Curves of Genus 2 on Abelian Surfaces

Ernst Kani

1 Introduction

Let A/K be an abelian surface over an algebraically closed field K. The question of determining the number N_A^* of isomorphism classes of smooth curves of genus 2 lying on A has been considered by many authors.

This question was first considered by Hayashida [H1], who determined N_A^* in 1965 in the case that $A = E \times E'$, where $E \sim E'$ are two isogeneous complex elliptic curves without complex multiplication, and in 1968 he also determined N_A^* in the case that $A = E \times E$, where E is an elliptic curve with complex multiplication (CM) by a maximal order; see [H2]. Moreover, in 1986 Ibukiyama, Katsura and Oort [IKO] determined N_A^* in the case that $A = E \times E'$, where E and E' are supersingular elliptic curves. More recently, Gélin, Howe and Ritzenthaler [GHR] used Hayashida's formula for N_A^* to give an algorithm for explicitly determining a set of representatives for the isomorphism classes of the set of genus 2 curves on $A = E \times E$ in Hayashida's situation [H2].

Since each smooth genus 2 curve C on A determines a principal polarization θ_C, the question of determining N_A^* is closely connected with the question of determining the number N_A of isomorphism classes of all principal polarizations on A. Indeed, the papers [H1], [H2] and [IKO] also determine the number N_A. All these results use the study of 2×2 Hermitian matrices with coefficients in $\mathrm{End}(E)$.

In this paper we want to introduce a different method for determining N_A and N_A^*, one that has the potential of also being applicable to arbitrary abelian surfaces.

In this method we make use of the *refined Humbert invariant* $q_\theta = q_{(A,\theta)}$ attached to a principal polarization θ on A as in [K4]. This invariant is a positive-definite quadratic form. Given a quadratic form q, a natural first question is to classify the set of isomorphism classes of principal polarizations on A with the same refined Humbert invariant. Thus, if $\mathcal{P}(A) \subset \mathrm{NS}(A)$ denotes the set of principal polarizations on A, then we want to determine the set $\overline{\mathcal{P}}(A, q) := \mathrm{Aut}(A)\backslash\mathcal{P}(A, q)$, where

$$\mathcal{P}(A, q) \ = \ \{\theta \in \mathcal{P}(A) : q_{(A,\theta)} \sim q\}.$$

Here and below, the symbol $\sim$ means that the two quadratic forms are equivalent.

The advantage of studying the set $\overline{\mathcal{P}}(A, q)$ is that there are several explicit formulae for its cardinality.

To state the result, let $q_A(D) = \frac{1}{2}(D.D)$ denote the intersection form on A, which defines an integral quadratic form on the Néron-Severi group $\mathrm{NS}(A)$, and consider the subgroup

$$G_A \ := \ \{\alpha \in \mathrm{Aut}(q_A) : \alpha(\mathcal{P}(A)) = \mathcal{P}(A)\}$$

consisting of those automorphisms of q_A which preserve the set $\mathcal{P}(A)$ of principal polarizations on A. It is easy to see that $G_A \geq H_A$, where H_A is the image of $\mathrm{Aut}(A)$ in $\mathrm{Aut}(\mathrm{NS}(A))$ via its action on $\mathrm{NS}(A)$. We then have the following first result.

Theorem 1 *If $\theta \in \mathcal{P}(A,q)$, then the number of isomorphism classes of principal polarizations in $\mathcal{P}(A,q)$ is given by the number of (H_A, S_θ)-double cosets in G_A, where $S_\theta = \{\alpha \in G_A : \alpha(\theta) = \theta\}$ denotes the stabilizer subgroup of θ in G_A. Thus,*

$$|\overline{\mathcal{P}}(A,q)| \;=\; |H_A \backslash G_A / S_\theta|. \tag{1}$$

In some cases the (finite) number on the right hand side of (1) can be computed directly, as was done in [K8]. However, for most cases (but not all) we can use a much simpler method. This method is based on the important and useful fact that there is a nice *mass formula* for $\overline{\mathcal{P}}(A,q)$. To state it, let us call

$$\mathbf{M}(\overline{\mathcal{S}}) \;=\; \sum_{\overline{\theta} \in \overline{\mathcal{S}}} \frac{1}{a(\overline{\theta})}$$

the *mass* of a subset $\overline{\mathcal{S}} \subset \overline{\mathcal{P}}(A) := H_A \backslash \mathcal{P}(A)$; here $a(\overline{\theta}) = |\mathrm{Aut}(\theta)|$, for any $\theta \in \mathcal{P}(A)$ such that $\overline{\theta} = H_A\theta$, and $\mathrm{Aut}(\theta) := H_A \cap S_\theta$. We then have the following mass formula:

Theorem 2 *If q is a quadratic form such that $\mathcal{P}(A,q) \neq \emptyset$, then*

$$\mathbf{M}(\overline{\mathcal{P}}(A,q)) \;=\; [G_A : H_A]/|\mathrm{Aut}(q)|. \tag{2}$$

It is a remarkable fact that in virtually all cases the weight $a(\theta)$ for $\theta \in \mathcal{P}(A,q)$ only depends on q. In the case that A is not isogeneous to a product of supersingular elliptic curves (i.e., A is not a supersingular surface), then we have:

Theorem 3 *Let A/K be an abelian surface which is not supersingular. If $\theta \in \mathcal{P}(A,q)$, where q is a quadratic form which does not represent 1, then $a(\theta)$ only depends on q. More precisely, if $r_n(q) := |\{(x_1,\ldots,x_r) \in \mathbb{Z}^r : q(x_1,\ldots,x_r) = n\}|$ denotes the number of representations of an integer n by q, then*

$$a(\theta) \;=\; a(q) := \max(1, r_4(q), 3r_4(q) - 12), \quad \textit{for all } \theta \in \mathcal{P}(A,q), \tag{3}$$

except when $q \sim 4x^2$, in which case $a(\theta) = 1$, for all $\theta \in \mathcal{P}(A,q)$. Thus, if we put $a(q)^* = a(q)$ when $q \not\sim 4x^2$ and $a(q)^* = 1$, when $q \sim 4x^2$, then

$$|\overline{\mathcal{P}}(A,q)| \;=\; [G_A : H_A]a(q)^*/|\mathrm{Aut}(q)|. \tag{4}$$

It is interesting (and useful) to note that if C/K is a genus 2 curve, then the number $a(\theta_C)$ is in many cases closely related to the order of the automorphism group $\mathrm{Aut}(C)$ of the curve.

Theorem 4 *If C/K is a curve of genus 2 such that q_C is either a binary or ternary form, then*

$$|\operatorname{Aut}(C)| \;=\; 2a(\theta_C) \;=\; 2a(q_C). \tag{5}$$

Furthermore, in this case the structure of $\operatorname{Aut}(C)$ *is completely determined by* $a(q_C)$.

We next observe that Theorem 3 implies a general formula for the number N_A^* of isomorphism classes of smooth curves of genus 2 on an abelian surface A. To state it, let $\mathfrak{C}(A) = \{C \subset A\}$ denote the set of smooth genus 2 curves lying on A, and let

$$\Theta_A^* = \{q : q \sim q_{(A,\theta_C)}, \text{ for some } C \in \mathfrak{C}(A)\}/\sim$$

denote the set of equivalence classes of integral quadratic forms which are equivalent to some $q_{(A,\theta_C)}$ with $C \in \mathfrak{C}(A)$. Furthermore, given any finite set Q of equivalence classes integral quadratic forms, put

$$S(Q) \;=\; \sum_{q\in Q} \frac{a(q)^*}{|\operatorname{Aut}(q)|} \;=\; \sum_{i=1}^{n} \frac{a(q_i)^*}{|\operatorname{Aut}(q_i)|},$$

where $q_1, \ldots, q_n$ is a system of representatives of the equivalence classes of Q, and $a(q_i)^*$ is as in (4). We then have:

Theorem 5 *If A/K is an abelian surface which is not supersingular, then the number N_A^* of isomorphism classes of curves of genus 2 on A is given by the formula*

$$N_A^* \;=\; [G_A : H_A] S(\Theta_A^*). \tag{6}$$

Note that it can happen that $N_A^* = 0$, i.e., that $\Theta_A^* = \emptyset$. This is clear if A has no principal polarization, i.e., if $\mathcal{P}(A) = \emptyset$. But even if $\mathcal{P}(A) \neq \emptyset$, then it can happen that $\Theta_A^* = \emptyset$. In that case $A \simeq E \times E'$ is a product surface, and the cases for which $N_A^* = 0$ were classified in [K4] and [K5], and also in Hayashida/Nishi [HN1] and [HN2] in special cases.

It is clear from formula (6) that N_A^* can be readily computed for a specific surface A, provided that we can compute the index $[G_A : H_A]$ and the set Θ_A^* because then $S(\Theta_A^*)$ can be determined by using results from the theory of quadratic forms; see §6.

In the case that $A \simeq E \times E'$ is an abelian product surface which is not supersingular, the index $[G_A : H_A]$ was computed in [K8], and the structure of Θ_A^* follows from the results in [K4], [K9] and Kir [Ki], as is shown in the proofs of Proposition 37 and Theorem 41 below. This, therefore, leads to an explicit formula (and/or algorithm) for computing N_A^* in those cases.

To explain this in more detail, suppose that first that A is a non-CM abelian product surface. In that case one can give an explicit formula for N_A^*, which is conveniently expressed in terms of the class number $h(\Delta)$ and the number of genera $g(\Delta)$ of positive primitive integral binary quadratic forms of discriminant Δ for certain values of Δ.

Theorem 6 *Let $A = E \times E'$, where $\mathrm{Hom}(E, E') = \mathbb{Z}h$ with $d := \deg(h) \geq 1$. If $d = 1$, then $N_A^* = 0$, and if $d > 1$, then*

$$N_A^* \;=\; 2^{\omega(d)-2}\left(\frac{h(-16d)}{g(-16d)} + c(d)\right), \tag{7}$$

where $\omega(d)$ denotes the number of distinct prime divisors of d, and $c(d) = \frac{h(-d)}{g(-d)}$, if $d \equiv 3 \pmod 4$, and $c(d) = -1$ if $d \equiv 2, 4, 6 \pmod 8$ and $c(d) = 0$ otherwise.

Note that this gives a more compact statement of the result of Hayashida [H1]; see Remark 40 below.

Now suppose that A is a CM abelian product surface, i.e., $A = E \times E'$, where E and E' are isogenous elliptic curves with complex multiplication. Let $q_{E,E'}$ denote the degree function on $\mathrm{Hom}(E, E')$, which is a binary quadratic form. If $\Delta = \mathrm{disc}(q_{E,E'})$ denotes its discriminant and $\Delta' := \Delta/\kappa^2$, where $\kappa = \mathrm{cont}(q_{E,E'})$ denotes the content of $q_{E,E'}$, then by [K8] we have that

$$[G_A : H_A] \;=\; 2^{\omega(\kappa)+1} g(\Delta')h(\Delta)h(\Delta')^{-1}. \tag{8}$$

Moreover, if $\mathrm{gen}(q)$ denotes the set of equivalence classes of quadratic forms which are genus-equivalent to a given quadratic form q (see Jones [Jo], Chapter V), and if $\mathrm{gen}(q)^* \subset \mathrm{gen}(q)$ denotes the subset of equivalence classes of forms $q' \in \mathrm{gen}(q)$ which do not represent 1, then we have the following special case of Theorem 46 below.

Theorem 7 *Let $A = E \times E'$ be a CM product surface. If $\Delta = \mathrm{disc}(q_{E,E'})$ is odd, then*

$$N_A^* \;=\; 2^{\omega(\kappa)+1} g(\Delta')h(\Delta)h(\Delta')^{-1} S(\mathrm{gen}(x^2 \perp 4q_{E,E'})^*). \tag{9}$$

Using this formula, one can explicitly compute N_A^* for each given CM product surface A, if Δ is odd. There is a similar (but much more complicated formula) in the case that Δ is even; see Theorem 46 below. In all cases this leads to an explicit algorithm for computing N_A^* which is given in §6. Moreover, at the end of the paper we present a table of the values of N_A^* for abelian CM surfaces A with $|\Delta| \leq 100$.

It is perhaps useful to mention that if $\theta \in \mathcal{P}(A, q)\backslash\mathcal{P}(A)^*$ is a principal polarization which does not come from a genus 2 curve, then in some cases $a(\theta)$ does not only depend on q, so Theorem 3 does not hold for such a q. This situation is studied in more detail in [K10].

This paper is organized as follows. In §2 we recall the definition of the refined Humbert invariant and prove the key Theorem 10 from which Theorem 1 follows easily, as is explained in §3. Moreover, the Mass Formula (Theorem 2) is an easy consequence of Theorem 1, as is shown in §4. In §5 we study the weight $a(\theta_C)$ of the principal polarization of a curve $C \in \mathfrak{C}(A)$ and prove Theorems 3 and 4. This uses results of [K7] and the knowledge of the possible automorphism groups of a genus 2 curve; see Igusa [Ig] and Shaska/Völklein [SV]. Furthermore, the formula for $a(\theta_C)$ is made more explicit in certain cases; see Proposition 32 and Corollary 35. Note that Theorem 5 follows easily from (4), as is explained in §5. Finally, in §6 we study abelian product surfaces and prove Theorems 6 and Theorems 46; the latter includes Theorem 7 above. In addition, we include an algorithm for computing the formula given in Theorem 46 and present a table of the values of N_A^* for A as in that theorem with $|\Delta| \le 100$.

2 The refined Humbert invariant

Let A/K be an abelian surface, and let $q_A : \mathrm{NS}(A) \to \mathbb{Z}$ be the integral quadratic form on $\mathrm{NS}(A)$ defined by (one-half of) the self-intersection pairing on the Néron-Severi group $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$ of A. Its associated bilinear form β_A is therefore the intersection pairing, i.e.,

$$\beta_A(D, D') \ := \ q_A(D + D') - q_A(D) - q_A(D') \ = \ (D.D'). \tag{10}$$

Let $\mathcal{P}(A) \subset \mathrm{NS}(A)$ denote the set of *principal polarizations* of A. Thus, by the Riemann-Roch Theorem on A (see [Mu], p. 150) we have that

$$\mathcal{P}(A) \ = \ \{\mathrm{cl}(D) : D \in \mathrm{Div}(A) \text{ is ample and } q_A(\mathrm{cl}(D)) = 1\},$$

where $\mathrm{cl}(D) \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$ denotes the class defined by the divisor $D \in \mathrm{Div}(A)$. In the sequel we will assume tacitly that $\mathcal{P}(A) \neq \emptyset$.

If $\theta \in \mathcal{P}(A)$, then put

$$\tilde{q}_{(A,\theta)}(D) = \beta_A(D, \theta)^2 - 4q_A(D) = (D.\theta)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}(A). \tag{11}$$

It is easy to see (see [K1]) that this defines a positive-definite quadratic form $q_{(A,\theta)}$ on the quotient space $\mathrm{NS}(A, \theta) := \mathrm{NS}(A)/\mathbb{Z}\theta$, so we have that $\tilde{q}_{(A,\theta)} = q_{(A,\theta)} \circ \pi_\theta$, where

$$\pi_\theta : \mathrm{NS}(A) \ \to \ \mathrm{NS}(A, \theta) \ := \ \mathrm{NS}(A)/\mathbb{Z}\theta$$

denotes the quotient map. The quadratic form $q_{(A,\theta)}$ or, more correctly, the quadratic module $(\mathrm{NS}(A, \theta), q_{(A,\theta)})$ is called the *refined Humbert invariant* of the principally polarized abelian surface (A, θ); cf. [K4]. Since $\mathrm{NS}(A, \theta) \simeq \mathbb{Z}^{\rho-1}$, where $\rho = \rho(A) = \mathrm{rank}(\mathrm{NS}(A))$ is the Picard number of A, we see that $q_{(A,\theta)}$ defines an equivalence class of integral, positive definite quadratic forms in $\rho - 1$ variables.

For what follows, it is of paramount importance to understand that isomorphisms of two such quadratic modules $(\mathrm{NS}(A, \theta_i), q_{(A,\theta_i)})$ are induced by suitable elements of the automorphism group

$$\mathrm{Aut}(q_A) = \{\alpha \in \mathrm{Aut}(\mathrm{NS}(A)) : q_A \circ \alpha = q_A\}$$

of the quadratic form q_A. However, since $\mathrm{Aut}(q_A)$ does not act on $\mathcal{P}(A)$, it is useful to consider the following subgroup $G_A \leq \mathrm{Aut}(q_A)$ which preserves the set of polarizations:

$$G_A \;:=\; \{\alpha \in \mathrm{Aut}(q_A) : \alpha(\mathcal{P}(A)) \;=\; \mathcal{P}(A)\}$$

As we shall see, G_A has index 2 in $\mathrm{Aut}(q_A)$. This follows from the following result:

Proposition 8 *If $\alpha \in \mathrm{Aut}(q_A)$, then $\alpha \in G_A$ if and only if $\alpha(\theta) \in \mathcal{P}(A)$, for some $\theta \in \mathcal{P}(A)$.*

Proof. Suppose that $\theta' := \alpha(\theta) \in \mathcal{P}(A)$, where $\theta \in \mathcal{P}(A)$, and let $D \in \mathcal{P}(A)$. Since $\alpha \in \mathrm{Aut}(q_A)$, we have that $(\alpha(D).\alpha(D)) = (D.D) = 2 > 0$, so by Corollary 2.2(b) of [K1] we have that either $D \in \mathcal{P}(A)$ or that $-D \in \mathcal{P}(A)$. Moreover, since $(\alpha(D).\alpha(\theta)) = (D.\theta) > 0$ because both are ample, it follows that that $\alpha(D) \in \mathcal{P}(A)$. Thus $\alpha(\mathcal{P}(A)) \subset \mathcal{P}(A)$.

Now since $\alpha^{-1}(\theta') = \theta$, a similar argument applied to α^{-1} shows that $\alpha^{-1}(\mathcal{P}(A)) \subset \mathcal{P}(A)$ and so we obtain that $\mathcal{P}(A) \subset \alpha(\mathcal{P}(A))$ and hence that $\alpha(\mathcal{P}(A)) = \mathcal{P}(A)$. Thus $\alpha \in G_A$. Since the converse implication is trivial, this proves the assertion.

Corollary 9 *We have that* $\mathrm{Aut}(q_A) = \langle -1_{\mathrm{NS}(A)} \rangle \times G_A$. *Thus* $[\mathrm{Aut}(q_A) : G_A] = 2$.

Proof. It is clear that $-1 = -1_{\mathrm{NS}(A)} \in \mathrm{Aut}(q_A)$ and that $-1 \in Z(\mathrm{Aut}(q_A))$. Now $-1 \notin G_A$ because if $\theta \in \mathcal{P}(A)$, then $-\theta \notin \mathcal{P}(A)$ because $(-\theta.\theta) < 0$. Thus $\langle -1 \rangle \cap G_A = \{1\}$.

It remains to show that $\langle -1 \rangle G_A = \mathrm{Aut}(q_A)$. For this, let $\alpha \in \mathrm{Aut}(q_A)$, and let $\theta \in \mathcal{P}(A)$. Then $q_A(\alpha(\theta)) = q_A(\theta) > 0$. Thus, by Corollary 2.2(b) of [K1] we have that either $\alpha(\theta) \in \mathcal{P}(A)$ or that $-\alpha(\theta) \in \mathcal{P}(A)$. In the former case we have that $\alpha \in G_A$ by Proposition 8 and in the latter case we have that $-\alpha \in G_A$, so either $\alpha \in G_A$ or $-\alpha \in G_A$. This proves the first assertion, and the second clearly follows from the first.

We now come to the main result of this section. This is closely related to what was stated without proof in Remark 17 of [K5].

Theorem 10 *If $\alpha \in G_A$ and if $\theta \in \mathcal{P}(A)$, then there is a unique isomorphism*

$$\overline{\alpha}_\theta : (\mathrm{NS}(A,\theta), q_{(A,\theta)}) \quad \overset{\sim}{\to} \quad (\mathrm{NS}(A,\alpha(\theta)), q_{(A,\alpha(\theta))})$$

of quadratic modules such that

$$\pi_{\alpha(\theta)} \circ \alpha \;=\; \overline{\alpha}_\theta \circ \pi_\theta. \tag{12}$$

Conversely, if $\theta, \theta' \in \mathcal{P}(A)$ and if

$$\overline{\alpha} : (\mathrm{NS}(A,\theta), q_{(A,\theta)}) \overset{\sim}{\to} (\mathrm{NS}(A,\theta'), q_{(A,\theta')})$$

is an isomorphism of quadratic modules, then there is a unique $\alpha \in G_A$ such that $\alpha(\theta) = \theta'$ and such that $\overline{\alpha} = \overline{\alpha}_\theta$.

Before proving this, let us observe the following important special case.

Corollary 11 *Let $\theta \in \mathcal{P}(A)$, and let $S_\theta = \{\alpha \in G_A : \alpha(\theta) = \theta\}$ denote its stabilizer in G_A. Then the map $\alpha \mapsto \overline{\alpha}_\theta$ defines a group isomorphism $S_\theta \xrightarrow{\sim} \mathrm{Aut}(q_\theta)$ which maps $S_\theta^+ := \{g \in S_\theta : \det(g) = 1\}$ onto $\mathrm{Aut}^+(q_\theta) := \{\alpha \in \mathrm{Aut}(q_\theta) : \det(\alpha) = 1\}$.*

Proof. By the first part of Theorem 10, the indicated rule defines a map $S_\theta \to \mathrm{Aut}(q_\theta)$, and it is immediate that this is a group homomorphism. By the second part of Theorem 10, this is a bijection and so the first assertion follows.

To prove the second assertion, it suffices to show that $\det(\overline{\alpha}_\theta) = \det(\alpha)$, for all $\alpha \in S_\theta$. For this, note that since $\theta \in \mathcal{P}(A)$ is a primitive element in $\mathrm{NS}(A)$, we can extend θ to a basis $D_1 = \theta, D_2, \ldots, D_r$ of $\mathrm{NS}(A)$. Then the matrix M of α with respect to this basis has the form $M = \left(\begin{smallmatrix} 1 & * \\ 0 & M_1 \end{smallmatrix}\right)$, and so $\det(\alpha) = \det(M) = \det(M_1)$.

Now since $\overline{D}_2 := \pi_\theta(D_2), \ldots, \overline{D}_r := \pi_\theta(D_r)$ is a basis of $\mathrm{NS}(A, \theta)$, it follows from (12) that M_1 is the matrix of $\overline{\alpha}_\theta$ with respect to this basis. Thus $\det(\overline{\alpha}_\theta) = \det(M_1) = \det(\alpha)$, which proves the determinant formula and hence the second assertion.

We now turn to the proof of Theorem 10. We begin with the following basic facts about the quadratic forms q_A and $q_\theta := q_{(A,\theta)}$.

Lemma 12 *Let $\theta \in \mathcal{P}(A)$, and put $\mathbb{Z}\theta^\perp := \{D \in \mathrm{NS}(A) : \beta_A(D, \theta) = 0\}$. Then*

$$\mathrm{NS}(A)_\theta^{(2)} := \{D \in \mathrm{NS}(A) : \beta_A(D,\theta) \equiv 0 \,(\mathrm{mod}\ 2)\} \;=\; \mathbb{Z}\theta \oplus \mathbb{Z}\theta^\perp, \tag{13}$$

and $m_\theta := [\mathrm{NS}(A) : \mathrm{NS}(A)_\theta^{(2)}] \mid 2$. Furthermore,

$$\pi_\theta(\mathrm{NS}(A)_\theta^{(2)}) = \mathrm{NS}(A,\theta)^{(2)} := \{\bar{D} \in \mathrm{NS}(A,\theta) : q_\theta(\bar{D}) \equiv 0 \,(\mathrm{mod}\ 2)\}, \tag{14}$$

and so $\mathrm{NS}(A,\theta)^{(2)}$ is a submodule of $\mathrm{NS}(A,\theta)$ of index m_θ. In addition, the restriction π'_θ of π_θ to $\mathbb{Z}\theta^\perp$ induces an isomorphism of quadratic modules:

$$\pi'_\theta : (\mathbb{Z}\theta^\perp, (-4q_A)_{|\mathbb{Z}\theta^\perp}) \quad \xrightarrow{\sim} \quad (\mathrm{NS}(A)_\theta^{(2)}, (q_\theta)_{|\,\mathrm{NS}(A)_\theta^{(2)}}). \tag{15}$$

Proof. Since $\mathrm{NS}(A)_\theta^{(2)}$ is the kernel of the homomorphism $D \mapsto \beta_A(D,\theta)\,(\mathrm{mod}\ 2)$, it is clear that $\mathrm{NS}(A)_\theta^{(2)}$ is a submodule of $\mathrm{NS}(A)$ of index $m_\theta \mid 2$. Clearly $\mathbb{Z}\theta^\perp \subset \mathrm{NS}(A)_\theta^{(2)}$. Furthermore, since $\beta_A(\theta,\theta) = 2q_A(\theta) = 2$, we see that $\mathbb{Z}\theta \subset \mathrm{NS}(A)_\theta^{(2)}$, and so $\mathbb{Z}\theta \oplus \mathbb{Z}\theta^\perp \subset \mathrm{NS}(A)_\theta^{(2)}$. (Note that $\mathbb{Z}\theta \cap \mathbb{Z}\theta^\perp = 0$ because q_A is positive definite on $\mathbb{Z}\theta$ and negative definite on $\mathbb{Z}\theta^\perp$ by the Hodge index theorem.)

To prove the opposite inclusion, let $D \in \mathrm{NS}(A)_\theta^{(2)}$. Then $n := \frac{\beta_A(D,\theta)}{2} \in \mathbb{Z}$, so $D' = D - n\theta \in \mathbb{Z}\theta^\perp$ and hence $D = n\theta + D' \in \mathbb{Z}\theta + \mathbb{Z}\theta^\perp$. This proves (13).

To prove (14), let $D \in \mathrm{NS}(A)^{(2)}_\theta$, so $D = n\theta + D'$, with $n \in \mathbb{Z}$ and $D' \in \mathbb{Z}\theta^\perp$ by (13). Then $\pi_\theta(D) = \pi_\theta(D')$, so $q_\theta(\pi_\theta(D)) = q_\theta(\pi_\theta(D')) = \tilde{q}_\theta(D') = -4q_A(D') \equiv 0 \,(\mathrm{mod}\ 2)$ by (11). Thus $\pi_\theta(\mathrm{NS}(A)^{(2)}_\theta) \subset \mathrm{NS}(A,\theta)^{(2)}$.

Conversely, suppose that $\bar{D} \in \mathrm{NS}(A,\theta)^{(2)}$. Then $\bar{D} = \pi_\theta(D)$ for some $D \in \mathrm{NS}(A)$ and we have that $\tilde{q}_\theta(D) = q_\theta(\bar{D}) \equiv 0 \,(\mathrm{mod}\ 2)$. Now $\tilde{q}_\theta(D) = \beta_A(D,\theta)^2 - 4q_A(D) \equiv \beta_A(D,\theta)^2 \,(\mathrm{mod}\ 2)$, so $2|\beta_A(D,\theta)$, and hence $D \in \mathrm{NS}(A)^{(2)}_\theta$. Thus $\bar{D} \in \pi_\theta(\mathrm{NS}(A)^{(2)}_\theta)$, which proves (14). Thus, since $\mathrm{NS}(A)^{(2)}_\theta$ is a submodule of $\mathrm{NS}(A)$, we see that $\mathrm{NS}(A,\theta)^{(2)} = \pi_\theta(\mathrm{NS}(A)^{(2)}_\theta)$ is a submodule of $\mathrm{NS}(A,\theta)$. Note that $m_\theta = [\mathrm{NS}(A) : \mathrm{NS}(A)^{(2)}_\theta] = [\mathrm{NS}(A,\theta) : \mathrm{NS}(A,\theta)^{(2)}]$ because $\mathrm{Ker}(\pi_\theta) = \mathbb{Z}\theta \subset \mathrm{NS}(A)^{(2)}_\theta$.

By (13) and (14) we see that $\pi_\theta(\mathbb{Z}\theta^\perp) = \mathrm{NS}(A,\theta)^{(2)}$. Thus, $\pi'_\theta : \mathbb{Z}\theta^\perp \xrightarrow{\sim} \mathrm{NS}(A,\theta)^{(2)}$ is an isomorphism because because $\mathrm{Ker}(\pi_\theta) \cap \mathbb{Z}\theta^\perp = 0$. For $D \in \mathbb{Z}\theta^\perp$ we have by definition that $\tilde{q}_\theta(D) = -4q_A(D)$, so $q_\theta(\pi'_\theta(D)) = -4q_A(D)$, and hence we obtain the indicated isomorphism (15) of quadratic modules.

Proof of Theorem 10. Suppose first that $\alpha \in G_A$, and put $\theta' = \alpha(\theta)$. Note that $\theta' \in \mathcal{P}(A)$ because $\alpha \in G_A$. Since $\mathrm{Ker}(\pi_{\theta'} \circ \alpha) = \alpha^{-1}(\mathbb{Z}\theta') = \mathbb{Z}\theta = \mathrm{Ker}(\pi_\theta)$, there is a unique isomorphism $\alpha_\theta : \mathrm{NS}(A,\theta) \xrightarrow{\sim} \mathrm{NS}(A,\theta')$ such that (12) holds. Now since $\alpha \in \mathrm{Aut}(q_A)$, we have that $\beta_A(\alpha(D),\theta') = \beta_A(\alpha(D),\alpha(\theta)) = \beta_A(D,\theta)$ and also $q_A(\alpha(D)) = q_A(D)$, for all $D \in \mathrm{NS}(A)$, so $\tilde{q}_{\theta'} \circ \alpha = \tilde{q}_\theta$, and hence it follows from (12) that $q_{\theta'} \circ \overline{\alpha}_\theta = q_\theta$. Thus, $\overline{\alpha}_\theta$ defines the indicated isomorphism of quadratic modules.

We now prove the converse. Thus, let $\theta, \theta' \in \mathcal{P}(A)$ be given, and let $\overline{\alpha}$ be the given isomorphism of quadratic modules. It is then clear from the definition and the fact that $\mathrm{NS}(A,\theta)^{(2)}$ is a submodule of $\mathrm{NS}(A,\theta)$ by Lemma 12 that $\overline{\alpha}$ restricts to an isomorphism $\overline{\alpha}^{(2)} : \mathrm{NS}(A,\theta)^{(2)} \xrightarrow{\sim} \mathrm{NS}(A,\theta')^{(2)}$. Thus, by (15) we obtain an isomorphism of quadratic modules

$$\alpha_1 := (\pi'_{\theta'})^{-1} \circ \overline{\alpha}^{(2)} \circ \pi'_\theta : \ (\mathbb{Z}\theta^\perp, (-4q_A)_{|\mathbb{Z}\theta^\perp}) \ \xrightarrow{\sim} \ ((\mathbb{Z}\theta')^\perp, (-4q_A)_{|(\mathbb{Z}\theta')^\perp}).$$

Note that this implies that $q_A \circ \alpha_1 = (q_A)_{|\mathbb{Z}\theta^\perp}$. Since $\mathrm{NS}(A)^{(2)}_\theta = \mathbb{Z}\theta \oplus \mathbb{Z}\theta^\perp$ by (13), it follows that there is a unique isomorphism $\alpha_2 : \mathrm{NS}(A)^{(2)}_\theta \xrightarrow{\sim} \mathrm{NS}(A)^{(2)}_{\theta'}$ such that $\alpha_2(\theta) = \theta'$ and $(\alpha_2)_{|\mathbb{Z}\theta^\perp} = \alpha_1$. Note that since $q_A(\theta) = 1 = q_A(\theta')$, it follows that $q_A(\alpha_2(D)) = q_A(D)$, for all $D \in \mathrm{NS}(A)^{(2)}_\theta$.

We observe that $m_\theta = m_{\theta'}$ because by Lemma 12 we have that $m_\theta = [\mathrm{NS}(A,\theta) : \mathrm{NS}(A,\theta)^{(2)}] = [\overline{\alpha}(\mathrm{NS}(A,\theta)) : \overline{\alpha}(\mathrm{NS}(A,\theta)^{(2)})] = [\mathrm{NS}(A,\theta') : \mathrm{NS}(A,\theta')^{(2)}] = m_{\theta'}$. Thus, if $m_\theta = 1$, then $\alpha := \alpha_2 \in \mathrm{Aut}((\mathrm{NS}(A), q_A))$ satisfies the desired properties.

Assume therefore that $m_\theta = m_{\theta'} = 2$. Since $\mathrm{NS}(A)^{(2)}_\theta$ has finite index in the free module $\mathrm{NS}(A)$, we see that α_2 extends uniquely to a $\mathbb{Q}$-linear automorphism α^0 of $\mathrm{NS}^0(A) = \mathrm{NS}(A) \otimes \mathbb{Q}$. Furthermore, if q^0_A denotes the natural extension of q_A to $\mathrm{NS}^0(A)$ (which is given by $q^0_A(x) = \frac{1}{n^2}q_A(nx)$, if $n \in \mathbb{Z}$, $n \neq 0$, is such that $nx \in \mathrm{NS}(A)$), then we see that $q^0_A(\alpha^0(x)) = q^0(x)$, for all $x \in \mathrm{NS}^0(A)$.

We now want to show that $\alpha^0(\mathrm{NS}(A)) = \mathrm{NS}(A)$. For this, note that $\mathrm{NS}(A) = \mathbb{Z}D_1 + \mathrm{NS}(A)_\theta^{(2)}$, where $D_1 \in \mathrm{NS}(A)$ satisfies $\beta_A(D_1, \theta) \equiv 1 \,(\mathrm{mod}\ 2)$. Clearly $2D_1 \in \mathrm{NS}(A)_\theta^{(2)}$. We now show:

Claim: $\alpha_2(2D_1) = 2D_2$, for some $D_2 \in \mathrm{NS}(A)$.

To construct D_2, put $D_2' := \alpha_2(2D_1) \in \alpha_2(\mathrm{NS}(A)_\theta^{(2)})) = \mathrm{NS}(A)_{\theta'}^{(2)}$ and $\bar{D}_2 := \overline{\alpha}(\pi_\theta(D_1)) \in \mathrm{NS}(A, \theta')$. Thus, there exists $D_2'' \in \mathrm{NS}(A)$ such that $\pi_{\theta'}(D_2'') = \bar{D}_2$. Then

$$D_2' \;=\; 2D_2'' + n\theta', \quad \text{for some } n \in \mathbb{Z}. \tag{16}$$

Indeed, $\pi_{\theta'}(D_2') = \pi_{\theta'}(\alpha_2(2D_1)) = \overline{\alpha}(\pi_\theta(2D_1)) = 2\overline{\alpha}(\pi_\theta(D_1)) = 2\bar{D}_2 = \pi_{\theta'}(2D_2'')$, and so (16) follows.

We next observe that $2|n$. For this, we compute as follows: $8q_A(D_1) = 2q_A(2D_1) = 2q_A(\alpha_2(2D_1)) = 2q_A(D_2') \overset{(16)}{=} 2q_A(2D_2''+n\theta')$. Since $2q_A(D) = \beta_A(D, D), \forall D \in \mathrm{NS}(A)$, we see that $2q_A(2D_2''+n\theta') = \beta_A(2D_2''+n\theta', 2D_2''+n\theta') = 4\beta_A(D_2'', D_2'')+4n\beta_A(D_2'', \theta')+2n^2$, so $n^2 = 4q_A(D_1)-2\beta_A(D_2'', D_2'')-2n\beta_A(D_2'', \theta') \equiv 0 \,(\mathrm{mod}\ 2)$, and hence $2|n$. Thus, $D_2 := D_2'' + \frac{n}{2}\theta' \in \mathrm{NS}(A)$, and so $D_2' = 2D_2$ by (16). This proves the claim.

From the claim we see that $\alpha^0(D_1) = \frac{1}{2}\alpha^0(2D_1) = \frac{1}{2}\alpha_2(2D_1) = \frac{1}{2}(2D_2) = D_2 \in \mathrm{NS}(A)$, so $\alpha^0(\mathrm{NS}(A)) \subset \mathrm{NS}(A)$ because $\alpha^0(\mathrm{NS}(A)_\theta^{(2)}) = \alpha_2(\mathrm{NS}(A)_\theta^{(2)}) = (\mathrm{NS}(A)_{\theta'}^{(2)} \subset \mathrm{NS}(A)$. Furthermore, since $[\alpha^0(\mathrm{NS}(A)) : \alpha^0(\mathrm{NS}(A)_\theta^{(2)})] = [\mathrm{NS}(A)) : \mathrm{NS}(A)_\theta^{(2)}] = [\mathrm{NS}(A)) : \mathrm{NS}(A)_{\theta'}^{(2)}]$, we see that $\alpha^0(\mathrm{NS}(A)) = \mathrm{NS}(A)$. Thus, the restiction $\alpha := (\alpha^0)_{|\,\mathrm{NS}(A)} \in \mathrm{Aut}((\mathrm{NS}(A), q_A))$.

We have that $\alpha(\theta) = \theta'$ by construction, so $\alpha \in G_A$ by Proposition 8. It remains to show that $\overline{\alpha}_\theta = \overline{\alpha}$, i.e., that (12) holds. If $D \in \mathrm{NS}(A)_\theta^{(2)}$, then $\pi_{\theta'}(\alpha(D)) = \pi_{\theta'}(\alpha_2(D)) = \overline{\alpha}(\pi_\theta(D))$ by the construction of α_2. Thus $2(\pi_{\theta'} \circ \alpha) = \pi_{\theta'} \circ (2\alpha) = \overline{\alpha} \circ (2\pi_\theta) = 2(\overline{\alpha} \circ \pi_\theta)$, and so (12) holds because $\mathrm{NS}(A, \theta')$ is torsionfree.

Finally, we show that $\alpha \in G_A$ is uniquely determined by the given properties. Indeed, suppose $\alpha' \in G_A$ is another element with $\alpha'(\theta) = \theta'$ and $\overline{\alpha'}_\theta = \overline{\alpha}$. Then $\alpha'(\mathbb{Z}\theta^\perp) = (\mathbb{Z}\theta')^\perp$ because $\alpha' \in \mathrm{Aut}(q_A)$. Thus, if $D \in \mathbb{Z}\theta^\perp$, then $\pi_{\theta'}(\alpha'(D)) = \overline{\alpha}(\pi_\theta(D)) = \pi_{\theta'}(\alpha(D))$, and so $\alpha'(D) = \alpha(D)$ because π_θ is injective on $(\mathbb{Z}\theta')^\perp$; see Lemma 12. Thus, α and α' agree on $\mathrm{NS}(A)_\theta^{(2)} = \mathbb{Z}\theta \oplus \mathbb{Z}\theta^\perp$. Since this has finite index in $\mathrm{NS}(A)$, it follows that $\alpha = \alpha'$, and so α is uniquely determined by the given properties.

In what follows, we shall frequently use the following fact which is a generalization of the easy part of Theorem 10.

Proposition 13 *If $\alpha : (\mathrm{NS}(A), q_A) \xrightarrow{\sim} (\mathrm{NS}(A'), q_{A'})$ is an isomorphism of quadratic modules, where A and A' are abelian surfaces, and if $\theta \in \mathcal{P}(A))$ and $\alpha(\theta) \in \mathcal{P}(A')$,* *then there is a unique isomorphism*

$$\overline{\alpha}_\theta : (\mathrm{NS}(A,\theta), q_{(A,\theta)}) \quad \overset{\sim}{\to} \quad (\mathrm{NS}(A',\alpha(\theta)), q_{(A',\alpha(\theta))})$$

such that (12) *holds. In particular, if* $f : A \overset{\sim}{\to} A'$ *is an isomorphism of abelian surfaces, then* $q_{(A,\theta)} \sim q_{(A',f_*(\theta))}$*, for all* $\theta \in \mathcal{P}(A)$*.*

Proof. The first assertion follows by a similar argument as that of the first part of the proof of Theorem 10. Moreover, if $f : A \overset{\sim}{\to} A'$ is an isomorphism of abelian surfaces, then f induces an isomorphism $f_* : \mathrm{NS}(A) \overset{\sim}{\to} \mathrm{NS}(A)$ such that $q_{A'} \circ f_* = q_A$ and such that $f_*\mathcal{P}(A) = \mathcal{P}(A')$. Thus, $\alpha = f_*$ satisfies the hypothesis of the first assertion, and so $(\mathrm{NS}(A,\theta), q_{(A,\theta)}) \simeq (\mathrm{NS}(A', f_*(\theta)), q_{(A',f_*(\theta))})$, i.e., $q_{(A,\theta)} \sim q_{(A',f_*(\theta))}$, for all $\theta \in \mathcal{P}(A)$.

3 The Structure of $\mathcal{P}(A,q)$

We now fix an integral quadratic form q in r variables, and consider the subset

$$\mathcal{P}(A,q) := \{\theta \in \mathcal{P}(A) : q_\theta \sim q\}$$

of $\mathcal{P}(A)$. Here $q_\theta = q_{(A,\theta)}$ is the refined Humbert invariant of (A,θ) and the condition $q_\theta \sim q$ means that we have an isomorphism $(\mathrm{NS}(A), q_{(A,\theta)}) \simeq (\mathbb{Z}^r, q)$ of quadratic modules. In the sequel we will tacitly assume that $r = \rho(A) - 1 = \mathrm{rank}(\mathrm{NS}(A)) - 1$, for otherwise $\mathcal{P}(A,q)$ is empty.

It is an immediate consequence of Theorem 10 that the group G_A acts transitively on the set $\mathcal{P}(A,q)$. More precisely:

Proposition 14 *If* $\theta \in \mathcal{P}(A,q)$*, then the map* $g \mapsto g(\theta)$ *defines a bijection of* G_A*-sets*

$$G_A/S_\theta \quad \overset{\sim}{\to} \quad \mathcal{P}(A,q), \tag{17}$$

where $S_\theta := \{\alpha \in G_A : g(\theta) = \theta\}$ *denotes the* G_A*-stabilizer of* θ*.*

Proof. If $g \in G_A$, then from the first part of Theorem 10 it follows that $(\mathrm{NS}(A, g(\theta)), q_{g(\theta))}) \simeq (\mathrm{NS}(A,\theta), q_\theta) \simeq (\mathbb{Z}^r, q)$, so $g(\theta) \in \mathcal{P}(A,q)$. This means that $\mathcal{P}(A,q)$ is a G_A-set.

Next, suppose that $\theta' \in \mathcal{P}(A,q)$. Then $q_{\theta'} \sim q \sim q_\theta$, so there exists an isomorphism $\overline{\alpha} : (\mathrm{NS}(A,\theta), q_\theta) \simeq (\mathrm{NS}(A,\theta'), q_{\theta'})$. By the second part of Theorem 10 there exists $g \in G_A$ such that $g(\theta) = \theta'$, and so G_A acts transitively on $\mathcal{P}(A,q)$. Thus, the assertion follows from this and the orbit-stabilizer theorem of group theory.

It follows from Proposition 14 that for any subgroup $H \leq G_A$, the set $H\backslash\mathcal{P}(A,q)$ of H-orbits of $\mathcal{P}(A,q)$ is given by the set of $H\backslash G_A/S_\theta$ of (H, S_θ)-double cosets of G_A, where $\theta \in \mathcal{P}(A,q)$.

In particular, this applies to the group $H = H_A$ which is the image of the automorphism group $\mathrm{Aut}(A)$ of A. To define H_A, recall that for any divisor $D \in \mathrm{Div}(A)$ and any automorphism $\alpha \in \mathrm{Aut}(A)$ we have the image divisor $\alpha_*(D)$ (which is defined by $\alpha_*(C) = \alpha(C)$ on prime divisors C of A). It is clear that α_* preserves intersection numbers and hence is compatible with numerical equivalence. We thus obtain that $\alpha_* \in \mathrm{Aut}(q_A)$. Moreover, it is easy to see that $\alpha_*(\mathcal{P}(A)) = \mathcal{P}(A)$, so $\alpha_* \in G_A$. It thus follows that the rule $\alpha \mapsto \alpha_*$ defines a group homomorphism

$$\varphi_A : \mathrm{Aut}(A) \ \rightarrow \ G_A$$

We denote the image of φ_A by $H_A := \varphi_A(\mathrm{Aut}(A)) \leq G_A$. Note that φ_A is never injective because $[-1]_A \in \mathrm{Ker}(\varphi_A)$, as is not difficult to see.

From the above discussion we thus obtain:

Corollary 15 *If $\theta \in \mathcal{P}(A, q)$, then the rule $g \mapsto H_A g(\theta)$ defines a bijection*

$$H_A \backslash G_A / S_\theta \quad \overset{\sim}{\rightarrow} \quad \overline{\mathcal{P}}(A, q) \ := \ H_A \backslash \mathcal{P}(A, q).$$

In particular,

$$|\overline{\mathcal{P}}(A, q)| \ = \ |H_A \backslash G_A / S_\theta|. \tag{18}$$

Note that this proves Theorem 1 of the Introduction.

4 The mass formula for $\overline{\mathcal{P}}(A, q)$

We next turn to the mass formula for $\overline{\mathcal{P}}(A, q)$. To formulate the result, let $\theta \in \mathcal{P}(A)$, and let

$$\mathrm{Aut}(\theta) \ := \ H_A \cap S_\theta$$

denote the *automorphism group* of θ, where, as before, $H_A = \varphi_A(\mathrm{Aut}(A))$ is the image of the automorphism group $\mathrm{Aut}(A)$ in G_A, and S_θ is the G_A-stabilizer of θ. It is immediate that if $\mathrm{Aut}(A, \theta) := \{\alpha \in \mathrm{Aut}(A) : \alpha^*\theta = \theta\}$, then

$$\mathrm{Aut}(\theta) \ = \ \varphi_A(\mathrm{Aut}(A, \theta)) \ \simeq \ \mathrm{Aut}(A, \theta)/\mathrm{Ker}(\varphi_A). \tag{19}$$

Note that S_θ is always a finite group because $S_\theta \simeq \mathrm{Aut}(q_\theta)$ by Corollary 11 and because q_θ is a positive quadratic form. Thus, $a(\theta) := |\mathrm{Aut}(\theta)| < \infty$, and we have

$$a(\theta) \mid |\mathrm{Aut}(q_\theta)|, \quad \text{for all } \theta \in \mathcal{P}(A). \tag{20}$$

We observe that if $\alpha \in H_A$, then

$$\mathrm{Aut}(\alpha(\theta)) \ = \ H_A \cap \alpha S_\theta \alpha^{-1} \ = \ \alpha(H_A \cap S_\theta)\alpha^{-1} \ = \ \alpha\,\mathrm{Aut}(\theta)\alpha^{-1}. \tag{21}$$

Thus, $a(\theta) = |\operatorname{Aut}(\theta)|$ has the same value for all elements in the H_A-orbit $\overline{\theta} = H_A\theta$ of θ, and so we can write $a(\overline{\theta}) := a(\theta)$. Thus, as in the introduction, we can define the *mass* of a subset $\overline{\mathcal{S}} \subset \overline{\mathcal{P}}(A) := H_A\backslash\mathcal{P}(A)$ by

$$\mathbf{M}(\overline{\mathcal{S}}) := \sum_{\overline{\theta}\in\overline{\mathcal{S}}} a(\overline{\theta})^{-1}.$$

In the case that $\overline{\mathcal{S}} = \overline{\mathcal{P}}(A,q)$, this mass is given by a simple formula, as was mentioned in Theorem 2.

Proof of Theorem 2. Let $\theta \in \mathcal{P}(A,q)$. We first observe that if $g \in G_A$, then the number of H_A-orbits of H_AgS_θ is

$$(22) \qquad |H_A\backslash H_AgS_\theta| \;=\; [S_\theta : S_\theta \cap g^{-1}H_Ag] \;=\; |S_\theta|\cdot|\operatorname{Aut}(g(\theta))|^{-1}.$$

Indeed, if $S_\theta = \coprod_i (S_\theta \cap g^{-1}H_Ag)s_i$, then one sees easily that $H_AgS_\theta = \coprod_i H_Ags_i$, and so the first equality of (22) follows. Moreover, since

$$S_\theta \cap g^{-1}H_Ag \;=\; g^{-1}(gS_\theta g^{-1} \,\cap\, H_A)g \;=\; g^{-1}(S_{g(\theta)} \,\cap\, H_A)g \;=\; g^{-1}\operatorname{Aut}(g(\theta))g,$$

we see that $[S_\theta : S_\theta \cap g^{-1}H_Ag] = \frac{|S_\theta|}{|S_\theta\cap g^{-1}H_Ag|} = \frac{|S_\theta|}{|\operatorname{Aut}(g(\theta))|}$ because $|S_\theta| < \infty$.

Now let $g_1,\ldots,g_t$ be a system of representatives of $H_A\backslash G_A/S_\theta$, so by Corollary 15 we have that $g_1(\theta),\ldots,g_t(\theta)$ is a system of representatives of $H_A\backslash\mathcal{P}(A,q)$. Thus

$$[G_A : H_A] \;=\; \sum_{i=1}^{t} |H_A\backslash H_Ag_iS_\theta| \;=\; \sum_{i=1}^{t} \frac{|S_\theta|}{|\operatorname{Aut}(g_i(\theta))|} \;=\; |S_\theta|\cdot\mathbf{M}(\overline{\mathcal{P}}(A,q)),$$

and so (2) follows because $|S_\theta| = |\operatorname{Aut}(q_\theta)| = |\operatorname{Aut}(q)|$ by Corollary 11 and by the fact that $q_\theta \sim q$ since $\theta \in \mathcal{P}(A,q)$.

When A is an abelian product surface, then the index $[G_A : H_A]$ was calculated in [K8]. In the non-CM case we have the following.

Proposition 16 *Let $A = E \times E'$, where $\operatorname{Hom}(E,E') = \mathbb{Z}h$ with $d := \deg(h) \geq 1$. If q is a binary quadratic form such that $\mathcal{P}(A,q) \neq \emptyset$, then*

$$(23) \qquad \mathbf{M}(\overline{\mathcal{P}}(A,q)) \;=\; 2^{\omega(d)}/|\operatorname{Aut}(q)|.$$

Proof. By Theorem 1 of [K8] we have that $[G_A : H_A] = 2^{\omega(d)}$, and so (23) follows from Theorem 2.

In the case of a CM abelian product surface $A \simeq E \times E'$ we obtain a similar result by using the index formula (8) which was mentioned in the introduction. For this, we recall the following (well-known) notation.

If $\Delta < 0$ is a quadratic discriminant, i.e., if $\Delta \equiv 0, 1 \pmod 4$, then let $h(\Delta) = |C(\Delta)|$ denote the order of the class group of primitive forms of discriminant Δ; cf. [Co], p. 29 and p. 50. Note that $h(\Delta) = |\operatorname{Pic}(\mathcal{O}_\Delta)|$, where $\mathcal{O}_\Delta$ denotes the order of discriminant Δ; cf. [Co], p. 137. Moreover, we let $g(\Delta) = [C(\Delta) : C(\Delta)^2]$ denote the number of genera of discriminant Δ. A formula for $g(\Delta)$ is given in formula (48) below.

Proposition 17 *Let $A = E \times E'$, where $q_{E,E'}$ is a binary quadratic form of discriminant Δ and content κ. Put $\Delta' = \Delta/\kappa^2$. If q is a ternary quadratic form, then*

$$a(\theta) \mid |\operatorname{Aut}^+(q)|, \quad \textit{for all } \theta \in \mathcal{P}(A, q). \tag{24}$$

Moreover, if $\mathcal{P}(A, q) \neq \emptyset$, then we have that

$$\mathbf{M}(\overline{\mathcal{P}}(A, q))|\operatorname{Aut}^+(q)| \;=\; 2^{\omega(\kappa)} g(\Delta') \frac{h(\Delta)}{h(\Delta')}. \tag{25}$$

Proof. By Theorem 3 of [K8] we have that $\det(h) = 1$, for all $h \in H_A$, so $\operatorname{Aut}(\theta) = H_A \cap S_\theta \leq S_\theta^+ := \{g \in S_\theta : \det(g) = 1\}$. Thus (24) follows because $S_\theta^+ \simeq \operatorname{Aut}^+(q)$ by Corollary 11.

By Theorem 2 of [K8] we have that (8) holds, so by Theorem 2 we obtain that $\mathbf{M}(\overline{\mathcal{P}}(A, q))|\operatorname{Aut}(q)| = 2^{\omega(\kappa)+1} g(\Delta') \frac{h(\Delta)}{h(\Delta')}$. Now for any ternary form q we have that $|\operatorname{Aut}(q)| = 2|\operatorname{Aut}^+(q)|$ because $-1 \in \operatorname{Aut}(q) \setminus \operatorname{Aut}^+(q)$, and so (25) follows.

Remark 18 If A/K is as in Proposition 17, then (24) implies that $a(\theta)|24$ because for any positive ternary form q we have that $|\operatorname{Aut}^+(q)| \mid 24$ by [Di], Theorem 105.

More generally, if A/K is any abelian surface and if q is a positive form with $\operatorname{rank}(q) \leq 3$, then $a(\theta)|48$, for any $\theta \in \mathcal{P}(A, q)$. Indeed, by (19) we know that $a(\theta) \mid |\operatorname{Aut}(q)|$, so if q is a ternary form, then $|\operatorname{Aut}(q)| = 2|\operatorname{Aut}^+(q)| \mid 48$ by Theorem 105 of [Di] again. Moreover, if q is a binary form, then $|\operatorname{Aut}(q)| = 2, 4, 8$, or 12 (see [Jo], Theorems 51a and 52), so again $a(\theta)|48$. If q has rank 1, then clearly $|\operatorname{Aut}(q)| = 2$. This proves the assertion. (Note that if $q = 0$, then $a(\theta) = 1$ because then $\operatorname{Aut}(J_C, \theta_C) = \{\pm 1\} = \operatorname{Ker}(\varphi_{J_C})$.)

5 The computation of $a(\theta)$

We now study the weight $a(\theta) = |\operatorname{Aut}(\theta)|$ of a principal polarization $\theta \in \mathcal{P}(A)$ in the case that $\theta = \operatorname{cl}(C)$ is the class of a smooth genus 2 curve C on A. For this, let

$$\mathcal{P}^*(A) \;=\; \{\operatorname{cl}(C) : C \in \mathfrak{C}(A)\},$$

where $\mathfrak{C}(A)$ denotes the set of smooth genus 2 curves C lying on A. Note that by the adjunction formula for $C \subset A$ we have that $\mathcal{P}^*(A) \subset \mathcal{P}(A)$. We recall the following basic fact from Proposition 6 of [K4] which characterizes the set $\mathcal{P}^*(A)$ inside $\mathcal{P}(A)$.

Proposition 19 *If $\theta \in \mathcal{P}(A)$ is any principal polarization, then*

$$\theta \in \mathcal{P}^*(A) \quad \Leftrightarrow \quad q_\theta(\bar{D}) \neq 1, \quad \textit{for any } \bar{D} \in \mathrm{NS}(A,\theta). \tag{26}$$

As a first step towards computing $a(\theta)$, we observe the following (well-known) fact about the polarized automorphism group $\mathrm{Aut}(A,\theta) = \{\alpha \in \mathrm{Aut}(A) : \alpha^*(\theta) = \theta\}$.

Proposition 20 *If A is an abelian surface, and if $\theta = \mathrm{cl}(C) \in \mathcal{P}^*(A)$, then the rule $\alpha \mapsto \alpha_* = (\alpha^*)^{-1}$ induces an isomorphism $\mathrm{Aut}(C) \simeq \mathrm{Aut}(A,\theta)$.*

Proof. If $\theta = \mathrm{cl}(C)$, then it follows from the universal property of the Jacobian that A is (isomorphic to) the Jacobian J_C of C, so $(A,\theta) \simeq (J_C,\theta_C)$, where θ_C is the theta-divisor of C. Moreover, it follows from Torelli's Theorem (see Milne [Mi], Theorem 12.1) and the fact that C is hyperelliptic that the indicated map gives an isomorphism $\mathrm{Aut}(C) \simeq \mathrm{Aut}(J_C,\theta_C) \simeq \mathrm{Aut}(A,\theta)$.

In view of formula (19), the above proposition gives us some information about the weight $a(\theta)$ when $\theta \in \mathcal{P}^*(A)$. To go further, we need more information about $\mathrm{Ker}(\varphi_A)$. The aim is to prove the following result.

Proposition 21 *Let (A,θ) be a principally polarized abelian surface such that $A \sim E \times E$, for some elliptic curve E. Then $\mathrm{Ker}(\varphi_A) = \{\pm 1_A\}$, except when $A \simeq E \times E$, where E is a CM elliptic curve with $j_E \in \{0, 1728\}$. Moreover, if $\theta = \mathrm{cl}(C) \in \mathcal{P}^*(A)$, then*

$$a(\theta) \;=\; \tfrac{1}{2}|\,\mathrm{Aut}(C)|. \tag{27}$$

As first step, we prove the following result.

Lemma 22 *If (A,θ) is a principally polarized abelian surface, then*

$$\mathrm{Ker}(\varphi_A) \;=\; \mathrm{Aut}(A) \cap C^0(\mathrm{End}^0_\theta(A)), \tag{28}$$

where $\mathrm{End}^0_\theta(A) = \{\alpha \in \mathrm{End}^0(A) : \hat{\alpha}\phi_\theta = \phi_\theta\alpha\}$ and $C^0(\mathrm{End}^0_\theta(A))$ denotes the centralizer of $\mathrm{End}^0_\theta(A)$ in $\mathrm{End}^0(A)$.

Proof. Recall from [K4], §11, that the map $D \mapsto \phi_\theta^{-1} \circ \phi_D$ induces an isomorphism

$$\Phi_\theta : \mathrm{NS}(A) \;\xrightarrow{\sim}\; \mathrm{End}_\theta(A) := \{\alpha \in \mathrm{End}(A) : r_\theta(\alpha) = \alpha\},$$

where $r_\theta(\alpha) = \phi_\theta^{-1} \circ \hat{\alpha} \circ \phi_\theta$. Moreover, by Proposition 58 of [K4] we have that

$$\Phi_\theta(\alpha^* D) \;=\; r_\theta(\alpha)\Phi_\theta(D)\alpha, \quad \text{for all } \alpha \in \mathrm{Aut}(A), D \in \mathrm{NS}(A). \tag{29}$$

From this we see that

$$\mathrm{Aut}(A,\theta) \;=\; \{\alpha \in \mathrm{Aut}(A) : r_\theta(\alpha) = \alpha^{-1}\}. \tag{30}$$

Indeed, if $\alpha \in \mathrm{Aut}(A)$, then $\alpha \in \mathrm{Aut}(A,\theta) \Leftrightarrow \alpha^*\theta = \theta \Leftrightarrow \Phi_\theta(\alpha^*\theta) = \Phi_\theta(\theta)$. Since $\Phi_\theta(\theta) = 1_A$, we see from (29) that the latter condition is equivalent to the equation $r_\theta(\alpha)1_A\alpha = 1_A$, and so (30) follows.

Since $\mathrm{Ker}(\varphi_A) = \{\alpha \in \mathrm{Aut}(A) : \alpha^*D = D, \forall D \in \mathrm{NS}(A)\}$ and since clearly $\mathrm{Ker}(\varphi_A) \le \mathrm{Ker}(A,\theta)$, we see from (29) and (30) that

$$\mathrm{Ker}(\varphi_A) \;=\; \{\alpha \in \mathrm{Aut}(A) : \alpha^{-1}\beta\alpha = \beta,\ \forall \beta \in \mathrm{End}_\theta(A)\} \;=\; \mathrm{Aut}(A) \cap C(\mathrm{End}_\theta(A)),$$

where $C(S) = \{\alpha \in \mathrm{End}(A) : \alpha\beta = \beta\alpha, \forall\beta \in S\}$ denotes the *centralizer* of a subset $S \subset \mathrm{End}(A)$ in $\mathrm{End}(A)$. Moreover, we observe that if $C^0(S) := \{\alpha \in \mathrm{End}^0(A) : \alpha\beta = \beta\alpha, \forall\beta \in S\}$, then $C^0(S) = C(S)\mathbb{Q}$ and $C^0(S) \cap \mathrm{End}(A) = C(S)$, and hence $\mathrm{Ker}(\varphi_A) = \mathrm{Aut}(A) \cap C^0(\mathrm{End}_\theta(A))$. This proves (28) because $\mathrm{End}^0_\theta(A) = \mathrm{End}_\theta(A)\mathbb{Q}$, and so $C^0(\mathrm{End}_\theta(A)) = C^0(\mathrm{End}^0_\theta(A))$.

We next compute the centralizer $C^0(\mathrm{End}^0_\theta(A))$ in the cases of interest here.

Lemma 23 *Let (A,θ) be a principally polarized abelian surface. If $A \sim E \times E$, for some elliptic curve E, then $\mathrm{End}_\theta(A)$ generates $\mathrm{End}^0(A)$ as a $\mathbb{Q}$-algebra, and hence $C^0(\mathrm{End}^0_\theta(A)) = Z(\mathrm{End}^0(A))$, where the latter denotes the centre of $\mathrm{End}^0(A)$. In particular, if E is not a CM-curve, then $C^0(\mathrm{End}_\theta(A)) = \mathbb{Q}\cdot 1_A$.*

Proof. Since $A \sim E^2$, it follows from the "basic construction" of [FK] that there exist elliptic curves $E_i \sim E$ and an isogeny $h : A' := E_1 \times E_2 \to A$ such that $h^*\theta = N\theta_{E_1,E_2}$, for some N; see [K6], Proposition 10. This means that if we put $\theta' := \theta_{E_1,E_2}$, then $\hat{h} \circ \phi_\theta \circ h = N\phi_{\theta'}$, i.e., $r_{\theta',\theta}(h)h = [N]_{A'}$, where $r_{\theta',\theta}(h) := \phi_{\theta'}^{-1}\hat{h}\phi_\theta$.

It is clear that the rule $\alpha \mapsto h^{-1} \circ \alpha \circ h$ defines an isomorphism of rings $c_h : \mathrm{End}^0(A) \xrightarrow{\sim} \mathrm{End}^0(A')$. From the above relation it follows that $c_h(r_\theta(\alpha)) = r_{\theta'}(c_h(\alpha))$, for all $\alpha \in \mathrm{End}^0(A)$; see [K4], formula (65). Thus, $c_h(\mathrm{End}^0_\theta(A)) = \mathrm{End}^0_{\theta'}(A')$, and so we see that it suffices to prove the assertions for (A',θ') in place of (A,θ).

Thus, we may assume (by changing notation) that $A = E \times E'$, where $E \sim E'$ are elliptic curves and $\theta = \theta_{E,E'}$. In this case we can use (as in [K4]) the identification of $\mathrm{End}(A)$ with certain 2×2 "matrices". Via this identification we have by [K4], Proposition 63, that

$$\mathrm{End}_\theta(A) \;=\; \left\{ \begin{pmatrix} [n_1] & h^t \\ h & [n_2] \end{pmatrix} : n_i \in \mathbb{Z}, h \in \mathrm{Hom}(E,E') \right\}.$$

Thus, for any $h \in \mathrm{Hom}(E,E')$ we have that $\alpha_h := \begin{pmatrix} 0 & h^t \\ h & 0 \end{pmatrix} \in \mathrm{End}_\theta(A)$, and also that $\beta := \mathrm{diag}(1,0) \in \mathrm{End}_\theta(A)$.

Let $\mathcal{E}$ denote the $\mathbb{Q}$-algebra generated by $\mathrm{End}_\theta(A)$. Then $\left(\begin{smallmatrix}0&0\\h&0\end{smallmatrix}\right) = \alpha_h\beta \in \mathcal{E}$. Similarly, $\left(\begin{smallmatrix}0&h^t\\0&0\end{smallmatrix}\right) = \beta\alpha_h \in \mathcal{E}$. Moreover, if $n = \deg(h) > 0$, and if $g \in \mathrm{End}(E)$, then $\left(\begin{smallmatrix}ng&0\\0&0\end{smallmatrix}\right) = \alpha_h\alpha_{hg}\beta \in \mathcal{E}$, and similarly, if $g' \in \mathrm{End}(E')$, then $\left(\begin{smallmatrix}0&0\\0&ng'\end{smallmatrix}\right) = \alpha_h\beta\alpha_{(g')^t h} \in \mathcal{E}$. Thus $\mathrm{End}^0(A) = \mathcal{E}$ because any element of $\mathrm{End}^0(A)$ can be written as a $\mathbb{Q}$-linear combination of the above elements.

This proves the first assertion, and second follows from the first because clearly $C^0(\mathrm{End}_\theta(A)) = C^0(\mathcal{E}) = C^0(\mathrm{End}^0(A)) = Z(\mathrm{End}^0(A))$.

To prove the last assertion, note that $\mathrm{End}^0(A) \simeq M_2(\mathrm{End}(E))$, so $Z(\mathrm{End}^0(A)) \simeq Z(\mathrm{End}^0(E)) = \mathbb{Q}$, if E is either non-CM or supersingular. Thus $\dim_{\mathbb{Q}}(Z(\mathrm{End}^0(A))) = 1$ in these cases. Since clearly $\mathbb{Q}\cdot 1_A \subset Z(\mathrm{End}^0(A))$, equality holds.

Proof of Proposition 21. By hypothesis, $A \sim E \times E$. Suppose first that E is not a CM elliptic curve. Then by Lemmas 22 and 23 we have that $\mathrm{Ker}(\varphi_A) = \mathrm{Aut}(A) \cap \mathbb{Q}\cdot 1_A = \{\pm 1_A\}$, the latter because $\deg(x1_A) = 1$ if and only if $x = \pm 1$. This proves the first assertion in this case.

Now suppose that E is a CM elliptic curve. Then by Theorem 2 of [K3] we have that $A \simeq E_1 \times E_2$, for some CM elliptic curves $E_1 \sim E_2 \sim E$. We are thus in the situation of Lemma 29 of [K8], and so it follows from that lemma that $\mathrm{Ker}(\varphi_A) = \{\pm 1_A\}$ except when $E_1 \simeq E_2$ and $j_{E_i} \in \{0, 1728\}$. This proves the first assertion in all cases.

Now suppose that $\theta = \mathrm{cl}(C) \in \mathcal{P}^*(A)$. Then $A \not\simeq E \times E$, where E a CM elliptic curve with $j_E \in \{0, 1728\}$, because in that case Theorem 2 of [K5] shows that $\mathcal{P}^*(A) = \emptyset$ since then $q_{E,E} \sim x^2 + y^2$ or $q_{E,E} \sim x^2 + xy + y^2$ when $j_E \in \{0, 1728\}$. Thus $|\,\mathrm{Ker}(\varphi_A)| = 2$ by the first assertion, and so formula (27) follows from this and Proposition 20 (together with formula (19)).

As a first application of Proposition 21 we prove the following result which is needed below and which extends a result of [AP], p. 142, to arbitrary characteristic (by a simpler proof).

Proposition 24 *If C/K is a curve of genus 2 such that* $\mathrm{Aut}(C) \simeq C_{10} := \mathbb{Z}/10\mathbb{Z}$, *then the Jacobian J_C of C is not isogeneous to $E \times E$, for any non-supersingular elliptic curve E/K.*

Proof. Let $q_C := q_{(J_C,\theta_C)}$ denote the refined Humbert invariant of (J_C, θ_C). We claim:

$$(31) \qquad \mathrm{Aut}(C) \simeq C_{10},\ \mathrm{rank}(q_C) \le 3 \quad \Rightarrow \quad a(\theta_C) = 1.$$

Indeed, since $\mathrm{Aut}(C) \simeq C_{10}$, it follows that there exists a $\sigma \in \mathrm{Aut}(J_C, \theta_C)$ of order 5 by Proposition 20. But then σ lies in $\mathrm{Ker}(\varphi_{J_C})$ because $a(\theta) \mid 48$ by Remark 18 and $5 \nmid 48$. Thus $\pm\sigma \in \mathrm{Ker}(\varphi_{J_C})$, so $\mathrm{Ker}(\varphi_{J_C}) = \mathrm{Aut}(J_C, \theta_C)$ and hence $a(\theta_C) = 1$, which proves the claim.

Now if J_C were isogeneous to $E \times E$, where E is a non-CM or a CM elliptic curve, then q_C would be a binary or ternary form, and then we would have that $a(\theta_C) = 5$ by Proposition 21, which contradicts (31). This proves the proposition.

Remark 25 If $p := \mathrm{char}(K) \neq 0$, and if C/K is a genus 2 curve such that $\mathrm{Aut}(C)$ has an element of order 10, then it can happen that J_C is isogeneous to $E \times E$, for some supersingular curve E/K. Indeed, if $p \neq 2, 5$, then this happens when $p \not\equiv 1 \pmod 5$; see [IKO], Proposition 1.13. In that case q_C is a quintic quadratic form and $a(\theta_C) = 5$ by Proposition 21.

We now want to connect the weight $a(\theta_C)$ of a genus 2 curve C/K to an invariant of the associated refined Humbert invariant q_C. To do this, let

$$i(G) \;:=\; |\{g \in G : \mathrm{ord}(g) = 2\}|$$

denote the number of involutions of a finite group G, and put $i^*(G) := i(G) - 1$. In addition, for any integer n let

$$r_n(q_C) \;=\; |R_n(q_C)|, \quad \text{where } R_n(q_C) \;=\; \{\overline{D} \in \mathrm{NS}(J_C, \theta_C) : q_C(\overline{D}) = n\}.$$

Then we have the following basic result from [K1] and [K7]:

Proposition 26 *If C/K is a genus 2 curve, then*

$$i^*(\mathrm{Aut}(C)) \;=\; r_4(q_C). \tag{32}$$

Thus, if $r_4(q_C) > 0$, then $J_C \sim E_1 \times E_2$, for some elliptic curves E_i/K. Moreover, if $r_4(q_C) \geq 3$, then $E_1 \sim E_2$.

Proof. As in [K7], §6, let $I(C) \subset \mathrm{Aut}(C)$ denote the set of elliptic involutions of C. Then $|I(C)| = i^*(\mathrm{Aut}(C))$. By Proposition 35 of [K7] we know that $|I(C)| = |\mathcal{S}_2(J_C, \theta_C)|$, where the latter denotes the number of elliptic subgroups on J_C of degree 2. On the other hand, by Theorem 1.5 of [K1] and the fact that $r_1(q_C) = 0$ by (26), this number equals $r_4(q_C)$, and so (32) follows.

If $r_4(q_C) > 0$, then $|S_2(J_C, \theta_C)| = r_4(q_C) > 0$, so there exists an elliptic subgroup $E_1 \leq J_C$, and hence $J_C \sim E_1 \times E_2$, for some elliptic curve E_2. Moreover, if $r_4(q_C) \geq 3$, then there exist $\sigma_1, \sigma_2 \in I(C)$ such that $\sigma_2 \neq \sigma_1, \sigma_C\sigma_1$, where σ_C denotes the hyperelliptic involution of C, and so it follows from Proposition 40 of [K7] that $\mathrm{rank}(q_C) \geq 2$. Since $\mathrm{rank}(q_C) = \rho(J_C) - 1 = \rho(E_1 \times E_2) - 1 = 1 + \mathrm{rank}(\mathrm{Hom}(E_1, E_2))$ by Proposition 23 of [K4], this means that $\mathrm{Hom}(E_1, E_2) \neq 0$, and so $E_1 \sim E_2$.

As an application, we can work out the value of $a(\theta)$ in the following special case which is not covered by Proposition 20.

Proposition 27 *Let C/K be a curve of genus* 2 *with* $\mathrm{Aut}(C) \simeq C_2 \times C_2$. *If* $\mathrm{rank}(q_C) = 1$, *then $q_C \sim 4x^2$ and we have that $a(\theta_C) = 1$.*

Proof. Since $i^*(\mathrm{Aut}(C)) = i^*(C_2 \times C_2) = 2$, we have by Proposition 26 that $r_4(q_C) = 2$. Since $\mathrm{rank}(q_C) = 1$, we have that $q_C \sim nx^2$, for some $n \in \mathbb{N}$. By Proposition 19 we have that $n > 1$, and so $n = 4$ because $r_4(q_C) > 0$. This proves the first assertion.

To prove the second assertion, we first observe that there exists an elliptic involution $\sigma \in I(C)$ because $|I(C)| = |i^*(\mathrm{Aut}(C))|$, as was mentioned in the proof of Proposition 26. (Thus $\mathrm{Aut}(C) = \langle \sigma, \sigma_C \rangle$, where σ_C denotes the hyperelliptic involution.) Let $f_\sigma : C \to E_\sigma := C/\langle\sigma\rangle$ denote the associated elliptic subcover of degree 2. Then $E := f_\sigma^*(J_{E_\sigma}) \in \mathcal{S}_2(J_C, \theta_C)$ is an elliptic subgroup of J_C. The class $[E] \in \mathrm{NS}(J_C, \theta_C)$ is a primitive element of $\mathrm{NS}(J_C, \theta_C)$ by Theorem 1.9 of [K1], so $\mathrm{NS}(J_C, \theta_C) = \mathbb{Z}[E]$ because $\mathrm{rank}(\mathrm{NS}(J_C, \theta_C)) = \mathrm{rank}(q_C) = 1$ by hypothesis. Since $\mathrm{NS}(J_C, \theta_C) = \mathrm{NS}(J_C)/\mathbb{Z}\theta_C$, this implies that $\mathrm{NS}(J_C) = \mathbb{Z}\theta_C + \mathbb{Z}\,\mathrm{cl}(E)$, where $\mathrm{cl}(E) \in \mathrm{NS}(J_C)$ denotes te class of E in $\mathrm{NS}(J_C)$.

Since $f_\sigma \circ \sigma = f_\sigma$, we have that $\sigma^* f_\sigma^* = f_\sigma^*$, so $\sigma^* E = E$, and hence $\sigma^*\,\mathrm{cl}(E) = \mathrm{cl}(E)$. Thus, since $\sigma^*\theta_C = \theta_C$ (because $\sigma^* = (\sigma_*)^{-1} \in \mathrm{Aut}(J_C, \theta_C)$ by Proposition 20), this implies that $\sigma^* D = D$, for all $D \in \mathrm{NS}(J_C) = \mathbb{Z}\theta_C + \mathbb{Z}\,\mathrm{cl}(E)$, which means that $\sigma^* \in \mathrm{Ker}(\varphi_{J_C})$. Thus, since also $\sigma_C^* = [-1]_{J_C} \in \mathrm{Ker}(\varphi_{J_C})$, we see that $\mathrm{Aut}(J_C, \theta_C) = \langle \sigma^*, \sigma_C^* \rangle \leq \mathrm{Ker}(\varphi_{J_C}) \leq \mathrm{Aut}(J_C, \theta_C)$, and so $\mathrm{Ker}(\varphi_{J_C}) = \mathrm{Aut}(J_C, \theta_C)$, which means by (19) that $a(\theta_C) = 1$.

Remark 28 It is not difficult to see that a curve C/K satisfying the hypotheses of Proposition 27 exists. In fact, there exist infinitely many such curves over K. Indeed, given any pair (E_1, E_2) of elliptic curves E_i/K with $E_1 \not\sim E_2$, then by Theorem 2 of [K2] there exists a curve C/K with surjective morphisms $f_i : C \to E_i$ of degree 2 for $i = 1, 2$. (If $\mathrm{char}(K) = 2$, then the same is true by Theorem 3.4 of [K2], provided we assume that neither E_1 nor E_2 is supersingular.) Thus, $C_2 \times C_2 \subset \mathrm{Aut}(C)$ and $\mathrm{rank}(q_C) = 1$ because $J_C \sim E_1 \times E_2$ and $\mathrm{Hom}(E_1, E_2) = 0$. (Use the argument of the proof of Proposition 26.) Furthermore, if $\mathrm{Aut}(C) > 4$ were possible, then it follows from (the proof of) Theorem 29 below that $i^*(G) = r_4(q_C) > 2$, and then $E_1 \sim E_2$ by Proposition 26, contradiction. Thus, $\mathrm{Aut}(C) \simeq C_2 \times C_2$, as claimed.

We will now establish the following connection between the weight $a(\theta_C)$ and the number $r_4(q_C)$ of representations of 4 by q_C.

Theorem 29 *Let C/K be a curve of genus* 2 *such that $r := \mathrm{rank}(q_C) \leq 3$, and put $r^* = \min(2, r)$. Moreover, let C_n denote the cyclic group of order n and D_n the dihedral group of order $2n$. Then we have the following possibilities for* $\mathrm{Aut}(C)$, $a(\theta_C)$

and for $r_4(q_C)$:

(33)

$\mathrm{Aut}(C)$	$a(\theta_C)$	$r_4(q_C)$
C_2	1	0
C_{10}	1	0
$C_2 \times C_2$	r^*	2
D_4	4	4
D_6	6	6
$C_3 \rtimes D_4$	12	8
$\mathrm{GL}_2(3)$	24	12

,

In particular, we have that

$$a(\theta_C) \ = \ a(q_C) \ := \ \max(1, r_4(q_C), 3r_4(q_C) - 12), \tag{34}$$

except when $q_C \sim 4x^2$, in which case $a(\theta_C) = 1$. Furthermore, if $a(\theta_C) > 1$, then

$$|\operatorname{Aut}(C)| \ = \ 2a(\theta_C) \ = \ 2a(q_C). \tag{35}$$

Proof. If $\mathrm{char}(K) \neq 2, 5$, then the first column of (33) gives the complete list of possibilities for $\mathrm{Aut}(C)$, for any genus 2 curve C/K; see [SV], Theorem 2. However, if $\mathrm{char}(K) = 5$, then there is another possibility, namely the case that $G := \mathrm{Aut}(C) \simeq 2^+S_5$, which is a certain double cover of the symmetric group S_5; see [SV], p. 711. But this case cannot occur in our situation, as will now be proved.

To see this, observe first that $i^*(G) \geq i(S_5) = 10$, since every transposition of S_5 lifts to an involution of G; see [SV], p. 711. Thus, by Proposition 26 we have that $J_C \sim E \times E$, and so by Proposition 21 we obtain that $a(\theta_C) = \frac{1}{2}|G| = 120$. But since $120 \nmid 48$, and $r \leq 3$, Remark 18 shows that this case is impossible.

If $\mathrm{char}(K) = 2$, then only the cases $\mathrm{Aut}(C) \simeq C_2$, $C_2 \times C_2$, and D_6 are possible here. Indeed, by the discussion of Igusa [Ig] on p. 645 (together with that on p. 647), we see that the last two cases are the cases ($1'$) and ($2'$) of Igusa [Ig]. But his other two cases ($3'$) and ($6'$) are not possible here. To see this, note first that in case ($6'$) we have that C has at least 10 elliptic involutions which are given by the rule $\sigma_{z,c} : (x, y) \mapsto (x + z^4, y + z^2x^2 + zx + c)$, where $z^5 = 1$ and $c^2 - c = 1$. (Note that these elements satisfy the relations given on p. 616 of [Ig], and hence define automorphisms of C. Moreover, a short computation shows that $\sigma_{z,c}^2 = 1$.) Thus, a similar argument as in the case of $\mathrm{char}(K) = 5$ shows that $J_C \sim E \times E$ and that $a(\theta_C) = \frac{1}{2}|\operatorname{Aut}(C)| = 80$, the latter by [Ig]. But since $80 \nmid 48$, this contradicts Remark 18. Moreover, in the case ($3'$) we know from the discussion on p. 648 of Igusa [Ig] that then C also has an elliptic involution. In fact, his argument shows that $D_4 \leq \mathrm{Aut}(C)$, so C has at least 4 elliptic involutions, and hence, as before, we see that $J_C \sim E \times E$, for some elliptic curve E/K. Thus, since $|\operatorname{Aut}(C)| = 32$ by [Ig], p. 245, we see that $a(\theta_C) = 16$ by Proposition 21, and hence $r = \mathrm{rank}(q_C) \geq 3$ by Remark 18 because

$16 \nmid 8$ and $16 \nmid 12$. This means that $r = 3$, so E is a CM elliptic curve. But then by Theorem 2 of [K3] we have that $A \simeq E_1 \times E_2$ is a CM product surface, and hence $a(\theta_C)|24$ by Remark 18, which is a contradiction since $16 \nmid 24$. Thus, this case is also impossible here, and so the first column gives a complete list of the automorphism groups when $r \leq 3$.

To verify the entries of the third column, it suffices in view of (32) to determine $i^*(G)$ for each group G appearing in the first column of (33).

For this, note first that it is clear that $i^*(G)$ has the indicated values for the first three entries of the third column. Moreover, if $G = D_n$, where n is even, then it is immediate that $i(G) = n + 1$, so the next two entries of the third column are also correct. If $G = C_3 \rtimes D_4$ (and D_4 acts on C_3 such that the elements of order 4 of D_4 act by inversion on C_3, as is mentioned in [SV]), then it is not difficult to see (by looking at centralizers of involutions) that there are 3 conjugacy classes of involutions of lengths 1, 2 and 6. Thus $i^*(G) = 8$ in this case. Finally, if $G = \mathrm{GL}_2(3)$, then by linear algebra over $\mathbb{F}_3$ we see that there are 2 conjugacy classes of involutions of lengths 1 and 12, so here $i^*(G) = 12$.

To verify the entries of the second column, note first that the first entry is clear by (19) because $[-1]_{J_C} \in \mathrm{Ker}(\varphi_{J_C}) \leq \mathrm{Aut}(J_C, \theta_C) \simeq C_2$ by Proposition 20. Moreover, the second entry follows from (31). Next, suppose that $\mathrm{Aut}(C) \simeq C_2 \times C_2$, so $J_C \sim E_1 \times E_2$ by Proposition 26 and hence $r = 1 + \mathrm{rank}(\mathrm{Hom}(E_1, E_2))$. If $r = 1$, then $a(\theta_C) = 1 = r^*$ by Proposition 27. If $r \geq 2$, then $\mathrm{Hom}(E_1, E_2) \neq 0$, so $E_1 \sim E_2$, and hence by Proposition 21 we obtain that $a(\theta_C) = \frac{1}{2}|\,\mathrm{Aut}(C)| = 2 = r^*$, which proves that the third entry of the second column is correct.

For the other 3 entries of the second column we have by the above discussion that $r_4(q_C) \geq 4$, so $J_C \sim E \times E$ by Proposition 26. We are thus in the situation of Proposition 21, and so in view of (27), the rest of the entries follow directly from those of the first column.

To verify (34), note first that

$$(36) \qquad \mathrm{Aut}(C) \simeq C_2 \times C_2 \text{ and } r^* = 1 \quad \Leftrightarrow \quad q_C \sim 4x^2.$$

Indeed, the one direction follows from Proposition 27. Conversely, if $q_C \sim 4x^2$, then clearly $r = 1 = r^*$, and $r_4(q_C) = r_4(4x^2) = 2$. Thus, by comparing the third column of (33) with the first, it follows that $\mathrm{Aut}(C) \simeq C_2 \times C_2$, which proves (36).

Combining (36) with Proposition 27 shows that $a(\theta_C) = 1$ when $q_C \sim 4x^2$.

Assume now that $q_C \not\sim 4x^2$. Then (34) follows from the second and third columns of table (33). Indeed, if $r_4(q_C) \leq 6$, then $3r_4(q_C) - 12 \leq r_4(q_C)$, and so the formula (34) holds for the first 5 entries of the table because $r^* = 2$ for the third entry by our assumption. For $r_4(q_C) = 8$ and $r_4(q_C) = 12$ we have that $3r_4(q_C) - 12 = 12$ and 24, respectively, so (34) holds in all cases.

Finally, if $q(\theta_C) > 1$, then we have either the cases of lines 4–6 of (33) or the case of line 3 with $r^* = 2$. In all these cases it is clear that (35) holds.

In order to deduce Theorems 3 and 4 from Theorem 29, we need the following two facts.

Lemma 30 *If A/K is an abelian surface which is not supersingular, then $\rho(A) \le 4$. In particular, we have that* $\mathrm{rank}(q_{(A,\theta)}) \le 3$*, for any $\theta \in \mathcal{P}(A)$.*

Proof. Since $\mathrm{rank}(q_{(A,\theta)}) = \rho(A) - 1$, as was mentioned in §2, it is clear that the second assertion follows from the first.

To prove the first assertion, consider first the case that A is not simple, so $A \sim E \times E'$ for some elliptic curves E/K and E'/K. Then $\rho(A) = \rho(E \times E') = 2 + \mathrm{rank}(\mathrm{Hom}(E, E'))$, so $\rho(A) \le 4$ except when $E \sim E'$ are supersingluar (in which case $\rho(A) = 6$). Thus, the first assertion holds in this case.

Assume next that A is simple, so $D := \mathrm{End}^0(A)$ is a division ring with centre $Z := Z(D)$. Thus $r := \dim_{\mathbb{Q}}(D) = d^2 e$, where $d^2 = \dim_Z(D)$ and $e = [Z : \mathbb{Q}]$. Furthermore, D has an involution $'$ and we have by [Mu], p. 190, that $\rho(A) = \dim_{\mathbb{Q}}(S)$, where $S = \{x \in D : x' = x\}$. Thus, the possibilities for $\rho := \rho(A)$ are given in in the table on p. 202 of Mumford [Mu]. Since here $g = 2$, we obtain the following results, depending on the type of $(D, ')$.

Type I: $d = 1, e|2 \Rightarrow r = \rho = 1$ or 2.

Type II: $d = 2, e = 1 \Rightarrow r = 4$ and $\rho = 3$.

Type III: $d = 2, e|2 \Rightarrow r = 4$ or 8 and $\rho = 1$ or 2.

Type IV: $(d, e) = (1, 2), (1, 4)$ or $(2, 2) \Rightarrow r = 2, 4$ or 8 and $\rho = 1, 2$ or 4.

Thus, in all cases we have that $\rho \le 4$, which proves the first assertion.

Lemma 31 *Let C/K be a curve of genus* 2 *with* $\mathrm{Aut}(C) \simeq C_{10}$*. If J_C is not supersingular, then J_C is simple and rank$(q_C) = 1$.*

Proof. If J_C were not simple, then $J_C \sim E_1 \times E_2$, for some elliptic curves E_i/K, $i = 1, 2$. Then $E_1 \not\sim E_2$ by Proposition 24 because J_C is not supersingular. Thus, $\mathrm{End}^0(J_C) \simeq \mathcal{E}_1 \oplus \mathcal{E}_2$, where $\mathcal{E}_i = \mathrm{End}^0(E_i)$, for $i = 1, 2$. Now by the hypothesis and Proposition 20 there exists a $\sigma \in \mathrm{End}^0(J_C)^\times$ of order 5, so there is a $\sigma_i \in \mathcal{E}_i^\times$ of order 5, for some $i = 1, 2$. But then $\mathbb{Q}(\zeta_5) \simeq \mathbb{Q}(\sigma_i) \subset \mathcal{E}_i$, which is impossible because $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ and either $[\mathcal{E}_i : \mathbb{Q}] \le 2$ or $[\mathcal{E}_i : \mathbb{Q}] = 4$ and $\mathcal{E}_i$ is not commutative.

Thus, J_C is simple, so $D := \mathrm{End}^0(J_C)$ is a division ring. As above, we see that there exists $\sigma \in \mathrm{Aut}(J_C) \le D^\times$ of order 5, so $L := \mathbb{Q}(\sigma) \subset D$ and $L \simeq \mathbb{Q}(\zeta_5)$. From (30) we see that $\sigma + \sigma^{-1} \in \mathrm{End}_{\theta_C}(J_C)$, so $\rho = \rho(J_C) \ge 2$ because $[\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) : \mathbb{Q}] = 2$.

Suppose that $\rho > 2$. Then $\rho = 3$ or 4 by Lemma 30. If $\rho = 3$, then D has type II by the table in the proof of Lemma 30, and then $r = 4$. But this means that $D = L$ is commutative, which contradicts the fact that $d = 2$. Thus, $\rho \ne 4$.

Next, suppose that $\rho = 4$. Then we are in case IV with $(d, e) = (2, 2)$, so $[D : Z] = 4$, where $Z = Z(D)$ is the centre of D. By [Mu], p. 201, Z is an imaginary quadratic field, so $L \cap Z = \mathbb{Q}$ because the unique quadratic subfield of $L \simeq \mathbb{Q}(\zeta_5)$ is real. But this means that $ZL \subset D$ is a field of degree 8, so $LZ = D$, and hence D is commutative, which contradicts the fact that $d = 2$. Thus $\rho \neq 4$, and so only $\rho = 2$ is possible. This implies that $\mathrm{rank}(q_C) = \rho - 1 = 1$, as claimed.

Proof of Theorem 3. To prove the first assertion, it suffices to show that $a(\theta) = a(q)^*$.

Since $\theta \in \mathcal{P}(A, q)$, we have that $q_\theta \sim q$ by definition, and so $r_n(q_\theta) = r_n(q)$, for all $n \geq 1$. In particular, $r_1(q_\theta) = 0$ because $r_1(q) = 0$ by hypothesis. Thus, $\theta = \mathrm{cl}(C)$ is the class of a genus 2 curve $C \subset A$ by (26), and hence $(A, \theta) \simeq (J_C, \theta_C)$. Since $r = \mathrm{rank}(q_C) \leq 3$ by Lemma 30, we are thus in the situation of Theorem 29, and so $a(\theta) = a(q_C)^*$ by (34). This shows that $a(\theta)$ only depends on q, and that (3) holds.

It is clear that (4) follows directly from the first assertion and from formula (2).

Proof of Theorem 4. Since $r = \mathrm{rank}(q_C) \leq 3$, we are in the situation of Theorem 29. Moreover, since $r \geq 2$, we have that $r^* = 2$ and that $\mathrm{Aut}(C) \not\simeq C_{10}$ by Lemma 31. In the remaining cases we see from the table (33) that (5) holds.

It is clear from (5) that q_C determines the order of $\mathrm{Aut}(C)$, and hence also $\mathrm{Aut}(C)$ because all the groups listed in the first column of (33) have different orders.

From (4) we can immediately deduce Theorem 5 of the introduction.

Proof of Theorem 5. If $\Theta_A^* = \emptyset$, then also $\mathfrak{C}(A) = \emptyset$, and so $N_A^* = 0$. Thus, in this case (6) holds because $S(\emptyset) = 0$.

Now suppose that Θ_A^* is nonempty, and let $q_1, \ldots, q_n$ be a system of representatives of the equivalence classes in the set Θ_A^*. Note that since the forms q_θ with $\theta \in \mathcal{P}(A)$ all have the same rank and discriminant (see Proposition 9 of [K4]), this set is necessarily finite by Watson [Wa], Theorem 11. It is clear from the definition that the sets $\mathcal{P}(A, q_i)$ are pairwise disjoint, so we obtain the decompositions

$$\mathcal{P}^*(A) \;=\; \coprod_{i=1}^{n} \mathcal{P}(A, q_i) \quad \text{and} \quad \overline{\mathcal{P}}^*(A) \;=\; \coprod_{i=1}^{n} \overline{\mathcal{P}}(A, q_i)$$

because the first decomposition is compatible with the H_A-action on these sets. Thus, since the map $C \mapsto \mathrm{cl}(C)$ defines a bijection $\mathrm{Aut}(A)\backslash\mathfrak{C}(A) \xrightarrow{\sim} \overline{\mathcal{P}}^*(A)$ by Torelli's Theorem, we see that

$$N_A^* \;=\; |\overline{\mathcal{P}}^*(A)| \;=\; \sum_{i=1}^{n} |\overline{\mathcal{P}}(A, q_i)| \;=\; \sum_{i=1}^{n} [G_A : H_A] \frac{a(q_i)^*}{|\,\mathrm{Aut}(q_i)|} \;=\; [G_A : H_A] S(\Theta_A^*),$$

which proves (6).

As was mentioned in the introduction, the quantities $a(q)$ and $|\,\mathrm{Aut}(q)|$ are easily computed for a given positive binary or ternary quadratic form q. By using the fact each such form is equivalent to a reduced form, we can give an explicit formula for $a(q)$ in terms of the coefficients of the form. We first consider the binary case.

Proposition 32 *Let C/K be a curve of genus 2 such that* $\mathrm{rank}(q_C) = 2$. *Then $q_C \sim q$, where $q(x,y) = ax^2 + bxy + cy^2$ is a reduced binary form, and*

$$\frac{1}{2}|\operatorname{Aut}(C)| \;=\; a(q_C) \;=\; \begin{cases} 1 & \text{if } a \neq 4 \\ 2 & \text{if } a = 4 \text{ and } c \neq 4 \\ 4 & \text{if } a = c = 4 \text{ and } b \neq 4 \\ 6 & \text{if } a = b = c = 4 \end{cases} \tag{37}$$

Furthermore, if $a(q_C) \neq 1$, then

$$|\operatorname{Aut}(q_C)| \;=\; 2a(q_C) \;=\; |\operatorname{Aut}(C)|. \tag{38}$$

Proof. The first assertion follows from [Wa], Theorem 7. Moreover, the first equality of (37) follows from Theorem 4, so to prove (37) it suffices to verify the second equality of (37).

Since q is reduced, $a = \min(q)$; see Watson [Wa], Theorem 7. Since $r_1(q_C) = 0$ by (26), we have that $a > 1$. Moreover, since $q_C(\overline{D}) \equiv 0, 1 \pmod 4$, for all $\overline{D} \in \mathrm{NS}(A, \theta_C)$, it follows that $a \geq 4$. Thus, if $a \neq 4$, then $\min(q) > 4$ and hence $r_4(q_C) = 0$, so $a(q_C) = \max(1, 0, -12) = 1$. This proves the first line of (37).

Now suppose henceforth that $a = 4$. If $c \neq 4$, then $c > a = 4$ because q is reduced, so $R_4(q) = \{(\pm 1, 0)\}$ (see [BV], Lemma 5.7.3), and hence $r_4(q) = 2$ in this case. This means that $a(q_C) = a(q) = \max(1, 2, -6) = 2$.

We are left with the case that $a = c = 4$. Since $q_C \equiv 0, 1 \pmod 4$, we see that $b \equiv 0 \pmod 4$, and so either $b = 0$ or $b = 4$. In the first case $q = 4x^2 + 4y^2$, so $R_4(q) = \{(\pm 1, 0), (0, \pm 1)\}$ and $r_4(q) = 4$, so $a(q_C) = \max(1, 4, 0) = 4$. In the second case we have that $q = 4x^2 + 4xy + 4y^2$, so $R_4(q) = \{(\pm 1, 0), (0, \pm 1), \pm(1, -1)\}$ and $r_4(q) = 6$, which means that $a(q_C) = a(q) = \max(1, 6, 6) = 6$. This proves (37).

To prove (38), it suffices in view of (37) to verify the first equality of (38). Now if $a(q_C) = 6$, then (38) holds because $|\operatorname{Aut}(4x^2 + 4xy + 4y^2)| = |\operatorname{Aut}(x^2 + xy + y^2)| = 2|\operatorname{Aut}^+(x^2 + xy + y^2)| = 12$, and similarly equation (38) holds when $a(q_C) = 4$ because $|\operatorname{Aut}(4x^2 + 4y^2)| = 8$. We are thus left with the case that $a(q_C) = 2$, so $a = 4$, and $c > 4$.

Since $q_C \equiv 0, 1 \pmod 4$, it follows that $c \equiv 0, 1 \pmod 4$. Suppose first that $c \equiv 0 \pmod 4$. Then also $b \equiv 0 \pmod 4$. Thus either $q = 4x^2 + 4c_1y^2$ or $4x^2 + 4xy + 4c_1y^2$ with $c_1 = c/4 \geq 2$. Thus, $a|b$, which means that q is an ambiguous form, and so $|\operatorname{Aut}(q)| = 2|\operatorname{Aut}^+(\frac{1}{4}q)| = 4$ because $c_1 > 1$. Thus (38) holds in this case.

Finally, suppose that $c \equiv 1 \pmod 4$, $c > 1$. Then $q(1, \pm 1) \equiv \pm b + 1 \pmod 4$, so again $b \equiv 0 \pmod 4$. Thus, we have the cases $q = 4x^2 + cy^2$ and $q = 4x^2 + 4xy + cy^2$. Since both these forms are ambiguous, we have that $|\operatorname{Aut}(q)| = 2|\operatorname{Aut}^+(q)| = 4$, the latter because $b^2 - 4ac = -16c$ or $-16(c-1)$, and these are not equal to -3 or -4. (Here we use Theorem 2.5.10 of [BV].) Thus (38) holds in all the asserted cases.

A similar method can be used for ternary forms. For this, we first prove the following result which is also of independent interest.

Proposition 33 *Let C/K be as in* Theorem 29. *If q_C is a primitive form and if $3|a(q_C)$, then q_C is a ternary form with $a(q_C) = r_4(q_C) = 6$ and there exists $c \equiv 1 \pmod 4$, $c > 1$, such that*

(39) $q_C \sim q_{1,c} := 4x^2+4y^2+cz^2+4yz+4xz+4xy$ *or* $q_C \sim q_{2,c} := 4x^2+4y^2+cz^2-4xy.$

Proof. Since $3|a(q_C) = \max(1, r_4(q_C), 3r_4(q_C) - 12)$, we see that $r_4(q_C) \geq 3$, and so $\mathrm{rank}(q_C) \geq 2$ by Proposition 26. Now if q_C were a binary form, then by (37) we see that $q_C \sim 4x^2 + 4xy + 4y^2$, which is not primitive. Thus, q_C has to be a ternary form.

Since q_C is assumed to be primitive, we have that $q_C \sim q = ax^2 + by^2 + cz^2 + Ryz + Sxz + Txy$ for some integers a, b, c, R, S, T with $\gcd(a, b, c, R, S, T) = 1$. Now as in the proof of Proposition 32 we have that $q_C \equiv 0, 1 \pmod 4$, so the same is true for q and for $q_1 := q(x, y, 0) = ax^2 + by^2 + Txy$, and hence it follows that $2|T$ (see [K7], Proposition 5). Similarly, by considering $q(x, 0, z)$ and $q(0, y, z)$ we see that also $2|S$ and $2|T$. Thus we can write q in the form $ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy$, where $r, s, t \in \mathbb{Z}$, and so q is a properly primitive ternary form in the sense of [Di].

By replacing q by an equivalent form, we may assume by Theorem 103 of [Di] that q is an Eisenstein reduced form. Note that a is the minimum of the form (by [Di], Theorem 101), so $a = 4$ because $q_C \equiv 0, 1 \pmod 4$ and $r_1(q_C) = 0$ and $r_4(q_C) > 0$.

Note that $3 \mid |\mathrm{Aut}^+(q)|$ because by the hypothesis, (5) and (24) we have that $3 \mid a(q_C) = a(\theta_C) \mid |\mathrm{Aut}^+(q_C)| = |\mathrm{Aut}^+(q)|$. We now look in the tables of Theorem 105 of [Di] to find the reduced forms satisfying the above conditions. Note that we can discard the cases that $a = b = c$ because this condition implies that q is not primitive since $a = 4$.

Suppose first that $r, s, t > 0$. Then the automorphs listed in lines 1–7 of the table on p. 179 of [Di] all have order 2, and those in line 8 have order 4. Thus, we are only left with the case of line 9, which means that $a = b = 2r = 2s = 2t$, i.e., $q = q_{1,c}$, for some c. Note that $c \geq b = 4$ since q is reduced. Moreover, $c \equiv 1 \pmod 2$ because otherwise q is not primitive, and so $c \equiv 1 \pmod 4$ because $q \equiv 0, 1 \pmod 4$.

Now suppose that $r, s, t \leq 0$. Here again the automorphs listed in lines 1–7 of the table on p. 180 of [Di] all have order 2, and those of line 8 have order 4. Moreover, the case of line 10 of the table can be discarded because then $b = c = -2r$, and hence q is not primitive. In addition, the case of line 11 is impossible because the condition $a = -3s$ implies that $3|4$. We are thus left with the case of line 9, so $a = b = -2t, r = s = 0$, which means that $q = q_{2,c}$, for some c. As in the case of $q_{1,c}$, it follows that $c \equiv 1 \pmod 4$ and that $c > 1$. This proves (39).

It remains to show that $r_4(q_C) = 6$. By (39), it suffices to show that $r_4(q_{i,c}) = 6$, for $i = 1, 2$ (and $c \equiv 1 \pmod 4$, $c > 1$). Since $q_{2,c}(x, y, z) = 4q_2(x, y) + cz^2$, where $q_2(x, y) = x^2 - xy + y^2$, we see that $R_4(q_{2,c}) = \{(x, y, 0) : (x, y) \in R_1(q_2)\}$ because q_2 is a positive form and $c \geq 5$, so $r_4(q_{2,c}) = r_1(q_2) = 6$. Moreover, since

$$q_{1,c}(x, y, z) = 2(x + y)^2 + 2(x^2 + z)^2 + 2(y + z)^2 + (c - 4)z^2,$$

we see that $R_4(q_{1,c}) = \{(x,y,0) : (x,y) \in R_1(q_1)\}$, where $q_1(x,y) = q_{1,c}(x,y,0) = x^2 + xy + y^2$. Indeed, if $c \geq 9$, then this is clear, so suppose that $c = 5$. If $(x,y,z) \in R_4(q_{1,5})$ and $z \neq 0$, then $z = \pm 2$ and $x + y = x + z = y + z = 0$, so $x = -y$ and $x = -z = y$, contradiction. Thus $r_4(q_{1,c}) = r_1(q_1) = 6$. We thus have that $r_4(q_C) = 6$, and so $a(q_C) = \max(1, 6, 6) = 6$, as claimed.

Corollary 34 *If C/K is as in* Theorem 29 *and if $r_4(q_C) > 6$, then q_C is a non-primitive ternary form.*

Proof. Since $r_4(q_C) > 6$, we have by Proposition 26 that $\operatorname{rank}(q_C) \geq 2$. Moreover, since this implies that $a(q_C) \geq r_4(q_4) > 6$, it follows from (37) that q_C cannot be a binary form, and hence q_C is a ternary form.

Since $r_4(q_C) > 6$, it follows from (33) that $r_4(q_C) = 8$ or 12, and so $a(q_C) = 12$ or 24. Thus $3|a(q_C)$, and so q_C cannot be primitive by Proposition 33.

This leads to the following method for computing $a(q_C)$ when q_C is a primitive ternary form.

Corollary 35 *Let q_C be a primitive ternary form. Then $q_C \sim q$, where q is Eisenstein reduced. Moreover, if we write $q(x,y,z) = ax^2 + by^2 + cz^2 + 2ryz + 2sxz + 2txy$, then we have that*

$$(40) \quad \tfrac{1}{2}|\operatorname{Aut}(C)| = a(q_C) = \begin{cases} 1 & \text{if } a \neq 4, \\ 2 & \text{if } a = 4 \text{ and } b \neq a, \\ 6 & \text{if } a = b = 4 \text{ and } (r,s,t) = (2,2,2) \text{ or } (0,0,-2), \\ 4 & \text{otherwise.} \end{cases}$$

Proof. Recall that from the proof of Proposition 33 that q_C is properly primitive, so the first assertion follows from Theorem 103 of [Di]. Moreover, we saw in that proof that $r_4(q) = 0$ if and only if $a \neq 4$, so the first line of (40) holds.

Now suppose that $a = 4$, so $r_4(q) > 0$. Since b is the second minimum of q (see [Di], Theorem 101), we see that $r_4(q) = 2$ if and only if $a = 4$ and $b \neq 4$. Thus, assume that $r_4(q) > 2$. By Theorem 29 and Corollary 34 we know that the only possibilities for $r_4(q) > 2$ are $r_4(q) = 4$ or 6. Furthermore, if $a(q_C) = r_4(q) = 6$, then by Proposition 33 we have that $q_C \sim q_{i,c}$ and then $q = q_{i,c}$ because by [Di], Theorem 104, any two equivalent Eisenstein-reduced forms are equal. Thus, $(r,s,t) = (2,2,2)$, if $i = 1$ and $(r,s,t) = (0,0,-2)$, if $i = 2$. Conversely, if $q = q_{i,c}$, then $r_4(q) = 6$, as was shown in the proof of Proposition 33. This shows that the first 3 cases of (40) are correct, and so it follows that $r_4(q) = 4$ in the remaining cases. This proves (40).

Remark 36 If q_C is an imprimitive ternary form, then the computation of $a(q_C)$ is more complicated. However, we can still compute $r_4(q_C)$ (and hence $a(q_C)$) if q_C is given explicitly.

Indeed, if $q_C \sim q$, where $q(x,y,z) = ax^2 + by^2 + cy^2 + ryz + sxz + txy$, then we can determine $R_n(q)$ by using Hermite's identity

$$4aq(x,y,z) \;=\; (2ax + ty + sz)^2 + q'(y,z), \tag{41}$$

where $q'(y,z)$ is a positive binary quadratic form; see Watson [Wa], p. 18. Thus, for a given n, the form $q'(y,z)$ can only take finitely many values m, and for each such an m the set $R_m(q')$ is easily computed. Moreover, for each $(y,z) \in R_m(q')$, we can find all possible x's (if any) such that $(x,y,z) \in R_n(q)$.

6 Abelian Product Surfaces

We now apply the method of Theorem 5 to give a formula for the number N_A^* in the case that $A = E \times E'$ is an abelian product surface. (Here we may assume that $E' \sim E$, for otherwise $N_A^* = 0$ by Remark 43 below.) For this, we need to know the index $[G_A : H_A]$ and the set Θ_A^*. In the non-CM case we have the following.

Proposition 37 *Let $A = E \times E'$, where* $\mathrm{Hom}(E,E') = \mathbb{Z}h$ *with* $d := \deg(h) \geq 1$. *Then $[G_A : H_A] = 2^{\omega(d)}$, and*

$$\Theta_A^* \;=\; \begin{cases} \mathrm{gen}(x^2+4dy^2)^* \cup \mathrm{gen}(4x^2+4xy+(d+1)y^2), & \textit{if } d \equiv 3 \pmod 4, \\ \mathrm{gen}(x^2+4dy^2)^*, & \textit{otherwise.} \end{cases} \tag{42}$$

Proof. The first assertion follows from Theorem 1 of [K8]. Moreover, the formula (42) was implicitly proven in [K4]. To see this, suppose first that $C \in \mathfrak{C}(A)$. Then C is a curve of type d in the terminology of [K4], so by Theorem 2 of [K4] we know that q_C is (equivalent to) a binary form of type d, and that q_C does not represent 1. Thus, by Theorem 13 of [K4] we have that $q_C \in \mathrm{gen}(x^2+4dy^2)^*$, if $d \not\equiv 3 \pmod 4$, or that $q_C \in \mathrm{gen}(x^2+4dy^2)^* \cup \mathrm{gen}(4x^2+4xy+(d+1)y^2)$, if $d \equiv 3 \pmod 4$. This shows that Θ_A^* is contained in the right hand side of (42).

Conversely, if q is a binary form contained in the right hand side of (42), then q is a form of type d by Theorem 13 of [K4], and then by Theorem 31 of [K4] there exists a curve $C \in \mathfrak{C}(A)$ such that $q_C \sim q$. This shows that the right side of (42) is contained in Θ_A^*, and so (42) holds.

Thus, to determine N_A^*, it suffices to compute $S(Q)$, where $Q = \mathrm{gen}(x^2+4dy^2)^*$ and $Q = \mathrm{gen}(4x^2+4xy+(d+1)y^2)$, the latter when $d \equiv 3 \pmod 4$. For this, the following result is useful.

Lemma 38 *If q is a primitive positive binary quadratic form of discriminant Δ, and if $u(\Delta) := |\,\mathrm{Aut}^+(q)|$, then*

$$\sum_{q' \in \mathrm{gen}(q)} \frac{1}{|\,\mathrm{Aut}(q')|} \;=\; \frac{h(\Delta)}{2u(\Delta)g(\Delta)}. \tag{43}$$

Proof. Recall that $|\operatorname{Aut}^+(q)| = 2$ if $\Delta \neq -3, -4$; see [BV], p. 29. Since $h(-3) = h(-4) = 1$, it follows that $u(\Delta) = |\operatorname{Aut}^+(q)|$ only depends on Δ.

Let $\approx$ denote proper (or $\mathrm{SL}_2(\mathbb{Z})$) equivalence of binary forms, and let $\mathrm{Gen}(q)$ denote the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of all binary forms which are genus-equivalent to q. By Corollary 3.14, Theorem 3.15 and Theorem 3.21 of [Co] we see that

$$|\mathrm{Gen}(q)| \;=\; \frac{h(\Delta)}{g(\Delta)}. \tag{44}$$

Consider the map $c_q : \mathrm{Gen}(q) \to \mathrm{gen}(q)$ which takes an $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of forms to its $\mathrm{GL}_2(\mathbb{Z})$-equivalence class. This map is clearly surjective, and we have that

$$|c_q^{-1}(q')| \cdot |\operatorname{Aut}(q')| = 2u(\Delta), \quad \text{for all } q' \in \mathrm{gen}(q). \tag{45}$$

Indeed, we have that $|c_q^{-1}(q')| = 1$ if and only if $q' \approx (q')^c$, where $(q')^c$ is the opposite of q', and the latter condition is equivalent to the condition that $|\operatorname{Aut}(q')| = 2|\operatorname{Aut}^+(q')| = 2u(\Delta)$; see Jones [Jo], p. 162. (Jones calls such classes *ambiguous.*) On the other hand, if $|c_q^{-1}(q')| > 1$, then $|c_q^{-1}(q')| = 2$, and then $|\operatorname{Aut}(q')| = |\operatorname{Aut}^+(q')| = u(\Delta)$, so (45) holds in all cases. Thus (43) follows because by (45) and (44) we obtain that

$$\sum_{q' \in \mathrm{gen}(q)} \frac{2u(\Delta)}{|\operatorname{Aut}(q')|} \;=\; \sum_{q' \in \mathrm{gen}(q)} |c_q^{-1}(q')| \;=\; |\mathrm{Gen}(q)| \;=\; \frac{h(\Delta)}{g(\Delta)}.$$

Proposition 39 *Let $d \geq 1$ and put $\varepsilon(d) = 1$, if $d \equiv 0, 1, 5 \pmod 8$ and $\varepsilon(d) = 0$ otherwise. Then*

$$4S(\mathrm{gen}(x^2 + 4dy^2)^*) \;=\; \frac{h(-16d)}{g(-16d)} - 1 + \varepsilon(d), \tag{46}$$

except when $d = 1$, in which case $4S(\mathrm{gen}(x^2 + 4dy^2)^*) = 0$. Moreover, if $d \equiv 3 \pmod 4$, then

$$4S(\mathrm{gen}(4x^2 + 4xy + (d+1)y^2)) \;=\; \frac{h(-d)}{g(-d)} + 1. \tag{47}$$

Proof. Suppose first that $d \equiv 3 \pmod 4$, and let $q' \in \mathrm{gen}(q)$, where $q = 4x^2 + 4xy + (d+1)y^2$. Then $\mathrm{cont}(q') = 4$ and $\Delta(q') = -16d$, so by Proposition 32 and its proof we see that $a(q')^* = a(q') > 1$ if and only if $q' \sim q = 4q_1$, where $q_1 = x^2 + xy + \frac{1}{4}(d+1)y^2$. Since $|\operatorname{Aut}(4q_1)| = 2u(-d)$ and $\frac{a(4q_1)}{|\operatorname{Aut}(4q_1)|} = \frac{1}{2}$ by (38), we see that

$$S(\mathrm{gen}(q)) \;=\; \frac{1}{2} - \frac{1}{2u(-d)} + \sum_{q' \in \mathrm{gen}(q)} \frac{1}{|\operatorname{Aut}(q')|} \;=\; \frac{u(-d) - 1}{2u(-d)} + \sum_{q' \in \mathrm{gen}(q_1)} \frac{1}{|\operatorname{Aut}(q')|}.$$

Since q_1 is primitive with $\Delta(q_1) = -d$, we obtain from (43) that $S(\mathrm{gen}(q)) = \frac{u(-d)-1}{2u(-d)} + \frac{h(-d)}{2u(-d)g(-d)}$. Now if $d = 3$, then $h(-d) = g(-d) = 1$ and $u(-d) = 6$, so $S(\mathrm{gen}(q)) = \frac{1}{2}$. Thus (47) holds in this case. If $d > 3$, then $u(-d) = 2$, so $S(\mathrm{gen}(q)) = \frac{1}{4} + \frac{h(-d)}{4g(-d)}$, so (47) holds in all cases.

The proof of (46) is similar. Put $q = x^2 + 4dy^2$, and let $q' \in \mathrm{gen}(q)$. Note that q' is primitive with $\Delta(q') = -16d$. We observe that $q' \in \mathrm{gen}(q)^* \Leftrightarrow r_1(q') = 0 \Leftrightarrow q' \sim q$, so $\mathrm{gen}(q)^* = \emptyset$ when $d = 1$ because $h(-16) = 1$. Thus $S(\mathrm{gen}(q)^*) = 0$ in this case, so assume henceforth that $d > 1$.

By Proposition 32 and its proof we see that $a(q') > 1$ if and only if $q' \sim q_d$, where $q_d = 4x^2 + dy^2$ when d is odd, and $q_d = 4x^2 + 4xy + (d+1)y^2$ when d is even. Note that the condition $q' \equiv 0, 1 \pmod 4$ implies that $d \equiv 1 \pmod 4$ in the first case and $d \equiv 0 \pmod 4$ in the second case. Thus, if $d \equiv 3 \pmod 4$, then $a(q') = 1$, for all $q' \in \mathrm{gen}(q)^*$. Thus, since $|\mathrm{Aut}(q)| = 2u(-16d) = 4$, for all $d \geq 1$, we obtain from (43) that

$$S(\mathrm{gen}(q)^*) \;=\; \sum_{q' \in \mathrm{gen}(q)^*} \frac{1}{|\mathrm{Aut}(q')|} \;=\; -\frac{1}{4} + \sum_{q' \in \mathrm{gen}(q)} \frac{1}{|\mathrm{Aut}(q')|} \;=\; -\frac{1}{4} + \frac{h(-16d)}{4g(-16d)},$$

and so (46) holds in this case because here $\varepsilon(d) = 0$.

Now suppose that $d \equiv 1 \pmod 4$. Then $q_d \in \mathrm{gen}(q')$, as can be seen by observing that the generic characters of q_d (see [Co], p. 55) all have the value 1. Thus, since $|\mathrm{Aut}(q_d)| = 2u(-16d) = 4$ because q_d is ambiguous, it follows from (38) that

$$S(\mathrm{gen}(q)^*) \;=\; \frac{1}{2} - \frac{1}{4} + \sum_{q' \in \mathrm{gen}(q)^*} \frac{1}{|\mathrm{Aut}(q')|} \;=\; \sum_{q' \in \mathrm{gen}(q)} \frac{1}{|\mathrm{Aut}(q')|} \;=\; \frac{h(-16d)}{4g(-16d)},$$

and so (46) holds in this case as well because here $\varepsilon(d) = 1$.

Finally, suppose that d is even. By looking at the generic characters of q_d in this case, we see that $q_d \in \mathrm{gen}(q)$ if and only $d \equiv 0 \pmod 8$, i.e., if and only if $\varepsilon(d) = 1$. Thus, if $\varepsilon(d) = 0$, then $a(q') = 1$, for all $q' \in \mathrm{gen}(q)^*$, and so a similar calculation as for $d \equiv 3 \pmod 4$ shows that (46) holds in this case. On the other hand, if $\varepsilon(d) = 1$, then $q_d \in \mathrm{gen}(q)^*$, and then a similar calculation as for $d \equiv 1 \pmod 4$ shows that (46) holds. This proves (46) in all cases.

We can use the above results to prove Theorem 6 of the introduction.

Proof of Theorem 6. From Theorem 5 and Proposition 37 it follows that $N_A^* = 2^{\omega(d)-2}(4S(\Theta^*))$. Using (42), we see from Proposition 39 that $4S(\Theta_A^*) = \frac{h(-16d)}{g(-16d)} + c(d)$, with $c(d) = \frac{h(-d)}{g(-d)}$, if $d \equiv 3 \pmod 4$, and with $c(d) = \varepsilon(d) - 1$, if $d \not\equiv 3 \pmod 4$ and $d > 1$. This proves (7). If $d = 1$, then $S(\Theta_A^*) = S(\mathrm{gen}(x^2 + 4y^2)^*) = 0$ by Proposition 39, and so $N_A^* = 0$ in this case.

Remark 40 The above Theorem 6 represents a restatement of Hayashida's formula on p. 18 of [H1] in much simpler and compact form. However, it is not so easy to see that (7) gives the same formula as that of [H1] because that formula is expressed in terms of the class number h of $\mathbb{Q}(\sqrt{-d})$. To see the connection, note first that h is related to $h(-16d)$ (and to $h(-d)$) by the formula of Theorem 7.24 in [Co]; this leads to the function ψ as defined in [H1]. Moreover, if we use the fact that

$$g(\Delta) \;=\; 2^{\omega(|\Delta|)-1+\mu(\Delta)}, \tag{48}$$

where $\mu(\Delta) = 1$, if $\Delta \equiv 0 \pmod{32}$, $\mu(\Delta) = -1$, if $\Delta \equiv 4 \pmod{16}$, and $\mu(\Delta) = 0$ otherwise (see [Co], p. 54 or [K4], formula (18)), then it is not difficult (but a bit tedious) to derive the formulae of Hayashida by considering each of the five case distinctions listed in Hayashida's paper.

We now turn to the case of a CM product surface $A = E \times E'$, i.e. one for which $E \sim E'$ is an elliptic curve with complex multiplication. Note that this case includes all abelian surfaces A which are isogeneous to $E_0 \times E_0$, for some CM elliptic curve E_0/K; see [K3], Theorem 2.

In this case the description of the index $[G_A : H_A]$ and of the set Θ_A^* is more complicated than in the non-CM case. To simplify the description, we introduce the following terminology and notation.

Definition. A principal polarization $\theta \in \mathcal{P}(A)$ is called *odd* if $q_{(A,\theta)}$ represents an odd integer. We denote the set of such θ's by $\mathcal{P}(A)^{\mathrm{odd}} \subset \mathcal{P}(A)$, and also write $\mathcal{P}(A)^{\mathrm{ev}} := \mathcal{P}(A) \setminus \mathcal{P}(A)^{\mathrm{odd}}$. The elements in $\mathcal{P}(A)^{\mathrm{ev}}$ are called *even polarizations.* We also put

$$\Theta_A^{\mathrm{odd}} := \{q : q \sim q_{(A,\theta)},\, \theta \in \mathcal{P}(A)^{\mathrm{odd}}\}/\!\sim \;\text{ and }\; \Theta_A^{\mathrm{ev}} := \{q : q \sim q_{(A,\theta)},\, \theta \in \mathcal{P}(A)^{\mathrm{ev}}\}/\!\sim .$$

Notation. If $q(x,y) = ax^2 + bxy + cy^2$ is a binary quadratic form, then let f_q denote the ternary form

$$f_q(x,y,z) \;=\; x^2 \perp q = x^2 + 4ay^2 + 4byz + 4cz^2.$$

In addition, if $2|b$ and $a \equiv 3 \pmod 4$, then write $a_1 = \frac{a+1}{4}$ and $b_1 = \frac{b}{2}$, and put

$$g_q(x,y,z) \;=\; x^2 + a_1^2 a(a+4)y^2 + (b_1^2 + c)z^2 - a_1 b(a+2)yz - bxz + a(2a_1+1)xy.$$

Similarly, if $2|b$ and $c \equiv 3 \pmod 4$, then write $c_1 = \frac{c+1}{4}$ and $b_1 = \frac{b}{2}$, and put

$$g_q'(x,y,z) \;=\; x^2 + c_1^2 c(c+4)y^2 + (b_1^2 + a)z^2 - c_1 b(c+2)yz - bxz + c(2c_1+1)xy.$$

Note that f_q, g_q and g_q' are primitive forms. Moreover, f_q is properly primitive in the sense of Dickson [Di], whereas $2g_q$ and $2g_q'$ are improperly primitive forms because the coefficient of xy in both q_q and g_q' is odd.

Using the above notation, we can now formulate the analogue of Proposition 37 for CM product surfaces. Recall from the introduction that $q_{E,E'}$ denotes the degree function on $\mathrm{Hom}(E,E')$, which is a binary quadratic form if $E \sim E'$ is a CM elliptic curve.

Theorem 41 *Let $A \simeq E \times E'$ be a CM product surface and let $q_{E,E'} \sim q$, where $q = ax^2+bxy+cy^2$ is a binary quadratic form. Let $\Delta = b^2-4ac$ denote its discriminant and $\kappa = \mathrm{cont}(q) = \gcd(a,b,c)$ its content. Then the index $[G_A : H_A]$ is given by the formula (8), and $\Theta_A^{\mathrm{odd}} = \mathrm{gen}(f_q)$. Furthermore, $\Theta_A^{\mathrm{ev}} \neq \emptyset$ if and only if*

$$(49) \qquad 2|b \quad \text{and} \quad a \equiv 3\,(\mathrm{mod}\ 4) \ \text{or}\ c \equiv 3\,(\mathrm{mod}\ 4) \ \text{or}\ a+b+c \equiv 3\,(\mathrm{mod}\ 4).$$

If this is the case, then $q \sim q' = a'x^2 + b'xy + c'y^2$ with $a' \equiv 3\,(\mathrm{mod}\ 4)$. Moreover, if $\Delta \equiv 16\,(\mathrm{mod}\ 32)$, then $q \sim q'' = a''x^2 + b''xy + c''y^2$ with $a'' \equiv 3\,(\mathrm{mod}\ 4)$ and $c'' \equiv a'' + 4\,(\mathrm{mod}\ 8)$. In addition, if (49) holds, then

(50)
$$\Theta_A^{\mathrm{ev}} = \mathrm{gen}(4g_{q'}), \textit{if } \Delta \not\equiv 16\,(\mathrm{mod}\ 32), \textit{and } \Theta_A^{\mathrm{ev}} = \mathrm{gen}(4g_{q''}) \cup \mathrm{gen}(4g'_{q''}), \textit{otherwise.}$$

In order to prove this important result, we require some auxiliary results. We first observe:

Proposition 42 *In the situation of* Theorem 41 *we have that $\mathcal{P}(A)^{\mathrm{ev}} \neq \emptyset$ if and only if $4|\Delta$ and $q_{E,E'}(h) \equiv 3\,(\mathrm{mod}\ 4)$, for some $h \in \mathrm{Hom}(E,E')$.*

Proof. Recall from Proposition 23 of [K4] that we have an isomorphism

$$(51) \qquad \mathbf{D} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E,E') \xrightarrow{\sim} \mathrm{NS}(A)$$

such that $q_A(\mathbf{D}(a,b,h)) = ab - \deg(h) = ab - q_{E,E'}(h)$. In particular, we see that

$$(52) \qquad \mathbf{D}(a,b,h) \in \mathcal{P}(A) \quad \Leftrightarrow \quad ab - \deg(h) = 1 \text{ and } a > 0.$$

Let $\theta \in \mathcal{P}(A)$, so $\theta = \mathbf{D}(a,b,ch) \in \mathcal{P}(A)$, where $h \in \mathrm{Hom}(E,E')$ is primitive and $a,b,c \in \mathbb{Z}$ satisfy $ab - c^2\deg(h) = 1$. Then there exists h' such that h, h' is a basis of $\mathrm{Hom}(E,E')$, and then $D_1 := \mathbf{D}(1,0,0)$, $D_2 := \mathbf{D}(0,1,0)$, $D_3 := \mathbf{D}(0,0,h)$ and $D_4 := \mathbf{D}(0,0,h')$ is a basis of $\mathrm{NS}(A)$. Note that $\Delta = (\deg(h+h') - \deg(h) - \deg(h'))^2 - 4\deg(h)\deg(h)$.

We observe from (11) that $\theta \in \mathcal{P}(A)^{\mathrm{ev}}$ if and only if $(\theta.D) \equiv 0\,(\mathrm{mod}\ 2)$, for all $D \in \mathrm{NS}(A)$. Since $(D_1.\theta) = b$, $(D_2.\theta) = a$, $(D_3.\theta) = -2\deg(h)$, $(D_4.\theta) = c(D_4.D_3)$, and since $\gcd(a,b,c) = 1$, we see that

$$(53) \qquad \theta = \mathbf{D}(a,b,ch) \in \mathcal{P}(A)^{\mathrm{ev}} \quad \Leftrightarrow \quad 2|a,\ 2|b,\ 2|(D_3.D_4).$$

Moreover, since $(D_3.D_4) = -\deg(h+h') + \deg(h) + \deg(h')$, it follows that $\Delta \equiv (D_3.D_4)^2 \pmod 4$, and so we have that $2|(D_3.D_4)$ if and only if $4|\Delta$.

Thus, if $\theta = \mathbf{D}(a,b,ch) \in \mathcal{P}(A)^{\mathrm{ev}}$, then $4|\Delta$ and $2|a$, $2|b$. Thus, since $ab - \deg(ch) = 1$, we see that $\deg(ch) = ab - 1 \equiv 3 \pmod 4$, which proves one direction of the proposition.

Conversely, suppose that $4|\Delta$ and that there exists $h^* \in \mathrm{Hom}(E,E')$ such that $\deg(h^*) = n = 4k-1$. Write $h^* = ch$, with h primitive, and put $a = 2$, $b = 2k$. Then $ab - \deg(ch) = 1$, so $\theta := \mathbf{D}(2,2k,ch) \in \mathcal{P}(A)$, and by (53) and by the sentence after it we see that $\theta \in \mathcal{P}(A)^{\mathrm{ev}}$. Thus $\mathcal{P}(A)^{\mathrm{ev}} \neq \emptyset$, and so the proposition follows.

Remark 43 Note that if $A = E \times E'$ where $\mathrm{Hom}(E,E') = 0$, then it follows from (52) that $\mathcal{P}(A) = \{\theta\}$, where $\theta = \mathbf{D}(1,1,0)$. Since $q_{(A,\theta)}(\mathbf{D}(1,0,0)) = 1$, it follows from (26) that $\theta \notin \mathcal{P}(A)^*$, so $\mathcal{P}(A)^* = \emptyset$ and hence $N_A^* = 0$.

We now examine the condition of Proposition 42 in more detail.

Lemma 44 *Let $q(x,y) = ax^2 + bxy + cy^2$ be a binary quadratic form and suppose that $4|\Delta = \mathrm{disc}(q)$. Then:*

(a) *We have that $q(x,y) \equiv 3 \pmod 4$, for some $x, y \in \mathbb{Z}$, if and only if* (49) *holds.*

(b) *If* (49) *holds, then $q \sim q'$, where $q' = a'x^2 + b'xy + c'y^2$ and $a' \equiv 3 \pmod 4$.*

(c) *If $\Delta \equiv 16 \pmod{32}$ and if* (49) *holds, then $q \sim q''$, where $q'' = a''x^2 + b''xy + c''y^2$ and $a'' \equiv 3 \pmod 4$ and $c'' \equiv a'' + 4 \pmod 8$.*

Proof. (a) If (49) holds for q, then clearly $q(x,y) \equiv 3 \pmod 4$, for some $x, y \in \mathbb{Z}$. Indeed, if $a \equiv 3 \pmod 4$, then $q(1,0) = a \equiv 3 \pmod 4$, and if $c \equiv 3 \pmod 4$, then $q(0,1) = c \equiv 3 \pmod 4$. Finally, if $a+b+c \equiv 3 \pmod 4$, then $q(1,1) = a+b+c \equiv 3 \pmod 4$.

Conversely, suppose that $q(x,y) \equiv 3 \pmod 3$, for some $x, y \in \mathbb{Z}$. Since $4|\Delta$, we have that $2|b$. Thus, if $x \equiv 1 \pmod 2$ and $y \equiv 0 \pmod 2$, then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv bxy \equiv 0 \pmod 4$, so $a \equiv q(x,y) \equiv 3 \pmod 4$. Similarly, if $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 2$, then $c \equiv q(x,y) \equiv 3 \pmod 4$. Now suppose that $x \equiv y \equiv 1 \pmod 4$. Then $x^2 \equiv y^2 \equiv 1 \pmod 4$, and $bxy \equiv \pm b \equiv b \pmod 4$ because $2|b$, so $a+b+c \equiv q(x,y) \equiv 3 \pmod 4$. Thus (49) holds because the case $x \equiv y \equiv 0 \pmod 4$ is not possible.

(b) In what follows, we will use the abbreviation $q = [a,b,c]$ to denote $q(x,y) = ax^2 + bxy + cy^2$. Now if $a \equiv 3 \pmod 4$, then we can take $q = q'$. If $c \equiv 3 \pmod 4$, then we can take $q' = [c,b,a] \sim q$. Finally, if $a+b+c \equiv 3 \pmod 4$, then we can take $q' = [a+b+c, b+2c, c] \sim q$.

(c) By part (b) we have that $q \sim q' = [a',b',c']$, with $a' \equiv 3 \pmod 4$ and $2|b'$. Suppose first that $b' \equiv 2 \pmod 4$, so $b' = 2b_1$ with b_1 odd. Then the condition $\Delta \equiv 16 \pmod{32}$ implies that $b_1^2 - a'c' \equiv 4 \pmod 8$. Since $b_1^2 \equiv 1 \pmod 8$, we obtain that $a'c' \equiv -3 \pmod 8$. Thus, if $a' \equiv 3 \pmod 8$, then $c' \equiv 7 \pmod 8$, and if $a' \equiv 7 \pmod 8$, then $c' \equiv 3 \pmod 8$. Thus, we can take $q'' = q'$ when $b' \equiv 2 \pmod 4$.

Now suppose that $b' \equiv 0 \pmod 4$. Then we can take $q'' = [a', b'+2a', a'+b'+c'] \sim q' \sim q$ because $b' + 2a' \equiv 2 \pmod 4$. This proves (c).

Remark 45 It is clear from condition (49) that $\mathcal{P}(A)^{\text{ev}} = \emptyset$ if Δ is odd or if $\text{cont}(q_{E,E'})$ is even. Furthermore, if $\Delta \equiv 4$ or $8 \pmod{16}$, then an argument similar to the proof of Lemma 44 shows that (49) holds if and only if $\text{cont}(q_{E,E'})$ is odd. On the other hand, if $\Delta \equiv 0$ or $12 \pmod{16}$, and $\text{cont}(q_{E,E'})$ is odd, then condition (49) may or may not hold for $q \sim q_{E,E'}$.

We are now ready to prove Theorem 41. For this, we will use results from [K8], [K5], [K9] and Kir [Ki].

Proof of Theorem 41. The index formula (8) follows from Theorem 2 of [K8]. Next, consider $\theta_0 := \mathbf{D}(1,1,0) \in \mathcal{P}(A)^{\text{odd}}$. A short computation shows that $q_{(A,\theta_0)} \sim f_q$; see formula (29) of [K9]. Thus, if we apply Theorem 20 of [K5] to the quadratic module (NS_A, q_A), then we obtain that $\Theta_A^{\text{odd}} \subset \text{gen}(f_q)$. It therefore follows from Theorem 2 of [K9] that $\Theta_A^{\text{odd}} = \text{gen}(f_q)$.

By Proposition 42 and Lemma 44(a) we see that $\mathcal{P}(A)^{\text{ev}} = \emptyset$ if and only if (49) holds. Moreover, the existence of the forms q' and q'' follows from Lemma 44.

We next observe that $4g_{q'} \in \Theta_A^{\text{ev}}$, if $4|\Delta$. Indeed, since $q' \sim q_{E,E'}$, there exists a basis h, h' of $\text{Hom}(E, E')$ such that $q_{E,E'}(xh + yh') = q'(x, y)$, so $a' = \deg(h)$. Then $\theta_{q'} := \mathbf{D}(2, \frac{1}{2}(a'+1), h) \in \mathcal{P}(A)^{\text{ev}}$ by (52) and (53), and a short computation shows that $q_{(A,\theta_{q'})}(xD_2 + yD_3^* + zD_4) = 4g_q(x, y, z)$, where the D_i are as in the proof of Proposition 42, and $D_3^* = -a'D_1 - \frac{1}{2}(a'+1)D_3$. Since the images of D_2, D_3^* and of D_4 in $\text{NS}(A, \theta_{q'})$ form a basis of $\text{NS}(A, \theta_{q'})$ by Proposition 29 of [K4], it follows that $q_{(A,\theta_{q'})} \sim 4g_q$. Similarly, if $\Delta \equiv 16 \pmod{32}$, and if $\theta_{q''} := \mathbf{D}(2, \frac{1}{2}(c+1), h')$, then we see that $\theta_{q''} \in \mathcal{P}(A)^{\text{ev}}$ and that $q_{(A,\theta_{q''})} \sim 4g'_{q''}$.

Now if $\Delta \not\equiv 16 \pmod{32}$, then by Theorem 21 of [Ki] we know that Θ_A^{ev} lies in a single genus so $\Theta_A^{\text{ev}} \subset \text{gen}(4g_{q'})$ since $4g_{q'} \in \Theta_A^{\text{ev}}$ as was shown above. Then by Theorem 1 of [Ki] it follows that $\Theta_A^{\text{ev}} = \text{gen}(4g_{q'})$.

On the other hand, if $\Delta \equiv 16 \pmod{32}$, then by Theorem 21 of [Ki] again we know that Θ_A^{ev} lies in two disjoint genera. Moreover, the proof of that result shows that in fact $\Theta_A^{\text{ev}} \subset \text{gen}(q_{(A,\theta'_1)}) \cup \text{gen}(q_{(A,\theta'_2)})$ with $\theta'_i = \mathbf{D}(2, \frac{1}{2}(r_i+1), h_i)$, where each $h_i \in \text{Hom}(E, E')$ is primitive of degree $r_i \equiv 3 \pmod 4$ and $r_2 \equiv r_1 + 4 \pmod 8$. It thus follows from what was said above that $\Theta_A^{\text{ev}} \subset \text{gen}(4g_{q''}) \cup \text{gen}(4g'_{q''})$. Moreover, Theorem 1 of [Ki] shows that equality holds, which proves (50).

Remark. Strictly speaking, the above proof of Theorem 41 is only valid when $\text{char}(K) = 0$ because Kir [Ki] makes this hypothesis. But if we use the argument of the proof of

Theorem 2 in [K9], then we see that the results of [Ki] can be extended to arbitrary characteristic.

We are now ready to prove Theorem 7, which will be deduced from the following much more general result. To state it, let

$$N_A^{*,\mathrm{odd}} = |\{C \in \mathfrak{C}(A) : \theta_C \in \mathcal{P}(A)^{\mathrm{odd}}\}/\simeq|$$

denote the number of isomorphism classes of curves on A whose theta-divisor lies in $\mathcal{P}(A)^{\mathrm{odd}}$, and let $N_A^{*,\mathrm{ev}} = |\{C \in \mathfrak{C}(A) : \theta_C \in \mathcal{P}(A)^{\mathrm{ev}}\}/\simeq|$, so $N_A^* = N_A^{*,\mathrm{odd}} + N_A^{*,\mathrm{ev}}$. We then have:

Theorem 46 *Let $A = E \times E'$ be a CM product surface over a field K. As before, let $\Delta = \mathrm{disc}(q_{E,E'})$, $\kappa = \mathrm{cont}(q_{E,E'})$ and $\Delta' = \Delta/\kappa^2$. Then*

$$N_A^{*,\mathrm{odd}} = \frac{2^{\omega(\kappa)+1}g(\Delta')h(\Delta)}{h(\Delta')}S(\mathrm{gen}(f_q)^*), \tag{54}$$

where f_q is as in Theorem 41*. Moreover, $N_A^{\mathrm{ev}} > 0$ if and only if condition* (49) *holds. If this is the case, and if $\Delta \not\equiv 16 \pmod{32}$, then*

$$N_A^{*,\mathrm{ev}} = \frac{2^{\omega(\kappa)+1}g(\Delta')h(\Delta)}{h(\Delta')}S(\mathrm{gen}(4g_{q'})), \tag{55}$$

where q' and $g_{q'}$ are as in Theorem 41*. Furthermore, if $\Delta \equiv 16 \pmod{32}$, and if* (49) *holds, and if q'', $g_{q''}$ and $g'_{q''}$ are as in* Theorem 41*, then*

$$N_A^{*,\mathrm{ev}} = \frac{2^{\omega(\kappa)+1}g(\Delta')h(\Delta)}{h(\Delta')}\left(S(\mathrm{gen}(4g_{q''})) + S(\mathrm{gen}(4g'_{q''}))\right). \tag{56}$$

Proof. Put $\mathcal{P}(A)^{*,\mathrm{odd}} = \mathcal{P}^*(A) \cap \mathcal{P}(A)^{\mathrm{odd}}$ and $\overline{\mathcal{P}}(A)^{*,\mathrm{odd}} = H_A\backslash\mathcal{P}(A)^{*,\mathrm{odd}}$. Then as in the proof of Theorem 5 in §5 we have that

$$\mathcal{P}(A)^{*,\mathrm{odd}} = \coprod_{f\in\Theta_A^{*,\mathrm{odd}}} \mathcal{P}(A,f) \quad \text{and} \quad \overline{\mathcal{P}}(A)^{*,\mathrm{odd}} = \coprod_{f\in\Theta_A^{*,\mathrm{odd}}} \overline{\mathcal{P}}(A,f),$$

and by a similar argument as in that proof we see that $N_A^{*,\mathrm{odd}} = |\overline{\mathcal{P}}(A)^{*,\mathrm{odd}}| = [G_A : H_A]S(\Theta_A^{*,\mathrm{odd}})$. Now by (50) and (26) we see that $\Theta_A^{*,\mathrm{odd}} = \mathrm{gen}(f_q)^*$, so (54) follows by using (8).

Next, consider $\theta \in \mathcal{P}(A)^{\mathrm{ev}}$. Since $4|\,\mathrm{cont}(q_{(A,\theta)})$, it follows that $q_{(A,\theta)}$ cannot represent 1, and so $\theta \in \mathcal{P}^*(A)$ by (26). Thus $\mathcal{P}(A)^{*,\mathrm{ev}} := \mathcal{P}^*(A) \cap \mathcal{P}(A)^{\mathrm{ev}} = \mathcal{P}(A)^{\mathrm{ev}}$ and $\overline{\mathcal{P}}(A)^{*,\mathrm{ev}} = H_A\backslash\mathcal{P}(A)^{*,\mathrm{ev}} = H_A\backslash\mathcal{P}(A)^{\mathrm{ev}} =: \overline{\mathcal{P}}(A)^{\mathrm{ev}}$. Thus, by a similar argument as above we see that $N_A^{*,\mathrm{ev}} = |\overline{\mathcal{P}}(A)^{*,\mathrm{ev}}| = |\overline{\mathcal{P}}(A)^{\mathrm{ev}}| = [G_A : H_A]S(\Theta_A^{\mathrm{ev}})$, and so (55) and (56) follow directly from (50) and (8).

Proof of Theorem 7. In this situation we have that $N_A^{*,\mathrm{ev}} = 0$ by Theorem 46 (see Remark 45), so $N_A^* = N_A^{*,\mathrm{odd}}$, which is given by (54). This proves Theorem 7.

Remark 47 If $A' = E_1 \times E_2$ is another CM product surface such that q_{E_1,E_2} and $q_{E,E'}$ are genus-equivalent, then $\Delta = \mathrm{disc}(q_{E_1,E_2}) = \mathrm{disc}(q_{E,E'})$ and $\kappa = \mathrm{cont}(q_{E_1,E_2}) = \mathrm{cont}(q_{E,E'})$, so by (8) we see that $[G_{A'} : H_{A'}] = [G_A : H_A]$. Moreover, it follows from Corollary 30 of [K9] that $\Theta^*_{A'} = \Theta^*_A$, so $S(\Theta^*_{A'}) = S(\Theta^*_A)$, and hence $N^*_{A'} = N^*_A$ by (6). Thus we see that N^*_A depends only on the genus of the form $q_{E,E'}$. Similarly, by using (54) we see that $N^{*,\mathrm{odd}}_A$ only depends on the genus of $q_{E,E'}$.

As was mentioned in the introduction, Theorem 46 allows us to compute N^*_A for each CM product surface $A = E \times E'$, provided we know the equivalence class of $q_{E,E'}$. Here is an algorithm for doing this.

Algorithm for computing N^*_A for a CM product surface $A = E \times E'$.
Suppose that $q_{E,E'} \sim q$, where $q(x, y) = ax^2 + bxy + cy^2$.

Part I: The Computation of $I := [G_A : H_A]$.

1) Compute $\kappa = \gcd(a, b, c)$ and $\Delta = b^2 - 4ac$. If $\kappa = 1$, then by formula (8) we have that $I = 2g(\Delta)$, where $g(\Delta)$ is given by formula (48).

2) If $\kappa > 1$, then by formula (8) we have that $I = 2^{\omega(\kappa)+1} g(\Delta')h(\Delta', \kappa)$, where $\Delta' = \frac{\Delta}{\kappa^2}$ and

$$h(\Delta', \kappa) \;:=\; \frac{h(\kappa^2\Delta')}{h(\Delta')} \;=\; \frac{\kappa}{w}\prod_{p|\kappa}\left(1 - \frac{1}{p}\left(\frac{\Delta'}{p}\right)\right);$$

see [Co], Corollary 7.28. Here $(\frac{\Delta'}{p})$ denotes the Legendre-Kronecker symbol and $w = 3$, if $\Delta' = -3$, $w = 2$, if $\Delta = -4$, and $w = 1$ otherwise.

Part II: The Computation of $N^{*,\mathrm{odd}}_A$.

1) Make a list L_1 of all positive, properly primitive, Eisenstein-reduced ternary forms f of discriminant $\mathrm{disc}(f) = 16\Delta$ in the sense of Watson [Wa] (or of determinant $d(f) = -4\Delta$ in the sense of [Di]) which satisfy the condition that $f \equiv 0, 1 \pmod 4$.

2) For each $f \in L_1$, check whether $f \in \mathrm{gen}(f_q)$, where $f_q = x^2 \perp 4q$. This is done by computing and comparing the genus invariants and genus characters of f and f_q; see [Di], §32. Let L_2 be the subset of forms satisfying this condition.

3) (Optional) Check that the list L_2 is correct by computing its mass $M(L_2) = \sum_{f\in L_2} |\operatorname{Aut}^+(f)|^{-1}$ and comparing it to the result given by the mass formula of Eisenstein/Smith/Brandt; see [K5]. Note that the automorphism group $\operatorname{Aut}^+(f)$ of a reduced form f can be computed by using [Di], Theorem 105.

4) Remove from L_2 the forms f for which $a = 1$ (in the notation of Corollary 35). Then the resulting list $L_3 = \{f_1, \dots f_t\}$ is a system of representatives of $\mathrm{gen}(f_q)^*$.

5) Use Corollary 35 and [Di], Theorem 105, to compute $\frac{a(f_i)}{2|\operatorname{Aut}^+(f_i)|}$, for $1 \le i \le t$, and add these to obtain the sum $S_1 := S(\mathrm{gen}(f_q)^*)$. Then by (54) we have that $N^{*,\mathrm{odd}}_A = IS_1$.

Part III: The Computation of N_A^*.

1) If condition (49) does not hold, then $N_A^* = N_A^{*,\mathrm{odd}}$, and we are done by Part II.

2) Assume henceforth that (49) holds. Compute $q' \sim q$ satisfying the condition of Theorem 41 by using the recipe given in the proof of Lemma 44(b). Moreover, if $\Delta \equiv 16 \pmod{32}$, then compute $q'' \sim q$ satisfying the conditions of Theorem 41 by using the recipe given in the proof of Lemma 44(c).

3) Make a list L_4 of all positive primitive Eisenstein reduced forms f of discriminant $\frac{\Delta}{4}$ such that $2f$ is improperly primitive (so $2f$ has determinant $d(2f) = -\frac{\Delta}{2}$).

4) If $\Delta \not\equiv 16 \pmod{32}$, then for each $f \in L_4$, check whether $f \in \mathrm{gen}(g_{q'})$, and let L_5 be the subset of forms satisfying this condition. If $\Delta \equiv 16 \pmod{32}$, then for each $f \in L_4$, check whether $f \in \mathrm{gen}(g_{q''}) \cup \mathrm{gen}(g'_{q''})$, and let L_5 be the subset of forms satisfying this condition. As before, this check is done by computing and comparing the genus invariants and genus characters of $2f$ and of $2g_{q'}$ (or of $2g_{q''}$ and $2g'_{q''}$); see [Di], §32.

5) For each $f \in L_5$, compute $a(4f) = \max(1, r_4(4f), 3r_4(4f) - 12)$, so $a(4f) = \max(1, r_1(f), 3r_1(f) - 12)$. Here $r_1(f)$ can be computed by the method of Remark 36. Moreover, $|\,\mathrm{Aut}(4f)| = 2|\,\mathrm{Aut}^+(2f)$ can be computed by using Theorem 105 of Dickson [Di]. Thus, by computing the sum S_2 of the terms $\frac{a(4f)}{|\,\mathrm{Aut}(4f)|}$ with $f \in L_5$, we obtain that $N_A^{*,\mathrm{ev}} = IS_2$ by (55) and (56). Thus $N_A^* = N_A^{*,\mathrm{odd}} + N_A^{*,\mathrm{ev}}$.

By using the above algorithm we obtain the following table of values for $N_A^{*,\mathrm{odd}}$ and N_A^* for $|\Delta| \le 100$. Here we write $q_{E,E'} = \kappa q'_{E,E'}$ and use the abbreviation $[a, b, c]$ for $q(x, y) = ax^2 + bxy + cy^2$ as in the proof of Lemma 44. The table below gives a representative of each of the $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of positive binary forms q with $|\Delta| = |\,\mathrm{disc}(q)| \le 100$. Note that by using Remark 47 the list could have been shortened by listing only one representative of each of the genera of the forms involved, but such a table would not be as convenient because it is then more difficult to identify a given form in the table.

It is useful to observe that the numbers N_A^* of the table below agree with those obtained by Hayashida [H2] in the cases that his formula applies; these cases are marked with an asterisk (*). Note that these are the precisely the cases for which $\Delta = \Delta'$ is a fundamental discriminant and q is the principal form of discriminant Δ.

$\lvert\Delta'\rvert$	$q'_{E,E'}$	κ	$N_A^{*,\text{odd}}$	N_A^*
3	$[1,1,1]$	1	0	0^*
		2	0	0
		3	1	1
		4	0	0
		5	2	2
4	$[1,0,1]$	1	0	0^*
		2	0	0
		3	0	2
		4	1	1
		5	2	2
7	$[1,1,2]$	1	0	0^*
		2	1	1
		3	4	4
8	$[1,0,2]$	1	0	1^*
		2	0	0
		3	2	4
11	$[1,1,3]$	1	1	1^*
		2	0	0
		3	6	6
12	$[1,0,3]$	1	0	1
		2	2	2
15	$[1,1,4]$	1	0	0^*
		2	2	2
15	$[2,1,2]$	1	1	1
		2	2	2
16	$[1,0,4]$	1	1	1
		2	2	2
19	$[1,1,5]$	1	1	1^*
		2	1	1
20	$[1,0,5]$	1	1	1^*
		2	0	0
20	$[2,2,3]$	1	0	2
		2	1	1
23	$[1,1,6]$	1	1	1^*
		2	3	3
23	$[2,1,3]$	1	1	1
		2	3	3
24	$[1,0,6]$	1	0	1^*
		2	2	2
24	$[2,0,3]$	1	1	2
		2	0	0
27	$[1,1,7]$	1	1	1
28	$[1,0,7]$	1	1	2
31	$[1,1,8]$	1	1	1^*
31	$[2,1,4]$	1	1	1
32	$[1,0,8]$	1	2	2
32	$[3,2,3]$	1	1	3
35	$[1,1,9]$	1	2	2^*
35	$[3,1,3]$	1	3	3
36	$[1,0,9]$	1	1	1
36	$[2,2,5]$	1	2	2
39	$[1,1,10]$	1	1	1^*
39	$[2,1,5]$	1	2	2
39	$[3,3,4]$	1	1	1
40	$[1,0,10]$	1	1	2^*
40	$[2,0,5]$	1	1	2
43	$[1,1,11]$	1	2	2^*
44	$[1,0,11]$	1	1	3
44	$[3,2,4]$	1	1	3
47	$[1,1,12]$	1	2	2^*
47	$[2,1,6]$	1	2	2
47	$[3,1,4]$	1	2	2
48	$[1,0,12]$	1	2	2
48	$[3,0,4]$	1	1	3
51	$[1,1,13]$	1	2	2^*
51	$[3,3,5]$	1	4	4
52	$[1,0,13]$	1	2	2^*
52	$[2,2,7]$	1	1	3
55	$[1,1,14]$	1	2	2^*
55	$[2,1,7]$	1	2	2
55	$[4,3,4]$	1	2	2
56	$[1,0,14]$	1	1	3^*
56	$[2,0,7]$	1	1	3
56	$[3,2,5]$	1	2	4
59	$[1,1,15]$	1	4	4^*
59	$[3,1,5]$	1	4	4
60	$[1,0,15]$	1	2	4
60	$[3,0,5]$	1	3	5

$\lvert\Delta'\rvert$	$q'_{E,E'}$	κ	$N_A^{*,\text{odd}}$	N_A^*
63	$[1,1,16]$	1	1	1
63	$[2,1,8]$	1	3	3
63	$[4,1,4]$	1	1	1
64	$[1,0,16]$	1	3	3
64	$[4,4,5]$	1	3	3
67	$[1,1,17]$	1	3	3^*
68	$[1,0,17]$	1	3	3^*
68	$[3,2,6]$	1	1	5
68	$[2,2,9]$	1	3	3
71	$[1,1,18]$	1	3	3^*
71	$[2,1,9]$	1	3	3
71	$[3,1,6]$	1	3	3
71	$[4,3,5]$	1	3	3
72	$[1,0,18]$	1	1	2
72	$[2,0,9]$	1	3	4
75	$[1,1,19]$	1	3	3
75	$[3,3,7]$	1	3	3
76	$[1,0,19]$	1	2	4
76	$[4,2,5]$	1	2	4
79	$[1,1,20]$	1	3	3^*
79	$[2,1,10]$	1	3	3
79	$[4,1,5]$	1	3	3
80	$[1,0,20]$	1	5	5
80	$[3,2,7]$	1	2	6
80	$[4,0,5]$	1	5	5
83	$[1,1,21]$	1	5	5^*
83	$[3,1,7]$	1	5	5

$\lvert\Delta'\rvert$	$q'_{E,E'}$	κ	$N_A^{*,\text{odd}}$	N_A^*
84	$[1,0,21]$	1	2	2^*
84	$[2,2,11]$	1	2	6
84	$[3,0,7]$	1	1	5
84	$[5,4,5]$	1	5	5
87	$[1,1,22]$	1	2	2^*
87	$[2,1,11]$	1	5	5
87	$[3,3,8]$	1	5	5
87	$[4,3,6]$	1	2	2
88	$[1,0,22]$	1	2	4^*
88	$[2,0,11]$	1	3	4
91	$[1,1,23]$	1	4	4^*
91	$[5,3,5]$	1	5	5
92	$[1,0,23]$	1	4	7
92	$[3,2,8]$	1	4	7
95	$[1,1,24]$	1	4	4^*
95	$[2,1,12]$	1	4	4
95	$[3,1,8]$	1	4	4
95	$[4,1,6]$	1	4	4
95	$[5,5,6]$	1	4	4
96	$[1,0,24]$	1	4	4
96	$[3,0,8]$	1	4	8
96	$[4,4,7]$	1	2	6
96	$[5,2,5]$	1	6	6
99	$[1,1,25]$	1	3	3
99	$[5,1,5]$	1	6	6
100	$[1,0,25]$	1	4	4
100	$[2,2,13]$	1	3	3

References

[AP] R. Accola, E. Previato, Covers of tori: genus two. *Lett. Math. Phys.* **76** (2006), 135–161.

[BV] J. Buchmann, U. Vollmer, *Binary Quadratic Forms.* Springer-Verlag, Berlin, 2007.

[Co] D. Cox, *Primes of the Form* $x^2 + ny^2$. Wiley & Sons, New York, 1989.

[Di] L. Dickson, *Studies in Number Theory.* U Chicago Press, Chicago, 1930. Reprinted by Chelsea Publ. Co., New York, 1957.

[FK] G. Frey, E. Kani, Curves of genus 2 covering elliptic curves and an arithmetical application. In: *Arithmetic Algebraic Geometry* (G. van der Geer, F. Oort, J. Steenbrink, eds.), Progress In Math. vol. 89, Birkhäuser, Boston, 1991, pp. 153-176.

[GHR] A. Gélin, E. Howe, C. Ritzenthaler, Principal polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. *Proc. 13th Algorithmic Number Theory Symposium.* Open Book Ser. **2** (2019), 257–274.

[H1] T. Hayashida, A class number associated with a product of two elliptic curves. *Natur. Sci. Rep. Ochanomizu Univ.* **16** (1965), 9–19.

[H2] T. Hayashida, A class number associated with the product of an elliptic curve with itself. *J. Math. Soc. Japan* **20** (1968), 26–43.

[HN1] T. Hayashida, M. Nishi, Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* **17** (1965), 1–16.

[HN2] T. Hayashida, M. Nishi, On certain type of Jacobian varieties of dimension 2. *Natur. Sci. Rep. Ochanomizu Univ.* **16** (1965), 49–57.

[IKO] T. Ibukiyama, T. Katsura, T. Oort, Supersingular curves of genus 2 and class numbers. *Compositio Math.* **57** (1986), 127–152.

[Ig] J.-I. Igusa, Arithmetic variety of moduli for genus 2. *Ann. Math.* **72** (1960), 612–649.

[Jo] B. Jones, *The Arithmetic Theory of Quadratic Forms.* Carus Math. Monograph No. 10, MAA, 1960.

[K1] E. Kani, Elliptic curves on abelian surfaces. *Manusc. math.* **84** (1994), 199–223.

[K2] E. Kani, The number of curves of genus two with elliptic differentials. *J. reine angew. Math.* **485** (1997), 93–121.

[K3] E. Kani, Products of CM elliptic curves. *Collectanea Math.* **62** (2011), 297–339.

[K4] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67** (2016), 21–54.

[K5] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *J. Number Theory* **139** (2014), 138–174.

[K6] E. Kani, Elliptic subcovers of a curve of genus 2 I. The isogeny defect. *Ann. Math. Québec* **43** (2019), 281–303.

[K7] E. Kani, Elliptic subcovers of a curve of genus 2 II. The refined Humbert invariant. *J. Number Theory* **193** (2018), 302–335.

[K8] E. Kani, The structure of $\mathrm{Aut}(q_A)$. Preprint, 30 pages.

[K9] E. Kani, The refined Humbert invariant for abelian product surfaces with complex multiplication. Preprint, 23 pages.

[K10] E. Kani, Principal polarizations on abelian product surfaces. Preprint, 17 pages.

[Ki] H. Kir, The refined Humbert invariant for imprimitive ternary forms. Preprint.

[Mi] J.S. Milne, Jacobian varieties. In: *Arithmetic Geometry.* (G. Cornell, J. Silverman, eds.), Springer-Verlag, New York, 1986; pp. 165–212.

[Mu] D. Mumford, *Abelian Varieties.* Oxford U Press, Oxford, 1970.

[SV] T. Shaska, H. Völklein, Elliptic subfields and automorphisms of genus 2 functions fields. In: *Algebra, Arithmetic and Geometry with Applications*, Springer-Verlag, Berlin, 2004; pp. 703–723.

[Wa] G. Watson, *Integral Quadratic Forms.* Cambridge U Press, Cambridge, 1960.

[We] A. Weil, Zum Beweis des Torellischen Satzes. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse* 1957, no. 2 = Œuvres II, pp. 307–327.