Maximilian Schmidt

Integrality of Seshadri constants and irreducibility of principal polarizations on products of two isogenous elliptic curves

Received: 3 November 2020 / Accepted: 30 April 2021 / Published online: 14 May 2021

Abstract. In this paper we consider the question of when all Seshadri constants on a product of two isogenous elliptic curves $E_1 \times E_2$ without complex multiplication are integers. By studying elliptic curves on $E_1 \times E_2$ we translate this question into a purely numerical problem expressed by quadratic forms. By solving that problem, we show that all Seshadri constants on $E_1 \times E_2$ are integers if and only if the minimal degree of an isogeny $E_1 \rightarrow E_2$ equals 1 or 2. Furthermore, this method enables a characterization of irreducible principal polarizations on $E_1 \times E_2$.

1. Introduction

For an ample line bundle L on a smooth projective variety X , the *Seshadri constant* of L at a point $x \in X$ is by definition the real number

$$\varepsilon(L, x) = \inf \left\{ \frac{L \cdot C}{\text{mult}_x(C)} \mid C \text{ irreducible curve through } x \right\}.$$

On abelian varieties, $\varepsilon(L, x)$ is independent of the chosen point x . Moreover, one knows by [3] that on abelian *surfaces* Seshadri constants are always rational numbers. In the present paper we focus on the question of when all Seshadri constants $\varepsilon(L)$ on a given abelian surface are *integers*. This question was first approached in [2], where it was shown that integrality of Seshadri constants on an abelian surface X is equivalent to requiring that for every ample line bundle L on X , either $\sqrt{L^2}$ is an integer or $\varepsilon(L)$ is computed by an elliptic curve. From work of Bauer and Schulz [4] one knows that the latter condition is always satisfied when X is a self-product $E \times E$ of an elliptic curve without complex multiplication. In the present paper we study the more general situation that X is a product $E_1 \times E_2$ of two isogenous elliptic curves without complex multiplication. One might hope that the Seshadri constants on these surfaces behave in a similar way as those on a self-product, since the surfaces $E_1 \times E_1$ and $E_1 \times E_2$ are isogenous. As our result will show, however, Seshadri constants exhibit quite unexpected behaviour under isogenies.

M. Schmidt (✉): Fachbereich Mathematik und Informatik, Philipps-Universität Marburg, Hans-Meerwein-Straße, 35032 Marburg, Germany.
e-mail: schmid4d@mathematik.uni-marburg.de

Mathematics Subject Classification: 14C20 · 14H40 · 14H52 · 14J99 · 14K02 · 14K99 · 11H55

A first indication of this phenomenon follows from work of Kani [11], who studied the question of when $E_1 \times E_2$ is the Jacobian of a smooth genus 2 curve, i.e., when $E_1 \times E_2$ carries an irreducible principal polarization. His result states that $E_1 \times E_2$ is *not* a Jacobian if and only if the minimal degree d of an isogeny $E_1 \rightarrow E_2$ satisfies

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

and for at most one more unknown value $d > 462$. Since the Seshadri constant of an irreducible principal polarization is $\frac{4}{3}$ by [15], it follows that on $E_1 \times E_2$ non-integer Seshadri constants occur in any event when d is not contained in the list above. Our result shows that non-integer Seshadri constants are even more frequent:

Theorem 1. *All Seshadri constants on $E_1 \times E_2$ are integers if and only if the minimal degree d of an isogeny $E_1 \rightarrow E_2$ equals 1 or 2.*

In particular, the non-integer Seshadri constants predicted by the theorem whenever $d \geq 3$ must come from polarizations other than principal polarizations whenever d is contained in the list above.

Our proof is based on the idea to study the intersection numbers of line bundles with elliptic curves on $E_1 \times E_2$, which allows us to rephrase the problem into a purely numerical question in terms of quadratic forms. We will solve that numerical problem by using reduction theory of binary quadratic forms. This approach also enables us to characterize irreducible principal polarizations on $E_1 \times E_2$ in terms of quadratic forms. Recall that two polarizations L_1 and L_2 are equivalent if there exists an automorphism ψ of X such that ψ^*L_1 is algebraically equivalent to L_2 , and denote the set of isomorphism classes of principal polarizations on $X = E_1 \times E_2$ by $P(X)$. We will see in Sect. 5 that there is a bijection between $P(X)$ and a set of certain quadratic forms:

$$P(X) \cong \left\{ M = \begin{pmatrix} A & B \\ B & C \end{pmatrix} \in M_2(\mathbb{Z}) \mid \begin{array}{l} 0 \leq 2B \leq A \leq C, \\ \gcd(A, B, C) = 1, \det(M) = d \end{array} \right\}.$$

We can characterize irreducible principal polarizations in these terms:

Theorem 2. *A matrix M as above corresponds to a class of reducible principal polarizations if and only if $B = 0$.*

In particular, there exists an irreducible principal polarization on $E_1 \times E_2$ if and only if d can be written as

$$d = AC - B^2, \quad 0 \leq 2B \leq A \leq C, \quad \gcd(A, B, C) = 1.$$

As an application we can use Theorem 2 to give an alternative proof of Kani's result mentioned above.

Throughout this paper we will work over the complex numbers and on the abelian surface $X = E_1 \times E_2$, and we denote by $\varphi : E_1 \rightarrow E_2$ an isogeny of smallest degree d .

2. Preliminaries

Let E_1 and E_2 be two isogenous elliptic curves without complex multiplication. Throughout this paper we will work on the abelian surface $X := E_1 \times E_2$ and we fix an isogeny $\varphi : E_1 \rightarrow E_2$ of smallest degree d . On the product surface X , denote by $F_1 = \{0\} \times E_2$ and $F_2 = E_1 \times \{0\}$ the fibers of the projections and by Δ the graph of the isogeny φ . The classes of these three elliptic curves on X form a basis of the Néron–Severi group $\text{NS}(X)$ (see [16, Theorem 22] or [5, Theorem 11.5.1]).

Proposition 2.1. *The intersection matrix of (F_1, F_2, Δ) on X is given by*

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & d \\ 1 & d & 0 \end{pmatrix}.$$

Note that the determinant of the intersection matrix coincides with the discriminant of the Néron–Severi group on X (see [1, Chp. 3]). This implies that (F_1, F_2, Δ) is a basis of $\text{NS}(X)$.

Proof. We argue as in [2, Proposition 2.1]. All three curves are elliptic, so we have $F_1^2 = F_2^2 = \Delta^2 = 0$. As each curve intersects the other ones transversely, it is enough to count the number of intersection points. So we have

$$F_1 \cdot F_2 = F_1 \cdot \Delta = 1,$$

since these curves intersect only in the origin. For F_2 and Δ one has

$$F_2 \cdot \Delta = \#\{(x, 0) \mid x \in E_1\} \cap \{(x, \varphi(x)) \mid x \in E_1\},$$

and this shows that we need to count the number of solutions $x \in E_1$ of the equation $\varphi(x) = 0$. But this number is equal to the degree of the isogeny φ , so we get

$$F_2 \cdot \Delta = \deg(\varphi) = d.$$

□

As a first application, we will compute Seshadri constants for line bundles in the cone generated by (F_1, F_2, Δ) :

Proposition 2.2. *Let L be a line bundle on X of the form*

$$L = \mathcal{O}_{E_1 \times E_2}(a_1 F_1 + a_2 F_2 + a_3 \Delta)$$

with non-negative coefficients a_i . Then one has

$$\begin{aligned} \varepsilon(L) &= \min \{L \cdot F_1, L \cdot F_2, L \cdot \Delta\} \\ &= \min \{a_2 + a_3, a_1 + da_3, a_1 + da_2\}. \end{aligned}$$

Proof. Let D be the divisor $a_1 F_1 + a_2 F_2 + a_3 \Delta$, and let C be any irreducible curve C passing through 0, which is not a component of D . As D is effective, we have

$$\begin{aligned} \frac{L \cdot C}{\text{mult}_0 C} &= \frac{D \cdot C}{\text{mult}_0 C} \geq \frac{\text{mult}_0 D \cdot \text{mult}_0 C}{\text{mult}_0 C} \geq a_1 + a_2 + a_3 \\ &\geq a_2 + a_3 = L \cdot F_1. \end{aligned}$$

This implies that $\varepsilon(L)$ is computed by one of the curves F_1 , F_2 or Δ . Their intersection numbers with L are given by the intersection matrix in Proposition 2.1 and this yields the assertion. $\square$

Remark 2.3. Let $\widehat{\varphi} : E_2 \rightarrow E_1$ be the dual isogeny corresponding to φ such that the maps $\varphi \circ \widehat{\varphi}$ and $\widehat{\varphi} \circ \varphi$ are the multiplication by d . Then the previous arguments can be used to see that the triple $(F_1, F_2, \widehat{\Delta})$ with $\widehat{\Delta} := \{x \in X \mid x_1 = \widehat{\varphi}(x_2)\}$ also forms a basis of $\text{NS}(X)$. Then, we can analogously formulate Proposition 2.2 for line bundles in the cone generated by $(F_1, F_2, \widehat{\Delta})$. In general the resulting cones will not coincide since it is possible to get negative coefficients by changing bases:

$$\begin{aligned} F_1 + \Delta &\equiv dF_1 + (1-d)F_2 + \overline{\Delta}, \\ F_2 + \overline{\Delta} &\equiv (1-d)F_1 + dF_2 + \Delta. \end{aligned}$$

In fact, the cones coincide if and only if $d = 1$, that is, if E_1 and E_2 are isomorphic.

For our purpose it will be useful to change the basis (F_1, F_2, Δ) of the Néron–Severi group by choosing an element which is orthogonal to F_1 and F_2 . We define $\nabla := \Delta - dF_1 - F_2$, then the triple (F_1, F_2, ∇) forms a basis of $\text{NS}(X)$ and the intersection matrix is given by

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2d \end{pmatrix}.$$

Proposition 2.4. *Consider a line bundle $L = \mathcal{O}_X(a_1 F_1 + a_2 F_2 + a_3 \nabla)$. Then L is ample if and only if the two inequalities*

$$\begin{aligned} 0 &< a_1, \\ 0 &< a_1 a_2 - d a_3^2 = \frac{L^2}{2}, \end{aligned}$$

are satisfied.

Proof. By the Nakai–Moishezon criterion for abelian varieties [5, Corollary 4.3.3] a line bundle L is ample if and only if both $L^2 = 2(a_1 a_2 - d a_3^2)$ and the intersection of L with any fixed ample line bundle L_0 are positive. By choosing the ample line bundle $L_0 := \mathcal{O}_{E \times E}(F_1 + F_2)$ the intersection of L with L_0 is given by $a_1 + a_2$. Now assume that L^2 is positive, then a_1 and a_2 are either both positive or both negative. Thus, the sum $a_1 + a_2$ is positive if and only if a_1 is positive. $\square$

3. Numerical classes of elliptic curves on X

In this section we will determine the intersection number of line bundles with elliptic curves. To this end, we need to know all elliptic curves on $E_1 \times E_2$. In [9] Hayashida and Nishi described the elliptic curves on E^n and with the same argument it immediately follows:

Lemma 3.1. *For every elliptic curve N on $X = E_1 \times E_2$ there are endomorphisms $\sigma_1 \in \text{End}(E_1) \cong \mathbb{Z}$ and $\sigma_2 \in \text{End}(E_2) \cong \mathbb{Z}$ such that N is a translate of the image of the map*

$$E_1 \rightarrow E_1 \times E_2, \quad x \mapsto (\sigma_1(x), \sigma_2 \circ \varphi(x)).$$

By the previous lemma we know that for every elliptic curve N on X , there are integers $(a, b) \neq (0, 0)$ such that N is a translate of

$$N_{a,b} := \{(ax, b\varphi(x)) \mid x \in E_1\}.$$

Note that for any multiple $(\lambda a, \lambda b)$ we have $N_{a,b} = N_{\lambda a, \lambda b} = m_\lambda(N_{a,b})$, where m_λ describes the multiplication with λ , which is a map of degree λ^2 that maps $N_{a,b}$ surjective onto itself.

Next, we want to describe the intersection numbers of elliptic curves with line bundles. For this, we have to determine the numerical class of the elliptic curves $N_{a,b}$. As $N_{a,b}$ and F_1 intersect transversely for $a \neq 0$, we have

$$N_{a,b} \cdot F_1 = \#(N_{a,b} \cap F_1) = \frac{\#\{(x \in E_1 \mid ax = 0)\}}{\deg(\sigma_{a,b})},$$

where $\sigma_{a,b} : E_1 \rightarrow N_{a,b}$ is the map $x \mapsto (ax, b\varphi(x))$. But the numerator is equal to the degree of the map $a : E_1 \rightarrow E_1, x \mapsto ax$, which has degree a^2 . If $a = 0$, then $N_{a,b} = F_1$ and, therefore, $N_{a,b} \cdot F_1 = 0 = \frac{a^2}{\deg(\sigma_{a,b})}$. With the same arguments we obtain

$$N_{a,b} \cdot F_1 = \frac{a^2}{\deg(\sigma_{a,b})}, \quad N_{a,b} \cdot F_2 = \frac{b^2 d}{\deg(\sigma_{a,b})}, \quad N_{a,b} \cdot \Delta = \frac{(b-a)^2 d}{\deg(\sigma_{a,b})},$$

and since $\nabla = \Delta - dF_1 - F_2$ we have

$$N_{a,b} \cdot \nabla = \frac{-2abd}{\deg(\sigma_{a,b})}.$$

The coefficients of the numerical representation of $N_{a,b}$ are then given by

$$\frac{1}{\deg(\sigma_{a,b})} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -2d \end{pmatrix}^{-1} \cdot \begin{pmatrix} a^2 \\ b^2 d \\ -2abd \end{pmatrix} = \frac{(b^2 d, a^2, ab)^T}{\deg(\sigma_{a,b})},$$

and, thus, we have

$$N_{a,b} \equiv \frac{b^2 d}{\deg(\sigma_{a,b})} F_1 + \frac{a^2}{\deg(\sigma_{a,b})} F_2 + \frac{ab}{\deg(\sigma_{a,b})} \nabla.$$

To fully understand the intersection numbers we have to determine the degree of the map $\sigma_{a,b}$. For this, we use the following criteria to identify elliptic curves on abelian varieties (see [11, Propositions 2.1, 2.3]):

Proposition 3.2. ([11]) *Let A be an abelian surface and $C_1, C_2 \subset A$ be two irreducible curves on A . Then $C_1 \cdot C_2 \geq 0$. Furthermore, $C_1 \cdot C_2 = 0$ if and only if C_1 is an elliptic curve and C_2 a translate of C_1 .*

Proposition 3.3. ([11]) *Let A be an abelian surface and $D \in \text{Div}(A)$ a divisor on A . Then $D \equiv mE$ for some $m \in \mathbb{Z}$ and some elliptic curve $E \subset A$ if and only if $D^2 = 0$. Moreover, $m > 0$ if and only if $\theta \cdot D > 0$ for an ample divisor $\theta \in \text{Div}(A)$.*

With these criteria we can calculate the degree of $\sigma_{a,b}$ and, thus, the numerical class of elliptic curves.

Lemma 3.4. *Let $N \subset X$ be an elliptic curve and let $\sigma_{a,b} : E_1 \rightarrow N_{a,b}$ be a map $x \mapsto (ax, b\varphi(x))$ such that the image $N_{a,b}$ is a translate of N . Then we have*

$$\deg(\sigma_{a,b}) = \gcd(a^2, b^2d, ab)$$

and, therefore, the numerical class of N is given by

$$N \equiv N_{a,b} \equiv \frac{b^2dF_1 + a^2F_2 + ab\nabla}{\gcd(a^2, b^2d, ab)}.$$

Proof. By our previous arguments the numerical class of $N_{a,b}$ is given by

$$N_{a,b} \equiv \frac{b^2d}{\deg(\sigma_{a,b})}F_1 + \frac{a^2}{\deg(\sigma_{a,b})}F_2 + \frac{ab}{\deg(\sigma_{a,b})}\nabla.$$

Since all the coefficients of the representation must be integers, it follows that $\deg(\sigma_{a,b})$ is a divisor of b^2d, a^2 and ab . Thus, $\deg(\sigma_{a,b})$ is a divisor of $\gcd(a^2, b^2d, ab)$. So, there exists a positive integer λ such that

$$\lambda \deg(\sigma_{a,b}) = \gcd(a^2, b^2d, ab).$$

If we show that $\lambda = 1$, then the assertion follows. By using the previous equation in the expression for $N_{a,b}$ we get

$$N_{a,b} \equiv \lambda \left(\frac{b^2d}{\gcd(a^2, b^2d, ab)}F_1 + \frac{a^2}{\gcd(a^2, b^2d, ab)}F_2 + \frac{ab}{\gcd(a^2, b^2d, ab)}\nabla \right) \equiv \lambda \overline{N},$$

where $\overline{N}$ is an element of $\text{NS}(X)$, since all the coefficients are integers.

Next, we make use of Proposition 3.3 to show that $\overline{N}$ is a positive multiple of an elliptic curve. Since $N_{a,b}$ is an elliptic curve by assumption, we can apply Proposition 3.3 to $N_{a,b}$ and by using $\overline{N} \equiv \frac{1}{\lambda}N_{a,b}$ we see that

$$\overline{N}^2 = \frac{1}{\lambda^2}N_{a,b}^2 = 0$$

and

$$\overline{N} \cdot (F_1 + F_2) = \frac{1}{\lambda}N_{a,b} \cdot (F_1 + F_2) > 0.$$

Thus, by Proposition 3.3 we have $\overline{N} \equiv mE$ for an elliptic curve E and $m \geq 1$. So, we obtain $N_{a,b} \equiv m\lambda E$.

Since $N_{a,b} \cdot E = \frac{1}{m\lambda} N_{a,b}^2 = 0$, it follows from Prop 3.2 that E is a translate of $N_{a,b}$ and, therefore, their numerical classes coincide. But since m and λ are positive integers, it follows that $m = \lambda = 1$. So, we have $\deg(\sigma_{a,b}) = \gcd(a^2, b^2d, ab)$ as claimed. $\square$

The natural question might arise whether it is possible to find for any given pair (a, b) another pair (a', b') such that the elliptic curves $N_{a,b}$ and $N_{a',b'}$ coincide and such that the degree of the map $\sigma_{a',b'} : E_1 \rightarrow N_{a',b'}$ is 1. While this is apparently true for $d = 1$ by dividing a and b by $\gcd(a, b)$, it is not true for $d > 1$, since it would imply that there exists a map of degree 1, i.e. an isomorphism, of E_1 to $N_{0,1} \cong E_2$.

Now we have the required tools to calculate the intersection numbers of elliptic curves with line bundles:

Proposition 3.5. *Let L be a line bundle with $L \equiv a_1 F_1 + a_2 F_2 + a_3 \nabla$ and $N_{a,b}$ an elliptic curve on X . Then the intersection number of L and $N_{a,b}$ is given by*

$$L \cdot N_{a,b} = \frac{1}{\gcd(a^2, db^2, ab)} \begin{pmatrix} a \\ b \end{pmatrix}^T \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Proof. This follows by explicitly calculating the intersection of the numerical class of $N_{a,b}$ given in Lemma 3.4 with the numerical class of L . $\square$

Remark 3.6. We denote the matrix associated with $L \equiv a_1 F_1 + a_2 F_2 + a_3 \nabla \in \text{NS}(X)$ through Proposition 3.5 by

$$M_L := \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix}.$$

Note that the map $L \mapsto M_L$ is an isomorphism between the abelian groups

$$\text{NS}(X) = \{a_1 F_1 + a_2 F_2 + a_3 \nabla \mid a_i \in \mathbb{Z}\} \cong \left\{ \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix} \mid a_i \in \mathbb{Z} \right\}.$$

It turns out that this representation enables an ampleness criterion for line bundles on X :

Corollary 3.7. *Let $L \equiv a_1 F_1 + a_2 F_2 + a_3 \nabla$ be a line bundle and M_L the corresponding matrix. Then $\det(M_L) = \frac{dL^2}{2}$ and the following are equivalent:*

- (i) L is ample.
- (ii) M_L is positive definite.
- (iii) The intersection $L \cdot E$ is positive for every elliptic curve E on X .

Proof. This is an immediate consequence of Propositions 2.4 and 3.5. $\square$

4. Integrality of Seshadri constants on X

In this section we will provide a complete answer, in terms of d , to the question whether there exists a non-integer Seshadri constant on X or not. For this, we first develop a criterion to check if all Seshadri constants are computed by elliptic curves. Obviously, if all Seshadri constants are computed by elliptic curves, then all Seshadri constants are integers by definition. Our starting point is:

Proposition 4.1. *The following are equivalent:*

- (i) *All Seshadri constants on X are computed by elliptic curves.*
- (ii) *Every ample line bundle L on X has a weakly submaximal elliptic curve, i.e., there exists an elliptic curve E on X such that $L \cdot N \leq \sqrt{L^2}$.*
- (iii) *For every positive definite matrix of the form*

$$M = \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix} \in M_2(\mathbb{Z})$$

there exists a coprime pair $(a, b) \in \mathbb{Z}^2$ such that the inequality

$$\frac{1}{\gcd(a, d)} \begin{pmatrix} a \\ b \end{pmatrix}^T \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \leq \sqrt{\frac{2 \det(M)}{d}}$$

is satisfied.

Proof. The implication (i) $\Rightarrow$ (ii) follows from the definition of Seshadri constants and the upper bound $\varepsilon(L) \leq \sqrt{L^2}$. The implication (ii) $\Rightarrow$ (i) is a result from Schulz. The argument can be found in the proof of [4, Theorem 4.5].

The equivalence of (ii) $\iff$ (iii) is a consequence of Proposition 3.5 and the fact that it is enough to consider coprime pairs (a, b) , since we have $L \cdot N_{a,b} = L \cdot N_{\lambda a, \lambda b}$ for any multiple $\lambda \in \mathbb{N}$. Moreover, if a and b are coprime, then $\gcd(a^2, b^2d, ab) = \gcd(a, d)$. $\square$

In Proposition 4.1 we have translated the question whether all Seshadri constants are computed by elliptic curves into a purely numerical problem. To progress further, we will use results for binary quadratic forms and apply them to our setting. We start by briefly collecting the relevant language and facts. Recall that a (binary) quadratic form $Q : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is given by

$$(x, y) \mapsto Ax^2 + Bxy + Cy^2 = \begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

where A, B and C are integers. We will denote Q by the triple (A, B, C) . A quadratic form Q is called *primitive* if $\gcd(A, B, C) = 1$. Two quadratic forms Q and P are called (properly) *equivalent* if there exists a matrix $S \in \mathrm{GL}_2(\mathbb{Z})$ such that $P(x, y) = Q(S(x, y))$ (and, respectively $\det(S) = 1$). It is more common to use proper equivalence with quadratic forms, since the classes of primitive quadratic forms of a fixed determinant form a group.

The crucial ingredient are so-called reduced forms and their properties:

Definition 4.2. A positive definite quadratic form (A, B, C) is called *reduced*, if the integers A, B and C satisfy $|B| \leq A \leq C$ and, if one of the inequalities is not strict, then $B \geq 0$.

Theorem 4.3. ([6, Theorem 2.8]) *Every positive definite quadratic form is properly equivalent to a unique reduced form. Moreover, there exists an effective algorithm to transform a given form into its unique reduced form.*

It follows that any positive definite quadratic form is *equivalent* to a unique form (A, B, C) with $0 \leq B \leq A \leq C$. This will be used in the last section.

Now, we turn our attention to the two relevant properties which we obtain by using reduced forms:

Proposition 4.4. ([6, (2.9), (2.12)]) *Let $Q = (A, B, C)$ be a reduced positive definite quadratic form. Then:*

- (i) *We have $A \leq \sqrt{\frac{4 \det(Q)}{3}}$.*
- (ii) *The two smallest integers represented by Q with coprime pairs are $Q(1, 0) = A$ and $Q(0, 1) = C$.*

With this, we can refine Proposition 4.1 in terms of reduced positive definite forms.

Proposition 4.5. *The following is equivalent:*

- (i) *All Seshadri constants on X are computed by elliptic curves.*
- (ii) *For every reduced positive definite quadratic form $Q = (A, B, C)$ and every $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ there exists a coprime pair $(a, b) \in \mathbb{Z}^2$ such that*

$$\frac{Q(a, b)}{\gcd(a\alpha + b\gamma, d)} \leq \sqrt{\frac{2 \det(Q)}{d}}.$$

Proof. To begin with, we will determine how a base change affects the inequality given in Proposition 4.1. Assume that we have a positive definite matrix M and for $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we set $R := S^T M S$. Then, by changing coordinates a coprime pair (x, y) corresponds to the coprime pair $(v, w) := S^{-1}(x, y)^T$ and it follows that

$$\frac{1}{\gcd(x, d)} \begin{pmatrix} x \\ y \end{pmatrix}^T M \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{\gcd(v\alpha + w\gamma, d)} \begin{pmatrix} v \\ w \end{pmatrix}^T R \begin{pmatrix} v \\ w \end{pmatrix}.$$

Thus, the change of basis leads to the inequality stated in the Proposition.

The implication (ii) $\Rightarrow$ (i) follows from the fact that every positive definite matrix appearing in Proposition 4.1 is by Theorem 4.3 equivalent to a unique reduced form. Thus, if the inequality holds for all reduced quadratic forms and all $S \in \mathrm{SL}_2(\mathbb{Z})$, then it already holds for every positive definite form.

The implication (i) $\Rightarrow$ (ii) is less apparent, since Proposition 4.1 gives a statement on positive definite quadratic forms given by

$$\begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix}, \quad (*)$$

whereas (ii) is a statement about *all* (reduced) positive definite quadratic forms. Let $Q = (A, B, C)$ be any reduced positive definite quadratic form and $S \in \mathrm{SL}_2(\mathbb{Z})$. First, we observe that the inequality in (ii) is invariant by scaling. Thus, Q and the coprime pair (a, b) satisfy the inequality if and only if it holds for the coprime pair (a, b) and all forms $\lambda Q = (\lambda A, \lambda B, \lambda C)$ for $\lambda > 0$, since we have

$$\frac{\lambda Q(a, b)}{\gcd(a\alpha + b\beta, d)} \leq \sqrt{\frac{2\lambda^2 \det(Q)}{d}}.$$

Now, by choosing $\lambda = 2d$ and applying the base change S we see that the corresponding matrix

$$M = 2d \cdot S^T \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} S$$

is of the form (*). Therefore, the inequality holds in fact for all reduced forms. $\square$

As a consequence of Theorem 4.3 and Proposition 4.5 the minimal intersection number with elliptic curves can be effectively computed:

Proposition 4.6. *Let L be a line bundle on X . Then there exists an effective algorithm to calculate $\varepsilon^*(L) := \min\{L \cdot N \mid N \subset X \text{ elliptic curve}\}$.*

Proof. Let M_L be the corresponding matrix to the line bundle L . By Theorem 4.3 there exists an algorithm which computes the reduced form $Q = (A, B, C)$ and the base change S such that $M_L = S^T Q S$. The claim follows from the fact that there exists only a finite number of pairs (a, b) such that $Q(a, b) \leq M$ for any upper bound M and by choosing the upper bound $M = dA$. $\square$

We now turn to the integrality question. If $d = 1$, then by [4, Theorem 2.2] every line bundle has a weakly submaximal elliptic curve and, thus, all Seshadri constants are integers. We give now a complete answer depending on the degree d whether all Seshadri constants are integers or if there exists rational Seshadri constants.

Theorem 4.7. *If $d = 1$ or $d = 2$, then all Seshadri constants are integers. Moreover, all Seshadri constants on X are computed by elliptic curves.*

The Theorem implies that $\varepsilon^*(L) = \varepsilon(L)$ and hence $\varepsilon(L)$ can be effectively computed by Proposition 4.6.

Proof. We will show that Proposition 4.5 applies in this situation. First note that, since the inequality in Proposition 4.5 does not depend on γ and δ , it is enough to consider coprime pairs (α, β) . Let $Q = (A, B, C)$ be a reduced positive definite quadratic form. We have to show that there exists a coprime pair (a, b) such that

$$\frac{Q(a, b)}{\gcd(a\alpha + b\beta, d)} \leq \sqrt{\frac{2 \det(Q)}{d}}. \quad (*)$$

First, assume that $d = 1$. Then, by Proposition 4.4 (i) it follows that we have for $(1, 0)$ the inequality

$$Q(1, 0) = A \leq \sqrt{\frac{4 \det(Q)}{3}} \leq \sqrt{2 \det(Q)}$$

and, thus, we have found a coprime pair.

Next, we treat the case $d = 2$. We claim that at least one of the pairs $(1, 0)$, $(0, 1)$, $(1, \pm 1)$ satisfies the inequality $(*)$. We will discuss three cases dependent on the divisibility of α and β by 2. Note that α and β cannot be both divisible by 2 at the same time, since they are coprime.

First, we assume that $\alpha \equiv 0$ and $\beta \equiv 1$ modulo 2. Then we have for $(a, b) = (1, 0)$

$$\frac{Q(1, 0)}{\gcd(\alpha, 2)} = \frac{A}{2} \leq \sqrt{\frac{\det(Q)}{3}},$$

where the last estimate follows from Proposition 4.4 (ii). Thus, $(1, 0)$ satisfies $(*)$.

Secondly, we treat the case $\alpha \equiv 1$ and $\beta \equiv 0$. We assume to the contrary that $(1, 0)$ and $(0, 1)$ do not satisfy $(*)$. So, we have

$$\frac{Q(1, 0)}{\gcd(\alpha, 2)} = A > \sqrt{\det(Q)},$$

and

$$\frac{Q(0, 1)}{\gcd(\beta, 2)} = \frac{C}{2} > \sqrt{\det(Q)}.$$

Then, by multiplying both inequalities we get

$$B^2 > 2AC,$$

but this is impossible, since Q is reduced and, therefore, $|B| \leq A \leq C$.

Lastly, we treat the case $\alpha \equiv 1$ and $\beta \equiv 1$. This time, we assume that $(1, 0)$ and $(1, \pm 1)$ do not satisfy $(*)$. Thus, we have

$$\frac{Q(1, 0)}{\gcd(\alpha, 2)} = A > \sqrt{\det(Q)},$$

and

$$\frac{Q(1, \pm 1)}{\gcd(\alpha \pm \beta, 2)} \geq \frac{A + C - |B|}{2} > \sqrt{\det(Q)}.$$

Then, after multiplying both inequalities we get

$$2A^2 + B^2 > 2AC + 2A|B|$$

which is impossible, since Q is reduced. $\square$

We turn our attention to proving the converse of Theorem 4.7. This amounts to finding a line bundle L with a non-integer Seshadri constant. One way to find such a bundle is by searching for irreducible principal polarizations on X , since these have $\varepsilon(L) = \frac{4}{3}$ by [15, Proposition 2]. The existence and number of irreducible principal polarizations has been studied by a number of authors (e.g. [7, 9, 10, 13, 14]). As mentioned in the introduction, Kani answered this question to a great extent for $E_1 \times E_2$:

Theorem 4.8. ([13, Theorem 5]) *There exists no irreducible principal polarization on X if and only if $d = 1$ or if d is an even idoneal number which is not divisible by 8. This is the case for*

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

and for at most one more $d^ > 462$.*

For a more thorough discussion of idoneal numbers and the existence of the additional number d^* we refer to [12] and [13].

We will now show that there in fact exists an ample line bundle with a non-integer Seshadri constant for every $d \geq 3$. (Such line bundles cannot be principal polarizations in the cases listed in Theorem 4.8.) For this, we will use Theorem 2 from [2]. So, the assertion follows, if we show that there exists a line bundle L such that $\varepsilon(L)$ is not computed by an elliptic curve and that $\sqrt{L^2}$ is not an integer.

Theorem 4.9. *If $d \geq 3$, then there exists a line bundle on X , which does not have a weakly submaximal elliptic curve.*

Proof. We will use Proposition 4.5. So, the issue is to exhibit a reduced positive definite form $Q = (A, B, C)$ and a matrix $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that for every coprime pair (a, b) the inequality

$$\frac{Q(a, b)}{\gcd(a\alpha + b\beta, d)} > \sqrt{\frac{2 \det(Q)}{d}}$$

is satisfied. We will show that the quadratic form $Q = (2, 1, d)$ and the matrix

$$S = \begin{pmatrix} 1 & \left\lceil \frac{d}{2} \right\rceil \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

satisfy for every coprime pair (a, b) the even stronger inequality

$$\frac{Q(a, b)}{\gcd(a + b\lceil \frac{d}{2} \rceil, d)} \geq 2 > \sqrt{\frac{8d-1}{2d}} = \sqrt{\frac{2 \det(Q)}{d}}. \quad (*)$$

The idea is as follows: We begin by exhibiting two properties a coprime pair (a, b) must satisfy, if it contradicts the inequality $(*)$. Then we show that no coprime pair can satisfy both properties at the same time.

First, we observe that it is enough to consider coprime pairs (a, b) with

$$Q(a, b) < 2d,$$

because any coprime pair (a, b) with $Q(a, b) \geq 2d$ will satisfy the inequality $(*)$ since the denominator is at most d .

Secondly, we claim that it is enough to consider coprime pairs $(a, b) \neq (1, 0)$ such that

$$d \text{ divides } a + b \left\lceil \frac{d}{2} \right\rceil.$$

To this end, we know by Proposition 4.4 that the two smallest non-zero integers represented by Q with coprime pairs are $Q(1, 0) = 2$ and $Q(0, 1) = d$. Since the pair $(1, 0)$ satisfies the inequality $(*)$, we may assume that $(a, b) \neq (1, 0)$ and, thus, $Q(a, b)$ is at least d . If such a coprime pair has $\gcd(a + b \left\lceil \frac{d}{2} \right\rceil, d) = q < d$, then we conclude

$$\frac{Q(a, b)}{\gcd(a + b \left\lceil \frac{d}{2} \right\rceil, d)} \geq \frac{d}{q} \geq 2,$$

as for any divisor q of d with $q \neq d$ the quotient $\frac{d}{q}$ is at least 2. Consequently, we are left with coprime pairs $(a, b) \neq (1, 0)$ such that $\gcd(a + b \left\lceil \frac{d}{2} \right\rceil, d) = d$.

Next, we will create a set of pairs which will contain all coprime pairs $(a, b) \neq (1, 0)$ such that $Q(a, b) < 2d$. We claim that if $|b| > 1$, then $Q(a, b)$ is at least $2d$. For this, we consider for a fixed b the function $x \mapsto Q(x, b)$, which has the minimum in $-\frac{b}{4}$. It follows that we have for every $x \in \mathbb{R}$

$$Q(x, b) \geq b^2 \frac{8d - 1}{8}$$

and for $|b| \geq 2$ we obtain $Q(x, b) \geq 2d$.

Thus, we only have to consider the cases $b = 1$ and $b = -1$. Now, we calculate the range of a depending on $b \in \{-1, 1\}$ by estimating the possible values of a such that $Q(a, b) = 2a^2 + ab + db^2 < 2d$ holds. We conclude by solving these two quadratic inequalities that

$$|a| \leq \frac{1}{4}(1 + \sqrt{8d + 1}). \quad (**)$$

It follows that all coprime pairs $(a, b) \neq (1, 0)$ with $Q(a, b) < 2d$ are contained in (the possibly bigger set):

$$Z = \{(n, \pm 1) \mid 0 \leq n \leq \left\lfloor \frac{1}{4}(1 + \sqrt{8d + 1}) \right\rfloor, n \in \mathbb{N}\}.$$

The crucial point is that if $d \geq 4$, then we can derive the following bounds for $a + b\lceil\frac{d}{2}\rceil$: If $b = 1$, then

$$0 < \left\lceil \frac{d}{2} \right\rceil \leq a + \left\lceil \frac{d}{2} \right\rceil \leq \left\lfloor \frac{1}{4}(1 + \sqrt{8d+1}) \right\rfloor + \left\lceil \frac{d}{2} \right\rceil < d$$

and if $b = -1$, then

$$-d < -\left\lceil \frac{d}{2} \right\rceil \leq a - \left\lceil \frac{d}{2} \right\rceil \leq \left\lfloor \frac{1}{4}(1 + \sqrt{8d+1}) \right\rfloor - \left\lceil \frac{d}{2} \right\rceil < 0.$$

(This is also the moment where the argument hinges on the choice of the matrix S .) As a consequence, the sum $a + b\lceil\frac{d}{2}\rceil$ always lies in the interval $(0, d)$ or in $(-d, 0)$ and, therefore, is not divisible by d . So, we conclude that every coprime pair (a, b) satisfies (*).

It remains to treat the case $d = 3$. The inequality (**) is not helpful in this case, since Z will then contain a pair (a, b) , namely $(1, 1)$, with $\gcd(a + b\lceil\frac{3}{2}\rceil, 3) = 3$, which, however, does not satisfy $6 = Q(1, 1) < 6$. Instead, in this case we can calculate all coprime pairs $(a, b) \neq (1, 0)$ with $Q(a, b) = 2a^2 + ab + 3b^2 < 6$ explicitly:

$$Z_3 = \{(0, 1), (1, -1)\}.$$

We see that none of the pairs $(a, b) \in Z_3$ satisfies $\gcd(a + 2b, 3) = 3$, which completes the proof. $\square$

So far we have found line bundles L whose Seshadri constants are not computed by elliptic curves. This concludes the first step of the proof of the converse of Theorem 4.7. It still might be possible that the Seshadri constants are all integers if $\varepsilon(L) = \sqrt{L^2} \in \mathbb{Z}$ (see [2, Ex. 1.1]). To exclude this, we have to show that L^2 is not a square number. With that we can deduce the even stronger statement:

Theorem 4.10. *If $d \geq 3$, then there exists a line bundle on X with a non-integer Seshadri constant.*

Proof. We will apply Theorem 2 from [2]. Thus, the claim follows, if we show that there exists a line bundle L such that $\varepsilon(L)$ is not computed by an elliptic curve and that $\sqrt{L^2}$ is not an integer. To find such a line bundle, we will use the binary quadratic form $Q = (2, 1, d)$ and matrix $S = \begin{pmatrix} 1 & \lceil\frac{d}{2}\rceil \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ given in Theorem 4.9 and apply the arguments from the proof of Proposition 4.5.

So, we consider the scaled quadratic form $Q' = 2dQ = (4d, 2d, 2d^2)$ together with the matrix S . By using the change of basis S we get the positive definite matrix

$$M = S^T \begin{pmatrix} 4d & d \\ d & 2d^2 \end{pmatrix} S = \begin{pmatrix} 4d & d \left(4\left\lceil \frac{d}{2} \right\rceil + 1 \right) \\ d \left(4\left\lceil \frac{d}{2} \right\rceil + 1 \right) & d \left(4\left\lceil \frac{d}{2} \right\rceil^2 + 2\left\lceil \frac{d}{2} \right\rceil + 2d \right) \end{pmatrix},$$

which by Remark 3.6 corresponds to the class of the ample line bundle

$$L = \mathcal{O}_X \left(4dF_1 + \left(4 \left\lceil \frac{d}{2} \right\rceil^2 + 2 \left\lceil \frac{d}{2} \right\rceil + 2d \right) F_2 - \left(4 \left\lceil \frac{d}{2} \right\rceil + 1 \right) \nabla \right),$$

which has no weakly submaximal elliptic curve by Theorem 4.9.

Thus, it is left to show that L^2 is not a perfect square. By using Corollary 3.7 we have for the self-intersection

$$L^2 = \frac{2 \det(M)}{d} = 16d^2 - 2d.$$

If d is odd, then $16d^2 - 2d \equiv 2$ modulo 4 and hence L^2 is not a perfect square. If d is even, then we write $d = 2^n d'$ for an odd integer $d' \geq 1$ and $n \geq 1$. If n is even, then $L^2 = 2^n (2^{n+4} d'^2 - 2d')$. Since 2^n is a square number, it is enough to show that $2^{n+4} d'^2 - 2d'$ can not be a perfect square. This, however, can not happen since it is 2 modulo 4.

Lastly, if n is odd, then $L^2 = 2^{n+1} (2^{n+3} d'^2 - d')$. Suppose to the contrary that L^2 is a perfect square. Then there exists an integer r such that $2^{n+3} d'^2 - d' = r^2$. We claim that d' already is a perfect square. Let p be a prime number such that p^{2n-1} is a divisor of d' . It follows that p^{2n-1} must be a divisor of r^2 and since r^2 is a perfect square it is divisible by p^{2n} . Thus, $d' = 2^{n+3} d'^2 - r^2$ is divisible by p^{2n} as well and, therefore, d' must be an odd square number. Then, however, $2^{n+3} d'^2 - d' \equiv 3$ modulo 4 and hence L^2 cannot be a square number, which is a contradiction. $\square$

Remark 4.11. Note that the application of Theorem 2 from [2] does not yield an explicit line bundle with a fractional Seshadri constant. Thus, the line bundles given in the proof do not necessarily have a non-integer Seshadri constant themselves, but they imply their existence. For such an example see [2, Proposition 2.8].

5. Classification of principal polarizations on X

In this section we will characterize the isomorphism classes of reducible and irreducible principal polarization. We give a brief summary of notation, which can be found in [14]. Two principal polarizations L_1 and L_2 are *equivalent* if there exists an automorphism ψ of X such that $\psi^* L_1 \equiv L_2$. We denote the isomorphism classes of principal polarizations on X by

$$P(X) = \{L \in \text{NS}(X) \mid L \text{ ample, } L^2 = 2\} / \sim.$$

Recall that we have the equality $\frac{dL^2}{2} = \det(M_L)$ and, thus, by Remark 3.6 a principal polarization L is given by a positive definite matrix $M_L = \begin{pmatrix} a_1 & -da_3 \\ -da_3 & da_2 \end{pmatrix}$ with determinant d . Furthermore, since the self-intersection is 2, it follows that the matrix M_L is primitive, that is $\gcd(a_1, da_2, da_3) = 1$. Thus, the quadratic form M_L is equivalent to a unique reduced form $Q = (A, 2B, C)$ with $0 \leq B \leq A \leq C$

and $\gcd(A, B, C) = 1$; we will call such forms *principally reduced forms of determinant d* . (Note that the matrices M_L in Remark 3.6 only have integer entries, thus the second entry of Q will be even.) With arguments from the proof of [14, Theorem 5.1.] the converse is true, that is, for any principally reduced form Q of determinant d there exists a principal polarization L on X such that M_L is equivalent to Q .

Moreover, it follows from [14, Chp. 5.] that two principal polarizations L_1 and L_2 are equivalent if and only if the positive definite forms M_{L_1} and M_{L_2} are equivalent to the same principally reduced form. Thus, we have a natural bijection between the isomorphism classes of principal polarizations and principally reduced forms:

$$P(X) \cong \{\text{principally reduced forms of determinant } d\}. \quad (*)$$

Lange studied in [14] the number of isomorphism classes of principal polarization by using the the isomorphism $\text{NS}(X) \cong \text{End}^{\text{sym}}(X)$. Thus, his approach is slightly different from ours. However, one can show that the matrix M_L induced by the intersection of L with elliptic curves (see Remark 3.6) is closely related to the image of L under the natural isomorphism $\Phi : \text{NS}(X) \rightarrow \text{End}^{\text{sym}}(X)$ given by the principal polarization $L_0 = \mathcal{O}_X(F_1 + F_2)$ [5, Proposition 5.2.1].

Using (*), we now characterize the principally reduced forms of reducible principal polarizations L , i.e., the polarizations such that $L \equiv E'_1 + E'_2$ with elliptic curves E'_i with $E'_1 \cdot E'_2 = 1$.

Theorem 5.1. *Let $Q = (A, 2B, C)$ be a principally reduced form of determinant d . Then the principal polarizations in the isomorphism class given by Q are reducible principal polarizations if and only if $B = 0$.*

In other words, irreducible principal polarizations correspond to principally reduced forms with $B \neq 0$.

Proof. First, assume that $B = 0$. Let $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ be a base change such that Q corresponds to a principal polarization L . It is enough to find an elliptic curve such that the intersection with L is 1. It follows for

$$M_L := S^T \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix} S,$$

that d divides $m_{2,2} = \beta^2 A + \delta^2 C$ and $m_{1,2} = \alpha\beta A + \delta\gamma C$. By using $AC = d$ and the coprime properties of α, β, γ and δ resulting from the fact that the determinant of S is 1, we can deduce that C is a divisor of β and A is a divisor of δ . Therefore, we see that $\gcd(\beta, d) = C$. Hence, we obtain

$$\frac{Q(0, 1)}{\gcd(\beta, d)} = 1.$$

Thus, the elliptic curve $N_{-\beta, \delta}$ which corresponds to $S^{-1}(0, 1)$ has intersection number 1 with L . Thus, L is reducible.

Let L be a reducible principal polarization. The issue is to find a base change $S \in \mathrm{GL}_2(\mathbb{Z})$ such that $S^T M_L S$ is a diagonal matrix. Since L is reducible, there exists two elliptic curves E'_1 and E'_2 on X such that $L \equiv E'_1 + E'_2$. By Lemma 3.1 there are coprime pairs (α, β) and (γ, δ) such that $E'_1 \equiv N_{\alpha, \beta}$ and $E'_2 \equiv N_{\gamma, \delta}$ with $\deg(\sigma_{\alpha, \beta}) = \gcd(\alpha, d)$ and $\deg(\sigma_{\gamma, \delta}) = \gcd(\gamma, d)$. We will show that the matrix

$$S := \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$$

has the required properties.

For that we first claim that α and γ are coprime. Let p be any prime number and we factorize $\alpha = p^r \alpha'$, $\gamma = p^s \gamma'$ and $d = p^t d'$. By Lemma 3.4 the numerical classes are given by:

$$N_{\alpha, \beta} \equiv \frac{d\beta^2 F_1 + \alpha^2 F_2 + \alpha\beta \nabla}{\gcd(\alpha, d)} = \frac{p^t d' \beta^2 F_1 + p^{2r} \alpha'^2 F_2 + p^r \alpha' \beta \nabla}{\gcd(p^r, p^t) \cdot \gcd(\alpha', d')},$$

$$N_{\gamma, \delta} \equiv \frac{d\delta^2 F_1 + \gamma^2 F_2 + \gamma\delta \nabla}{\gcd(\gamma, d)} = \frac{p^t d' \delta^2 F_1 + p^{2s} \gamma'^2 F_2 + p^s \gamma' \delta \nabla}{\gcd(p^s, p^t) \cdot \gcd(\gamma', d')}.$$

If p is a common factor of α and γ , then $1 \leq r, s$. Without loss of generality we assume that $1 \leq r \leq s$. Then we deduce by explicitly calculating the intersection number $N_{\alpha, \beta} \cdot N_{\gamma, \delta} = 1$ that

$$1 = \frac{p^{2r+t}}{\gcd(p^r, p^t) \cdot \gcd(p^s, p^t)} \cdot \frac{\alpha'^2 \delta^2 d' + p^{2(s-r)} \gamma'^2 \beta^2 d' - 2p^{m-n} \alpha' \beta \gamma' \delta d}{\gcd(\alpha', d') \cdot \gcd(\gamma', d')}.$$

For all $t \geq 0$ both factors are integers and, moreover, the left factor is at least p . Thus, this equation represents a factorization of 1, but this is impossible and, therefore, α and γ are coprime.

Next, we will show that S has determinant ± 1 . The map

$$\sigma_{\alpha, \beta} \times \sigma_{\gamma, \delta} : E_1 \times E_1 \rightarrow E'_1 \times E'_2 \cong X$$

is an isogeny and we have for the degree

$$\deg(\sigma_{\alpha, \beta} \times \sigma_{\gamma, \delta}) = \deg(\sigma_{\alpha, \beta}) \cdot \deg(\sigma_{\gamma, \delta}) = \gcd(\alpha, d) \cdot \gcd(\gamma, d) = \gcd(\alpha\gamma, d),$$

where the last equality comes from the fact that α and γ are coprime. Thus, the degree of $\sigma_{\alpha, \beta} \times \sigma_{\gamma, \delta}$ is at most d . On the other hand, the minimal degree of any isogeny $E_1 \times E_1 \rightarrow E_1 \times E_2$ is at least d and, hence, the $\gcd(\alpha\gamma, d)$ equals d . From the equation given by the intersection $N_{\alpha, \beta} \cdot N_{\gamma, \delta} = 1$ we then deduce that

$$1 = (\alpha\delta - \beta\gamma)^2 = \det(S)^2.$$

Lastly, by using explicit calculations we see that

$$S^T M_L S = \begin{pmatrix} \gcd(\alpha, d) & 0 \\ 0 & \gcd(\gamma, d) \end{pmatrix}.$$

Note that if $\gcd(\alpha, d) > \gcd(\gamma, d)$, then we swap the roles E'_1 and E'_2 . This completes the proof. $\square$

To conclude, we briefly return to Kani's result in Theorem 4.8. His proof is based on studying the *refined Humbert invariant*

$$q_L(D) = (D \cdot L)^2 - 2D^2, \quad D \in \text{Div}(A),$$

as a positive definite quadratic form on the quotient $\text{NS}(A)/\mathbb{Z}L$. We provide here an alternative proof of Kani's result, as a consequence of the characterization of irreducible principal polarizations given by Theorem 5.1. For this, we use a criterion by Grube [8, Chp. 9] to characterize idoneal numbers, which can be refined as follows [12, Remark 18 (b)]:

Proposition 5.2. ([8, 12]) *An integer $n \geq 1$ is an idoneal number if and only if for every $B = 1, \dots, \lfloor \sqrt{\frac{n}{3}} \rfloor$, and for every representation*

$$n + B^2 = AC$$

with $2B \leq A \leq C$ and $\gcd(A, 2B, C) = 1$, we have either $A = C$ or $A = 2B$.

Proof of Theorem 4.8. To begin with, we claim that d is an idoneal number. By Theorem 5.2 there does not exist an irreducible principal polarization on X if and only if there does not exist a representation $d + B^2 = AC$ with $\gcd(A, B, C) = 1$ and $0 < 2B \leq A \leq C$. Thus, by the previous criterion 5.2 it follows that d is an idoneal number.

To complete the claim, we have to show that for an idoneal number d there does not exist a representation $d + B^2 = AC$ with $\gcd(A, B, C) = 1$ and $0 < 2B \leq A \leq C$ if and only if $d \equiv 2, 4, 6$ modulo 8.

To this end, we first show that there exists an irreducible polarization if d is odd or if d is divisible by 8. If d is odd, then we have $(A, B, C) = (2, 1, \frac{d+1}{2})$. If d is divisible by 8, then we have $(4, 2, \frac{d+4}{4})$ for $d > 8$ and $(3, 1, 3)$ for $d = 8$.

Lastly, we show that there does not exist an irreducible polarization if d is idoneal and $d \equiv 2, 4, 6$ modulo 8.

Case 1 Let d be an idoneal number with $d \equiv 2$ or $d \equiv 6$, then we have $d = 2d'$ for an odd number d' . Assume that we have a representation $d + B^2 = AC$ with $\gcd(A, B, C) = 1$ and $C \geq A \geq 2B > 0$. Since d is idoneal, it follows from Proposition 5.2 that $A = 2B$ or $A = C$.

Case 1.1 If $A = 2B$, then $2d' + B^2 = 2BC$ and it follows that B is even. But then $2d' = 2BC - B^2$ is divisible by 4 which is impossible since d' is odd.

Case 1.2 If $A = C$, then we have $2d' + B^2 = C^2$. Since $\gcd(A, B, C) = 1$, it follows that B and C are odd. But then $2d' = (C - B)(C + B)$ is divisible by 8 which is a contradiction.

Case 2 Let d be an idoneal number with $d \equiv 4$, then we have $d = 4d'$ for an odd number d' . Assume that we have a factorization $d + B^2 = AC$ with $\gcd(A, B, C) = 1$ and $C \geq A \geq 2B > 0$. Again, we either have $A = 2B$ or $A = C$.

Case 2.1 If $A = 2B$, then $4d' + B^2 = 2BC$ and it follows that B is even. Thus, there exists an odd number B' and $n \geq 1$ such that $B = 2^n B'$. Since we have $4d' + 2^{2n} B'^2 = 2^{n+1} B' C$, it follows that $n = 1$, because otherwise d' would be

divisible by 2. But then C has to be an even number, since we have $d' + B' = B'C$. This, however, is impossible, because then we would have $\gcd(A, B, C) \geq 2$.

Case 2.2 If $A = C$, then we argue as in case 1.2 and deduce that $4d' = (C - B)(C + B)$ is divisible by 8 which is a contradiction since d' is odd. $\square$

Acknowledgements Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- [1] Bauer, T., Borndräger, C.: Nef cone volumes and discriminants of abelian surfaces. *J. Pure Appl. Algebra* **222**(8), 2330–2341 (2018)
- [2] Bauer, T., Grimm, F.F., Schmidt, M.: On the integrality of Seshadri constants of abelian surfaces. *Eur. J. Math.* **6**, 1264–1275 (2020)
- [3] Bauer, T., Szemberg, T.: Seshadri constants on abelian surfaces (an appendix to: Bauer, Th.: Seshadri constants and periods of polarized abelian varieties). *Math. Ann.* **312**, 618–623
- [4] Bauer, T., Schulz, C.: Seshadri constants on the self-product of an elliptic curve. *J. Algebra* **320**, 2981–3005 (2008)
- [5] Birkenhake, C., Lange, H.: *Complex Abelian Varieties*. Springer (2004)
- [6] Cox, D.A.: *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*. Wiley (1989)
- [7] Earle, C.: The genus two Jacobians that are isomorphic to a product of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties, Contemporary Mathematics*, vol. 397, pp. 27–36. American Mathematical Society, Providence, RI (2006)
- [8] Grube, F.: Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen. *Z. Math. Phys.* **19**, 492–519 (1874)
- [9] Hayashida, T., Nishi, M.: Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* **17**(1), 1–16 (1965)
- [10] Ibukiyama, T., Katsura, T., Oort, F.: Supersingular curves of genus two and class numbers. *Compos. Math.* **57**, 127–152 (1986)
- [11] Kani, E.: Elliptic curves on abelian surfaces. *Manuscripta Math.* **84**, 199–223 (1994)
- [12] Kani, E.: Idoneal numbers and some generalizations. *Ann. Sci. Math. Quebec* **36**, 501–534 (2012)
- [13] Kani, E.: The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collectanea Math.* **67**, 21–54 (2016)
- [14] Lange, H.: Principal polarizations on products of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties, Contemporary Mathematics*, vol. 397, pp. 153–162. American Mathematical Society, Providence, RI, (2006)

- [15] Steffens, A.: Remarks on Seshadri constants. *Math. Z.* **227**, 505–510 (1998)
- [16] Weil, A.: *Variétés abéliennes et courbes algébriques*. Hermann, Paris (1948)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.