NÉRON-SEVERI GROUPS OF PRODUCT ABELIAN SURFACES

JULIAN ROSEN AND ARIEL SHNIDMAN

ABSTRACT. Let $E$ and $E'$ be elliptic curves with $\text{Hom}(E, E') = \mathbb{Z}$. We parameterize the Néron-Severi group of $A = E \times E'$ in terms of binary quadratic forms. As an application, we determine whether $A$ contains a smooth curve of any fixed genus and whether $A$ admits a very ample line bundle of any fixed degree. In particular, we determine which of these abelian surfaces embed in $\mathbb{P}^4$, i.e. which come from the Horrocks-Mumford bundle.

Contents

1. Introduction 1
2. Preliminaries on abelian surfaces 6
3. Product abelian surfaces of Picard number 2 9
4. Product abelian surfaces of Picard number 3 9
5. Smooth polarizations on $A_m$ 16
6. Very ample polarizations on $A_m$ 18
References 26

1. Introduction

Let $A$ be an abelian surface over an algebraically closed field $k$ of characteristic 0. A polarization $L$ on $A$ is the class in $\text{NS}(A) = \text{Pic}(A)/\text{Pic}^0(A)$ of an ample line bundle. The degree $d = d(L)$ of $L$ is by definition

$$d = \chi(L) = h^0(A, L) = \frac{1}{2}(L.L).$$

We say $L$ is smooth if it is represented by $\mathcal{O}(C)$ for some smooth curve $C$, necessarily of genus $d + 1$. We say $L$ is very ample if it is represented by a very ample line bundle.

Question 1. Given an abelian surface $A$ and an integer $d \geq 1$, does there exist a smooth (resp. very ample) polarization on $A$ of degree $d$?

The main tool available to determine whether a given polarization $L$ is smooth or very ample is the following marvelous result due mostly to Reider (see Section 2).

Theorem 1.1 (Reider, [BL]). Let $L \in \text{NS}(A)$ be ample. Then $L$ is smooth if and only if $L.E > 1$ for all elliptic curves $E \subset A$. If $d = \deg(L) \geq 5$ and $L$ is indivisible in $\text{NS}(A)$, then $L$ is very ample if and only if $L.E > 2$ for all elliptic curves $E \subset A$.

Remark Note that if $L.E = 1$, then $L$ cannot be smooth because any smooth $C \in |L|$ admits a degree 1 map to the elliptic curve $A/E$. Hence $C$ is an elliptic curve, and $L$ is not ample. Similarly, if $L.E \leq 2$, then $L|_E$ is not very ample, and so neither is $L$. The content of the theorem is that the converse statements are true as well. Note also that if $L$ is very ample, then $L$ is smooth by Bertini’s theorem.

Remark A very ample $L \in \text{Pic}(A)$ has degree $d \geq 5$. Indeed, $d = h^0(A, L)$ and $A$ cannot embed in $\mathbb{P}^3$, since $H^1(A, \mathbb{Z}) \neq 0$. 
An abelian surface $A$ containing an elliptic curve is said to be split. Otherwise we say $A$ is simple. Reider’s theorem implies that on simple abelian surfaces, every indivisible polarization of degree $d \geq 5$ is both smooth and very ample. Question 1 is therefore equivalent to the purely arithmetic question of determining the integers $d$ which are represented by the intersection form on $\text{NS}(A)$. When $A$ is split, Question 1 has a more geometric flavor, as the elliptic curves on $A$ need to be taken in to account. The present work considers abelian surfaces which are products of elliptic curves.

1.1. Outline of approach. We consider product surfaces $A = E \times E'$ such that $E$ and $E'$ do not possess CM by the same imaginary quadratic field. These are exactly the product surfaces with Picard number $\rho(A) := \text{rk}(\text{NS}(A))$ equal to 2 or 3.\footnote{Note that there are split abelian surfaces of Picard number 2 and 3 which are not products of elliptic curves.}

In the case $A = E \times E'$ with $E$ and $E'$ not isogenous (equivalently, $\rho(A) = 2$), $\text{NS}(A)$ is generated by the horizontal and vertical divisors, and up to translation these are the only elliptic curves on $A$. It is straightforward to answer Question 1 in this case, and this is done in Section 3.

The case $A = E \times E'$ with $E$ isogenous to $E'$ is more difficult because $\rho(A) \geq 3$ and there are infinitely many elliptic curves on $A$. If $\text{End}(E) = \text{End}(E') = \mathbb{Z}$, then $\text{NS}(A)$ is freely generated by the horizontal axis, the vertical axis, and the graph of a minimal isogeny $\lambda : E \to E'$. The integer $m := \deg(\lambda)$ is independent of the choice of product structure on $A$, and (following Kani) we refer to $A$ as an abelian surface of type $m$. If $A$, $B$ are abelian surfaces of Picard number 3 and the same type $m$, then there is an isomorphism $\text{NS}(A) \cong \text{NS}(B)$ preserving the intersection pairing (see Section 4). By Reider’s Theorem 1.1, the answer to Question 1 depends only on the intersection pairing on $\text{NS}(A)$, so the answers for $A$ and $B$ will be the same.

For a fixed positive integer $m$, let $A_m = E \times E'$ be a product surface of Picard number 3 and type $m$. We associate with $L \in \text{NS}(A)$ the quadratic form

$$q_L : \text{Hom}(E, A_m) \to \mathbb{Z},$$

$$f \mapsto \deg(f^*L).$$

The corresponding bilinear form is integer valued, and degenerate over $\mathbb{Z}/m\mathbb{Z}$. The group $\text{Hom}(E, A_m)$ has rank 2, and with respect to an appropriately chosen basis the quadratic form $q_L$ has matrix

(1.1) \[
\begin{pmatrix}
ma & mb \\
mb & c
\end{pmatrix} : a, b, c \in \mathbb{Z}.
\]

In fact, $L \mapsto q_L$ gives a bijection

$$\Phi : \text{NS}(A_m) \to V_m,$$

where $V_m$ is the space of all integral quadratic forms of the shape (1.1). This bijection has the following properties:

1. If $L \in \text{NS}(A_m)$ is ample, then $q_L$ is positive definite.
2. If $L$ has degree $d$, then $q_L$ has discriminant $-4md$.
3. $\Phi$ is equivariant for the action of $\text{Aut}(A_m) \cong \Gamma_0(m)$ on both sides.
4. If $F$ is the image of a map $f : E \to A_m$, then

$$q_L(f) = \deg(f) \cdot (L.F).$$

Suppose now that $L \in \text{NS}(A_m)$ has degree $d$, and for simplicity assume that $d$ is a prime not dividing $m$ and that $d \not\equiv 3 \pmod{4}$. Property (4) implies that $L.F = n$ for some elliptic curve $F \subset A_m$ isomorphic to $E$ if and only if $q_L$ represents $n$. In particular, $L.F = 1$ for some $F \cong E$ if and only if $q_L$ corresponds to the trivial class in the class group $\text{Pic}(\mathcal{O}_{-4md})$ of quadratic forms of discriminant $-4md$. Similarly, $L.F = 2$ if and only if $q_L$ corresponds to the ideal class $[p]$ of the prime $p \subset \mathcal{O}_{-4md}$ above the rational prime 2. Note that $[p]$ is 2-torsion under our simplifying
We analyze the bijection 

Theorem 1.4. Theorem 1.3. for the surfaces

\[ \text{q-classes of integral quadratic forms of discriminant \(N\)} \]

has degree \(A\) smooth polarizations on the product surface

\[ \text{q-smooth if and only if} \]

\[ \text{Aut(} \text{)} \text{which acts on} \]

\[ \text{A-admits a very ample polarization of degree} \]

\[ \text{A-integer. Then} \]

\[ \text{to count the number of degree} \]

\[ \text{(smooth or very ample) polarizations on} \]

\[ \text{A-up to Aut(A)-equivalence.} \]

1.2. Results. We answer Question 1.1 for product abelian surfaces \(A/k\) which are not isogenous to a self-product of a CM elliptic curve. Recall that we assume \(k = \bar{k}\) has characteristic 0.\(^2\) Our first result (which is proven in Theorem 3.3) concerns product surfaces whose factors are not isogenous.

**Theorem 1.2.** Suppose \(A = E \times E'\) with \(E, E'\) non-isogenous elliptic curves, and let \(d\) be a positive integer. Then \(A\) admits a smooth polarization of degree \(d\) if and only if \(d\) is composite. For \(d \geq 5\), \(A\) admits a very ample polarization of degree \(d\) if and only if \(d\) is neither a prime nor twice a prime.

Next suppose \(E\) and \(E'\) are isogenous with \(\text{End}(E) = \mathbb{Z}\), and that the minimal isogeny \(\lambda : E \to E'\) has degree \(m \geq 1\). As before, we set \(A_m = E \times E'\) and let \(\text{Pic}(\mathcal{O}_N)\) denote the group of isomorphism classes of integral quadratic forms of discriminant \(N\). We prove the following result concerning smooth polarizations on the product surface \(A_m:\)

**Theorem 1.3.** Let \(m, d \geq 1\). Then \(A_m\) admits a smooth polarization of degree \(d\) if and only if \(md \geq 2\) and at least one of the following conditions is satisfied:

- \(d\) is composite.
- \((m, d) > 1\).
- \(md\) is odd or divisible by 8.
- \(\text{Pic}(\mathcal{O}_{-4md})\) is not 2-torsion.

We also prove an analog of Theorem 1.3 for very ample polarizations.

**Theorem 1.4.** Suppose \(m \geq 1, d \geq 5\).

- If \(d\) is not a prime or twice a prime, then \(A_m\) admits a very ample polarization of degree \(d\).
- If \(d = p\) is prime, then \(A_m\) admits a very ample polarization of degree \(d\) if and only if either \(p|m\) or \(\text{Pic}(\mathcal{O}_{-4md})\) is not 2-torsion.
- If \(d = 2p\) is twice a prime, then \(A_m\) admits a very ample polarization of degree \(d\) if and only if either \(p|m\), \(\text{Pic}(\mathcal{O}_{-4md})\) is not 2-torsion, \(2||m\), or \(16|m\).\(^2\)

\(^2\)This is mainly for simplicity of exposition — the same results should hold in arbitrary characteristic.
It is well known that there are only finitely many integers $N > 0$ such that the group $\text{Pic}(\mathcal{O}_{-4N})$ is 2-torsion. Such integers $N$ are referred to as idoneal numbers. A result of Weinberger [We], which was refined by Kani [K4], gives a classification of the idoneal numbers (see below). This result uses the Generalized Riemann Hypothesis (GRH) for quadratic Dirichlet characters in a relatively minor way. Combining this classification with Theorem 1.3, we obtain the following results regarding smooth polarizations on $A_m$.

**Theorem 1.5.** Suppose $m, d \geq 1$. If we assume GRH, then $A_m$ admits a smooth polarization of degree $d$ if and only if at least one of the following conditions holds:

1. $(d, m) > 1$.
2. $d$ is composite.
3. $md$ is not on the following list of 21 integers:

\[ \{1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, 102, 130, 190, 210, 330, 462\} \]

If we do not assume GRH, then the same statement is true except it is possible that the list (*) should include one extra integer $N \equiv 2 \pmod{4}$. In particular, there are (unconditionally) only finitely many pairs $(m, d)$ for which $A_m$ does not admit a smooth polarization of degree $d$.

It is well known that an abelian surface $A$ is the Jacobian of a smooth genus 2 curve if and only if $A$ contains a smooth polarization $L$ of degree $d = 1$. As a consequence of Theorem 1.5, we recover a theorem of Kani [K1, Theorem 5], which determines which of the product surfaces $A_m$ are Jacobians:

**Corollary 1.6.** If we assume GRH, then $A_m$ is the Jacobian of a smooth curve of genus two if and only if $m$ does not belong to the list of integers (*). Unconditionally, there may be one extra even value of $m$ for which $A_m$ is not a Jacobian.

Several unconditional results can be deduced from Theorem 1.5. We give a few examples. The first was first proved by Hayashida [Ha]:

**Corollary 1.7.** If $m > 1$ is odd, then $A_m$ is a Jacobian.

The next unconditional result concerns smooth curves on $A_1$:

**Corollary 1.8.** Let $A_1 = E \times E$ be the self-product of an elliptic curve $E$ without CM. Then $A_1$ contains smooth curves of every genus except 0, 2, and 3.

Theorem 1.5 implies that for large enough $m$, $A_m$ contains smooth curves of every genus $g \geq 1$. If we assume GRH then $m > 462$ suffices. An example of an unconditional result along these lines is:

**Corollary 1.9.** If $m$ is a prime not equal to 2, 3, 5, 11, or 29, then $A_m$ contains smooth curves of every genus $g \geq 1$.

Theorem 1.3 and its corollaries are proved in Section 5.

Finally, we write $S^*$ for the set of idoneal numbers. Then $S^*$ contains the set

\[ S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848\} \]

of known idoneal numbers, and $S^* = S$ assuming GRH [We]. Unconditionally, $S^*$ contains at most one extra squarefree integer $N^*$ not found in $S$. If $N^*$ exists and is odd then $S^* = S \cup \{N^*\}$. If $N^*$ exists and is even, then $S^* = S \cup \{N^*, 4N^*\}$ [K4, Cor. 23].

Theorem 1.4 and the above classification of idoneal numbers imply:
Corollary 1.10. Let $m \geq 1$ and suppose $d = p \geq 5$ is a prime. Then $A_m$ admits a very ample polarization of degree $p$ if and only if at least one of the following conditions hold:

1. $p|m$.
2. $mp \not\in S^*$.

Similarly, $A_m$ admits a very ample polarization of degree $2p$ if and only if at least one of the following conditions hold:

1. $p|m$.
2. $2|m$ or $16|m$.
3. $2mp \not\in S^*$.

In particular, there are finitely many pairs $(m,d)$ with $d \geq 5$, such that $A_m$ does not admit a very ample polarization of degree $d$. If we assume GRH then any such pair satisfies $md < 1848$.

It is well known that every abelian surface $A$ embeds in $\mathbb{P}^5$, and no abelian surface can embed in $\mathbb{P}^3$. Moreover, $A$ embeds in $\mathbb{P}^4$ if and only if $A$ is the zero-locus of a section of the Horrocks-Mumford bundle on $\mathbb{P}^4$ [HM, Theorem 5.2] if and only if $A$ admits a very ample polarization $L$ of degree $d = 5$. The previous corollary therefore allows us to determine which product surfaces $A_m$ embed in $\mathbb{P}^4$:

Corollary 1.11. Assume GRH. Then the surface $A_m$ embeds in $\mathbb{P}^4$ if and only if $m$ is not one of the following integers:

$$1, 2, 3, 6, 8, 9, 12, 14, 17, 21, 24, 26, 33, 38, 42, 48, 56, 66, 69, 77, 104, 152, 168, 264, 273.$$  

Unconditionally, there are at most two more values of $m$ for which $A_m$ does not embed in $\mathbb{P}^4$.

Theorem 1.4 is proved in Section 6.

1.3. Related work. There is a long history of studying principal (i.e. degree 1) polarizations on split abelian surfaces in terms of quadratic forms. See for example [H0], [HN], [L], [K1], and [K2]. The use of the quadratic form $q_L$ appears implicitly in both [HN] and [K1].

It is especially interesting to compare the methods of [K1] and [K2] with our own. Kani also uses quadratic forms to count smooth principal polarizations $L$ (so $d = 1$) on product abelian surfaces $A$. To such an $L$ he attaches the quadratic form $Q_L(D) := (D, L)^2 - 2(D, D)$ on $\text{NS}(A)/\langle L \rangle$ which has rank $\rho(A) - 1$. When $A = A_m$, this quadratic space has rank 2 and discriminant $-16m$, as opposed to our quadratic space which has rank 2 and discriminant $-4m$. The connection between these two quadratic forms is as follows (to simplify things, assume $m \not\equiv 3 \pmod{4}$). If $e : \text{Pic}(O_{-16m}) \to \text{Pic}(O_{-4m})$ is the natural surjective map, then one can compute (see [K1, Cor. 18])

$$e([Q_L]) = [q_L]^2.$$  

Let us briefly hint at the moduli theoretic nature of this equality. Kani’s form $Q_L$ does not depend on any choice of product decomposition $A_m \cong E \times E'$, whereas our quadratic form relies on such a choice. If $A_m \cong F \times F'$ is another such decomposition corresponding to a new quadratic form $q_L'$, then $[q_L]$ and $[q_L']$ differ by a 2-torsion element in $\text{Pic}(O_{-4m})$; hence the class $[q_L]^2$ is independent of the choice of decomposition $A_m \cong E \times E'$. Kani’s quadratic form $Q_L$ is natural when studying $A_m$ inside the larger moduli space of principally polarized abelian surfaces; indeed, the definition of $Q_L$ applies to any such surface. Our quadratic form $q_L$ only makes sense for split abelian surfaces, but is well suited for studying $A_m$ inside the 1-dimensional moduli space of (polarized) Abelian surfaces of type $m$.}

\footnote{This moduli space is isomorphic to $Y_0(m)/w_m$, where $Y_0(m)$ is the usual modular curve and $w_m$ is the canonical Atkin-Lehner involution on $Y_0(m)$.}
Suppose now that \( \rho(E \times E') = 4 \), i.e. that \( \text{End}(E)_Q \cong \text{End}(E')_Q \) is an imaginary quadratic field. For each \( L \in \text{NS}(A) \), we define as before a quadratic form \( q_L : \text{Hom}(E, E \times E') \to \mathbb{Z} \), which now has rank 4. However, \( q_L \) is not just a quadratic form, but also an \( \mathcal{O} \)-hermitian module, where \( \mathcal{O} \) is a certain order in the imaginary quadratic field \( \text{End}(E)_Q = \text{End}(E')_Q \). Once again we can write down an \( \text{Aut}(A) \)-equivariant correspondence between \( \text{NS}(A) \) and a space of \( \mathcal{O} \)-hermitian modules with certain properties. On the other hand, mimicking the correspondence between binary quadratic forms and ideal classes in imaginary quadratic rings, there is a correspondence between \( \mathcal{O} \)-hermitian modules and ideal classes in definite quaternion algebras. This last correspondence has been studied before but not fully developed.

In future work, we plan to use both of these correspondences to answer Question 1 for abelian surfaces of Picard number 4. In fact, we will show that the answer in the case \( d = 4 \) can be deduced from the results of this paper using specialization arguments, i.e. by working in positive characteristic and lifting polarizations. One again finds that almost all such abelian surfaces are Jacobians which contain smooth curves of every genus and very ample line bundles of every degree \( d \geq 5 \).

1.4. **Acknowledgments.** The authors thank Ernest H. Brooks for many helpful discussions. The second author was partially supported by National Science Foundation RTG grant DMS-0943832.

2. **Preliminaries on abelian surfaces**

Let \( A \) be an abelian surface over an algebraically closed field \( k \) of characteristic 0. By definition, the Néron-Severi group of \( A \) is \( \text{NS}(A) = \text{Pic}(A)/\text{Pic}^0(A) \). Concretely, \( \text{NS}(A) \) is isomorphic to the group of divisors on \( A \), modulo the subgroup of divisors in the kernel of the intersection pairing

\[ \text{Div}(A) \times \text{Div}(A) \to \mathbb{Z}. \]

It is well known that \( \text{NS}(A) \) is a free abelian group of rank at most 4.

We often abuse notation and consider divisors and line bundles as elements of \( \text{NS}(A) \). In particular, if we are given an isomorphism \( \phi : E \times E' \cong A \), with \( E, E' \) elliptic curves, then we write \( h \) and \( v \) for the classes of \( \phi(E \times \{0\}) \) and \( \phi(\{0\} \times E') \) in \( \text{NS}(A) \). These are the horizontal and vertical axes with respect to the product decomposition \( \phi \), but \( \phi \) will generally not be mentioned explicitly.

**Definition** An ample line bundle \( L \) on \( A \) is smooth if some line bundle \( D \) contains a smooth (connected) curve. A class \( M \in \text{NS}(A) \) is smooth if some line bundle \( L \) in the class of \( M \) is smooth.

**Lemma 2.1.** If \( L \in \text{Pic}(A) \) is globally generated and ample, then \( L \) is smooth.

**Proof.** By Bertini’s theorem, \( |L| \) contains a smooth but possibly reducible divisor \( D \). We may write \( D = \sum_{i=1}^{n} C_i \) with \( C_i \) smooth curves and \( C_i C_j = 0 \) for \( i \neq j \). If \( n = 1 \), then we are done. Otherwise, the \( C_i \) must be elliptic curves, for higher genus smooth curves on \( A \) are automatically ample. But then \( C_i^2 = 0 \) and so \( D^2 = 0 \), which contradicts the fact that \( L \) is ample.

**Proposition 2.2.** Suppose \( A = E \times E' \) is a product of two elliptic curves and let \( h, v \in \text{NS}(A) \) be the two axes. Then \( L \in \text{Pic}(X) \) is ample if and only if \( L.L > 0 \) and \( L.(h + v) > 0 \).

**Proof.** See [BL, 4.3.3].

The following result, describing the group \( \text{NS}(A) \) for a product surface, is well-known.

**Proposition 2.3.** If \( A = E \times E' \) is a product of elliptic curves, then the map

\[ \mathbb{Z} \oplus \text{Hom}(E, E') \oplus \mathbb{Z} \to \text{NS}(A) \]

\[ (a, \lambda, b) \mapsto (a - 1)h + \Gamma_\lambda + (b - \deg(\lambda))v, \]

is an isomorphism of groups. Here, \( \Gamma_\lambda \subset E \times E' \) is the graph of \( \lambda : E \to E' \).
Recall that an ample line bundle $L \in \text{Pic}(A)$ is of type $(d_1,d_2)$ if the kernel of the isogeny 
\[ \phi_L : A \to A \] is isomorphic to $(\mathbb{Z}/d_1\mathbb{Z})^2 \times (\mathbb{Z}/d_2\mathbb{Z})^2$, with $d_1$ dividing $d_2$.

**Proposition 2.4.** Let $A$ be an abelian surface and suppose $L \in \text{Pic}(A)$ is ample of type $(d_1,d_2)$. Then the following are equivalent.

1. $L$ is not smooth.
2. $d_1 = 1$ and there are elliptic curves $E,E'$ and an isomorphism of polarized abelian varieties 
   \[ (A,L) \cong (E \times E', h + d_2v), \]
   where $h$ and $v$ are the natural horizontal and vertical divisors on $E \times E'$.
3. There exists an elliptic curve $E \subset A$ such that $E.L = 1$.

**Proof.** (2) clearly implies (3) and (3) implies (2) by [BL, 5.3.13]. (2) implies (1) because any $C$ in $|L|$ visibly admits a non-constant map to an elliptic curve of degree 1. So suppose that $|L|$ has no smooth curves. Then we must have $d_1 = 1$, because otherwise $L$ is globally generated and hence has smooth curves by Lemma 2.1. If $d_2 > 1$, then by [BL, 10.1.1], $L$ has a fixed component if and only if there is an isomorphism of polarized abelian surfaces as in (2). So we may assume $L$ has no fixed component. If $d_2 \geq 3$, then $L$ is again globally generated by [BL, 10.1.2]. If $d_2 = 2$, then $L$ has four base points, but the general member of $|L|$ is smooth by [BL, 10.1.3]. Finally, if $d_2 = 1$, then by Matsusaka-Ran [BL, 11.8.1] either the single curve $C \in |L|$ is smooth or there is an isomorphism $A \cong E \times E'$ identifying $L$ with the canonical principal polarization on $E \times E'$. \(\square\)

**Theorem 2.5** (Reider). Let $d \geq 5$ and let $L \in \text{Pic}(A)$ be ample of type $(1,d)$. Then $L$ is very ample if and only if there are no elliptic curves $E \subset A$ such that $E.L \leq 2$.

**Proof.** See [BL, 10.4]. \(\square\)

The classes of elliptic curves in $\text{NS}(A)$ can be described purely in terms of the intersection pairing:

**Proposition 2.6** ([K3]). A class $L \in \text{NS}(A)$ is the class of an elliptic curve $E \subset A$ if and only if $L$ is indivisible in $\text{NS}(A)$, $(L,L) = 0$, and $L.H > 0$ for some ample $H \in \text{NS}(A)$.

A consequence of Proposition 2.4 and Theorem 2.5 is that being smooth or very ample is a numerical property for line bundles on an abelian surface. Moreover, Proposition 2.6 shows that the smooth and very ample classes are in fact determined by the intersection pairing on $\text{NS}(A)$.

**Definition** A polarization $L \in \text{NS}(A)$ is merely ample if $L$ is not very ample.\(^4\)

The following is a more precise version of Reider’s theorem for polarizations of odd degree.

**Theorem 2.7.** Let $A$ be an abelian surface and let $L \in \text{NS}(A)$ be a polarization of odd degree $d \geq 5$. If $L$ is smooth and merely ample, then there exist elliptic curves $E,F \subset A$ such that $E.L = 2, E[2] = F[2] = E \cap F$, and $\mu^*L \equiv 2dh + 2v \in \text{NS}(E \times F)$, where $\mu : E \times F \to A$ is the subtraction 4-isogeny.

Conversely, suppose $d \geq 1$, not necessarily odd. If $E$ and $F$ are elliptic curves and $\phi : E[2] \to F[2]$ is an isomorphism of groups, then the quotient $B = E \times F/\Gamma_\phi$ admits a degree $d$ polarization $L \in \text{NS}(B)$ such that $\pi^*L = 2dh + 2v$. Here, $\Gamma_\phi \subset E \times F$ is the graph of $\phi$ and $\pi : E \times F \to B$ is the canonical 4-isogeny. Moreover, $L.\pi(E \times 0) = 2$, so $L$ is not very ample.

**Proof.** By Reider’s theorem, $L.E = 2$ for some elliptic curve $E \subset A$. Let $F$ be the complementary elliptic curve corresponding to $E$ with respect to the polarization $L$ (see [BL, §5.3]) and write 

\[ \mu : E \times F \to A \]

for the subtraction isogeny. Since $L.E = h^0(L|_E) = 2$, one knows that $\ker \mu = E \cap F \subset E[2]$ [BL, 5.3.11].

\(^4\)Recall from the introduction that a polarization is ample by definition.
We claim that \( \ker \mu = E[2] \). We set \( M = \mu^* L \) and note that \( M = ah + 2v \in \text{NS}(E \times F) \) for some integer \( a \), by [BL, 5.3.6]. As \( L \) has degree \( d \), we must have \( a = \frac{2}{d} \text{deg}(\mu) \). So if \( \ker \mu \neq E[2] \), then \( \text{deg}(\mu) = 2 \) and \( \mu^* L = dh + 2v \). But in order for \( M \) to be in the image of \( \mu^* : \text{NS}(A) \rightarrow \text{NS}(E \times F) \), we need \( \ker(\mu) \subset K(M) \), where \( K(M) \) is the kernel of \( \phi_M : E \times F \rightarrow \tilde{E} \times \tilde{F} \) [M, §23]. Since \( K(M) = E[2] \times F[d] \) and \( d \) is odd, this can only happen if \( \mu \) is a map of the form

\[
E \times F \rightarrow E/H \times F \cong A
\]

for a subgroup \( H \subset E[2] \) of order 2. In that case, \( L = dh + \tilde{v} \) with respect to the decomposition \( A \cong E/H \times F \), so \( L \) is not smooth, a contradiction. So \( \ker \mu = E[2] = F[2] \) and \( \mu^* L = 2dh + 2v \), as claimed.

For the converse statement, we again set \( M = 2dh + 2v \). We need to show that there exists \( L \in \text{NS}(B) \) such that \( \pi^* L = M \). This is the case if and only if \( \ker \pi \subset K(M) \) and \( \ker \pi \) is isotropic for the Riemann form \( e^M \) [M, §23]. As \( K(M) = E[2] \times F[2d] \), which contains the 2-torsion on \( E \times F \), the first condition is satisfied. To prove the second condition, we choose a basis \( P, Q \) for \( E[2] \cong \mathbb{F}_2^2 \) and compute

\[
e^M((P, \phi(P)), (Q, \phi(Q))) = e_2(P, Q)e_2(\phi(P), \phi(Q)) = (-1)^2 = 1,
\]

showing that \( \ker \mu \) is isotropic. \( \square \)

**Remark** For \( d \) odd, we can interpret Proposition 2.4 and Theorem 2.7 in terms of moduli problems as follows. Let \( A_2(d) \) be the moduli stack of \((1, d)\)-polarized abelian surfaces \((A, L)\), and let \( Z \subset A_2(d) \) be the locus of pairs \((A, L)\) with \( L \) merely ample. Then \( Z \) has two components, one isomorphic to \( Y(1) \times Y(1) \) and another admitting a finite étale map from the modular diagonal quotient surface \( \text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \backslash \text{Y}(2) \times \text{Y}(2) \). Here, \( \text{Y}(N) \) is the moduli stack of elliptic curves with full level \( N \) torsion structure.

**Remark** If \( d \) is even then the merely ample locus \( Z \subset A_2(d) \) has a third component which admits a finite étale map from \( Y_1(2) \times Y_1(2) \).

**Lemma 2.8.** Let \( f : A \rightarrow B \) be an isogeny of abelian surfaces and \( L \in \text{Pic}(B) \). If \( L \) is smooth then \( f^* L \) is smooth. If \( L \) is a very ample bundle and \( \text{deg}(f^* L) \) is squarefree, then \( f^* L \) is very ample.

**Proof.** The very ampleness statement follows from Theorem 2.5. Indeed, it suffices to show that \( f^* L.E > 2 \) for any elliptic curve \( E \) on \( A \). But \( f_\* E = nE' \) for some elliptic curve \( E' \) on \( B \) and so

\[
(f^* L.E) = f_\*(f^* L.E) = (L.f_\* E) = n(L.E') > 2,
\]

as desired. A similar proof using Proposition 2.4 works for smoothness. \( \square \)

**Lemma 2.9.** If \( A \) is an abelian surface and \( E, F \subset A \) elliptic curves subgroups, then \( E.F = 0 \) if and only if \( E = F \).

**Lemma 2.10.** Let \( A \) be an abelian surface and \( L \in \text{NS}(A) \) a polarization of degree \( d \geq 5 \). Then there is at most one elliptic curve \( E \subset A \) such that \( L.E = 2 \).

**Proof.** Suppose \( F \subset A \) is another such elliptic curve. By the Hodge index theorem, we have

\[
4d(E.F) = L^2(E + F)^2 \leq (L.(E + F))^2 = 16,
\]

so \( d(E.F) \leq 4 \). This forces \( (E.F) = 0 \); hence \( E = F \) by Lemma 2.9. \( \square \)

**Definition** Two polarizations \( L, M \in \text{NS}(A) \) are **equivalent** if there exists \( \alpha \in \text{Aut}(A) \) such that \( L = \alpha^* M \).

In the following definitions the term ‘polarizations’ is used as an abbreviation for the phrase ‘equivalence classes of polarizations’.

**Definition** For integers \( d \geq 1 \),
• $N(A, d)$ is the number of polarizations on $A$ of degree $d$.
• $N_{sm}(A, d)$ is the number of smooth polarizations on $A$ of degree $d$.
• $N_{va}(A, d)$ is the number of very ample polarizations on $A$ of degree $d$.

3. Product abelian surfaces of Picard number 2

Let $E, E'$ be non-isogenous elliptic curves and set $A = E \times E'$. Then NS($A$) = $\mathbb{Z}h + \mathbb{Z}v$, where $h$ is the class of the horizontal divisor $E \times 0$ and $v$ is the class of the vertical divisor $0 \times E'$. If $L \equiv ah + bv$, then the degree of $L$ is $d(L) = \frac{1}{2}L.L = ab$. The only elliptic curves on $A$ are translations of $h$ and $v$.

Proposition 3.1. $L \equiv ah + bv \in \text{NS}(A)$ is ample if and only if $a$ and $b$ are both positive.

Proof. This follows from Proposition 2.2. \hfill $\square$

Our next theorem computes $N(A, d)$, $N_{sm}(A, d)$, and $N_{va}(A, d)$ for $A = E \times E'$ a product of non-isogenous curves.

Theorem 3.2. If $A$ is a product of two non-isogenous elliptic curves, then

1. $N(A, d) = \sigma_0(d)$.
2. $N_{sm}(A, d) = \begin{cases} \sigma_0(d) - 2 & \text{if } d > 1 \\ 0 & \text{if } d = 1. \end{cases}$
3. $N_{va}(A, d) = \begin{cases} \sigma_0(d) - 4 & d \geq 5 \text{ even} \\ \sigma_0(d) - 2 & d \geq 5 \text{ odd}. \end{cases}$

Here, $\sigma_0(d)$ is the number of divisors of $d$.

Proof. Note that Aut($A$) $\cong \mathbb{Z}/2 \times \mathbb{Z}/2$ acts trivially on NS($A$). The theorem now follows immediately from Proposition 2.4 and Theorem 2.5. \hfill $\square$

As an immediate consequence, we can determine for which $d$ there exist smooth or very ample polarizations on $A$.

Theorem 3.3. Let $d$ be a positive integer. Then $A$ admits a smooth polarization of degree $d$ if and only if $d$ is composite. For $d \geq 5$, $A$ admits a very ample polarization of degree $d$ if and only if $d$ is neither a prime nor twice a prime.

Corollary 3.4. There exists a smooth projective curve $C \subset A$ of genus $g = d + 1 \geq 2$ if and only if $d$ is composite.

Corollary 3.5. The surface $A$ is not the Jacobian of a smooth genus 2 curve.

Corollary 3.6. There is no embedding $A \hookrightarrow \mathbb{P}^4$.

Proof. $A$ admits no very ample line bundles of degree 5. \hfill $\square$

4. Product abelian surfaces of Picard number 3

In this section we let $E$ and $E'$ be isogenous elliptic curves without CM and set $A = E \times E'$. By Proposition 2.3, $\rho(A) = 3$. Let $\lambda : E \to E'$ be a cyclic isogeny satisfying $\ker \lambda \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \geq 1$. Thus Hom($E, E'$) is simply $\mathbb{Z}\lambda$. Then NS($A$) $\cong \mathbb{Z}h \oplus \mathbb{Z}v \oplus \text{Hom}(E, E')$, with $h$ and $v$ the horizontal and vertical classes as before. The inverse isomorphism sends $\lambda$ to

$$X_{\lambda} := [\Gamma_\lambda] - h - mv.$$ 

The class $X_{\lambda}$ is orthogonal to $h$ and $v$ and if $L \equiv ah + bX_{\lambda} + cv$, then the degree of $L$ is

$$d = \frac{1}{2}(L.L) = ac - b^2m.$$
Lemma 4.1. \( L \) is ample if and only if \( d > 0 \) and \( a, c > 0 \).

Proof. This follows from Proposition 2.2. \( \square \)

Associated with the class \( L \equiv ah + bX_\lambda + cv \in \text{NS}(A) \) is the quadratic form
\[
q_L: \text{Hom}(E, A_m) \to \mathbb{Z}
\]
\[
f \mapsto \deg(f^* L).
\]
Using the natural basis \( \{(1, 0), (0, \lambda)\} \) for
\[
\text{Hom}(E, A_m) = \text{Hom}(E, E) \oplus \text{Hom}(E, E'),
\]
one computes
\[
q_L([y], x\lambda) = amx^2 - 2bmx y + cy^2.
\]
Note that the basis above is canonically (up to a choice of minimal isogeny \( \lambda \)) attached to the polarized abelian surface \((A_m, h + v)\), i.e. it is only canonical once a decomposition \( A_m \cong E \times E' \) has been chosen.

Notation Let \( V_m \) be the space of even integral binary quadratic forms \( q = [A, 2B, C] \) with \( A \) and \( B \) divisible by \( m \).\(^5\) For \( d \geq 1 \), let \( V_{m,d} \subset V_m \) be the set of positive definite \( q \) of discriminant \(-4md\).

The set \( V_m \) has a natural action of \( \Gamma_0(m) \) by linear transformation of variable. Here, \( \Gamma_0(m) \) is the subgroup of \( \text{GL}_2(\mathbb{Z}) \) with lower left corner divisible by \( m \). This action preserves the subsets \( V_{m,d} \). We also note that \( \text{Aut}(A_m) \) is isomorphic to \( \Gamma_0(m) \) via
\[
\begin{pmatrix} a & b \\ c\lambda & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ mc & d \end{pmatrix}.
\]

In this paper we think of \( q_L \) as the quadratic form \([am, -2bm, c]\); in other words, we implicitly choose the above canonical basis for \( \text{Hom}(E, A_m) \), and write out the quadratic form \( q_L \) as a quadratic polynomial in terms of this basis. We could be more abstract and avoid using bases altogether, but this mostly obfuscates matters. More to the point though, we cannot avoid choosing a product decomposition \( A_m = E \times E' \), and once this decomposition is fixed, the basis above is natural.

Theorem 4.2. The map \( L \mapsto q_L \) is a bijection \( \text{NS}(A_m) \to V_m \) with the following properties:

1. \( L \) is ample if and only if \( q_L \) is positive definite.
2. The discriminant of \( q_L \) is \(-4m \deg(L)\)
3. The correspondence is \( \Gamma_0(m) \)-equivariant

\(^5\)As usual, we write \([a, b, c]\) for the quadratic form \( ax^2 + bxy + cy^2\).
In particular, for any \( d \geq 1 \) there is an induced bijection
\[
\text{Aut}(A_m) \backslash \text{NS}(A_m)^{\text{amp}} \rightarrow \Gamma_0(m) \backslash V_{m,d},
\]
where \( \text{NS}(A_m)^{\text{amp}} \) is the set of ample classes of degree \( d \) in \( \text{NS}(A_m) \).

**Proof.** The fact that \( L \mapsto q_L \) is a bijection follows immediately from the explicit formula for \( q_L \). Property (1) follows from Lemma 4.1; (2) and (3) are simple computations. \( \square \)

The set \( \Gamma_0(m) \backslash V_{m,d} \) can be understood in terms of the more familiar \( \text{GL}_2(\mathbb{Z}) \)-equivalence relation on quadratic forms. Before explaining this, we first describe the elliptic curves on \( A_m \) and determine the different decompositions of \( A_m \) as a product of elliptic curves. Such decompositions are in bijection with reducible principal polarizations, i.e. polarizations of the form \( F + F' \) for two elliptic curves \( F, F' \in \text{NS}(A_m) \) such that \( F, F' = 1 \).

For each \( k \) dividing \( m \), let \( H_k \) be the unique subgroup of \( \ker(\lambda : E \rightarrow E') \) of order \( k \) and set \( E_k = E/H_k \).

**Proposition 4.3.** Any elliptic curve on \( A_m \) is isomorphic to \( E_k \) for some \( k \) dividing \( m \). For each divisor \( k \) of \( m \) satisfying \( (k, m/k) = 1 \), there is an isomorphism \( A_m \cong E_k \times E_{m/k} \), giving a reducible principal polarization on \( A \). Up to automorphisms of \( A_m \), these are the only reducible principal polarizations.

**Proof.** Any elliptic curve on \( A_m \) is isogenous to \( E \). It is therefore the image of a cyclic isogeny \( f_{x,y} : E \rightarrow A_m = E \times E' \), where \( x \) and \( y \) are integers and where
\[
f_{x,y}(P) = (x(P), y(\lambda(P))).
\]
The kernel of \( f_{x,y} \) is \( H_k \), where \( k = \gcd(x, m) \). The proves the first part of the proposition.

For the second part, note that \( E_1 = E \) and \( E_m = E' \). The natural projections \( E_{k_1} \rightarrow E_{k_2} \) for \( k_1 | k_2 \) form a lattice of isogenies corresponding to the lattice of divisors of \( m \). As the number \( m \) is an invariant of the abelian surface, the only possible way to write \( A_m \cong E_k \times E_j \) for some \( j \) dividing \( m \) is if \( j = k' := m/k \) and \( (k, k') = 1 \). For if \( j \neq k' \) or \( (k, k') > 1 \), one checks (using dual isogenies if necessary) that \( E_k \) and \( E_j \) are connected by an isogeny of degree less than \( m \).

The last thing to check is that \( A_m \) really is isomorphic to the product of \( E_k \times E_{k'} \) when \( (k, k') = 1 \). One can write down an isomorphism explicitly as follows. Let \( \lambda_k : E_k \rightarrow E_k = E_k = E_k \) be the natural projection, and let \( \lambda_k : E_k \rightarrow E_k \) be the unique isogeny such that \( E_k \cong E_k \). Let \( m \) be integers such that \( rk - sk' = 1 \) and consider the map \( \phi : E \times E' \rightarrow E_k \times E_{k'} \) defined by
\[
\phi : (P, Q) \mapsto (r\lambda_k(P) - \mu_k(Q), s\lambda_{k'}(Q) - s\lambda_{k'}(P)).
\]
One checks that if \( (P, Q) \in \ker(\phi) \), then \( rkP - \hat{\lambda}(Q) = sk'P \). As \( rk - sk' = 1 \), \( P \) must be 0. But then \( Q \) is in the kernel of both \( \mu_k \) and \( \mu_{k'} \), and is therefore also 0. So \( \phi \) is an isomorphism. \( \square \)

Now we explain the connection with the more familiar class groups, but first some terminology.

**Definition** An integral binary quadratic form \((A, 2B, C)\) is matrix-primitive if \( \gcd(A, B, C) = 1 \), i.e. if the corresponding symmetric bilinear form is primitive.

**Notation** For any integer \( D \), let \( V_{4D}^{\text{mp}} \) be the space of matrix-primitive quadratic forms of discriminant \( 4D \).

**Remark** If \( D \) is odd, then we think of \( V_{4D}^{\text{mp}} = V_{4D}^{\text{prim}} \cup V_{4D}^{\text{prim}} \) as the union of the primitive quadratic forms of discriminant \( 4D \) and (twice) the primitive quadratic forms of discriminant \( D \). Note that the second set is empty if \( D \equiv 3 \pmod{4} \). If \( D \) is even, then \( V_{4D}^{\text{mp}} = V_{4D}^{\text{prim}} \).

To prove the main theorems, we will carefully analyze the set \( \text{Aut}(A_m) \backslash \text{NS}(A_m)^{\text{amp}} \) for squarefree values of \( d \). If \( L \equiv ah + bx + cv \in \text{NS}(A_m)^{\text{amp}} \), and \( d = \text{deg}(L) = ac - b^2m \) is squarefree, then \( L \) is indivisible in \( \text{NS}(A) \), i.e. \( \gcd(a, b, c) = 1 \). Notice that even though \( L \) is indivisible in \( \text{NS}(A) \), \( q_L \).
may not be matrix-primitive. But the matrix-content of \( q_L \), that is \( \gcd(\alpha m, \beta m, c) = \gcd(c, m) \), is a divisor of \( \gcd(m, d) \). Thus \( \frac{1}{(c, m)} q_L \) is in \( V_{-4md/g^2}^{\text{mp}} \).

**Proposition 4.4.** Let \( d \geq 1 \) be squarefree. Then the map \( L \mapsto \frac{1}{(c, m)} q_L \) induces a surjective map

\[
\Psi_{m,d} : \text{Aut}(A_m) \backslash \text{NS}(A_m)^{\text{amp}}_{d} \rightarrow \prod_{g|(m,d)} \text{GL}_2(\mathbb{Z}) \backslash V_{-4md/g^2}^{\text{mp}}.
\]

The fiber above an element \( [q] \in \text{GL}_2(\mathbb{Z}) \backslash V_{-4md/g^2}^{\text{mp}} \) has size \( |\Gamma_0(m) \backslash \Gamma_0(m/g) / \text{Aut}(q)| \).

In particular, if \( m \) and \( d \) are coprime, then \( \Psi_{m,d} : L \mapsto [q_L] \) is a bijection

\[
\text{Aut}(A_m) \backslash \text{NS}(A_m)^{\text{amp}}_{d} \rightarrow \text{GL}_2(\mathbb{Z}) \backslash V_{-4md/g^2}^{\text{mp}}.
\]

**Remark** Unless \( q \) is 2-torsion in the class group, we have \( \text{Aut}(q) = \{ \pm 1 \} \), which acts trivially. In this case, the size of the fibers of \( \Psi_{m,d} \) is simply the index of \( \Gamma_0(m) \) in \( \Gamma_0(g') \). If \( q \) is 2-torsion, \( \text{Aut}(q) / \{ \pm 1 \} \) has size 2 whenever \( q \) has discriminant \( D < -4 \).

**Proof.** It is not hard to see that \( \Psi_{m,d} \) is surjective. For instance, if \( q = 1 \), then given a matrix-primitive quadratic form \( q \) of discriminant \( -4md \), one can find a \( \text{GL}_2(\mathbb{Z}) \)-equivalent form in \( V_{m,d} \) by moving the double root of \( q \) over \( \mathbb{Z}/m\mathbb{Z} \) to 0, at least if \( m \) is odd. If \( m \) is even then a little more care is required. First recall that in this case, \( q \) is automatically primitive. We can find an equivalent form with middle and outer coefficient divisible by \( m \), but we need the middle coefficient divisible by \( 2m \). This is automatic if \( m \) is not divisible by 4. If \( m \) is divisible by 4, and if \( q \) has middle coefficient only divisible by \( m \) and not \( 2m \), then \( \gamma \cdot q \in V_{m,d} \), where

\[
\gamma = \begin{pmatrix} 1 & \frac{m}{2} \\ 0 & 1 \end{pmatrix}.
\]

This approach works for all \( g|(d, m) \) by simply multiplying the corresponding matrix-primitive form in \( V_{m/g,d/g} \) by \( g \).

To count preimages, one checks by a direct computation that if two forms in \( V_{m,d} \) are \( \text{GL}_2(\mathbb{Z}) \) equivalent, then they are in fact \( \Gamma_0(g')\)-equivalent, where \( g' = m/(c, m) \). Now, the \( \Gamma_0(m) \)-equivalence classes which map to \( q \) under \( \Psi_{m,d} \) are indexed by the cosets of \( \Gamma_0(m) \) in \( \Gamma_0(g') \). And one checks that two \( \Gamma_0(m) \)-classes collapse if and only if the corresponding cosets are in the same orbit of the automorphism group \( \text{Aut}(q) \subset \Gamma_0(g') \) of \( q \in V_{m,d} \) acting on the coset space \( \Gamma_0(m) \backslash \Gamma_0(g') \) on the right. \( \square \)

**Remark** Here is a more geometric way to count the preimages of the map \( \Psi_{m,d} \) above points where \( g > 1 \), which will be useful for us later on. If \( L \equiv ah + bX_\lambda + cv \) and \( (c, m) = g \), then we consider the \( g \)-isogeny

\[
f : A_m = E \times E' \xrightarrow{\lambda_g} E_g \times E_{g'} =: A_{m/g},
\]

where \( E_g \) is the elliptic curve from Proposition 4.3 and \( \lambda_g : E \rightarrow E_g \) is the natural isogeny. We choose the usual basis \( \{ h, X_{\mu_g}, v \} \) for \( \text{NS}(A_{m/g}) \), where \( \mu_g : E_g \rightarrow E_{g'} \) satisfies \( \lambda = \mu_g \circ \lambda_g \). One computes

\[
f^* h = h, \quad f^* X_{\mu_g} = X_\lambda, \quad f^* v = gv.
\]

Thus \( L = f^* M \) for a polarization \( M \in \text{NS}(A_{m/g}) \) of degree \( d/g \). In this way, you reduce to the case where \( (d, m) = 1 \). But note that if \( M, M' \in \text{NS}(A_{m/g}) \) are \( \text{Aut}(A_{m/g}) \)-equivalent, it is not in general true that \( f^* M \) and \( f^* M' \) are \( \text{Aut}(A_m) \)-equivalent. As \( \text{Aut}(m/g) = \Gamma_0(m/g) \), the discrepancy is measured exactly by the coset space \( \Gamma_0(m) \backslash \Gamma_0(m/g) / \text{Aut}(M) \).

For squarefree \( d \), Proposition 4.4 gives a formula for \( N(A_m, d) \) in terms of class numbers of imaginary quadratic orders. Recall that the \( \text{GL}_2(\mathbb{Z}) \)-equivalence classes of primitive forms of discriminant \( D < 0 \) are in bijection with the group \( \text{Cl}(O_D) \) but with the set \( \text{Cl}(O_D)^+ \) in which
ideal classes and their inverses are identified. Here, Cl(O_D) is the class group of the quadratic order of discriminant D. We write \( h^+(D) = |\text{Cl}(O_D)^+| \) and record this formula in the case where \((m,d) = 1\).

**Corollary 4.5.** If \((d, m) = 1\) and \(d\) is squarefree, then

\[
N(A_m, d) = \begin{cases} h^+(-4md) & \text{md even} \\ h^+(-4md) + h^+(-md) & \text{md odd.} \end{cases}
\]

Note that \( h(-md) = 0 \) when \( md \equiv 1 \pmod{4} \).

The bijection in Theorem 4.2 also gives a nice description of the \( \text{Aut}(A_m) \)-equivalence classes of elliptic curves on \( A_m \):

**Proposition 4.6.** The map \( L \mapsto q_L \) induces a bijection between the set of \( \text{Aut}(A_m) \)-equivalence classes of elliptic curves on \( A_m \) and the set of \( \Gamma_0(m) \)-equivalence classes of primitive integral binary quadratic forms of discriminant 0. The latter set is in bijection with the orbits of \( \Gamma_0(m) \) acting on \( \mathbb{P}^1(\mathbb{Q}) \). If \( k|m \), then the number of \( \text{Aut}(A_m) \)-equivalence classes of elliptic curves isomorphic to \( E_k = E/H_k \) is equal to the number of units in \( (\mathbb{Z}/f_k\mathbb{Z})^\times/\{\pm 1\} \), where \( f_k = \gcd(k, m/k) \).

**Proof.** Let \( E_{a,b} \) be the image of \( f_{a,b} : E \to A_m \), as in the proof of Proposition 4.3. Then \( E_{a,b} \) is isomorphic to \( E_k \) where \( k = \gcd(a, m) \), and one computes

\[
E_{a,b} \equiv (a^2/k)h + (ab/k)X_\lambda + h^2k'v \in \text{NS}(A_m),
\]

where \( k' = m/k \). Thus \( q_{E_{a,b}} \) is the quadratic form \( k'(ax - by)^2 \) of discriminant 0. The first two statements of the proposition are now clear once we note that the elliptic curves in \( \text{NS}(A_m) \) are exactly the indivisible classes \( F \) such that \( FF = 0 \) and \( h^0(F) > 0 \) [K3]. The last statement now follows from [GZ, p. 234]; note though that our \( \Gamma_0(m) \) contains elements of determinant \(-1\). \( \square \)

The map \( \Psi_{m,d} \) of Proposition 4.4 has an important extra equivariance property, which we elaborate on for the remainder of this section. For each \( k|m \), we write \( k' \) for the complementary divisor \( m/k \). If \((k, k') = 1\), we may consider the endomorphism

\[
\epsilon_k = \lambda_k \times \tilde{\mu}_{k'} : A_m = E \times E' \to E_k \times E_{k'} \cong A_m.
\]

Note that we have implicitly chosen an isomorphism \( A_m \cong E_k \times E_{k'} \), so the map \( \epsilon_k \) is not very well defined. In any case, it has degree \( k^2 \) and \( w_k = \frac{1}{k} (\epsilon_k)_* \) is an automorphism of the quadratic space \( \text{NS}(A) \). In fact,

\[
w_k(h) = h_k, \quad w_k(X_\lambda) = X_\lambda, \quad w_k(v) = v_k \tag{4.1}
\]

where \( h_k, X_\lambda, v_k \) is the standard basis on \( \text{NS}(E_k \times E_{k'}) \). Straightforward computations result in the following lemma, which highlight the connection between the collection of \( w_k \) and the Atkin-Lehner involutions on \( X_0(m) \). We write \( \omega(m) \) for the number of primes dividing \( m \).

**Lemma 4.7.** The \( w_k \) commute with each other, and satisfy \( w_k^2 = 1 \). Moreover, up to \( \text{Aut}(A_m) \), the automorphism \( w_k : \text{NS}(A_m) \to \text{NS}(A_m) \) is independent of the choice of decomposition \( A_m = E \times E' \) and the choice of isomorphism \( A_m \cong E_k \times E_{k'} \) above. The \( w_k \) therefore define a canonical action of \( (\mathbb{Z}/2\mathbb{Z})^{\omega(m)} \) on \( \text{NS}(A_m) \).

For each \( k|m \) and each \( L \in \text{NS}(A_m) \), define the quadratic form

\[
q^k_L : \text{Hom}(E_k, A_m) \to \mathbb{Z}
\]

\[
f \mapsto \deg(f^*L).
\]
We embed $\text{Hom}(E_k, A_m)$ inside $\text{Hom}(E, A_m)$ via $g \mapsto g \circ \lambda_k$, where $\lambda_k : E \to E_k = E/H_k$ is the natural map. Then the restriction of $q_\ell$ to the subspace $\text{Hom}(E_k, A_m)$ is equal to $kq_L^k$. Written in the standard basis $\{\lambda_k \times 0, 0 \times \mu_k\}$ for $\text{Hom}(E_k, E \times E')$, this means

$$q_L^k(y\lambda_k \times x\mu_k) = ak'x^2 - 2bmxy + cky^2,$$

i.e. $q_L^k = [ak', -2bm, kc]$.

**Lemma 4.8.** Let $L \in \text{NS}(A_m)$ and suppose $k|m$ and satisfies $(k, k') = 1$. Then $q_{w_k(L)}^k$ and $q_L$ are isomorphic quadratic forms.

**Proof.** This follows from (4.1) and transport of structure. \hfill \square

Recall that for any quadratic discriminant $D < 0$, we may identify $\text{GL}_2(\mathbb{Z})\backslash V_D^{\text{prim}}$ with $\text{Pic}(O_D)^+$, where $\text{Pic}(O_D)$ is the Picard group of the quadratic order of discriminant $D$ and $\text{Pic}(O_D)^+$ is the set obtained by identifying an element and its inverse. We will write $\text{Cl}(D)$ for $\text{Pic}(O_D)^+$. If $g^2|D$ and $D/g^2$ is a discriminant, then extension of ideals induces a surjective group homomorphism

$$e_g : \text{Cl}(D) \to \text{Cl}(D/g^2),$$

and hence a surjective map

$$e_g : \text{Cl}(D) \to \text{Cl}(D/g^2).$$

If $q$ is a primitive quadratic form of discriminant $D$, then we write $[g]$ for the corresponding class in $\text{Pic}(O_D)$ or $\text{Cl}(D)$. We warn the reader now that we tend to conflate $\text{Cl}(D)$ and $\text{Pic}(O_D)$ whenever there is no harm in doing so.

Now suppose $(k, k') = 1$ and $L \in \text{NS}(A_m)$ has degree $d$, for some squarefree $d \geq 1$. We write $g = \text{gcd}(k, d)$. For each $k$ we have the primitive quadratic form $f_k = \frac{1}{g}[k, 0, k'd]$ of discriminant $-4md/g^2$. The class $[f_k]$ is 2-torsion, as can be seen from Lemma 6.1. If, for example, $(m, d) = 1$, then the classes $[f_k] \in \text{Cl}(-4md)$ form a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(m)}$. The following key proposition relates $q_L$ to $q_L^k$.

**Proposition 4.9.** Let $L \in \text{NS}(A_m)$ have degree $d \geq 1$ and suppose $q_L$ is primitive. Also suppose $k|m$ satisfies $(k, k') = 1$ and write $g = (k, d)$. Then

$$e_g ([q_L]) \cdot [f_k] = \left[\frac{1}{g}q_L^k\right] \in \text{Pic}(O_{-4md/g^2}).$$

If $q_L$ is merely matrix-primitive, then

$$e_g \left(\frac{1}{2}q_L\right) \cdot [g_k] = \left[\frac{1}{2g}q_L^k\right] \in \text{Pic}(O_{-md/g^2}),$$

where $g_k = \frac{1}{2}[k, k, (k + k'd)/4]$.

**Proof.** We only prove the first equation, the proof of the second being similar. We first find a quadratic form representing $e_g(q_L)$. Note that $(c, m) = 1$, since $q_L = [am, -2bm, c]$ is primitive. Then as $ac - mb^2 = d$, we must have $(c, g) = 1$ and $g|a$. We claim that

$$e_g([q_L]) = [am/g^2, -2bm/g, c].$$

This follows from the following lemma.

**Lemma 4.10.** Let $g \geq 1$ be an integer. If $q(x, y)$ is a primitive quadratic form of discriminant $D < 0$ and $h(x, y) = q(gx, y)$ is primitive of discriminant $g^2D$, then $e_g([h]) = [g]$.  

14
Proof. The quadratic form \( q = [a, b, c] \) corresponds to the proper \( \mathcal{O}_D \)-ideal \( I = a\mathbb{Z} + \left( \frac{-b+\sqrt{D}}{2} \right) \mathbb{Z} \), and \( h = [aq^2, b, c] \) corresponds to \( q^2 a\mathbb{Z} + \left( \frac{-kb+k\sqrt{D}}{2} \right) \mathbb{Z} \). The latter is equivalent to the ideal \( I_g = ga\mathbb{Z} + \left( \frac{-b+\sqrt{D}}{2} \right) \mathbb{Z} \) in \( \text{Pic}(\mathcal{O}_{D/g^2}) \). As \( I \) is the \( \mathcal{O}_D \)-ideal generated by \( I_g \), the lemma follows. \( \square \)

To prove the first equation in the proposition it now suffices to show that
\[
[am/g^2, -2bm/g, c] \cdot [k/g, 0, k'd/g] = [ak'/g, -2bm/g, ck/g]
\]
in the class group. We prove this using the old-fashioned definition of Gauss composition. Actually, we will use Dirichlet’s method of composition \([C]\): the product \([a, b, c] \cdot [a', b', c']\) of two primitive forms of discriminant \( D \) is equal to
\[
[a'a/e^2, B, e^2(B^2 - D)/(4a'a')],
\]
where \( e = \gcd(a, a', (b + b')/2) \) and \( B \) is an integer satisfying
\[
B \equiv b \pmod{2a/e} \quad B \equiv b' \pmod{2a'/e} \quad B^2 \equiv D \pmod{4a'a/e^2}.
\]
In our case we have \( D = -4md/g^2, e = k/g \), and \( B = -2mb/g \). Using this rule, we verify (4.2) and finish the proof of the proposition. \( \square \)

**Corollary 4.11.** Suppose \( L \) is ample of degree \( d \), \( q_L \) is primitive, and \( (k, k') = 1 \). Then
\[
e_g(\Psi_{m,d}(L)) \cdot [f_k] = \Psi_{m,d}(w_k(L)) \in \text{Cl}(\mathcal{O}_{4md/g^2}).
\]
If \( L \) is merely matrix-primitive, then
\[
e_g(\Psi_{m,d}(L)) \cdot [g_k] = \Psi_{m,d}(w_k(L)) \in \text{Cl}(\mathcal{O}_{-md/g^2}).
\]
**Proof.** Take \( L \) to be \( w_k(L) \) in Lemma 4.8, and then use Proposition 4.9. \( \square \)

Let \( W(m) \) be the group \((\mathbb{Z}/2\mathbb{Z})^{\omega(m)}\). Then Corollary 4.11 essentially says that \( \Psi_{m,d} \) is \( W(m) \)-equivariant. This is not exactly true because the target of \( \Psi_{m,d} \) does not quite have an action of \( W(m) \), as the 2-torsion classes \([f_k]\) lie in different class groups. However, in many situations we have actual \( W(m) \)-equivariance, as the following lemma shows:

**Corollary 4.12.** Suppose \( d \) is squarefree, \((m, d) = 1\), and \( md \not\equiv 3 \pmod{4} \). Then \( \Psi_{m,d} \) is equivariant for the action of \( W(m) \), i.e. the following square commutes for each \( k\mid m \) satisfying \((k, m/k) = 1\):
\[
\begin{array}{ccc}
\text{Aut}(A_m) \backslash \text{NS}(A_m)_{d}^{\text{amp}} & \xrightarrow{w_k} & \text{Aut}(A_m) \backslash \text{NS}(A_m)_{d}^{\text{amp}} \\
\Psi_{m,d} \downarrow & & \downarrow \Psi_{m,d} \\
\text{Cl}(-4md) & \xrightarrow{[f_k]} & \text{Cl}(-4md)
\end{array}
\]
**Proof.** This follows from the previous corollary. The condition on \( md \) guarantees that for any ample \( L \) of degree \( d \), \( q_L \) is primitive and not just matrix primitive and that the target of \( \Psi_{m,d} \) is \( \text{Cl}(-4md) \) and not \( \text{Cl}(-4md) \coprod \text{Cl}(-md) \). \( \square \)

**Remark** When \( md \equiv 3 \pmod{4} \), the square above still commutes if the top row is restricted to those \( L \) such that \( q_L \) is primitive. If we restrict \( \Psi_{m,d} \) to the \( q_L \) which are merely matrix-primitive (so that the target of the vertical maps is actually \( \text{Cl}(-md) \)), then \( \Psi_{m,d} \) is equivariant with respect to the \([g_k]\) from Proposition 4.9.
To determine $N_{\text{sm}}(A_m, d)$, it now suffices to identify the non-smooth (or reducible) polarizations of degree $d$. By Proposition 2.4, this is equivalent to counting the product polarizations on $A_m$ of the form

$$L = dh + v$$

with respect to some product decomposition $A_m = E_1 \times E_2$ of $A_m$.

**Corollary 5.1.** Let $\omega(m)$ be the number of distinct primes dividing $m$. Then the number of non-smooth polarizations on $A_m = E \times E'$ of degree $d$ is equal to

$$\begin{cases} 
1 & \text{if } m = 1 \\
2^{\omega(m)-1} & \text{if } m > d = 1 \\
2^{\omega(m)} & \text{if } m > 1 \text{ and } d > 1.
\end{cases}$$

**Proof.** This follows from Proposition 4.3. The non-smooth polarizations of degree $d$ are the product polarizations as in Proposition 2.4 coming from the $2^{\omega(m)}$ different product decompositions $A_m \cong E_k \times E_{k'}$. If $d = 1$, then the order of the product does not matter, giving half as many polarizations. \[\square\]

The corollary above simply counts the non-smooth polarizations. We can be more precise and identify the image of the non-smooth polarizations under the map $\Psi_{m,d}$. Unless otherwise stated, we assume for the rest of the section that $d$ is squarefree.

**Proposition 5.2.** Let $L_k$ be the product polarization $dh_k + v_k$, where $h_k, v_k$ are axes with respect to a decomposition $A_m \cong E_k \times E_{k'}$. Then under the composition

$$\Psi_{m,d} : \text{Aut}(A_m) \backslash \text{NS}(A_m)_d^\text{amp} \rightarrow \Gamma_0(m) \backslash \text{V}_{m,d} \rightarrow \coprod_{g \mid (m,d)} \text{GL}_2(\mathbb{Z}) \backslash \text{V}_{4md/g^2}.\,$$

$L_k$ is sent to the 2-torsion class $[f_k] = \frac{1}{g}[k,0,k'] \in \text{Cl}(-4md/g^2)$, where $g = (k,d)$. \[\square\]

**Proof.** Up to $\text{Aut}(A_m)$-equivalence, we have $L_k = dh_k + v_k = w_k(L)$, where $L = L_1 = dh + v$. Now, $q_k = [md,0,1]$ is primitive and represents 1, so $\Psi_{m,d}(L)$ is the trivial class in $\text{Cl}(-4md)$ (see Lemma 6.2). By Corollary 4.11, we have

$$\Psi_{m,d}(L_k) = \Psi_{m,d}(w_k(L)) = e_g(\Psi_{m,d}(L)) \cdot [f_k] = [f_k],$$

as desired. \[\square\]

Theorem 4.2, Proposition 4.4 and Corollary 5.1 give an explicit formula for $N_{\text{sm}}(A_m, d)$ when $d$ is squarefree. For general squarefree $d$ the formula is a little complicated, so we write down the formula only for $d$ prime to $m$.

**Corollary 5.3.** Let $A_m = E \times E'$ with $E \rightarrow E'$ a cyclic isogeny of degree $m$ and $\text{End}(E) = \mathbb{Z}$. Suppose $d > 1$ is squarefree and prime to $m$. Then

$$N_{\text{sm}}(A_m, d) = \begin{cases} h^+(-4md) - 2^{\omega(m)} & \text{md even} \\
h^+(-4md) + h^+(-md) - 2^{\omega(m)} & \text{md odd},\end{cases}$$

and if $m > 1$, then

$$N_{\text{sm}}(A_m, 1) = \begin{cases} h^+(-4m) - 2^{\omega(m)-1} & \text{m even} \\
h^+(-4m) + h^+(-m) - 2^{\omega(m)-1} & \text{m odd}.
\end{cases}$$

Here $h^+(D) = \#\text{Cl}(D)$.

Restricting to primes $d$ such that $(m, d) = 1$, we have the following more useful result.
Corollary 5.4. Let $A_m = E \times E'$ with $E \rightarrow E'$ a cyclic isogeny of degree $m$ and $\text{End}(E) = \mathbb{Z}$. Suppose $d$ is a prime not dividing $m$ or that $d = 1$. Then

$$N_{sm}(A_m, d) = \begin{cases} 0 & m = d = 1 \\ \frac{1}{2} [h(-4md) + h(-md)] & md \text{ odd and } md > 1 \\ \frac{1}{2} h(-4md) & 8|m \\ \frac{1}{2} [h(-4md) - h(-4md)] & md \text{ even, not divisible by } 8. \end{cases}$$

where $h(D)$ is the size of the class group $\text{Cl}(D)$ of discriminant $D$ and $h_2(D) = \#\text{Cl}(D)[2]$.

Proof. This follows from a simple computation using the previous corollary and the following classical fact [C, Prop. 3.11].

Proposition 5.5. Let $D \equiv 0, 1 \pmod{4}$ be negative, and let $r$ be the number of odd primes dividing $D$. Define $\mu = r$ if $D$ is odd and if $D = -4n$, with $n > 0$, set

$$\mu = \begin{cases} r & \text{if } n \equiv 3 \pmod{4} \\ r + 1 & \text{if } n \equiv 1, 2 \pmod{4} \\ r + 1 & \text{if } n \equiv 4 \pmod{8} \\ r + 2 & \text{if } n \equiv 0 \pmod{8}. \end{cases}$$

Then $\#\text{Cl}(D)[2] = 2^\mu - 1$.

We can now prove Theorem 1.3, stated in the introduction, which determine the set of integers $d$ such that $N_{sm}(A_m, d) \neq 0$, i.e. such that $A_m$ contains a smooth curve of genus $d + 1$.

Proof of Theorem 1.3. If $d$ is composite then $N_{sm}(A_m, d) > 0$. Indeed, if $d = pq$ is a factorization, then $ph + qv$ is globally generated, hence smooth by Lemma 2.1, and of degree $d$. So we may assume $d$ is prime or equal to 1. If $(m, d) = 1$, then Corollary 5.4 gives the result. Now assume that $d = p$ is prime and divides $m$. We show case by case that there is at least one smooth line bundle $L \in \text{NS}(A_m)$ of degree $p$.

Since $p$ divides $m$, the image of $\Psi_{m,d}$ is $V_{-4md}^{mp} \cup V_{-4md/d}^{mp}$. The $2^{\omega(m)}$ non-smooth polarizations always land in either $V_{-4md}^{\text{prim}} \cup V_{-4md/d}^{\text{prim}}$.

(1) Case: $d = 2$. In this case $m$ is even and the target of $\Psi_{m,d}$ is $V_{-8m}^{mp} \cup V_{-2m}^{mp}$.

(a) Subcase: $m$ divisible by 4. Then $\#\text{Cl}(-8m)[2] = 2^{\omega(m)}$. Since $V_{-2m}^{mp}$ is non-empty and $\Psi_{m,d}$ is surjective, we conclude $N_{sm}(A, d) > 0$.

(b) Subcase: $-m/2 \equiv 1 \pmod{4}$. The image of $\Psi_{m,d}$ is then $V_{-8m}^{\text{prim}} \cup V_{2m}^{\text{prim}} \cup V_{-m/2}^{\text{prim}}$. Since $V_{-m/2}^{\text{prim}}$ is not empty and contains only smooth polarizations, $N_{sm}(A, d) > 0$.

(c) Subcase: $-m/2 \equiv 3 \pmod{4}$. The image of $\Psi_{m,d}$ is $V_{-8m}^{\text{prim}} \cup V_{-2m}^{\text{prim}}$ in this case. We have $\#\text{Cl}(-8m)[2] = 2^{\omega(m)-1}$ and $\#\text{Cl}(-2m)[2] = 2^{\omega(m)-1}$. So there are $2^{\omega(m)}$ images under $\Psi_{m,d}$, which is the same as the number of non-smooth polarizations. But the fibers of $\Psi_{m,d}$ above elements of $q \in V_{-2m}^{\text{prim}}$ have size $|\Gamma_0(m)/\Gamma_0(m/2)/\text{Aut}(q)|$. When $m > 2$, $\text{Aut}(q)$ acts on the three element set $\Gamma_0(m)/\Gamma_0(m/2)$ by a quotient of size at most 2, so the fibers are singletons and $N_{sm}(A_m, d) > 0$.

If $m = 2$, then consider the line bundle $L = 2h + X_3 + 2v$. Neither $q_L$ nor $q_2^L$ are primitive, hence they cannot represent 1. Since $E$ and $E_2 = E'$ are the only elliptic curves on $A_2$ up to abstract isomorphism, this shows that $L.F > 1$ for any elliptic curve $F$ on $A_2$. So $L$ is smooth and $N_{sm}(A_2, 2) > 0$. 

□
(2) Case: $d > 2$.

(a) Subcase: $m$ odd. Then $\text{Cl}(-md)$ is non-empty if $m$ and $d$ are different (mod 4), in which case $N_{\text{sm}}(A, d) > 0$. If $m \equiv d$ (mod 4), then $\#\text{Cl}(-4md) = 2^{\omega(m)+1} > 2^{\omega(m)}$, so $N_{\text{sm}}(A, d) > 0$.

(b) Subcase: $m$ even. Then $\#\text{Cl}(-4md)[2]$ is at least $2^{\omega(m)}$, which is the number of non-smooth polarizations. Since $\text{Cl}(-4m/d)$ is non-empty, $N_{\text{sm}}(A, d) > 0$.

Below we give a sampling of some consequences of Corollary 1.5, which has now been proved. Note that some of these are conditional on GRH, but many of them are not.

**Corollary 5.6.** There exists an integer $N$ which does not depend on $m$, such that $A_m$ contains a smooth curve of genus $g$ for all $g > N$. If you assume GRH, we may take $N = 30$. Unconditionally, there are at most 7 values of $g$ for which $A_m$ does not have a smooth curve of genus $g$.

**Corollary 5.7.** There exists an integer $N$ such that for all $m > N$, $A_m$ contains smooth curves of each genus $g \geq 1$. If we assume GRH, then we may take $N = 462$.

*Proof of Corollary 1.8.* We have seen that $A$ has a smooth polarization of degree $d$ when $d$ is composite. If $d > 2$ is prime $> 2$, then $d$ is not on the list in Corollary 1.5. This is true unconditionally since the possible extra value $N$ is even. The values $d = 1$ and $d = 2$ are on the list, so $A$ is not a Jacobian and does not contain smooth curves of genus 2 and 3.

*Proof of Corollary 1.9.* $A_2$ is not a Jacobian, so assume that $m$ is odd. If $d = 1$, then $N_{\text{sm}}(A, d) > 0$ since $md = m$ is not in the set $R$ of integers listed in Corollary 1.5. If $d = 2$, then $N_{\text{sm}}(A_m, 2) = 0$ when $m = 3, 5, 11, 29$. For other values of $m$, we must consider the possibility that $m = N/2$, where $N$ is the possible extra idoneal number in $R$. But if so, then $h(-4N) = h(-8m) = h_2(-8m) \leq 2$, and the largest such $N$ is $N = 58$ (see [Wa] for example). So $N_{\text{sm}}(A_m, 2) > 0$ as long as $m \neq 3, 5, 11, 29$. If $d > 2$ is prime then $N_{\text{sm}}(A_m, d) > 0$ as $md$ is odd and hence not in the set $R$.

Using the tables of [Wa] and the technique of the previous proof, one can deduce much stronger unconditional results. We leave these to the interested reader.

6. **Very ample polarizations on $A_m$**

Before proving Theorem 1.4, we record some basic facts about quadratic forms and ideal classes.

**Lemma 6.1.** Primitive quadratic forms $[a, ab, c]$ of discriminant $D$ correspond to 2-torsion ideal classes in $\text{Pic}(\mathcal{O}_D)$.

*Proof.* Recall that a primitive form $[a, b, c]$ of discriminant $D$ corresponds to the class of the ideal $\mathbb{Z}a + \mathbb{Z}\frac{-b + \sqrt{D}}{2}$ in the quadratic ring of discriminant $D$. Moreover, conjugation of ideals induces inversion on the class group. As the ideal $(a, -\frac{ab + \sqrt{D}}{2})$ is fixed by conjugation, it follows that the corresponding ideal classes are 2-torsion. \hfill $\square$

**Lemma 6.2.** Let $f = [a, b, c]$ be a primitive positive definite quadratic form of discriminant $D$ and let $[a]$ be the corresponding class of proper $\mathcal{O}_D$-ideals. Then $[a]$ contains an ideal of norm $a$.

**Lemma 6.3.** Let $D$ be a quadratic discriminant and $g \geq 1$ an integer. Then the kernel of the natural map $\text{Pic}(\mathcal{O}_D) \to \text{Pic}(\mathcal{O}_D)$ has size

$$\prod_{p | \frac{g}{\prod_{D / p} \left(1 - \frac{D}{p} \frac{1}{p}\right)}}$$
Proof. See [C] for proofs.

The next few propositions count the number of (equivalence classes of) smooth but merely ample line bundles on $A_m$

**Proposition 6.4.** Let $d \geq 5$ be odd and squarefree and let $m \geq 1$ be odd. Then there are $2^{\omega(m)}$ \text{Aut}(A_m)-equivalence classes of smooth and merely ample line bundles of degree $d$ on $A_m$.

**Proof.** First we construct $2^{\omega(m)}$ such line bundles. For each $k|m$ such that $(k, k') = 1$, we choose an isomorphism $E_k \times E_{k'} \cong A_m$. We let $\lambda_k : E_k \to E_{k'}$ be the usual minimal isogeny of degree $m$. Since $m$ is odd, $\lambda_k$ induces an isomorphism $E_k[2] \cong E_{k'}[2]$. We let $G_k \subset E_k \times E_{k'}$ be the subgroup

$\{(P, \lambda_k(Q)) : P \in E_k[2]\},$

which is abstractly isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. In fact, $G_k = \Gamma_{\lambda_k}[2]$, where $\Gamma_{\lambda_k}$ is the graph of $\lambda_k$. Since $E_k \times E_{k'} \cong \Gamma_{\lambda_k} \times E_{k'}$

the quotient $E_k \times E_{k'}/G_k$ is isomorphic to $A_m$. Write $\pi : E_k \times E_{k'} \to A_m$ for the induced 4-isogeny. Then by Theorem 2.7, there exists a merely ample $L_k \in \text{Pic}(A_m)$ such that $\pi^*L_k = 2dhk + 2v_k$, where $h_k$ and $v_k$ are the axes with respect to this decomposition $E_k \times E_{k'}$.

To prove that $L_k$ is smooth, we may assume $k = 1$ (we could always relabel the elliptic curves on $A_m$). If $L_k$ is not smooth, then there exists a decomposition $A_m \cong F \times F'$ such that $L \equiv dh + v$, where $h$ and $v$ are axes with respect to this new decomposition. But then $(dh + v.E) = 2$, which forces $E.h = 0$ and hence $F = E$. Then $q_L = [dm, 0, 1]$ which does not represent 2, contradicting $L.E = 2$. This shows the existence of smooth but merely ample $L_k$ for each of the $2^{\omega(m)}$ divisors $k|m$ satisfying $(k, m/k) = 1$. The $L_k$ have the property that $L_k.F = 2$, for some elliptic curve $F$ isomorphic to $E_k$. By Lemma 2.10, the $L_k$ are in different $\text{Aut}(A_m)$-equivalence classes.

Finally, we need to show that any smooth and merely ample line bundle $M$ of degree $d$ is $\text{Aut}(A_m)$-equivalent to one of the $L_k$. By Reider’s theorem, $M.F = 2$ for some elliptic curve which is isomorphic to $E_k$ for some $k|m$. As $q^k_M = [ak', -2bm, ck]$ represents 2, we must have $(k, k') \leq 2$. Since $m$ is odd, this means $(k, k') = 1$ and again we may assume $k = 1$. Writing $L$ for $L_1$, we need to show that $L$ and $M$ are $\text{Aut}(A_m)$-equivalent. But both $q_L$ and $q_M$ are matrix-primitive and represent 2 and so are $\text{GL}_2(\mathbb{Z})$-equivalent to the form $[2, 2, (1 + md)/2]$. In other words, $\Psi_{m,d}(L) = \Psi_{m,d}(M)$. Since $\Psi_{m,d}$ is injective on the set of equivalence classes of $L$ for which $q_L$ is matrix-primitive, we see that $L$ and $M$ are $\text{Aut}(A_m)$-equivalent.

**Proposition 6.5.** Let $d \geq 5$ be odd and squarefree and suppose $m$ is even but not divisible by 8. If $L \in \text{NS}(A_m)$ has degree $d$ and is merely ample, then $L$ is not smooth.

**Proof.** First assume that $m \equiv 2 \pmod{4}$. As $L$ is merely ample, we have $L.F = 1$ or $L.F = 2$ for some elliptic curve $F \subset A_m$. We may assume that $L.F = 2$ and we need to show that $L.F' = 1$ for some elliptic curve $F'$. $F$ is isomorphic to $E_k$ for some $k|m$ and $q^k_{L} = [ak', -2bm, ck]$ represents 2. This implies $(k, k') = 1$. Thus after reindexing the elliptic curves on $A_m$, we may assume $k = 1$ and $q_L$ represents 2. As $-4md$ is a fundamental discriminant, $q_L$ is primitive and we must have $[q_L] = [f_2]$. By Corollary 4.11, we have

$1 = [f_2]^2 = [q_L] \cdot [f_2] = [q_{w_2(L)}].$

So there exists an elliptic curve $F_0 \subset A_m$ such that $w_2(L)F_0 = 1$. Hence $L.w_2(F_0) = 1$, showing that $L$ is not smooth.

Now assume that $m \equiv 4 \pmod{8}$ and again suppose $L.F = 2$ for an elliptic curve $F$ isomorphic to $E_k$. As $q^k_{L} = [ak', -2bm, ck]$ represents 2 and $a$ and $c$ are odd (since $ac = mb^2 + d$), we must
Proposition 6.6. Let $d \geq 5$ be odd and squarefree and suppose $m$ is divisible by 8. Then there are $2^{\omega(m)} \text{Aut}(A_m)$-equivalence classes of smooth and merely ample line bundles of degree $d$ on $A_m$.

Proof. First we construct, for each $k|m$ such that $(k,k') = 2$, a smooth and merely ample line bundle $L_k$ such that $L_k . F = 2$ for some elliptic curve $F$ isomorphic to $E_k$. Note that there are $2^{\omega(m)}$ such divisors $k$ and that the $L_k$ are not $\text{Aut}(A_m)$-equivalent to one another by Lemma 2.10. It suffices to construct $L_k$ when $k = 2$, because we can always relabel the elliptic curves on $A_m$.

To construct $L_2$, we consider the following elliptic curves on $A_m = E \times E'$:

$$E_2 \equiv 2h + X_\lambda + (m/2)v$$
$$F \equiv (m/2)h + (m/4 + 1)X_\lambda + 2(m/4 + 1)^2 v.$$ 

$E_2$ is the image of the map $E \to A_m$ given by $P \mapsto (2P, \lambda(P))$, and $F$ is the image of the map $P \mapsto (\frac{m}{2}P, \left(\frac{m}{4} + 1\right)\lambda(P))$. These two elliptic curves intersect in $(E_2,F) = 4$ points. In fact, the four points are given by $(0,0)$, $(0,\lambda(R))$, $(S,0)$ and $(S,\lambda(R))$, where $S$ generates the order 2 subgroup $H_2$ of $\ker \lambda$ and $S$ is any other order 2 point on $E$. We therefore have $E_2[2] = F[2]$. Now consider the subtraction map

$$\mu : B := E_2 \times F \to E \times E' = A_m$$
$$(P,Q) \mapsto P - Q.$$ 

By Theorem 2.7, there is a merely ample $L_2 \in \text{NS}(A_m)$ of degree $d$ such that $\mu^*L = 2dh_B + 2v_B$.

On the other hand, $L_2$ is smooth. For if otherwise, then $L_2 = \tilde{h} + \tilde{d}v$ with respect to some product decomposition of $A_m$, and as $(\tilde{h} + \tilde{dv}, E_2) = 2$, we must have $\tilde{v}.E_2 = 0$. This forces $\tilde{v} = E_2$, but $E_2$ is not a direct factor of $A_m$ as $(2,m/2) > 1$, so we have a contradiction.

It remains to show that any smooth and merely ample $M$ on $A_m$ of degree $d$ is $\text{Aut}(A_m)$-equivalent to one of the $L_k$. We have $M.F = 2$ for some elliptic curve $F$ isomorphic to $E_k$ for some $k|m$. As $q^k_M$ represents 2, we must have $(k,k') = 2$ and we may, as usual, assume $k = 2$. We now set $L = L_2$ and show that $M$ and $L$ are $\text{Aut}(A_m)$-equivalent. If we write $q^2_M = 2h(x,y)$ for a quadratic form $h$ which represents 1, then $h(2x,y) = q_M$. In particular, $q_M$ is primitive. By Lemma 4.10, $[q_M]$ is in the kernel of

$$e_2 : \text{Pic}(O_{-4md}) \to \text{Pic}(O_{-md}),$$

which has size 2. But $[q_M] = \Psi_{m,d}(M)$ cannot be trivial because that corresponds to the nonsmooth class $d(h + v)$. So $[q_M]$ is the generator of $\ker(e_2)$. The same argument applies to $L_2$, so $\Psi_{m,d}(L_2) = \Psi_{m,d}(M)$. Since $q_M$ and $q_{L_2}$ are primitive, this implies that $L_2$ and $M$ are $\text{Aut}(A_m)$-equivalent.

Propositions 6.4, 6.5, and 6.6 and their proofs suggest that if $L$ is merely ample, then $\Psi_{m,d}(L)$ is 2-torsion in its corresponding class group. We prove this next in certain cases. The proof is essentially the translation of the proofs above from the language of algebraic geometry to the language of quadratic forms via the correspondence of Theorem 4.2.
Proposition 6.7. Suppose \( d = p \) or \( d = 2p \) for an odd prime \( p \) and let \( L \in \text{NS}(A_m) \) be merely ample of degree \( d \geq 5 \). Assume that \( m \) is odd if \( d \) is even. Then \( \Psi_{m,d}(L) \) is 2-torsion in its class group.

Proof. Write \( L = ah + bX_1 + cv \). If \( L \) is not smooth, then \( \Psi_{m,d}(L) \) is 2-torsion by Proposition 5.2. So assume \( L \) is smooth and merely ample. Then by Proposition 2.4 and Theorem 2.5, there is an elliptic curve \( E_k \) on \( A_m \) such that \( E_k.L = 2 \). Here, \( E_k = E/H_k \) for some divisor \( k \) of \( m \) and \( k' = k/m \). This means that the quadratic form

\[
q_L^k(x, y) = ak'x^2 - 2bmy + cky^2
\]

represents 2.

(1) Case: \( q_L^k \) is a multiple of 2.

(a) Subcase: \( m \) is odd. It follows that \( a \) and \( c \) are even, \( b \) and \( d \) are odd, and \( (k, k') = 1 \).

As \( \frac{1}{2}q_L^k \) represents 1, its class in \( \text{Cl}(-md) \) is the trivial class. By Lemma 4.8, \( [\frac{1}{2}q_{w_k(L)}] \) is also the trivial class. By Corollary 4.11 applied to \( w_k(L) \), we have

\[
\Psi_{m,d}(L) = e_g(\Psi_{m,d}(w_k(L))) \cdot [g_k] = e_g(1) \cdot [g_k] = [g_k],
\]

where \( g = (k, d) \). The class \([g_k] \) is 2-torsion by Lemma 6.1, which proves the proposition in this subcase.

(b) Subcase: \( m \) is even and \( (m, d) = 1 \). In particular, \( d = ac - mb^2 \) is prime. In this case, both \( a \) and \( c \) are odd, so \( k \) and \( k' \) are even and \( (k/2, k'/2) = 1 \). To ease notation, we write \( D = -md \) and as usual write \( \mathcal{O}_D \) for the quadratic order of discriminant \( D \).

Consider the following quadratic forms of discriminant \( 4D \):

\[
f_1 = [k/2, 0, 2k'd]
\]

\[
f_2 = [2k, 0, k'd/2].
\]

At least one of these is primitive, call it \( f_k \), and so it makes sense to consider the product \([f_k] \cdot [q_L] \) in the class group \( \text{Cl}(4D) \). Dirichlet composition of forms gives \([f_k] \cdot [q_L] = [h_k] \), where \( h_k \) is one of

\[
h_1 = [2ak', -2bm, kc/2],
\]

\[
h_2 = [ak'/2, -2bm, 2kc]
\]

depending on whether we chose \( f_1 \) or \( f_2 \). We claim that \([h_k] \) is 2-torsion in \( \text{Pic}(\mathcal{O}_D) \).

In fact, \([h_k] \) is in the kernel of the natural map

\[
e_2 : \text{Pic}(\mathcal{O}_D) \to \text{Pic}(\mathcal{O}_D),
\]

which establishes the claim as \( \ker(e_2) \) has size 2 by Lemma 6.3. To see that \([h_k] \in \ker(e_2) \), note that

\[
h_1(x, y) = \frac{1}{2}q_L^k(2x, y) \quad \text{and} \quad h_2(x, y) = \frac{1}{2}q_L^k(x, 2y),
\]

and use Lemma 4.10 and the fact that \( [\frac{1}{2}q_L^k] \) is trivial in \( \text{Pic}(\mathcal{O}_D) \). Finally, \( f_k \) is 2-torsion in \( \text{Cl}(4D) \) as well, so we see that \([q_L] = [f_k] \cdot [h_k] \) is 2-torsion in \( \text{Cl}(4D) \), as desired.

(c) Subcase: \( m \) is even and \( d \) is a prime \( p \) which divides \( m \). If \( (c, p) = 1 \), then \( q_L \) is primitive and we can argue as in the previous case. So suppose \( p \) divides \( c \), hence \( p \) divides \( k \) as well. The quadratic form \( q_L \) has content \( p \) and we let \( q \) be the primitive form \( \frac{1}{p}q_L \) of discriminant \( -4m/p \). As before, we have

\[
[k/2p, 0, 2k'] \cdot [q] = [h_k],
\]

(6.1)
in the class group $\text{Cl}(-4m/p)$, where $h_k$ is either
\[ [2ak'/p^2, -2bm'/p, kc/2] \text{ or } [ak'/2p^2, -2bm/p, 2kc], \]
whichever one is primitive. Assume for simplicity that the former is primitive (a similar argument holds if only the other is primitive). If we set $z(x, y) = \frac{1}{2}q_L^k(x, 2y)$, then $h_k(x, y) = z(x/p, y)$. We have maps
\[ e_2 : \text{Pic}(\mathcal{O}_{-4mp}) \to \text{Pic}(\mathcal{O}_{mp}) \]
\[ e_p : \text{Pic}(\mathcal{O}_{-4mp}) \to \text{Pic}(\mathcal{O}_{-4m/p}), \]
and one checks as before that $e_2([z]) = [\frac{1}{2}q_L^k]$ is 1 and $e_p([z]) = [h_k]$. The first equation implies that $[z]$ is two-torsion and thus $[h_k]$ is 2-torsion by the second equation. Finally, we deduce from (6.1) that $[q] = [\frac{1}{2}q_L^k] = \Psi_{m,d}(L)$ is 2-torsion in $\text{Cl}(-4m/p)$.

(2) Case: $q_L^k$ is primitive: In this case $(k, k') = 1$. If $md$ is a multiple of 4, then one quickly gets a contradiction to the fact that $q_L^k$ is primitive and represents 2. So there are two subcases to consider:

(a) Subcase: $md$ is even. In this case, $q_L^k$ corresponds to the class of an ideal $\mathfrak{a}$ in $\mathcal{O}_{-4md}$ of norm 2, by Lemma 6.2. But there is a single prime above the rational prime 2 in the maximal order containing $\mathcal{O}_D$ and as $\mathfrak{a}$ must be a prime ideal, $\mathfrak{a}$ is uniquely determined. We conclude that $q_L^k$ is $\text{GL}_2(\mathbb{Z})$-equivalent to the 2-torsion class $[2, 0, md/2]$. Corollary 4.11 and Lemma 4.8 then give
\[ e_g([2, 0, md/2]) \cdot [f_k] = \Psi_{m,d}(L), \]
which shows that $\Psi_{m,d}(L)$ is 2-torsion.

(b) Subcase: $md$ is odd. First note that $md \equiv 1 \pmod{4}$ in this case, for if $md \equiv 3 \pmod{4}$, then there are no primitive quadratic forms of discriminant $-4md$ which represent 2. Since $md \equiv 1 \pmod{4}$, the prime 2 ramifies in the corresponding quadratic field. We conclude as before that $[q_L^k]$ is the 2-torsion class $[2, 2, (1 + md)/2]$ and
\[ e_g([2, 2, (1 + md)/2]) \cdot [f_k] = \Psi_{m,d}(L), \]
since $\Psi_{m,d}(L)$ is 2-torsion. □

Notation We write $H(D)$ for the number of isomorphism classes of primitive integral symmetric bilinear forms of rank 2 and determinant $D$.

Of course, primitive integral symmetric bilinear forms of determinant $D$ are in bijection with matrix-primitive quadratic forms of discriminant $-4D$. If one wants a bijection with primitive integral quadratic forms, then primitive quadratic forms of discriminant $d \equiv 1 \pmod{4}$ correspond to bilinear forms of discriminant $-D$. If $D > 0$, then we can relate $H(D)$ to the classical class numbers $h(d)$ of positive definite quadratic forms of discriminant $d$ up to $\text{SL}_2(\mathbb{Z})$-equivalence as follows:
\[ H(D) = \frac{1}{2} \begin{cases} h(-4D) + h_2(-4D) & D \not\equiv 3 \pmod{4} \\ h(-4D) + h_2(-4D) + h(-D) + h_2(-D) & D \equiv 3 \pmod{4} \end{cases} . \]
Here, $h_2(d)$ is the number of 2-torsion classes.

Notation We write $H_2(D)$ for the number of primitive integral symmetric bilinear forms of rank 2 and determinant $D$ which correspond to 2-torsion classes of quadratic forms.

Theorem 6.8. Suppose $p \geq 5$ is prime and $(m, p) = 1$. Then $N_{va}(A_m, p) = H(mp) - H_2(mp)$.

Proof. This follows from a simple computation using Propositions 6.4, 6.5, 6.6, Corollary 5.1, and Proposition 6.1. □
Proof of Theorem 1.4. If $d$ is not prime or twice a prime, then we can write $d = pq$ with $p$ and $q$ both larger than 2. Then $L = ph + qv$ is very ample, being the product of pull backs of very ample line bundles on $E$ and $E'$. So $N_{\text{va}}(A_m, d) > 0$ if $d$ is not a prime or twice an odd prime. Theorem 1.4 now follows from Theorems 6.9 and 6.10, which we prove next.

Theorem 6.9. If $d = p \geq 5$ is prime, then $N_{\text{va}}(A_m, d) = 0$ if and only if $(m, d) = 1$ and $\text{Cl}(-4md)$ is 2-torsion.

Theorem 6.10. If $p \geq 3$ is prime, then $N_{\text{va}}(A_m, 2p) = 0$ if and only if

1. $(m, p) = 1$.
2. $\text{Cl}(-4md)$ is 2-torsion.
3. If we factor $m = \prod_p p^{a_p}$, then $a_2$ is either 0, 2, or 3.

Proof of Theorem 6.9. If $(m, p) = 1$, the theorem follows from Theorem 6.8. Note that this is true even when $mp \equiv 3 \pmod{4}$ because if $\text{Cl}(-4mp)$ is 2-torsion, then $\text{Cl}(-mp)$, being a quotient of $\text{Cl}(-4mp)$, is 2-torsion as well.

So assume now that $d = p$ divides $m$. We will show that there is a very ample line bundle of degree $p$ on $A_m$. We proceed case-by-case and use the letters $d$ and $p$ interchangeably.

1. Case: $m$ is odd.
   (a) Subcase: $md \equiv 1 \pmod{4}$. In this case $\Psi_{m,d}$ maps to $\text{Cl}(-4mp) \coprod \text{Cl}(-4m/p)$. It follows from the analysis in Case (2a) of Proposition 6.7 that any smooth but merely ample $L$ which maps to $\text{Cl}(-4m/p)$ does not map to classes of the form $[a,0,b]$. So only non-smooth $L$ map to such classes. In fact, exactly half of the $2^{\omega(m)}$ non-smooth $L$ map to $\text{Cl}(-4m/p)$: those corresponding to divisors $k$ divisible by $p$. We have $h_2(-4m/p) = 2^{\omega(m)}$, so these non-smooth $L$ either map 2-to-1 or 1-to-1 to over the points of the form $[a,0,b] \in \text{Cl}(-4m/p)$, depending on whether $p^2|d$ or not. On the other hand, the fibers of the surjective map $\Psi_{m,d}$ are of size $\# \Gamma_0(m) \setminus \Gamma_0(m/p)/\text{Aut}(q)$. The size of $\Gamma_0(m) \setminus \Gamma_0(m/p)$ is either $p$ or $p+1$, depending on whether $p^2|d$ or not. As $q$ has even discriminant, $\text{Aut}(q)$ has either 4 or 8 elements, but it acts on the coset space through a quotient of size at most 2.\footnote{If $|\text{Aut}(q)| = 8$, then $[q] = [x^2 + y^2]$ and there are 4 diagonal automorphisms.} Since $p \geq 5$, we see that in all cases, the fibers of $\Psi_{m,d}$ above points of the form $[a,0,b] \in \text{Cl}(-4m/p)$ are larger than 2, so there must be a very ample line bundle in each of those fibers. So $N_{\text{va}}(A_m, d) > 0$ in this subcase, as desired.

(b) Subcase: $md \equiv 3 \pmod{4}$. This time $\Psi_{m,d}$ maps onto

$$\text{Cl}(-4mp) \coprod \text{Cl}(-mp) \coprod \text{Cl}(-4m/p) \coprod \text{Cl}(-m/p).$$

However the $2^{\omega(m)}$ non-smooth $L$ map to the even discriminant groups and the rest of the merely ample $L$ map to the odd discriminant groups, by the analysis in Case (1a) of Proposition 6.7. But

$$h_2(-4mp) + h_2(-4m/p) = 2^{\omega(m)} + h_2(-4m/p) > 2^{\omega(m)},$$

so there must be at least one very ample $L$ of degree $d$, i.e. $N_{\text{va}}(A_m, d) > 0$.

2. Case: $m$ even, not divisible by 8. In this case, $\Psi_{m,d}$ maps onto

$$\text{Cl}(-4mp) \coprod \text{Cl}(-4m/p).$$

We have $h_2(-4mp) = 2^{\omega(m)-1}$ and $h_2(-4m/p)$ is either $2^{\omega(m)-1}$ or $2^{\omega(m)-2}$, depending on whether $p^2|d$ or not. But if $L \in \text{NS}(A_m)$ has degree $p$ and is merely ample, then it is also not smooth, by Proposition 6.5. So on the one hand, the merely ample $L$ map either
1-to-1 or 2-to-1 onto Cl(−4mp/p), whereas the fibers of Ψm,d above such points have size
#Γm,0/Γm,0/Aut(q) > 2. There therefore must be some very ample L of degree p and
Nm,0(Am,d) > 0.
(3) Case: m ≡ 0 (mod 8). In this case, Ψm,d maps onto

\text{Cl}(−4mp) \prod \text{Cl}(−4mp).

By Proposition 6.6 and Corollary 5.1, there are exactly 2ω(m)+1 merely ample classes of line
bundles. On the other hand, #\text{Cl}(−4mp)[2] = 2ω(m) and #\text{Cl}(−4mp/p)[2] is either 2ω(m)
or 2ω(m)−1, depending on whether p2|m or not. The fibers of Ψm,d above Cl(−4mp)[2] are
singletons and the fibers above q ∈ Cl(−4mp)/[2] are of size

Γm,0/m,0/\text{Aut}(q).

The coset space Γm,0/m,0/\text{Aut}(q) has size p or p+1 depending on whether p2|m, and Aut(q)
acts through a quotient of size at most 2. Thus the fibers of Ψm,d above Cl(−4mp/p) have
size at least p/2 > 2. This shows that there are more than 2ω(m)+1 degree p polarizations
on Am, hence Nm,0(Am,p) > 0, as desired.

\qed

Proof of Theorem 6.10. We again break into several cases.

(1) Case: m odd and (p,m) = 1. In this case, Ψm,d maps the isomorphism classes of degree
d polarizations L ∈ NS(Am) bijectively onto Cl(−4md). The merely ample L map to
Cl(−4md)[2], which has size 2ω(m)+1. The non-smooth L map to the 2ω(m) forms [k,0,kd].
The smooth merely ample line bundles must map to the remaining 2-torsion classes by
Proposition 6.7; these are of the form [2k,0,kp]. Conversely, if [gL] = [2k,0,kp] for k
such that (k,k') = 1, then L is smooth and merely ample. Indeed, by Proposition 4.9,
[qL] = [qL] · [kp] = [2,0,mp], which represents 2. So LEk = 2 and L isn’t very ample.
Altogether, we have accounted for the 2ω(m)+1 2-torsion classes in Cl(−4md), showing that

Nm,0(Am,d) = \frac{1}{2} |h(−4md) − h2(4md)|.

(2) Case: m odd and p divides m. Let f : Am → A2m be any degree 2 isogeny. For example,
let A2m = E × E'' where E'' = E'/P with P ∈ E any point of order 2 and set

f = \text{id} \times \pi : A_m = E \times E' \rightarrow E \times E'' = A_{2m}.

By Theorem 6.9, there exists a very ample line bundle M of degree p on A2m. Then
f* M ∈ NS(Am) has degree 2p and is very ample by Lemma 2.8. When p = 3, there is no
very ample M, for degree reasons. However, it is still true that there exists an M for which
M.F > 2 for all elliptic curves F ∈ A2m. This is enough for the proof of Lemma 2.8 to go through.\footnote{Here and in some other cases, we leave the details for the case p = 3 to the reader.}
Thus Nm,0(Am,d) > 0.
(3) Case: m ≡ 2 (mod 4). If p|m, then Nm,0(Am,d) > 0. Indeed, we may choose an isogeny
f : Am → A2m and by Theorem 6.9, there is a very ample line bundle M ∈ NS(Am/2) of
degree p. Then f*M ∈ NS(Am) is very ample of degree 2p = d.
Assume now that (p,m) = 1. We will construct a very ample L on Am of degree 2p using
the 2-isogeny

f : Am = E × E' \xrightarrow{\text{id} \times \mu_{m/2}} E \times E_{m/2} = Am/2.

Let M ∈ NS(Am/2) be smooth of degree p and satisfying M.F = 2 for some elliptic curve
F ∈ A_m/2 which is abstractly isomorphic to E_m/2. The existence of such an M follows from
the proof of Proposition 6.4. By Proposition 4.6, we may choose α ∈ Aut(Am/2) such that
\( \alpha^*F = \{0\} \times E_{m/2} \). Set \( g = \alpha \circ f \), so that \( g : A_m \to A_{m/2} \) is a 2-isogeny. We have \( g^*F = v \) and \( g_*v = 2F \). Thus,

\[
(g^*M.v) = (M.g_*v) = 2(M.F) = 4.
\]

On the other hand, \( g^*M \) is smooth because \( M \) is smooth. So if \( g^*M \) is not very ample, then there exists an elliptic curve \( F' \subset A \) such that \( (g^*M.F') = 2 \) and so \( (M.g_*F') = 2 \).

Note that \( g_*F' \) is an elliptic curve for otherwise it is twice an elliptic curve and this would contradict the smoothness of \( M \). By Lemma 2.10, we must have \( g_*F' = F \). This shows that \( F' = v \) and hence \( (g^*M.v) = 2 \), which contradicts our computation above. So \( g^*M \) is very ample and \( N_{va}(A_m, d) > 0 \).

(4) Case: \( m \equiv 0 \pmod{4} \).

(a) Subcase: \( p \) divides \( m \). Consider a 2-isogeny \( f : A_m \to A_{m/2} \). By Theorem 6.9, there is a very ample \( L \in \text{NS}(A_{m/2}) \) of degree \( p \), so \( f^*L \) is very ample of degree \( 2p \). Hence \( N_{va}(A_m, d) > 0 \).

(b) Subcase: \( (p, m) = 1 \) and \( m \not\equiv 0 \pmod{16} \). Then \( \Psi_{m,d} \) maps onto \( \text{Cl}(-8mp) \prod \text{Cl}(-2mp) \).

If \( L \equiv ah + bX + cv \) maps to \( \text{Cl}(-8mp) \), then \( a \) is even and \( L = f^*M \), where \( f \) is the 2-isogeny

\[
A_m = E \times E' \to A_{m/2} = E \times E_{m/2}
\]

and \( M \) has degree \( p \). If \( L \) is not very ample, then \( M \) is not very ample and by Proposition 6.5, we see that \( M \) is not even smooth. Conversely, if \( M \in \text{NS}(A_{m/2}) \) of degree \( p \) is not smooth, then \( M.F = 1 \) for some elliptic curve \( F \subset A_{m/2} \) and therefore \( f^*M.f^*F = 2 \).

So \( f^*M \) has degree \( 2p \) and is not very ample. There are \( 2^{\omega(m)} \) such \( M \) up to \( \text{Aut}(A_{m/2}) \)-equivalence, and they give rise to \( 2^{\omega(m)+1} \text{Aut}(A_m) \)-equivalence classes of non-very-ample \( L \) of degree \( 2p \), because \( [\Gamma_0(m/2) : \Gamma_0(m)] = 2 \) and \( \text{Aut}(q_M) \) acts trivially on the cosets.

Similarly, if \( \Psi_{m,d}(q_L) \in \text{Cl}(-2mp) \), then \( c \) is even and \( L = g^*M \) where \( g \) is the 2-isogeny

\[
A_m = E \times E' \to E_2 \times E' = A_{m/2},
\]

and \( M \) has degree \( p \). There are again \( 2^{\omega(m)+1} \) different \( L \) which are not very ample.

On the other hand, \( h_2(-8mp) = 2^{\omega(m)+1} \) and \( h_2(-2mp) = 2^{\omega(m)} \) with fibers of \( \Psi_{m,d} \) above points in \( \text{Cl}(-2mp) \) having size exactly \( 2 \). So \( N_{va}(A_m, d) = 0 \) if and only if both \( \text{Cl}(-4md) \) and \( \text{Cl}(-md) \) are 2-torsion if and only if \( \text{Cl}(-4md) \) is 2-torsion.

(c) Subcase: \( (p, m) = 1 \) and \( m \equiv 0 \pmod{16} \). We will construct a very ample divisor of degree \( 2p \) on \( A_m \). We consider the 2-isogeny

\[
f : A_m = E \times E' \xrightarrow{\lambda_2 \times \text{id}} E_2 \times E' = A_{m/2}.
\]

We write \( \lambda_0 : E_2 \to E' \) for the unique map satisfying \( \lambda = \lambda_0 \circ \lambda_2 \), i.e. \( \lambda_0 \) is a minimal isogeny connecting \( E_2 \) and \( E' \). By Proposition 6.6, \( A_{m/2} \) has a smooth line bundle \( L \) of degree \( p \) such that \( L.E_4 = 2 \), where \( E_4 \subset A_{m/2} \) is the image of the map

\[
E_2 \to E_2 \times E'
\]

\[
R \mapsto (2R, \lambda_0(R)).
\]

We refer to it as \( E_4 \) because it is abstractly isomorphic to the elliptic curve we’ve been calling \( E_4 \) on \( A_m \). With respect to the surface \( A_{m/2} \), though, this is the elliptic curve we called \( E_2 \) in the proof of Proposition 6.6. We think of \( E_2 \subset A_m \) as the image of the map \( E \to A_m : P \mapsto (2P, \lambda(P)) \) as usual. It is easy to check that \( f(E_2) = E_4 \). As \( E_2 \)
and $E_4$ are not abstractly isomorphic, this forces the induced map $f : E_2 \to E_4$ to have degree 2. So $f^*E_4 = E_2$ and $f_*E_2 = 2E_4$, giving

$$(f^*L.E_2) = (L.2E_4) = 4.$$  

But if $F \subset A_m$ is an elliptic curve on $A_m$ such that $(f^*L.F) = 2$, then $(L.f_*F) = 2$ and $f_*F = E_4$ by Lemma 2.10. But this forces $F = E_2$, and hence a contradiction:

$$4 = (f^*L.E_2) = (f^*L.F) = 2.$$  

We conclude that $f^*L$ is very ample of degree $2p$ and $N_{va}(A_m, d) > 0$.  

\[ \square \]

References

[BL] Ch. Birkenhake, H. Lange, Complex abelian varieties, Springer-Verlag, Grundlehren 302 (1992).
[C] D.A. Cox, Primes of the form $x^2 + ny^2$, John Wiley, 1989.
[GZ] B. Gross, D. Zagier, Heegner points and derivatives of L-series, Inv. Math. 84 (1986), 225-320.
[Ha] T. Hayashida, A class number associated with a product of two elliptic curves. Natur. Sci. Rep. Ochanomizu Univ. 16 (1965), 9-19.
[HN] T. Hayashida and M. Nishi, Existence of curves of genus two on a product of two elliptic curves. J. Math. Soc. Japan 17 (1965), 1-16.
[HM] G. Horrocks and D. Mumford, A rank 2 vector bundle on $\mathbb{P}^4$ with 15,000 symmetries, Topology 12 (1973), 63-81.
[K1] E. Kani, The moduli space of Jacobians isomorphic to a product of two elliptic curves. Preprint, 39pp.
[K2] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms, J. Number Theory, to appear.
[K3] E. Kani, Elliptic curves on abelian surfaces. Manus. math. 84 (1994), 199-223.
[K4] E. Kani, Idoneal numbers and some generalizations. Ann. Sci. Math. Québec, 36 (2012), 501-534.
[L] H. Lange, Principal polarizations on products of elliptic curves. In: The Geometry of Riemann Surfaces and Abelian Varieties. Contemp. Math. 397, AMS, Providence, RI, 2006, pp. 153-162.
[M] D. Mumford, Abelian Varieties. Oxford U Press, Oxford, 1970.
[Wa] M. Watkins, Class numbers of imaginary quadratic fields. Math. Comp. 73 (2004), 907-938.
[We] P. Weinberger, Exponents of the class groups of complex quadratic fields. Acta Arith. 22 (1973), 117-124.