( B \) that diagonalizes \( S \) as \( \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix} \).

Denote the first basis element of \( B \) by 1 and the second by \( \rho \), so elements of \( B \) are written as \( x + y\rho \) with \( x, y \in K \). Then \( B \) becomes a quaternion algebra with \( \rho^2 = -s > 0 \), \( \rho u = \overline{\pi} \rho \) for \( u \in K \). The quaternion algebra \( B \) comes equipped with a positive definite involution \( \dagger \) given by \( (x + y\rho)^\dagger = \overline{x} + y\rho \).

The quaternion algebra \( B \) acts on \( M \otimes \Q \) (that is, on itself) by left multiplication, and Shimura showed that this induces an embedding \( \iota : B \to \text{End}(A) \otimes \Q \). Moreover, the Rosati-involution on \( \text{End}(A) \) induces \( \dagger \) on \( B \), and \( R = \iota^{-1}(\text{End}(A)) \) consists exactly of those elements of \( B \) that map \( M \) to itself.

If we now take a maximal real quadratic subring \( R_1 \subset R \) on which \( \dagger \) is trivial, then the Shimura curve corresponding to \( (M, S) \) is contained in the Humbert surface of \( R_1 \). If we take two such subrings \( R_1 \) and \( R_2 \) with non-isomorphic fraction fields, then the intersection of the corresponding Humbert surfaces is a finite union of irreducible curves, and one of these curves is our Shimura curve.

We will not need to do the construction above for the case where \( x \) is a \( (2, 2) \)-isogeny, because we can then always use the following construction.

Suppose still that \( S \) is indefinite. Then \( \mu \) takes the value 0 if and only if \( B \) is \( \text{Mat}_2(Q) \). If this is the case, then the symmetric idempotents of \( B \) show that \( A \) is isogenous to a product of elliptic curves \( E \) and \( F \), and the structure of \( B \) gives rise to an isogeny \( E \to F \). The degree \( d \) of this isogeny is constant on our Shimura curve. In particular, the candidate pairs \( (E, F) \) are parametrized by the modular polynomial \( \Phi_d \), and we can obtain \( A \) from \( \Phi_d \) via glueing techniques. We give an example of this construction in the proof of Lemma 7.2.

6. Glueings

In this section we recall how to glue two elliptic curves to obtain a Jacobian of a genus-2 curve. Glueing is a method for explicitly exhibiting abelian surfaces that are \( (n, n) \)-isogenous to a given pair of elliptic curves. This will enable us to explicitly
compute the abelian surfaces that occur for \( K = \mathbb{Q}[x] \) imaginary quadratic or not a domain. We will illustrate this method for \( n = 2 \) in the next section.

6.1. **Glueing Elliptic Curves.** Let \( E_1 \) and \( E_2 \) be complex elliptic curves and let \( n \in \mathbb{Z}_{>1} \) be an integer. Let \( \psi : E_1[n] \to E_2[n] \) be an anti-isometry with respect to the Weil pairing, i.e., an isomorphism such that \( e_n(\psi(P), \psi(Q)) = e_n(P, Q)^{-1} \) holds for all \( P, Q \in E_1[n] \). If \( \psi \) is an anti-isometry, then graph \( \psi \) is maximally isotropic with respect to the Weil pairing on \( (E_1 \times E_2)[n] \). By Lemma 2.5, this implies that graph \( \psi \) is the kernel of an \((n, n)\)-isogeny to a unique principally polarized abelian variety \( A = (E_1 \times E_2)/\text{graph } \psi \). We say that we glue \( E_1 \) and \( E_2 \) along their \( n \)-torsion via \( \psi \) and call the \((n, n)\)-isogeny \( E_1 \times E_2 \to A \) an \( n \)-glueing.

The following shows that glueings are a very general kind of \((n, n)\)-isogenies.

**Lemma 6.1.** Let \( E_1, E_2 \) be elliptic curves and \( n \) a prime number. Then every \((n, n)\)-isogeny \( E_1 \times E_2 \to A \) for any \( A \) is either an \( n \)-glueing or of the form \( E_1 \times E_2 \to (E_1/C_1) \times (E_2/C_2) \) for \( C_1 \subset E_1 \) of order \( n \).

**Proof.** It suffices to prove that every isotropic subgroup \( \Gamma \subset E_1 \times E_2 \) with \( \Gamma \cong (\mathbb{Z}/n\mathbb{Z})^2 \) is either of the form \( C_1 \times C_2 \) or is the graph of an anti-isometry \( E_1 \to E_2 \).

There are \((n^2 - 1)/(n - 1)\) maximally isotropic subgroups by Lemma 2.5, of which

\[
((n^2 - 1)/(n - 1))^2 = n^2 + 2n + 1
\]

are products \( C_1 \times C_2 \) and \((n^2 - 1)n = n^3 - n \) are graphs of anti-isometries. As we have \((n^4 - 1)/(n - 1) = (n^2 + 2n + 1) + (n^3 - n)\), this covers all cases. \(\square\)

Some glueings are the Jacobian of a genus-2 curve. In fact, we have the following result.

**Theorem 6.2** (Kani [10, Thm. 3]). Let \( (E_1, E_2, n, \psi) \) be as above Lemma 6.1 and assume \( n \) is prime. Then the glueing associated to this pair is the Jacobian of a genus-2 curve if and only if there do not exist an integer \( k \) strictly between 0 and \( l \) and an isogeny \( h : E_1 \to E_2 \) of degree \( k(n - k) \) with the property

\[
h|_{E_1[n]} = k \circ f.
\]

We can explicitly write down algebraic equations for glueings for small primes \( n \). The case \( n = 2 \) goes back to Legendre. Explicit constructions for \( n = 3 \) are more recent [11] and the case \( n = 5 \) is still actively studied [18]. We recall the constructions for \( n = 2, 3 \) in the remainder of this section.

6.2. **2-glueing.** We now make the case \( n = 2 \) more explicit. We follow Serre’s explanation [17, Sec. 27] of Legendre’s method. Let \( (E_1, E_2, n = 2, \psi) \) be as above and write each curve \( E_i \) in the form \( E_i : y^2 = g_i \) for a cubic polynomial \( g_i \in \mathbb{C}[x] \). We see that the double cover \( E_1 \to \mathbb{P}^1 \) given by the \( x \)-coordinate has four ramification points, which are exactly the points in \( E_1[2] = \{ P_1, P_2, P_3, P_4 \} \). Let \( Q_j = f\psi(P_j) \) and apply a fractional linear transformation of the \( x \)-coordinate of \( E_2 \) to get \( x(Q_3) = x(P_j) \) for \( j = 1, 2, 3 \).

**Remark 6.3.** By Theorem 6.2, the glueing corresponding to \((E_1, E_2, 2, \psi)\) as above is the Jacobian of a curve of genus 2 if and only if \( \psi \) is not of the form \( h|_{E_1[2]} \) for an isomorphism \( h : E_1 \to E_2 \), that is, if and only if \( x(Q_3) \) and \( x(P_4) \) are distinct.
Assume that we have \(x(Q_4) \neq x(P_4)\). Let \(K_1\) and \(K_2\) be the function fields of \(E_1\) and \(E_2\) as quadratic extensions of \(\mathbb{Q}(x)\) and let \(K_{12}\) be their composite. Let \(K_0 \subset K_{12}\) be the other intermediate extension of degree 2. The field \(K_0\) is ramified over \(\mathbb{Q}(x)\) only at \(x(P_j)\) and \(x(Q_4)\), so \(K_0\) has genus 0. The extension \(K_{12}/K_0\) is ramified in the 6 places of \(K_0\) lying over the three points \(x(P_j)\) for \(j = 1, 2, 3\). In particular, it follows from the Riemann-Hurwitz genus formula that the curve \(C\) with function field \(K_{12}\) has genus 2. The Jacobian of \(C\) is (2,2)-isogenous to \(E_1 \times E_2\) via an isogeny with kernel graph \(\psi\).

In terms of equations, Legendre’s glueing construction can be described as follows. Choose a Legendre model of \(E_1\) so that we have \(x(P_1) = \infty, x(P_2) = 0, x(P_3) = 1\) and let \(a = x(P_4)\). As above we have \(x(Q_j) = x(P_j)\) for \(j = 1, 2, 3\). Let \(b = x(Q_4) \neq a\), so \(E_1\) and \(E_2\) are given by

\[
E_1 : y^2 = x(x - 1)(x - a), \quad E_2 : y^2 = x(x - 1)(x - b).
\]

The curve \(C_0\) with function field \(K_0\) is given by \(C_0 : y^2 = (x - a)(x - b)\) and has a parametrization

\[
t \mapsto \left(x = a + \frac{(a-b)t^2}{1-t^2}, \quad y = \frac{(a-b)t}{1-t^2}\right).
\]

The extension \(K_{12}/K_0\) ramifies at the points with \(x \in \{\infty, 0, 1\}\), i.e., with \(t^2 \in \{1, a/b, (a-1)/(b-1)\}\). In particular, the genus-2 curve \(C = C(a, b)\) obtained by glueing \(E_1\) and \(E_2\) as above is:

\[
C(a, b) : s^2 = (t^2 - 1)(t^2 - \frac{a}{b})(t^2 - \frac{a-1}{b-1}).
\]

6.3. 3-glueing. In [11, Example 6], Kuhn studies 3-glueings and gives an example of a family of genus-2 curves \(C\) such that \(J(C)\) is the image of a \((3,3)\)-isogeny from a product of elliptic curves. The curve

\[
C : y^2 = (x^3 + ax^2 + bx + c)(4cx^3 + bx^2 + 2bcx + c^2)
\]

is a 3-glueing of two elliptic curves with \(j\)-invariants

\[
j(E_1) = \frac{16(972a^3 - 405bc^2 - 216ab^3c - 12b^5 - a^2b^4)^3}{(27c^2 - b^2)^3(27c^2 - 18abc + 4a^2c + 4b^3 - a^2b)\cdot 27c^2 - 18abc + 4a^2c + 4b^3 - a^2b^2}.
\]

We will use these formulas in our calculations in the next section.

7. The case of \((2,2)\)-endomorphisms

In this section, we give all principally polarized abelian surfaces that have a \((2,2)\)-isogeny to themselves. We use the computer algebra package MAGMA [3] to help us with the computations. We give some of them in terms of a hyperelliptic model of the form \(y^2 = f(x)\), and others in terms of their homogeneous Igusa invariants \(I_2, I_4, I_6, I_{10}\) (denoted \(A, B, C, D\) by Igusa [9] and \(A', B', C', D'\) by Mestre [15]). Mestre’s algorithm [15] computes a hyperelliptic model from these Igusa invariants.

We start by introducing short notation for the elliptic curves and curves of genus 2 that appear in our lists. If \(D\) is a negative quadratic discriminant and \(h(D)\) is the class number of the order \(\mathcal{O}_D\) of discriminant \(D\), let \(E_D^1, \ldots, E_D^{h(D)}\) be the isomorphism classes of elliptic curves over \(\mathbb{C}\) with endomorphism ring \(\mathcal{O}_D\). If
\(h(D) = 1\), then we denote \(E_D^1\) also by \(E_D\). Table 1 on page 16 defines a list of curves of genus 2 in terms of their Igusa invariants \(I_2, I_4, I_6, I_{10}\). All curves in the table are isogenous to a product of elliptic curves. In fact, these curves have a subscript \(D\) or \(D_1, D_2\) in their notations, and these subscripts indicate that their Jacobian is isogenous to \(E_D^1 \times E_D^1\) or \(E_D^1 \times E_D^1\).

Now that we have the notation for our output, let us compute all abelian surfaces with a \((2, 2)\)-endomorphism \(x\). In the case \(Z[x] = Z[\sqrt{2}]\), we know from Lemma 4.1 that there is only a single Humbert surface \(H_8\), which is computed by Gruenewald [7]. Now suppose \(Z[x]\) is imaginary quadratic. We start with the case where the Hermitian form \(S\) of Section 4.2 is definite.

**Lemma 7.1.** Let \(A\) be a principally polarized abelian surface over \(C\) and \(x : A \to A\) a \((2, 2)\)-isogeny. If \(Z[x]\) is imaginary quadratic and \(S\) of Section 4.2 is definite, then \(A\) is isomorphic to one of \(E_{-4} \times E_{-4}, E_{-7} \times E_{-7}, E_{-8} \times E_{-8}\), and \(J(C_{-8})\).

**Proof.** Example 3.3 shows that \(Z[x]\) is the maximal order of the imaginary quadratic field of discriminant \(D \in \{-4, -7, -8\}\). By replacing \((M, T)\) by its complex conjugate, we may assume that \(S\) is positive definite.

The case \(D = -8\) is the positive definite case of Example 4.6, which yields \(E_{-8} \times E_{-8}\) and exactly one other abelian surface. We will now construct that abelian surface. With respect to the basis \(\frac{1}{2}, \frac{1}{2}\sqrt{-2} \pmod{Z[\sqrt{-2}]\rangle}\) of \(E_{-8}[2]\), we have

\[
\sqrt{-2} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \text{and we define} \quad \psi = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.
\]

Let \(g : E_{-8} \times E_{-8} \to A = E_{-8} \times E_{-8}/(\text{graph } \psi)\) be the glueing of \(E_{-8}\) with itself along \(\psi\). Multiplication by \(x = \sqrt{-2}\) on \(E_{-8} \times E_{-8}\) sends graph \(\psi\) to itself because \(\psi\) and \(\sqrt{-2}\) commute on \(E_{-8}[2]\). In particular, the endomorphism \(x\) induces an endomorphism \(gxg^{-1} \in \text{End}(A)\). The fact that both \(x\) and the quotient map \(g\) are \((2, 2)\)-isogenies implies that \(gxg^{-1}\) is also a \((2, 2)\)-isogeny.

Using the formula of Section 6.2, we find \(A = J(C_{-8})\) with \(C_{-8}\) as in Table 1.

The cases \(D = -4\) and \(D = -7\) are analogous to Example 4.6, but yield only \(E_D \times E_D\), because there is only one positive definite isomorphism class of pairs \((M, S)\).

| \(C\) | \((I_2 : I_4 : I_6 : I_{10})(C)\) |
|---|---|
| \(C_{-3}\) | \((40 : 45 : 555 : 6)\) |
| \(C_{-6}\) | \((92 : 108 : 4104 : 24)\) |
| \(C_{-6}'\) | \((76 : 252 : 5160 : 24)\) |
| \(C_{-7}\) | \((10840 : 2004345 : 7846230105 : 131736761856)\) |
| \(C_{-8}\) | \((20 : -20 : -40 : 8)\) |
| \(C_{-15}\) | \((20 : 225 : 1185 : -384)\) |
| \(C_{-20}^{-}\) | \((-156 + 448i : -17620 + 840i : 690600 - 1793200i : 126664 + 4527152i)\) \((i^2 = -1)\) |
| \(C_{-4,-7}^{-}\) | \((8 + 20a : -1035 - 450a : 87246 + 33606a : 25164 + 9504a)\) \((a^2 = 7)\) |
| \(C_{-4,-8}\) | \((24 : 30 : 366 : 2)\) |

Table 1. A list of genus-2 curves and the homogeneous Igusa invariants that define them.
Lemma 7.2. Let $A$ be a principally polarized abelian surface over $\mathbb{C}$. There exists a $(2,2)$-isogeny $x : A \to A$ with $\mathbb{Z}[x]$ imaginary quadratic and $S$ indefinite, if and only if $A$ is a point on one of the following Shimura curves:

1. the curve in $\mathbb{A}_2$ of which the points are the products $E \times E$ of an elliptic curve $E$ with itself;
2. the curve in $\mathbb{A}_2$ of which the points are the products $E \times F$ for all 2-isogenies $E \to F$;
3. the Zariski closure of the image of the map $\mathbb{C} \setminus \{0,1\} \to \mathbb{A}_2$ given by $u \mapsto C(u,1-u)$, where $C(u,v)$ is given as in Section 6.2 by
   $$ C(a,b) : y^2 = (x^2 - 1)(x^2 - \frac{b}{a})(x^2 - \frac{b - 1}{a - 1}); $$
4. the Zariski closure of the image of the map $\mathbb{C} \setminus \{-1,0,1\} \to \mathbb{A}_2$ given by $u \mapsto C(u^2,\frac{(u-1)^2}{(u+1)^2})$;
5. the Zariski closure of the image of the map $X \to \mathbb{A}_2 : (u,v) \mapsto C(u,v)$, where $X \subset \mathbb{A}^2$ is given by Figure 1 on page 18.

Each of these 5 Shimura curves has genus 0.

Proof. As in the proof of Lemma 7.1, the ring $\mathbb{Z}[x]$ is the maximal order of the imaginary quadratic field of discriminant $D = -4, -7, \text{ or } -8$. This time, the case $D = -8$ is the indefinite case of Example 4.6. We find six Shimura curves, each corresponding to $\mathcal{M} = \mathbb{Z}[x] \times \mathbb{Z}[x]$ and

- $T = T_3 = \frac{1}{\delta} \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right)$ or $T = T_4 = \frac{1}{\delta} \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right)$.

Note that $T_3$ and $T_4$ are equivalent for odd $D$, so that we actually have only five distinct Shimura curves, which we will now compute.

Let $f : E \to F$ be a degree-$n$ isogeny of elliptic curves. If $a,b \in \mathbb{Z}$ are such that $a^2 + b^2n = l$, then we have an $(l,l)$-isogeny

$$ x = \left( \begin{array}{cc} a & bf' \\ -bf & a \end{array} \right) \in \text{End}(E \times F) $$

such that $\mathbb{Z}[x]$ is quadratic of discriminant $D = -4b^2n$. Indeed, we have $x^2 - 2ax + l = 0$ and $x' = 2a - x$, hence $x'x = l$.

The products $E \times F$ form a curve $S$ in the moduli space $\mathbb{A}_2$, and that curve $S$ is covered by the modular curve $Y_0(n)$ of $n$-isogenies $E \to F$. Any such $S$ is contained in one of the Shimura curves we are looking for. By the construction in [2, §9.6], the Shimura curves are irreducible, so that $S$ is in fact equal to one of the Shimura curves.

We apply the above to $l = 2$, $D = -4$, $n = a = b = 1$, $F = E$, $f = \text{id}_E$, which yields the Shimura curve of all squares $E \times E$ of elliptic curves $E$. We also apply it to $l = 2$, $D = -8$, $n = 2$, $a = 0$, $b = 1$, which yields the Shimura curve of all products $E \times F$ for which $F$ is 2-isogenous to $F$. We have now found 2 of our 5 Shimura curves.

We will find more Shimura curves by looking at $(k,k)$-isogenies $g : E \times F \to A$ for small $k$ and checking if the element $gxg^{-1} \in \text{End}_\mathbb{Q}(A)$ (with $x$ as above) is in $\text{End}(A)$. As in the proof of Lemma 7.1, the fact that $g$ is a $(k,k)$-isogeny and $x$
that every 2-isogeny \( f \) is an \((E, E)\) transformation of the x-coordinate sending \( \infty \) to itself and swapping 0 and 1 maps \( E \) to \( y^2 = x(x-1)(x-u) \) with \( u = 1 - v \). Therefore, we find \( E \times E/(\text{graph } \psi) \cong J(C(u, 1 - u)) \) as in Section 6.2.

For the case \( D = -8 \) (with \( n = l = 2, a = 0, b = 1 \)), recall from [21, Ex. 4.8] that every 2-isogeny \( f : E \to F \) can be written in the form
\[
E : y^2 = x(x-1)(x-a^2), \quad F : y^2 = x(x-1)(x-\frac{1-a}{1+a})^2
\]
with \( \ker f = \langle (0,0) \rangle \), \( \ker f' = \langle (0,0) \rangle \) and \( a \in C \setminus \{ -1, 0, 1 \} \). The map \( \psi : E[2] \to F[2] \) given by \( (0,0) \to (0,0) \) and \( (1,0) \to (1,0) \) satisfies \( \psi f' \psi = f \) and we find curve \( (4) \).

For the only remaining Shimura curve (with \( D = -7 \)), we apply the above to \( l = 8 \), \( D = -28 \), \( n = 7 \), \( a = b = 1 \). Let \( f : E \to F \) be a 7-isogeny and let \( \psi_j = f_j \mid [E[j] : E[j]] \). Let \( A = E \times F/(\text{graph} \, \psi_2) \) and let \( g \) be the quotient map. We need to show that \( \frac{1}{2}g x g^{-1} \) is an endomorphism of \( A \), i.e. that \( x \) maps \( 2^{-1} \text{graph} \, \psi_2 \) to \( \text{graph} \, \psi_2 \). Choose a basis of \( E[4] \). As \( f \) has odd degree, the image of this basis under \( f \) is a basis of \( E[4] \).

We have \( 2^{-1} \text{graph} \, \psi_2 = \text{graph} \, \psi_4 + (E[2] \times 0) \). Given \( P \in E[4] \), we find \( x(P, \psi_4(P)) = (P + f'_j \psi_4 P, -f P + \psi_4 P) = (8P, 0) = 0 \). Let \( P \in E[2] \) be any element. We find \( x(P,0) = (P, -f P) = (P, f P) \in \text{graph} \, \psi_2 \). This shows that indeed \( x \) maps \( 2^{-1} \text{graph} \, \psi_2 \) to \( \text{graph} \, \psi_2 \).

Next, let \( X \) be the set of triples \( x = (f, P_1, P_2) \) consisting of a 7-isogeny \( f : E \to F \) and a basis \( P_1, P_2 \) of the 2-torsion of \( E \). We will compute a model for the modular curve \( X \), together with the glueing map to \( A_2 \).

As before, let \( Y_0(1) \) be the modular curve of \( l \)-isogenies \( f : E \to F \). Let \( Y(l) \) be the modular curve of elliptic curves \( E \) together with a basis of the \( l \)-torsion. We have natural maps \( \pi_E, \pi_F : X \to Y(2) \), given by \( \pi_E(x) = (E, P_1, P_2) \) and \( \pi_F(x) = (F, f(P_1), f(P_2)) \), and natural maps \( \pi_E, \pi_F : Y_0(1) \to Y(1) = A_1 \), given by \( \pi_E : f \mapsto j(E) \) and \( \pi_F : f \mapsto j(F) \). See also Figure 2 on page 19. In fact, \( Y_0(1) \) is exactly the zero-locus of the modular polynomial \( \Phi_l \in \mathbb{Z}[X,Y] \) when \( X \) and \( Y \) are \( \pi_E \) and \( \pi_F \).

Next, we have \( Y(2) = C \setminus \{ 0, 1 \} \), where \( a \in C \setminus \{ 0, 1 \} \) corresponds to the elliptic curve \( y^2 = x(x-1)(x-a) \) with the basis \( (0,0), (1,0) \) of the 2-torsion. To glue \( E \) to \( F \) along graph \( f_j \) for all \( x \in X \), we need a description of \( X \) from which \( a = \pi_E(f) \) and \( b = \pi_F(f) \) can be read off. This means that we want a description of \( X \) as a subvariety of \( Y(2) \times Y(2) \). We have the natural map \( j : Y(2) \to Y(1) \) given by \( j(a) = 2^g(a^2 - a + 1)^3(a-1)^{-2}a^{-2} \). Let \( W = (j \times j)^{-1}(Y_0(7)) \), so \( X \subset W \subset Y(2) \times Y(2) \) and \( W \) is the zero locus of \( P = \Phi_7(j(u), j(v)) \in \mathbb{Q}[u,v] \).

We factor the numerator of \( P \) using MAGMA as a product of 6 irreducible polynomials in \( \mathbb{Q}[u,v] \). Note \( W = \sqcup X^\sigma \), where \( \sigma \in \text{Aut}(F[2]) \) acts by changing

![Figure 2](image-url)  
Figure 2. The curves \( X, Y(2), Y(1) \) and \( Y_0(7) \) from the proof of Lemma 7.2.
the basis of $F[2]$. As $\Aut(F[2])$ has order 6, we find that $X$ is the zero locus of exactly one of the 6 factors of the numerator of $P$.

To select the correct factor, we now prove that $S$ is a subset of the Humbert surface $H_8$. Let

$$y = \begin{pmatrix} 1 & f' \\ f & -1 \end{pmatrix}, \quad \text{so} \quad \frac{1}{2}(x - y) = \begin{pmatrix} 0 & 0 \\ -f & 1 \end{pmatrix}.$$  

We compute that $g^{1/2}(x - y)g^{-1}$ (and hence $g^{1/2}yg^{-1}$) is an endomorphism of $A$. We have $y' = y$ and $(\frac{1}{2}y)^2 = 2$, hence $S \subset H_8$. Using the defining equation for $H_8$ from [7], we find that exactly one out of our 6 candidates for $S$ lies on $H_8$, so we know that this is the correct one.

Now only the statement about the genus remains. The first two Shimura curves are birational to $Y(1)$ and $Y_0(2)$, which are known to have genus 0. The third and fourth are defined as the image of a rational map from $\mathbb{P}^1$, hence also have genus 0. We used MAGMA to compute that the genus of $S$ is also 0. \hfill $\square$

A Weil $q$-number is an algebraic integer $\pi$ such that $\pi\overline{\pi} = q$ for every embedding of $\pi$ into $\mathbb{C}$.

**Lemma 7.3.** If $K = \mathbb{Q}[x]$ is a quartic CM-field and $x$ is a Weil $2$-number, then the characteristic polynomial $P_x$ is an irreducible polynomial of degree 4 of the form

$$f = X^4 - a_1X^3 + (4 + a_2)X^2 - 2a_1X + 4,$$

where $a_1$ and $a_2$ are integers.

Tables 2 and 3 list exactly the possible pairs $(a_1, a_2)$ (up to replacing $x$ by $-x$ and $a_1$ by $-a_1$) such that $f$ is irreducible and its roots satisfy $x\overline{x} = 2$, together with all complex principally polarized abelian surfaces of which the endomorphism ring contains a subring isomorphic to $\mathbb{Z}[X]/f$. The Galois group of the field $\mathbb{Q}[X]/f$ is $C_2 \times C_2$ for $f$ as in Table 2 and $D_4$ for $f$ as in Table 3.

**Proof.** Suppose $x$ is a Weil $2$-number of degree 4 and let $\beta = x + 2/x = x + \overline{x}$, so $\beta$ is a totally real algebraic integer of degree at most 2. As we have $x^2 - \beta x + 2 = 0$,

| $a_1$ | $a_2$ | principally polarized abelian varieties |
|-------|-------|----------------------------------------|
| 0     | 7     | $E_{-7} \times E_{-7}$                |
| 0     | 6     | $J(C_{-8}), E_{-3} \times E_{-12}$    |
| 0     | 5     | $J(C_{-3}), E_{-3} \times E_{-3}, J(C_{-15}), E_{-15}^1 \times E_{-15}^2$ |
| 1     | 5     | $E_{-3} \times E_{-3}$                |
| 0     | -3    | $J(C_{-20}) (i^2 = -1), J(C_{-15}), E_{-15}^1 \times E_{-15}^2$ |
| 0     | -2    | $J(C_{-6}), J(C_{-6}^2), E_{-3} \times E_{-3}, E_{-3} \times E_{-12}$ |
| 2     | -2    | $E_{-3} \times E_{-3}, E_{-4} \times E_{-4}$ |
| 3     | 1     | $J(C_{-15}), E_{-3} \times E_{-3}$    |

Table 2. All Weil $2$-numbers that generate quartic fields that contain an imaginary quadratic subfield are roots of $f = X^4 - a_1X^3 + (4 + a_2)X^2 - 2a_1X + 4$ with $a_1, a_2$ as in the table. For each such Weil $2$-number $x$, the column on the right lists all principally polarized abelian surfaces over $\mathbb{C}$ of which the endomorphism ring contains $x$. 
we find that $\beta$ is not rational. Let $a_1$ be the trace of the real quadratic integer $\beta$ and $a_2$ its norm. Then $f$ as in the lemma is the minimal polynomial of $x$. As $x$ is non-real, we find that $\beta^2 - 8$ is totally negative, which gives upper bounds on the absolute values of $a_1$ and $a_2$. For all $a_1, a_2$ up to those bounds with $a_1 \geq 0$, we checked if $f$ is irreducible and its roots are Weil 2-numbers.

For each resulting $a_1, a_2$ where $K = \mathbb{Q}[x]$ is a quartic CM-field that does not contain an imaginary quadratic subfield, it turned out that $\mathbb{Z}[x, \overline{x}]$ is its ring of integers, and an algorithm to compute Table 3 is given in [23].

For the remaining cases, where $K = \mathbb{Q}[x]$ does contain an imaginary quadratic subfield, the precision needed for the complex analytic method as in [23] is not known, so we have to resort to alternative methods. The method of Section 4.3 gives at least one representative of each isomorphism class of principally polarized abelian varieties with the endomorphism $x$.

This already allows us to compute Table 2 by numerical approximation, without guarantee of correctness, using the same techniques as in [23].

To get a proof of the entries in the table, let $\phi_1, \phi_2$ be the two embeddings $K \to \mathbb{C}$ that map $\xi$ to the positive imaginary axis. Let $K_1 \subset K$ be the unique imaginary quadratic subfield such that $\phi_1$ and $\phi_2$ are equal on $K_1$. Then $A$ is isogenous to the square $E \times E$ of an elliptic curve $E$ with CM by the ring of integers $\mathcal{O}_{K_1}$ of $K_1$ (see [12, Theorem 1.3.5] or see the definite case in the discussion of Section 5). We can thus prove Table 2 by gluing techniques.

\textbf{Lemma 7.4.} Let $A$ be a principally polarized abelian surface over $\mathbb{C}$ and $x : A \to A$ a $(2, 2)$-isogeny. If $\mathbb{Q}[x]$ is not a field, then $A$ is one of the following:

\begin{enumerate}
  \item the 5 polarized products $E_{-4} \times E_{-4}, E_{-4} \times E_{-7}, E_{-4} \times E_{-8}, E_{-7} \times E_{-7}$ and $E_{-7} \times E_{-8},$
  \item the Jacobians of the 4 curves $C_{-7}, C_{-4,-8},$ and $C_{-4,-7},$ where $a^2 = 7$.
\end{enumerate}

Conversely, each of these abelian surfaces has such an endomorphism $x$.

\textbf{Proof.} Given $A$ and $x$, let $E_1, E_2, n, \lambda$ be as in Lemma 3.1. As we can interchange $E_1$ and $E_2$, and we can replace $x$ by $\pm x$ or $\pm \overline{x}$, we have without loss of generality $\text{Tr} \beta_1 > \text{Tr} \beta_2$, $|\text{Tr} \beta_1| \geq |\text{Tr} \beta_2|$, and $\text{Im} \beta_1 > 0$. 

| $a_1$ | $a_2$ | $(I_2 : I_4 : I_6 : I_{10})$ |
|-------|-------|-------------------------------|
| 1     | −4    | $(-36 + 36a : -45 : 46 : 5a : 28 - 20a), (a^2 = 2)$ |
| 1     | −3    | $(69 - 21a : 330 - 150a : 22416 - 5256a : -2792 + 680a), (a^2 = 17)$ |
| 1     | −1    | $(153 - 27a : 1098 - 162a : 135432 - 21168a : -7944 + 1240a), (a^2 = 41)$ |
| 2     | −1    | $(72 : 90 + 90a, -3132 + 2916a : 1152 - 128a), (a^2 = 17)$ |

Table 3. All Weil 2-numbers that generate quartic fields that do not contain an imaginary quadratic subfield are roots of $f = X^4 - a_1X^3 + (a_1 + a_2)X^2 - 2a_1X + 4$ with $a_1, a_2$ as in the table.

For each such Weil 2-number $x$, the principally polarized abelian surfaces over $\mathbb{C}$ of which the endomorphism ring contains $x$ are exactly the Jacobians of the curves of genus 2 of which the Igusa invariants are listed next to the values of $a_1$ and $a_2$. 

\begin{itemize}
  \item For each resulting $a_1, a_2$ where $K = \mathbb{Q}[x]$ is a quartic CM-field that does not contain an imaginary quadratic subfield, it turned out that $\mathbb{Z}[x, \overline{x}]$ is its ring of integers, and an algorithm to compute Table 3 is given in [23].
  \item For the remaining cases, where $K = \mathbb{Q}[x]$ does contain an imaginary quadratic subfield, the precision needed for the complex analytic method as in [23] is not known, so we have to resort to alternative methods. The method of Section 4.3 gives at least one representative of each isomorphism class of principally polarized abelian varieties with the endomorphism $x$.
\end{itemize}
Example 3.3 shows that $\mathbf{Z}[\beta_j]$ is the maximal order of the imaginary quadratic field of discriminant $-4, -7,$ or $-8,$ which has class number 1. Therefore, we get exactly one curve $E_j$ for a given $\beta_j$ and hence (1) lists exactly all examples with $n = 1.$

Now assume $n$ is minimal with the properties of Lemma 3.1, and suppose that $n \neq 1.$ Let $p|n$ be a prime and let $S = \ker \lambda \cap (E_1 \times E_2)[p].$ As $\lambda$ is an $(n, n)$-isogeny, its kernel is maximally isotropic in $(E_1 \times E_2)[n]$ by Lemma 2.5. This implies that $S$ is maximally isotropic in $(E_1 \times E_2)[p].$ By Lemma 6.1, it follows that $S$ is either a product $C_1 \times C_2$ of subgroups $C_j \subset E_j[p]$ of order $p,$ or $S$ is the graph of an anti-isometry $\psi : E_1[p] \rightarrow E_2[p].$ Moreover, as $(\beta_1, \beta_2)$ induces an endomorphism of $A,$ it sends $\ker \lambda$ to itself and hence sends $S$ to $S.$

Note that $S = C_1 \times C_2$ is not possible. Indeed, it would imply that $E_j/C_j$ has CM by $\mathbf{Z}[\beta_j]$ and that we have an $(n/p, n/p)$-isogeny $E_1/C_1 \times E_2/C_2 = (E_1 \times E_2)/S \rightarrow (E_1 \times E_2)/\ker \lambda = A,$ contradicting minimality of $n.$

Therefore, $S$ is the graph of an anti-isometry $\psi : E_1[p] \rightarrow E_2[p],$ and the fact that $(\beta_1, \beta_2)$ sends $S$ to itself implies that $\beta_2 \circ \psi = \psi \circ \beta_1$ holds on $E_1[p].$

Let $T = (\text{Tr}\beta_1 \mod p) = (\text{Tr}\beta_2 \mod p) \in \mathbf{Z}/p\mathbf{Z}.$ We find that we are in one of the following cases:

1. $\beta_1 = 1 + i,$ $\beta_2 = \pm i\sqrt{7},$ $p = n = 2,$ $T = 0,$
2. $\beta_1 = 1 + i,$ $\beta_2 = \frac{1}{2}(-1 \pm i\sqrt{7}),$ $p = n = 3,$ $T = -1,$
3. $\beta_1 = 1 + i,$ $\beta_2 = -1 \pm i,$ $p = 2,$ $n \in \{2, 4\},$ $T = 0,$
4. $\beta_1 = \frac{1}{2}(1 + i\sqrt{7}),$ $\beta_2 = \frac{1}{2}(-1 \pm i\sqrt{7}),$ $p = n = 2,$ $T = 1.$

We can dismiss case 3, and the special case of 4 where $\text{Im} \beta_2 < 0,$ because of the following argument. In those cases, we identify $E_1$ with $E_2$ and find that $\beta_2 - \beta_1$ is a multiple of 2 in the endomorphism ring of $E_1,$ hence $(\beta_1, \beta_2)$ and $(\beta_1, \beta_1)$ are equal on $(E_1 \times E_2)[2],$ showing that $(\beta_1, \beta_1)$ induces an endomorphism of $(E_1 \times E_2)/S$ with both eigenvalues of the analytic representation equal to $\beta_1.$ By Lemma 7.1 this implies that $(E_1 \times E_2)/S \cong E_1 \times E_2$ as a polarized abelian variety, contradicting minimality of $n.$

In case 1, the difference $\beta_2 - \overline{\beta_2}$ is a multiple of 2, so the above argument shows that the two possible signs lead to the same set of abelian surfaces. Therefore, can restrict to $\text{Im} \beta_2 > 0$ in this case without loss of generality.

Only the cases 1, 2, and 4 remain and in each of these cases except case 2, we can assume $\text{Im} \beta_2 > 0.$ The group $E_j[p] = (C/\mathbf{Z}[\beta_j])[p] = \frac{1}{p}(\mathbf{Z}[\beta_j]/p\mathbf{Z}[\beta_j]),$

has a basis $1/p, \beta_j/p$ and we express $\beta_j$ and $\psi$ by matrices with respect to these bases. The identity $\beta_2 \psi = \psi \beta_1$ puts some restrictions on the coefficients of $\psi.$ Moreover, the Weil pairing $\epsilon_p$ on $E_j[p]$ satisfies $\epsilon_p(1/p, \beta_j/p) = \exp(\pm(2\pi i)/p),$ where the sign is the sign of the imaginary part of $\beta_j.$ In particular, the map $\psi$ is an anti-isometry if and only if its determinant is $\pm(-1)$ in $\mathbf{Z}/p\mathbf{Z}.$ We now have a system of equations for the coefficients of $\psi,$ which we solve.

For case 1, we find 2 solutions, which yield isomorphic quotients $(E_1 \times E_2)/S,$ since the groups $S$ are mapped to each other by $\text{Aut}(E_1 \times E_2) = \text{Aut}(E_1) \times \text{Aut}(E_2).$ Glueing techniques show that the quotient is $J(C_{-4, -8}).$ For case 4, we find 1 solution, which yields $J(C_{-7}).$
Only case 2 remains. We find 4 solutions with \( \text{Im} \beta_2 > 0 \) and 4 solutions with \( \text{Im} \beta_1 < 0 \). Each of these sets of 4 solutions is an \( \text{Aut}(E_1 \times E_2) \)-orbit, so that there are at most 2 quotient abelian surfaces.

Section 6.3 gives Kühn’s parametrization of a set of curves \( C \) of genus 2 such that \( J(C) \) is the image of a \((3, 3)\)-isogeny from a product of elliptic curves. As this parametrization includes a formula for the \( j \)-invariants of \( E_1 \) and \( E_2 \), we can solve for \( j(E_2) = 1728 \) and \( j(E_1) = -3375 \) This yields equations for 6 pairwise non-isomorphic curves \( C \) of genus 2 of which the Jacobian is the image of a \((3, 3)\)-isogeny from \( E_1 \times E_2 \).

We claim that this list of 6 curves contains all curves \( C \) such that \( J(C) \) is \((3, 3)\)-isogenous to \( E_1 \times E_2 \). Indeed, the kernel of the isogeny \( E_1 \times E_2 \to J(C) \) is the graph of an anti-isometry by Lemmas 2.5 and 6.1. There are 24 anti-isometries from \( E_1[3] \) to \( E_2[3] \), which are partitioned into 6 orbits of composition with \( \mathbb{Z}[i]^* \) on the right, hence the list of candidate curves is complete.

The points in \( \mathcal{A}_2 \) corresponding to these candidate curves are partitioned into two Galois orbits over \( \mathbb{Q} \): one of length 2 and one of length 4. As we have found only two possibilities \( A = (E_1 \times E_2)/\text{graph}(\psi) \), and isomorphism classes of endomorphism rings over \( \mathbb{C} \) are invariant under conjugation over \( \mathbb{Q} \), our two \( A \) cannot lie in the Galois orbit of length 4, so they form the Galois orbit of length 2. They are the \( C_{-4, -7} \) listed in the lemma. Using the generators for \( W_2 \) computed in [5], we easily check that \( C_{-4, -7} \) indeed lies in the space \( W_2 \). \(\square\)

We now state and prove a more explicit version of Theorem 1.2.

**Theorem 7.5.** The reduced variety \( \mathcal{M}'_{2, 2} \) is the disjoint union of the Humbert surface \( H_8 \) of discriminant 8, which is irreducible, and the following 12 CM points:

1. \( E_{-4} \times E_{-7}, E_{-4} \times E_{-8}, E_{-7} \times E_{-8}, \)
2. \( C_{-15}, C_{-4, -8}, C_{a_{-4, -7}} \quad (a^2 = 7) \), and
3. the 6 CM points corresponding to the curves with \( a_1 = 1 \) of Table 3.

**Proof.** The variety \( \mathcal{M}'_{2, 2} \) is the union of \( H_8 \), the Shimura curves of Lemma 7.2, and the CM points of Lemmas 7.1, 7.3, and 7.4. For any elliptic curve \( E \), we have \( E \times E \in H_8 \) because of the endomorphism

\[
\begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}
\]

The same holds for any product \( E \times F \) where \( f : E \to F \) is a 2-isogeny, because of

\[
\begin{pmatrix}
0 & f' \\
f & 0
\end{pmatrix}
\]

This proves that the first two Shimura curves of Lemma 7.2 are on \( H_8 \), as well as all of the polarized products of Lemma’s 7.1 and 7.3, and 2 of the 5 polarized products of Lemma 7.4. The remaining three polarized products don’t lie on the Humbert surface since their endomorphism rings are direct products of rings without \( \sqrt{2} \), hence we list those in (1).

This leaves only the last three Shimura curves of Lemma 7.2 and the Jacobians in Tables 1 and 3. For these, we could compute the endomorphism rings by looking at their constructions, as we did for the polarized products. However, it is much easier to evaluate the equation of \( H_8 \) (given in [7]) in their Igusa invariants to decide whether they lie on \( H_8 \). Of Table 1, it turns out that all curves are points on the
Humbert surface, except the three listed in (2). Of Table 3, only two curves are points on the Humbert surface, and the other six are listed in (3).

References

[1] Hyman Bass. Torsion free and projective modules. Trans. Amer. Math. Soc., 102:319–327, 1962.
[2] Christina Birkenhake and Herbert Lange. Complex abelian varieties, volume 302 of Grundlehren der mathematischen Wissenschaften. Springer, second edition, 2004.
[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system I: The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
[4] Reinier Bröker and Kristin Lauter. Modular polynomials for genus 2. London Mathematical Society, Journal of Computation and Mathematics, 12:326–339, 2009.
[5] Régis Dupont. Moyenne arithmético-géométrique, suites de borchardt et applications, 2006. PhD-thesis (École Polytechnique, Paris).
[6] Gerhard Frey and Tanja Lange. Varieties over special fields. In Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauter, editors, Handbook of elliptic and hyperelliptic curve cryptography, pages 87–113. Chapman & Hall/CRC, 2006.
[7] David Gruenewald. Humbert surface data, 2008. http://echidna.maths.usyd.edu.au/~davidg/thesis.html.
[8] Tsuyoshi Hayashida and Mieo Nishi. Existence of curves of genus two on a product of two elliptic curves. J. Math. Soc. Japan, 17(1):1–16, 1965.
[9] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. Annals of Mathematics, 72(3):612–649, 1960.
[10] Ernst Kani. The number of curves of genus two with elliptic differentials. J. reine angew. Math., 485:93–121, 1997.
[11] Robert M. Kuhn. Curves of genus 2 with split Jacobian. Transactions of the American Mathematical Society, 307(1):41–49, 1988.
[12] Serge Lang. Complex Multiplication, volume 255 of Grundlehren der mathematischen Wissenschaften. Springer, 1983.
[13] Serge Lang. Algebraic Number Theory, volume 110 of Graduate Texts in Mathematics. Springer, second edition, 1994.
[14] Reynald Lercier, David Lubicz, and Frederik Vercauteren. Point counting on elliptic and hyperelliptic curves. In Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauter, editors, Handbook of elliptic and hyperelliptic curve cryptography, pages 407–454. Chapman & Hall/CRC, 2006.
[15] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In Effective methods in algebraic geometry (Castiglioncello, 1990), volume 94 of Progr. Math., pages 313–334. Birkhäuser Boston, Boston, MA, 1991.
[16] James Milne. Abelian varieties. In G. Cornell and J.H. Silverman, editors, Arithmetic Geometry, pages 103–150. Springer-Verlag, New York, 1986.
[17] Jean-Pierre Serre. Rational points on curves over finite fields. Notes by F. Gouvée of lectures at Harvard University, 1985.
[18] Tony Shaska. Curves of genus 2 with (n, n) split Jacobians. J. Symbolic Computation, 31:603–617, 2001.
[19] Goro Shimura. On analytic families of polarized abelian varieties and automorphic functions. Ann. of Math. (2), 78:149–192, 1963.
[20] Goro Shimura. Arithmetic of unitary groups. Ann. of Math. (2), 79:369–409, 1964.
[21] Joseph H. Silverman. The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics. Springer, 1986.
[22] Anne-Monika Spallek. Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen. PhD thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.
[23] Marco Streng. Computing Igusa class polynomials. arXiv:0903.4766, http://www.math.leidenuniv.nl/~streng/icp.pdf, 2008.
[24] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[25] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

Reinier Bröker, Brown University, Department of Mathematics, Providence, RI, 02912, USA

E-mail address: reinier@math.brown.edu

Kristin Lauter, Microsoft Research, One Microsoft Way, Redmond, WA, 98052, USA

E-mail address: klauter@microsoft.com

Marco Streng, University of Warwick, Mathematics Institute, Coventry CV4 7AL, United Kingdom

E-mail address: marco.streng@gmail.com

URL: http://www.warwick.ac.uk/~masjap