The existence of Jacobians isomorphic to a product of two elliptic curves

Ernst Kani

1 Introduction

Let E_1 and E_2 be two elliptic curves over an algebraically closed field K. The purpose of this paper is to study the question of whether or not the product surface $E_1 \times E_2$ can be the Jacobian of a (smooth, irreducible) curve C of genus 2. By properties of the Jacobian, this question is equivalent to the question of whether or not there is such a curve C on $E_1 \times E_2$.

This question was first investigated in 1965 by Hayashida and Nishi[7], [6] who obtained partial results. Later Ibukiyama, Katsura and Oort[8] settled the case that E_1 and E_2 are supersingular (see Theorem 5 below).

In studying the moduli spaces of genus 2 curves C whose Jacobians are isomorphic to a product of two elliptic curves, the following result was obtained in [11]:

Theorem 1 *Suppose that* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h \neq 0$*, and put* $d = \deg(h)$*. Then there is* no *genus* 2 *curve on* $E_1 \times E_2$ *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 the following* 21 *values of* d*,*

(1) $d = 1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, 102, 130, 190, 210, 330, 462,$

and for at most one more value $d = d^* > 462$*. If the* Euler/Gauss Conjecture *(or if the* Generalized Riemann Hypothesis*) is true, then no such extra* d^* *exists.*

This, therefore, answers the above question in the case that E_1 and E_2 are isogenous elliptic curves without complex multiplication, if we leave aside the difficult number-theoretic question of whether or not an extra idoneal number d^* exists. (A discussion of this question and its history can be found in [12].)

In this paper we answer the above question in the remaining case that E_1 and E_2 are isogenous elliptic curves with complex multiplication. (Note that if E_1 and E_2 are not isogenous, then this question is uninteresting; cf. Remark 9.) Before stating the result, we make the important observation (cf. Corollary 8) that the existence of genus 2 curves on $E_1 \times E_2$ depends only on the nature of the quadratic form q_{E_1,E_2} on $\mathrm{Hom}(E_1, E_2)$ which is defined by

$$q_{E_1,E_2}(f) := \deg(f) \quad \text{for} \quad f \in \mathrm{Hom}(E_1, E_2).$$

Note that by fixing a basis of $\mathrm{Hom}(E_1, E_2)$ we obtain an explicit binary quadratic form and hence (by considering all bases) a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of forms.

Theorem 2 *Let $E_1 \sim E_2$ be two isogenous CM elliptic curves over K. Then there is* no *genus* 2 *curve on $E_1 \times E_2$ if and only if q_{E_1,E_2} is equivalent to one of the* 15 *forms $f(x,y) = ax^2 + bxy + cy^2$ whose coefficients (a,b,c) are in the following list:*

$$\begin{aligned}\mathcal{L} \;=\; & \{k(1,1,1) : k = 1,2,4,6,10\} \cup \{k(1,0,1) : k = 1,2,6\} \cup \{(1,1,2),(1,1,4)\} \\ & \cup \{2(1,1,c) : c = 3,9\} \cup \{2(1,0,c) : c = 2,5\} \cup \{2(2,0,3)\}.\end{aligned}$$

Note that if we restrict attention to those CM-curves E_i for which $\mathrm{End}(E_i)$ is a maximal order, then q_{E_1,E_2} is a primitive form (cf. Remark 38) and so Theorem 2 shows that there are only 4 such exceptional forms. Thus, the above result includes the result of Hayashida and Nishi[7], who considered only the maximal order case.

By using the results of [13], we can determine all the *CM abelian product surfaces* (i.e. abelian surfaces which are isogenous to $E \times E$, where E is a CM elliptic curve) which are "exceptional"; cf. Corollary 59. In particular:

Corollary 3 *Up to isomorphism, there are at most* 15 *isomorphism classes of CM abelian product surfaces over K which do not contain a genus* 2 *curve. Moreover, if* $\mathrm{char}(K) = 0$*, then there are precisely* 15 *such surfaces.*

This result can also be turned into an *existence theorem* which is valid over an arbitrary ground field, as follows.

Corollary 4 *Let A/K_0 be an abelian surface such that A is isogenous to $E \times E$, where E/K_0 is a CM elliptic curve with* $\mathrm{rank}(\mathrm{End}_{K_0}(E)) = 2$*, and assume that the discriminant $\Delta = \Delta(A)$ of the intersection pairing on the Néron-Severi group* $\mathrm{NS}(A)$ *of A divides the discriminant $\Delta_E = \Delta(q_{E,E})$ of E. Then there exist elliptic curves E_1 and E_2/K_0 such that $A \simeq E_1 \times E_2$. Moreover, if $-\Delta$ is not equal to one of the* 15 *discriminants of the forms in $\mathcal{L}$, i.e. if*

$$\Delta \notin \{3,4,7,12,15,16,32,44,48,80,96,108,140,144,300\}, \tag{2}$$

then there is a genus 2 *curve C/K_0 on A and hence $J_C \simeq A \simeq E_1 \times E_2$.*

Note that the above corollary is a special case of a more precise result (Theorem 61) which is proven in section 7. In addition, we observe that the extra condition that $\Delta(A)|\Delta_E$ is unnecessary if K is algebraically closed or finite; cf. Remark 62.

For completeness we also mention the following analogue of Theorems 1 and 2 in the supersingular case which was proven (but not explictly stated) by Ibukiyama, Katsura and Oort [8].

Theorem 5 (Ibukiyama/Katsura/Oort) *If E_1 and E_2 are two supersingular curves over K, then there is no genus* 2 *curve on $E_1 \times E_2$ if and only if* $\mathrm{char}(K) = 2$ *or* 3.

The first main ingredient of the proof of Theorem 2 is *refined Humbert invariant* q_θ which was defined in [11] (see also [10]). As is explained in §2, this allows us to translate the problem of finding genus 2 curves on $E_1 \times E_2$ into a problem about the classification of quadratic forms with certain properties.

Due to its various ramifications, this classification theorem is perhaps also of independent interest, for it can be viewed as a generalization of the problem of classifying idoneal numbers, as is explained in more detail in [12]. Indeed, one of the key steps of this result is the classification (given in §5) of (special) *idoneal-valued* binary quadratic forms which are introduced here in §3. (Roughly speaking, a special idoneal-valued form is a quadratic form whose small values are all special idoneal numbers, i.e. those idoneal numbers which appear in Theorem 1.) In addition, it turns out that there is close connection between this problem and the *class-number one problem* for forms in $r \geq 3$ variables. This problem, which was studied in a series of papers by Watson[20], is to classify all positive definite quadratic forms q whose class number $c(q) := \#\mathrm{gen}(q) = 1$; i.e. to determine those forms q whose *genus* $\mathrm{gen}(q)$ consists only of a single equivalence class.

As the following result shows, these two classification problems are also connected to other classification problems, and this connection is established via the *θ-construction*, which is an abstract version of the refined Humbert invariant q_θ in the context of quadratic forms. This construction, which associates to an arbitrary quadratic form Q in r variables and a $\theta \in \mathbb{Z}^r$ with $Q(\theta) = 1$ a certain equivalence class Q_θ of forms in $r-1$-variables, is studied in detail in §4, and leads to the following *classification theorem* of quadratic forms.

Theorem 6 *Let $q(x,y) = ax^2 + bxy + cy^2$ be a positive-definite binary quadratic form such that either b is odd or that $q(x,y) \not\equiv 3 \pmod 4$, for all $x, y \in \mathbb{Z}$. If $f_q(x,y,z) = z^2 + 4q(x,y)$ and $Q(x,y,z,w) = xy - q(z,w)$, then the following conditions are equivalent:*

(i) *$c(f_q) = 1$;*

(ii) *$1 \in f'(\mathbb{Z}^3)$, for all $f' \in \mathrm{gen}(f_q)$;*

(iii) *$1 \in Q_\theta(\mathbb{Z}^3)$, for all $\theta \in \mathbb{Z}^4$ with $Q(\theta) = 1$;*

(iv) *q is a special idoneal-valued form;*

(v) *q is equivalent to one of 15 forms of the list $\mathcal{L}$ of* Theorem 2.

The proof this theorem occupies most of this paper (§4-7). As was mentioned above (and is explained in detail in §3), Theorem 2 follows immediately from it once one has certain established properties of the refined Humbert invariant which are presented in §2.

This research was partially supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC), and also by the Graduiertenkolleg of the Institute of Experimental Mathematics (IEM) of the University of Duisburg/Essen. I would like to express my appreciation to Gerd Frey and to the IEM for their hospitality, and to thank him for his interest and helpful comments on this paper.

2 Curves on product surfaces

As was mentioned in the introduction, the first step in proving Theorem 2 is to translate the problem of finding genus 2 curves on the product surface $E_1 \times E_2$ into a problem about quadratic forms. For this, we recall from [11] the following facts about such curves.

Let A be an abelian surface over an algebraically closed field K, and let $\mathcal{P}^{irr}(A)$ denote the set of smooth, irreducible genus 2 curves C on A. By the adjunction formula on A, the self-intersection number of C is $C^2 = 2$, so

$$\mathcal{P}^{irr}(A) \subset \mathcal{P}(A) := \{\theta \in \mathrm{Div}(A) : \theta \geq 0, \theta^2 = 2\},$$

where $\mathrm{Div}(A)$ denotes the group of divisors on A. Here the notation $\mathcal{P}^{irr}(A)$ reflects the fact (due to Weil[21]) that if $\theta \in \mathcal{P}(A)$, then $\theta \in \mathcal{P}(A)^{irr}$ if and only if θ is an irreducible curve. (Thus, if θ is irreducible, then it is also smooth.)

To decide whether or not $\theta \in \mathcal{P}(A)$ is irreducible, we shall use the *refined Humbert invariant* q_θ defined in [11] (which by [10] is closely related to the classical Humbert invariant defined by Humbert). This is the quadratic form defined by the formula

$$q_\theta(D) = (D.\theta)^2 - 2D^2, \quad D \in \mathrm{Div}(A), \tag{3}$$

where (.) denote intersection numbers. It is clear that q_θ can be viewed as a quadratic form on the *Néron-Severi group* of A, i.e. on the quotient group $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where the equivalence relation $D_1 \equiv D_2$ (numerical equivalence) means that $(D_1.D) = (D_2.D)$, $\forall D \in \mathrm{Div}(A)$. Moreover, a short computation (using the fact that $\theta^2 = 2$) shows that q_θ is actually a quadratic form on $\mathrm{NS}(A, \theta) := \mathrm{NS}(A)/\mathbb{Z}\theta$, and the Hodge Index Theorem shows that q_θ is positive definite (on $\mathrm{NS}(A, \theta)$).

One of the key properties of q_θ is the following *irreducibility criterion* (cf. [11], Proposition 6): if $\theta \in \mathcal{P}(A)$, then

$$\theta \text{ is irreducible} \quad \Leftrightarrow \quad q_\theta(D) \neq 1, \text{ for all } D \in \mathrm{Div}(A). \tag{4}$$

The above criterion translates the existence of genus 2 curves on A into a problem that only involves the integral quadratic form q_A defined by the intersection pairing on $\mathrm{NS}(A) \simeq \mathbb{Z}^\rho$. To make this precise, put

$$q_A(D) = \tfrac{1}{2}(D.D), \quad \text{for } D \in \mathrm{NS}(A),$$

which is an *integral* quadratic form by the Riemann-Roch theorem ([15], p. 150). Then the refined Humbert invariant $q_\theta = (q_A)_\theta$ associated to $\theta \in \mathcal{P}(A)$ is given by

$$(q_A)_\theta(D) = \beta_{q_A}(D, \theta)^2 - 4q_A(D), \quad \text{for } D \in \mathrm{NS}(A), \tag{5}$$

where β_{q_A} denotes the bilinear form associated to the quadratic form q_A (cf. §3).

Proposition 7 *There is a genus* 2 *curve on the abelian surface* A *if and only if there is a* $\theta \in \mathrm{NS}(A)$ *with* $q_A(\theta) = 1$ *and* $(q_A)_\theta(D) \neq 1$*, for all* $D \in \mathrm{NS}(A)$*.*

Proof. If such a curve C exists, then its class $\theta = cl(C)$ in $\mathrm{NS}(A)$ satisfies $q_A(\theta) = \frac{1}{2}C^2 = 1$ and $(q_A)_\theta(D) \neq 1$, for all $D \in \mathrm{NS}(A)$ by (4). Conversely, if $\theta \in \mathrm{NS}(A)$ satisfies these properties, then by [10], Corollary 2.4, there is an effective curve C on A such that its class $cl(C)$ equals either θ or $-\theta$. Thus, $C \in \mathcal{P}(A)$. Since $(q_A)_{-\theta} = (q_A)_\theta$, it thus follows from (4) that $C \in \mathcal{P}(A)^{irr}$.

So far, the above results are true for an arbitrary abelian surface A. If we now specialize to the case that $A = E_1 \times E_2$ is a product surface, then we can relate q_A to the binary quadratic form q_{E_1,E_2} defined by the degree map on $\mathrm{Hom}(E_1, E_2)$, i.e. by

$$q_{E_1,E_2}(f) \;=\; \deg(f), \quad \text{if } f \in \mathrm{Hom}(E_1, E_2) \;\simeq\; \mathbb{Z}^r,$$

where $r = \mathrm{rank}(\mathrm{Hom}(E_1, E_2))$. (Note that this defines a $\mathrm{GL}_r(\mathbb{Z})$-equivalence class of quadratic forms in r variables.)

Now by Proposition 22 of [11] we have an isomorphism $\mathrm{NS}(A) \simeq \mathbb{Z}^2 \oplus \mathrm{Hom}(E_1, E_2)$ and via this identification we have

$$q_{E_1\times E_2}(x, y, f) = xy - q_{E_1,E_2}(f), \quad \text{for } x, y \in \mathbb{Z},\ f \in \mathrm{Hom}(E_1, E_2). \tag{6}$$

In other words, $q_{E_1\times E_2} \sim (xy) \perp (-q_{E_1,E_2})$, where xy denotes the quadratic form defined by the hyperbolic plane (and $\sim$ denotes equivalence of quadratic forms). We thus obtain:

Corollary 8 *Let* E_1 *and* E_2 *be two elliptic curves over* K*, and let* $q \sim q_{E_1,E_2}$ *be a quadratic form in* r *variables. Put* $Q = xy \perp (-q)$*. Then there is* no *curve of genus* 2 *on* $E_1 \times E_2$ *if and only if for every* $\theta \in \mathbb{Z}^{r+2}$ *with* $Q(\theta) = 1$ *there exists an* $x = x_\theta \in \mathbb{Z}^{r+2}$ *such that* $Q_\theta(x) = 1$*.*

Remark 9 Note that the above corollary applies to arbitrary elliptic curves E_1, E_2 (including the supersingular case). It also applies to the case that E_1 and E_2 are not isogenous, i.e. $r = 0$. Then we have that $Q(x, y) = xy$, so the only solution of $Q(\theta) = 1$ is $\theta = \pm(1, 1)$ and then $Q_\theta(x, y) = (x+y)^2$. Since $Q_\theta(1, 0) = 1$, we conclude that in the non-isogenous case there is never a curve of genus 2 on $E_1 \times E_2$.

3 The main result

By Corollary 8, the *geometric problem* of finding genus 2 curves on the product surface $A = E_1 \times E_2$ has been translated into a purely *arithmetic problem* involving the quadratic form q_A. In this section we formulate this problem in the context of

quadratic forms and present the main result which connects the original problem with other interesting problems about quadratic forms.

For this, let $Q(x_1, \ldots, x_r) = \sum_{i \leq j} a_{ij} x_i x_j$ be an integral quadratic form in r variables, and let

$$\mathcal{P}(Q) = \{x \in \mathbb{Z}^r : Q(x) = 1\}.$$

denote the set of representations of 1 by Q. For each $\theta \in \mathcal{P}(Q)$, let Q_θ be defined by

$$Q_\theta(x) = \beta_Q(x, \theta)^2 - 4Q(x), \tag{7}$$

where β_Q is the bilinear form associated to Q. Since this is naturally a quadratic form on the quotient $\mathbb{Z}^r/\mathbb{Z}\theta$ (cf. §4), we thus obtain (after choosing a basis of $\mathbb{Z}^r/\mathbb{Z}\theta \simeq \mathbb{Z}^{r-1}$), an equivalence class $\bar{Q}_\theta$ of quadratic forms in $r-1$ variables. We call this construction of $\bar{Q}_\theta$ the *θ-construction*; it will be studied in more detail in the next section.

The discussion in the previous section (cf. Corollary 8) leads us to consider the following problem.

Problem 10 Classify the positive definite quadratic forms q in r variables such that $Q := xy \perp (-q)$ satisfies the following property:

$$Q_\theta \to 1, \quad \text{for all } \theta \in \mathcal{P}(Q). \tag{8}$$

Here, the symbol $Q_\theta \to 1$ means that Q_θ represents 1, i.e. that $\mathcal{P}(Q_\theta) \neq \emptyset$.

Remark 11 If $\theta \in \mathcal{P}(Q)^{ev} := \{\theta \in \mathcal{P}(Q) : \beta_Q(x, \theta) \equiv 0 \,(\mathrm{mod}\ 2), \forall x \in \mathbb{Z}^r\}$, then (7) shows that $Q_\theta(x) \equiv 0 \,(\mathrm{mod}\ 4)$, for all $x \in \mathbb{Z}^r$, so clearly Q_θ cannot represent 1. Thus, if $\mathcal{P}(Q)^{ev} \neq \emptyset$ or, equivalently, if $\mathcal{P}(Q) \neq \mathcal{P}(Q)^{odd} := \mathcal{P}(Q) \setminus \mathcal{P}(Q)^{ev}$, then Q cannot satisfy (8).

In the case that $r = 1$, i.e. that $q(x) = nx^2$, for some $n \geq 1$, Problem 10 was (implicitly) solved in [11]. In this case it was found that (8) holds if and only if n is an *idoneal number* (in the sense of Euler) satisfying certain extra conditions. Thus, by using the results of Euler, Grube[5] and Weinberger[22] on the classification of idoneal numbers, one obtains Theorem 1.

The key result in the above case was the fact (cf. [11], Proposition 15) that

$$\{\bar{Q}_\theta : \theta \in \mathcal{P}(Q)^{odd}\} \;=\; \mathrm{gen}(x^2 + 4ny^2); \tag{9}$$

here $\mathrm{gen}(f)$ denotes the genus of the (binary) quadratic form f. This yields a direct connection to the idoneal numbers of Euler because we have the well-known relation (due to Grube; cf. [12]) that

$$n \geq 1 \text{ is idoneal} \quad \Leftrightarrow \quad \#\mathrm{gen}(x^2 + ny^2) = 1. \tag{10}$$

A (partial) generalization of (9) is proved for all $r \geq 1$ in the next section; cf. Theorem 20. For this, we require the (well-known) generalization of the notion of a genus for binary forms to forms in an arbitrary number of variables: if q is a quadratic form in r variables, then its *genus* $\mathrm{gen}(q)$ is the set of equivalence classes of quadratic forms in r variables which are *genus-equivalent* (or *semi-equivalent*) to q; cf. Watson[18], p. 72. (Here, as in [18], equivalence means $\mathrm{GL}_r(\mathbb{Z})$-equivalence.)

Following Watson[20], we call

$$c(q) = \#\mathrm{gen}(q)$$

the *class number* of the form q. In view of (10), the following problem, which was studied by Watson in a series of papers in the years 1963–1978 (cf. [20] and the references therein), can be viewed as a generalization of the classification problem of idoneal numbers (cf. [12]):

Problem 12 (Watson) *Find all the equivalence classes of positive definite primitive forms q with class number 1, i.e. with $c(q) = 1$.*

As we shall see below in Theorem 13, Watson's problem is closely related to Problem 10, but this fact is far from obvious.

Another problem that turns out to be is closely related to the above problems is the problem of classifying all (special) *idoneal-valued* quadratic forms which are defined as follows.

Definition. Let $q(x_1, \ldots, x_r)$ be a positive definite quadratic form in r variables. We say that q is an *idoneal-valued* form if its only (proper) values $\leq |\Delta(q)|$ are idoneal numbers, i.e. if

$$q \to n \leq |\Delta(q)| \quad \Rightarrow \quad n \text{ is an idoneal number;} \tag{11}$$

here, the symbol $q \to n$ means that q *properly represents* n, i.e. that there exist $x_1, \ldots, x_r \in \mathbb{Z}$ with $\gcd(x_1, \ldots, x_r) = 1$ such that $q(x_1, \ldots, x_r) = n$, and $\Delta(q)$ denotes the *discriminant* of q; cf. [18], p. 2.

In addition, we say that q is a *special idoneal-valued form* if

$$q \to n \leq |\Delta(q)| \quad \Rightarrow \quad 4n \text{ is an idoneal number,} \tag{12}$$

and if in addition we have that $q \not\to n$, for any $n \equiv 3 \pmod 4$ when $\Delta(q) \not\equiv 1 \pmod 4$, and that $q \not\to n$, for any $n \equiv 3 \pmod 4$ with $n < |\Delta(q)|$ when $\Delta(q) \equiv 1 \pmod 4$.

At first sight it might seem unlikely that (special) idoneal-valued quadratic forms in 2 variables exist at all. However, there are some, and they are classified in the following theorem which can be viewed as the main result of this paper:

Theorem 13 *Let $q(x,y) = ax^2 + bxy + cy^2$ be a positive definite binary quadratic form, and let $f_q(x,y,z) = z^2 + 4q(x,y)$ and $Q(x,y,z,w) = xy - q(z,w)$. Assume that $\mathcal{P}(Q) = \mathcal{P}(Q)^{odd}$ or, equivalently, that either $\Delta := b^2 - 4ac \equiv 1 \pmod 4$ or that $q \not\to n$, for any $n \equiv 3 \pmod 4$. Then the following conditions are equivalent:*

(i) *$c(f_q) = 1$;*

(ii) *$f' \to 1$, for all $f' \in \mathrm{gen}(f_q)$;*

(iii) *$Q_\theta \to 1$, for all $\theta \in \mathcal{P}(Q)$;*

(iv) *q is a special idoneal-valued form;*

(v) *q is equivalent to one of 15 forms whose coefficients (a,b,c) are in the following list:*

$$\begin{aligned}\mathcal{L} \;=\; & \{k(1,1,1) : k = 1,2,4,6,10\} \cup \{k(1,0,1) : k = 1,2,6\} \cup \{(1,1,2),(1,1,4)\} \\ & \cup \{2(1,1,c) : c = 3,9\} \cup \{2(1,0,c) : c = 2,5\} \cup \{2(2,0,3)\}.\end{aligned}$$

The proof of this theorem (which is a restatement of Theorem 6) is quite long and will occupy the rest of this paper; cf. §7, where all parts are put together. Note that this theorem immediately implies Theorem 2 of the introduction, as we now show.

Proof of Theorem 2. By Corollary 8, there is no genus 2 curve on $E_1 \times E_2$ if and only if $q = q_{E_1,E_2}$ satisfies condition (iii) of Theorem 13. Since $E_1 \sim E_2$ has CM, it follows that $\mathrm{rank}(\mathrm{Hom}(E_1,E_2)) = 2$, and so q is a positive definite binary quadratic form. Thus, the assertion of Theorem 2 follows from the equivalence (iii) $\Leftrightarrow$ (v) of Theorem 13, together with Remark 11.

Note that the notion of a special idoneal-valued quadratic form can be used to unify the CM and non-CM cases (Theorems 1 and 2) as follows:

Corollary 14 *Let $E_1 \sim E_2$ be two isogenous elliptic curves over K, and assume that E_1 is not supersingular. Then there is* no *genus 2 curve on $E_1 \times E_2$ if and only if q_{E_1,E_2} is a special idoneal-valued form.*

Proof. If E_1 has CM, i.e. if $r = \mathrm{rank}(\mathrm{Hom}(E_1,E_2)) = 2$, then by the above proof of Theorem 2, this follows from the equivalence (iii) $\Leftrightarrow$ (iv) of Theorem 13.

If E_1 does not have CM, i.e. if $\mathrm{End}(E_1) = \mathbb{Z}$, then $\mathrm{Hom}(E_1,E_2) = \mathbb{Z}h$, for some h and $q_{E_1,E_2}(xh) = nx^2$, where $n = \deg(h)$. Since $\Delta(q_{E_1,E_2}) = n$, and $n = q(1 \cdot h)$ is the only value which is primitively represented by n, it is clear that q_{E_1,E_2} is a special idoneal-valued form if and only if $n \not\equiv 3 \pmod 4$ and $4n$ is not idoneal. Since this is equivalent to the condition that either $n = 1$ or that n is even but $n \not\equiv 0 \pmod 8$ (cf. [11], Corollary 34 or [12], Theorem 36) we see from Theorem 1 that this condition is equivalent to the condition that $E_1 \times E_2$ does not contain any genus 2 curve.

4 The θ-construction

In this section we study the θ-construction (cf. §3) in the general context of quadratic R-modules. Here R can be an arbitrary commutative ring (in which 2 is not a zero-divisor), but in the applications we only need the cases that $R = \mathbb{Z}$, $\mathbb{Z}_p$ or $\mathbb{R}$.

Let (X, q) be a *quadratic R-module*. Thus, X is an R-module and q is a quadratic form in the sense of Milnor/Husemoller[14], p. 110, i.e. $q : X \to R$ is a function which satisfies (i) $q(rx) = r^2 q(x)$, for all $r \in R$ and (ii) the map $\beta_q : X \times X \to R$ defined by

$$\beta_q(x, y) = q(x + y) - q(x) - q(y), \quad \text{for all } x, y \in X, \tag{13}$$

is an R-bilinear map. If this is the case, then we call β_q the *bilinear map associated to q*. Note that $\beta_q(x, x) = 2q(x)$.

Let $\theta \in \mathcal{P}(q) = \mathcal{P}(X, q) := \{x \in X : q(x) = 1\}$, and put

$$q_\theta(x) = \beta_q(x, \theta)^2 - 4q(x), \quad \text{for } x \in X. \tag{14}$$

Clearly, q_θ is again a quadratic form on X with associated bilinear form

$$\beta_{q_\theta} = 2\beta_\theta, \quad \text{where} \quad \beta_\theta(x, y) = \beta_q(x, \theta)\beta_q(y, \theta) - 2\beta_q(x, y), \ \forall x, y \in R. \tag{15}$$

Indeed, clearly β_θ is symmetric and R-bilinear and we have

$$q_\theta(x) \ = \ \beta_\theta(x, x), \tag{16}$$

and so the formula $\beta_{q_\theta} = 2\beta_\theta$ follows immediately.

Since $\beta_q(\theta, \theta) = 2q(\theta) = 2$, it follows from the definition (15) of β_θ that

$$\beta_\theta(x, r\theta) = 0, \quad \text{for all } r \in R, \tag{17}$$

and so β_θ defines a bilinear form $\bar{\beta}_\theta$ on the quotient module $\bar{X}_\theta = X/R\theta$. In particular, q_θ induces a quadratic form $\bar{q}_\theta$ on X_θ and we have by (15) that $\beta_{\bar{q}_\theta} = 2\bar{\beta}_\theta$. Thus, $(\bar{X}_\theta, \bar{q}_\theta)$ is quadratic R-module, and if $\pi_\theta : X \to X_\theta = X/R\theta$ denotes the quotient map, then we have $q_\theta(x) = \bar{q}_\theta(\pi_\theta(x))$, for all $x \in X$.

Remark 15 (a) The above construction clearly generalizes the θ-construction presented in §3. To see this, note first that if $q : \mathbb{Z}^r \to \mathbb{Z}$ is an integral quadratic form in r variables, then $(\mathbb{Z}^r, q)$ is a quadratic $\mathbb{Z}$-module, and if $q' : \mathbb{Z}^r \to \mathbb{Z}$ is another quadratic form, then $(\mathbb{Z}^r, q) \simeq (\mathbb{Z}^r, q') \overset{\text{def}}{\Leftrightarrow} \exists \alpha \in \mathrm{Aut}(\mathbb{Z}^r) = \mathrm{GL}_r(\mathbb{Z})$ such that $q' \circ \alpha = q \Leftrightarrow q \sim q'$, where $\sim$ denotes $\mathrm{GL}_r(\mathbb{Z})$-equivalence of forms. Thus, the isomorphism classes of quadratic modules (X, q) with $X \simeq \mathbb{Z}^r$ can be identified with the equivalence classes of quadratic forms in r variables.

From this we see that if $q : \mathbb{Z}^r \to \mathbb{Z}$ is an integral quadratic form in r variables, and if $\theta \in \mathcal{P}(q) = \mathcal{P}(\mathbb{Z}^r, q)$, then $(\mathbb{Z}^r/\mathbb{Z}\theta, \bar{q}_\theta)$ defines an equivalence class $\bar{q}_\theta$ of quadratic

forms in $r-1$ variables because the condition $q(\theta)=1$ implies that the quotient $\mathbb{Z}^r/\mathbb{Z}\theta$ is torsionfree and hence is free of rank $r-1$.

(b) For later use we observe that the θ-construction is compatible with base-change, i.e. if $\varphi: R \to R'$ is a ring homomorphism, then for any $\theta \in \mathcal{P}(X,q)$ we have an isomorphism

$$(\overline{(X_{R'})}_{\theta\otimes 1}, \overline{(q_{R'})}_{\theta\otimes 1}) \ \xrightarrow{\sim}\ (\bar{X}_\theta, \bar{q}_\theta)\otimes R := ((\bar{X}_\theta)\otimes_R R', \bar{q}_\theta \otimes id_{R'}), \tag{18}$$

where $X_{R'} = X\otimes_R R'$ and $q_{R'} = q_R \otimes R' : X\otimes_R R' \to R\otimes_R R' = R'$. (Indeed, by the right-exactness of the tensor product, the canonical map $\pi_\theta \otimes id_{R'} : X_{R'} = X\otimes_R R' \to \bar{X}_\theta \otimes_R R'$ induces an isomorphism $X_{R'}/R'(\theta\otimes 1) \simeq \bar{X}_\theta \otimes_R R'$ because $R'(\theta\otimes 1)$ is the image of $(R\theta)\otimes_R R'$ in $X_{R'}$, and from this (18) follows immediately.)

As was explained in the previous section, we are interested in studying the set

$$\Theta(X,q) = \{(\bar{X}_\theta, \bar{q}_\theta) : \theta \in \mathcal{P}(q)\}/\simeq$$

of isomorphism classes of quadratic modules resulting from the θ-construction. A first result in this direction is given by:

Proposition 16 *If $\alpha \in \mathrm{Aut}(X,q) := \{\alpha \in \mathrm{Aut}_R(X) : q\circ\alpha = q\}$, then*

$$q_{\alpha(\theta)}\circ\alpha \ = \ q_\theta, \quad \textit{for all } \theta \in P(q), \tag{19}$$

and hence α induces an isometry $\bar{\alpha} : (\bar{X}_\theta, \bar{q}_\theta) \xrightarrow{\sim} (\bar{X}_{\alpha(\theta)}, \bar{q}_{\alpha(\theta)})$.

Proof. Clearly, the group $\mathrm{Aut}(X,q)$ acts (on the right) on $P(q)$. If $\alpha \in \mathrm{Aut}(X,q)$, then by (13) we see that $\beta_q \circ (\alpha\times\alpha) = \beta_q$, and so for $x \in X$ we have $q_{\alpha(\theta)}(\alpha(x)) = \beta_q(\alpha(x),\alpha(\theta))^2 - 4q(\alpha(x)) = \beta_q(x,\theta)^2 - 4q(x) = q_\theta(x)$, which proves (19).

Moreover, since $\alpha(\mathrm{Ker}(\pi_\theta)) = \alpha(R\theta) = R\alpha(\theta) = \mathrm{Ker}(\pi_{\alpha(\theta)})$, there is a unique R-module isomorphism $\bar{\alpha} : X_\theta \xrightarrow{\sim} X_{\alpha(\theta)}$ such that $\pi_{\alpha(\theta)}\circ\alpha = \bar{\alpha}\circ\pi_\theta$, and by (19) we see that $\bar{\alpha}$ is an isometry.

Remark 17 The above result shows that the map $\theta \mapsto (\bar{X}_\theta, \bar{q}_\theta)$ induces a surjection

$$\mathcal{P}(X,q)/\mathrm{Aut}(X,q) \quad \to \quad \Theta(X,q).$$

Now if $[R : 2R] \le 2$, then one can show that this is in fact a bijection; indeed, one can show more precisely that if $\theta_1, \theta_2 \in \mathcal{P}(X,q)$, then any isometry $\bar{\alpha} : (\bar{X}_{\theta_1}, \bar{q}_{\theta_1}) \xrightarrow{\sim} (\bar{X}_{\theta_2}, \bar{q}_{\theta_2})$ can be lifted to an isometry $\alpha \in \mathrm{Aut}(X,q)$ with $\alpha(\theta_1) = \theta_2$. Since this is not needed below (and is somewhat tedious to prove), the proof of this fact will not be given here.

By combining the above proposition with a basic fact about isometries of quadratic modules over local rings, we obtain the following important result.

Proposition 18 *If R is a local ring with $2 \in R^\times$, then $\mathrm{Aut}(X,q)$ acts transitively on $\mathcal{P}(X,q)$ and hence we have $(\bar{X}_{\theta_1}, \bar{q}_{\theta_1}) \simeq (\bar{X}_{\theta_2}, \bar{q}_{\theta_2})$, for all $\theta_1, \theta_2 \in \mathcal{P}(X,q)$.*

Proof. By [14], Lemma (4.2), we know that for every $\theta_1, \theta_2 \in \mathcal{P}(X,q)$ there is a reflection $\alpha \in \mathrm{Aut}(X,q)$ such that $\alpha(\theta_1) = \theta_2$. Thus, $\mathrm{Aut}(X,q)$ acts transitively on $\mathcal{P}(X,q)$, and so the last assertion follows from this and Proposition 16.

The above result implies in particular that when p is an odd prime, then the $\bar{q}_\theta$'s are all p-adically equivalent in the sense of Watson[18], p. 50, and/or Jones[9], p. 82.

Corollary 19 *If $q : \mathbb{Z}^r \to \mathbb{Z}$ is a quadratic form in r variables, and p is an odd prime or $p = \infty$, then $\bar{q}_{\theta_1} \sim_p \bar{q}_{\theta_2}$, for all $\theta_1, \theta_2 \in \mathcal{P}(q)$.*

Proof. If p is an odd prime, then $2 \in \mathbb{Z}_p^\times$, and so by Proposition 18 we have that $(\overline{(X_p)}_{\theta_1}, \overline{(q_p)}_{\theta_1}) \simeq (\overline{(X_p)}_{\theta_2}, \overline{(q_p)}_{\theta_2})$, where q_p denotes the canonical extension of q to $X_p = \mathbb{Z}_p^r = X \otimes \mathbb{Z}_p$ (with $X = \mathbb{Z}^r$). By base-change (cf. Remark 15(b)), this means that $(\bar{X}_{\theta_1}, \bar{q}_{\theta_1}) \otimes \mathbb{Z}_p \simeq (\bar{X}_{\theta_2}, \bar{q}_{\theta_2}) \otimes \mathbb{Z}_p$, which by definition means that $\bar{q}_{\theta_1} \sim_p \bar{q}_{th_2}$.

If $p = \infty$, then by replacing $\mathbb{Z}_p$ by $\mathbb{R}$, an analogous argument yields the result.

If R is a (local) ring for which $2 \notin R^\times$, then the results of Proposition 18 are in general not true. One reason for this is that there may exist proper $\mathrm{Aut}(X,q)$-invariant subsets $\mathcal{P}(X,q)^{ev}$ and $\mathcal{P}(X,q)'$ of $\mathcal{P}(X,q)$, which would therefore prevent $\mathrm{Aut}(X,q)$ from acting transitively on $\mathcal{P}(X,q)$. These sets are defined as follows:

$$\begin{aligned} \mathcal{P}(X,q)^{ev} &= \{\theta \in \mathcal{P}(X,q) : \beta_q(x,\theta) \in 2R, \text{ for all } x \in X\} \\ \mathcal{P}(X,q)' &= \{\theta \in \mathcal{P}(X,q) : q_\theta(x) \in 1 + 8R, \text{ for some } x \in X\} \end{aligned}$$

Thus, if $2 \notin R^\times$, then $\mathcal{P}(X,q)' \subset \mathcal{P}(X,q)^{odd} := \mathcal{P}(X,q) \setminus \mathcal{P}(X,q)^{ev}$. It is immediate that these sets are $\mathrm{Aut}(X,q)$-invariant, and hence give rise to sets

$$\Theta(X,q)^{ev}, \quad \Theta(X,q)^{odd} \quad \text{and} \quad \Theta(X,q)'$$

by replacing in the definition of $\Theta(X,q)$ the set $\mathcal{P}(X,q)$ by $\mathcal{P}(X,q)^{ev}$, $\mathcal{P}(X,q)^{odd}$, and $\mathcal{P}(X,q)'$, respectively. We shall prove:

Theorem 20 *For any integral quadratic form $q : X = \mathbb{Z}^r \to \mathbb{Z}$ in r variables with $\Delta(q) \neq 0$, the set $\Theta(X,q)'$ lies in a single genus, i.e. for any $\theta \in \mathcal{P}(X,q)'$ we have*

$$\mathrm{gen}(\bar{q}_\theta) \supset \{\bar{q}_{\theta_1} : \theta_1 \in \mathcal{P}(\mathbb{Z}^r, q)'\}/\sim . \tag{20}$$

Moreover, if there exists $\theta_0 \in \mathcal{P}(X,q)$ with $\mathcal{P}(\bar{X}_{\theta_0}, \bar{q}_{\theta_0}) \neq \emptyset$, then $\mathcal{P}(X,q)' = \mathcal{P}(X,q)^{odd}$ and hence $\Theta(X,q)^{odd} = \Theta(X,q)'$ lies in a single genus.

As a first step towards proving this, we note the following:

Lemma 21 *If $R = \mathbb{Z}_2$, then*

$$\mathcal{P}(X,q)' \;=\; \{\theta \in \mathcal{P}(X,q) : 1 \in q_\theta(X)\}. \tag{21}$$

Proof. Let $\theta \in \mathcal{P}(X,q)'$. Then there exists $x \in X$ such that $\mu := q_\theta(x) \in 1 + 8\mathbb{Z}_2$. Then μ is the square of a 2-adic unit, so $\mu = \mu_1^2$, for some $\mu_1 \in \mathbb{Z}_2^\times$. Then $x_1 := \mu_1^{-1}x$ satisfies $q_\theta(x_1) = \mu_1^{-2}q_\theta(x) = 1$, so $1 \in q_\theta(X)$. This proves that $\mathcal{P}(X,q)'$ is contained in the right hand side of (21), and so (21) follows since the other inclusion is trivial.

By the above lemma we see that the key to proving Theorem 20 is to analyze the condition that $1 \in q_\theta(X)$ or, equivalently, that $\mathcal{P}(\bar{X}_\theta, \bar{q}_\theta) \neq \emptyset$. It turns out that this condition is closely related to the existence of a *hyperbolic plane* in X.

Definition. A *hyperbolic plane* in a quadratic R-module (X,q) is an R-submodule $H = Rx_1 + Rx_2$ of X such that

$$q(r_1x_1 + r_2x_2) \;=\; r_1r_2, \quad \text{for all } r_1, r_2 \in R. \tag{22}$$

Any basis $\{x_1, x_2\}$ of H for which (22) holds is called a *hyperbolic basis* of H.

Remark 22 If $H = Rx_1 + R_x$ is a hyperbolic plane in (X,q), then

$$\beta_q(r_1x_1 + r_2x_2, r_1'x_1 + r_2'x_2) \;=\; r_1r_2' + r_2r_1', \quad \text{for all } r_1, r_2, r_1', r_2' \in R, \tag{23}$$

and so we see that $q_{|H}$ is non-degenerate, and that x_1 and x_2 are R-linearly independent. Thus, $H = Rx_1 \oplus Rx_2 \simeq R^2$. Moreover, we have that

$$X \;= H \oplus H^\perp, \quad \text{where } H^\perp = \{x \in X : \beta_q(x,h) = 0, \forall h \in H\}$$

because if $x \in X$, then

$$x = x_H + x^\perp, \text{ where } x_H = \beta_q(x,x_2)x_1 + \beta_q(x,x_1)x_2 \in H \text{ and } x^\perp = x - x_H \in H^\perp. \tag{24}$$

The following result classifies the structure of the spaces $(\bar{X}_\theta, \bar{q}_\theta)$ when $\mathcal{P}(\bar{X}_\theta, \bar{q}_\theta) \neq \emptyset$. For this we shall use the following (usual) notation: if $a \in R$, then $\langle a \rangle_R$ denotes the (rank 1) quadratic R-module (Rx, q_a), where $q_a(rx) = r^2a$, for all $r \in R$.

Proposition 23 *Suppose that $[R : 2R] \leq 2$. If $\theta \in \mathcal{P}(X,q)$, then the following conditions are equivalent:*

(i) *$\mathcal{P}(\bar{X}_\theta, \bar{q}_\theta) \neq \emptyset$, i.e. $\exists x \in X$ such that $q_\theta(x) = 1$;*

(ii) *there is a hyperbolic plane H in (X,q) with $\theta \in H$;*

(ii′) *there is a hyperbolic plane H in (X,q) such that $\theta = x_1 + x_2$ for some hyperbolic basis $\{x_1, x_2\}$ of H;*

(iii) *there is an R-submodule X' of X such that*

$$(\bar{X}_\theta, \bar{q}_\theta) \;\simeq\; \langle 1 \rangle_R \;\oplus\; (X', -4q_{|X'}); \tag{25}$$

(iii′) *there is a hyperbolic plane H in (X,q) containing θ such that (25) holds for $X' = H^\perp$.*

Proof. Since the implications (iii′) ⇒ (iii) ⇒ (i) and (ii′) ⇒ (ii) are trivial, it is enough to verify that (ii) ⇒ (i) ⇒ (ii′) ⇒ (iii′).

(ii) ⇒ (i): Write $H = Rx_1 + Rx_2$ and $\theta = rx_1 + sx_2$ with $r, s \in R$. Put $x = rx_1$. Since $rs = q(\theta) = 1$, we have by (23) that $\beta_q(x, \theta) = rs = 1$, and so $q_\theta(x) = \beta_q(x, \theta)^2 - 4q(x) = 1^2 - 0 = 1$.

(i) ⇒ (ii′): We first note that since $q_\theta(x) = \beta_q(x, \theta)^2 - 4q(x) = 1$, there is an $r \in R$ such that $\beta_q(x, \theta) = 1 + 2r$. Indeed, if $R = 2R$, then this is trivial. Otherwise we have by hypothesis that $R = 2R\dot\cup(1 + 2R)$, and then $\beta_q(x, \theta) \in 1 + 2R$ because if $\beta_q(x, \theta) \in 2R$, then $1 = \beta_q(x, \theta)^2 - 4q(x) \in 2R$, contradiction. Thus, in both cases $\beta_q(x, \theta) = 1 + 2r$ for some $r \in R$.

Put $x_1 = x - r\theta$ and $x_2 = \theta - x_1$. Then $\theta = x_1 + x_2$, so it is enough to show that $H = Rx_1 + Rx_2$ is a hyperbolic plane in (X, q). For this we first observe that $\beta_q(x_1, \theta) = \beta_q(x, \theta) - r\beta_q(\theta, \theta) = 1 + 2r - r(2) = 1$, and so $q(x_1) = 0$ because by (17) we have $q_\theta(x_1) = q_\theta(x) = 1$ and so $4q(x_1) = \beta_1(x_1, \theta)^2 - q_\theta(x_1) = 1^2 - 1 = 0$. Next we note that $\beta_q(x_1, x_2) = \beta_q(x_1, \theta) - \beta_q(x_1, x_1) = 1 - 2(0) = 1$. Finally, $\beta_q(x_2, x_2) = 0$ because $\beta_q(x_2, \theta) = \beta_q(\theta, \theta) - \beta_q(x_1, \theta) = 2 - 1 = 1$ and so $\beta_q(x_2, x_2) = \beta_q(\theta, x_2) - \beta_q(x_1, x_2) = 1 - 1 = 0$. From these identities and the R-bilinearity of β_q it is clear that (22) holds, and so $H = Rx_1 + Rx_2$ is a hyperbolic plane with hyperbolic basis $\{x_1, x_2\}$.

(ii′) ⇒ (iii′): Let $\bar x_1 = \pi_\theta(x_1) \in \bar X_\theta$. Then $\bar q_\theta(\bar x_1) = q_\theta(x_1) = 1$, the latter by the proof of (ii) ⇒ (i). Then we have

$$\bar X_\theta \;=\; R\bar x_1 \,\oplus\, (R\bar x_1)^\perp \tag{26}$$

because if $\bar x \in \bar X_\theta$, then $\bar x = \beta_\theta(\bar x, \bar x_1)\bar x_1 + \bar x'$, where $\bar x' = x - \beta_\theta(\bar x, \bar x_1)\bar x_1 \in (R\bar x_1)^\perp$. (Note that $\bar\beta_\theta(\bar x', \bar x_1) = \bar\beta_\theta(\bar x, \bar x_1) - \bar\beta_\theta(\bar x, \bar x_1)\bar\beta_\theta(\bar x_1, \bar x_1) = 0$ because by (16) we have $\bar\beta_\theta(\bar x_1, \bar x_1) = q_\theta(x_1) = 1$.)

Thus, (25) follows once we have shown that the restriction $\pi' = (\pi_\theta)_{|H^\perp}$ of π_θ to $H^\perp$ induces an isometry

$$\pi' : (H^\perp,\, -4q_{|H^\perp}) \;\xrightarrow{\sim}\; ((R\bar x_1)^\perp, (\bar q_\theta)_{|(Rx_1)^\perp}). \tag{27}$$

For this, note first that π' is clearly injective because $\mathrm{Ker}(\pi_\theta) = R\theta \subset H$ and so $\mathrm{Ker}(\pi') = \mathrm{Ker}(\pi_\theta) \cap H^\perp \subset H \cap H^\perp = 0$.

Next we observe that $\pi'(H^\perp) = (R\bar x_1)^\perp$. Indeed, if $x \in H^\perp$, then $\beta_q(x, x_i) = 0$, for $i = 1, 2$, and so $\beta_q(x, \theta) = 0$, and hence $\beta_\theta(x, x_1) = 0 - 2\beta_q(x_1, x_1) = 0$, which means that $\pi'(x) \in (R\bar x_1)^\perp$. Conversely, let $\bar x \in (R\bar x_1)^\perp$; thus, $\bar\beta_\theta(\bar x, \bar x_1) = 0$. Let $\tilde x \in X$ be such that $\pi_\theta(\tilde x) = \bar x$ and put $r := \beta_q(\tilde x, x_1)$ and $x := \tilde x - r\theta$. Then $\pi_\theta(x) = \pi_\theta(\tilde x) = \bar x$. Moreover, since $\beta_q(\theta, x_i) = 1$, we have $\beta_q(x, x_1) = \beta_q(\tilde x, x_1) - r\beta_q(\theta, x_1) = r - r(1) = 0$. Thus $0 = \bar\beta_\theta(\bar x, \bar x_1) = \beta_\theta(x, x_1) = \beta_q(x, \theta)\beta_q(x_1, \theta) - 2\beta_q(x_1, x_1) = \beta_q(x, \theta) \cdot 1$, i.e. $\beta_q(x, \theta) = 0$ and hence also $\beta_q(x, x_2) = \beta_q(x, \theta - x_1) = 0 - 0 = 0$. This means that $x \in H^\perp$, and so $\bar x = \pi'(x) \in \pi'(H^\perp)$.

We thus have that $\pi' : H^\perp \xrightarrow{\sim} (R\bar{x}_1)^\perp$ is an isomorphism of R-modules. Now if $x \in H^\perp$, then $\beta_q(x,\theta) = 0$, and hence $\bar{q}_\theta(\pi'(x)) = q_\theta(x) = \beta(x,\theta)^2 - 4q(x) = -4q(x)$. This shows that π' defines an isometry (27) and hence (iii′) holds.

For later reference we observe the following consequence of the above results.

Corollary 24 *Let $q : X = \mathbb{Z}^r \to \mathbb{Z}$ be an integral quadratic form such that (X,q) contains a hyperbolic plane H. If $q' = -q_{|H^\perp}$ is positive definite, then q_θ is positive definite, for all $\theta \in \mathcal{P}(X,q)$.*

Proof. Let $\{x_1, x_2\}$ be a hyperbolic basis of H and let $\theta_1 = x_1 + x_2$. Then $\theta_1 \in \mathcal{P}(X,q)$ and by Proposition 23 we know that $q_{\theta_1} \sim x^2 + 4q'$ is positive definite. Now if $\theta \in \mathcal{P}(X,q)$, then $q_\theta \sim_\infty q_{\theta_1}$ by Proposition 18 (with $R = \mathbb{R}$), and so q_θ is also positive-definite.

For further applications of the above proposition, we shall use the following fundamental Cancellation Theorem in the theory of quadratic modules:

Proposition 25 *Suppose that $R = \mathbb{Z}_p$ (or that $R = \mathbb{R}$) and that $q : X = R^r \to R$ is a quadratic form with $\Delta(q) \neq 0$. If H_1 and H_2 are two hyperbolic planes in (X,q), then their orthogonal complements are isometrically isomorphic.*

Proof. If p is odd (or if $R = \mathbb{R}$), then this follows form the general Cancellation Theorem (O'Meara[16], Theorem 92:3) because H_1 and H_2 are isomorphic. (Here we do not require that H_1 and H_2 are hyperbolic planes.) If $p = 2$, then this is Theorem 93:14 of O'Meara[16], p. 256.

Corollary 26 *If q_1 and q_2 are two integral quadratic forms in r variables with $\Delta(q_i) \neq 0$ such that $xy \perp q_1 \sim xy \perp q_2$, then q_1 and q_2 are genus-equivalent.*

Proof. By Proposition 25 we know that $q_1 \sim_p q_2$ are p-adically equivalent for all primes p (including $p = \infty$), so q_1 and q_2 are genus-equivalent.

Remark 27 The converse of this corollary is also true, as is mentioned in Conway and Sloane[4], p. 378 (without proof). Thus, q_1 and q_2 are genus-equivalent if and only if $xy \perp q_1 \sim xy \perp q_2$. (To prove the converse, note that $c(xy \perp q_1) = 1$, which follows from Theorem 1(iii) of [19] by observing that xy and hence $xy \perp q_1$ is universal.)

From this, together with Proposition 23, we can conclude that the quadratic modules in $\Theta(X,q)'$ are all 2-adically isomorphic (and hence lie in the same genus).

Corollary 28 *If $q : X = \mathbb{Z}_2^r \to \mathbb{Z}_2$ is a 2-adic quadratic form with $\Delta(q) \neq 0$, then $(\bar{X}_{\theta_1}, \bar{q}_{\theta_1}) \simeq (\bar{X}_{\theta_2}, \bar{q}_{\theta_2})$, for all $\theta_1, \theta_2 \in \mathcal{P}(X,q)'$.*

Proof. By Lemma 21 and Proposition 23 we know that there exist hyperbolic planes H_i in (X,q) such that $(\bar{X}_{\theta_i}, \bar{q}_{\theta_i}) \simeq \langle 1\rangle_R \oplus (H_i^{\perp}, -4q_{|H_i^{\perp}})$, for $i = 1, 2$. By the Cancellation Theorem (Proposition 25) we know that $(H_1^{\perp}, q_{|H_1^{\perp}}) \simeq (H_2^{\perp}, q_{|H_2^{\perp}})$, so also $(H_1^{\perp}, -4q_{|H_1^{\perp}}) \simeq (H_2^{\perp}, -4q_{|H_2^{\perp}})$, and hence $(\bar{X}_{\theta_1}, \bar{q}_{\theta_1}) \simeq (\bar{X}_{\theta_2}, \bar{q}_{\theta_2})$.

Proof of Theorem 20. Let $\theta_1, \theta_2 \in \mathcal{P}(\mathbb{Z}^r, q)'$. Then by Corollaries 19 and 28 we have that $\bar{q}_{\theta_1} \sim_p \bar{q}_{\theta_2}$, for all primes p (including $p = \infty$), and so $\bar{q}_{\theta_1}$ and $\bar{q}_{\theta_2}$ are genus equivalent. This proves (20).

Now suppose that $\exists \theta_0 \in \mathcal{P}(X,q)$ such that $1 \in \bar{q}_{\theta_0}$. Then by Proposition 23 we know that there exists a hyperbolic plane $H = \mathbb{Z}x_1 + \mathbb{Z}x_2$ in (X,q).

Let $\theta \in \mathcal{P}(X,q)^{odd}$. Then we can write $\theta = n_1x_1 + n_2x_2 + y$ with $n_1, n_2 \in \mathbb{Z}$ and $y \in H^{\perp}$. Note that for any $x = m_1x_1 + m_2x_2 + x^{\perp} \in X$ we have by (23) that

$$\beta_q(x,\theta) \;=\; n_1m_2 + n_2m_1 + \beta_q(x^{\perp}, y). \tag{28}$$

To show that $\theta \in \mathcal{P}(X,q)'$, we distinguish two cases.

Case 1: $n_1 \equiv 1 \,(\mathrm{mod}\ 2)$ or $n_2 \equiv 1 \,(\mathrm{mod}\ 2)$.

Assume first that $n_1 \equiv 1 \,(\mathrm{mod}\ 2)$. Then by (28) we have $\beta_q(x_1, \theta) = n_1$, so $q_\theta(x_2) = \beta_q(x_1,\theta)^2 - 4q(x_1) = n_1^2 - 0 = n_1^2 \equiv 1 \,(\mathrm{mod}\ 8)$. Thus $\theta \in \mathcal{P}(X,q)'$. Similarly, if $n_2 \equiv 1 \,(\mathrm{mod}\ 2)$, then $\theta \in \mathcal{P}(X,q)'$.

Case 2: $n_1 \equiv n_2 \equiv 0 \,(\mathrm{mod}\ 2)$.

By hypothesis, $\exists x_0 \in X$ such that $\beta_q(x_0, \theta) \equiv 1 \,(\mathrm{mod}\ 2)$. By (24) we have $x_0 = (x_0)_H + x_0^{\perp}$ with $(x_0)_H \in H$ and $x^{\perp} \in H^{\perp}$, and by (28) we see that $b := \beta_q(x_0^{\perp}, \theta) \equiv \beta_q(x_0, \theta) \equiv 1 \,(\mathrm{mod}\ 2)$. Thus, if we put $x' = x_1 - q(x_0^{\perp})x_2 \in H$ and $x = x' + x_0^{\perp}$, and $m_i = \beta_q(x, x_i)$, then $\beta_q(x,\theta) = n_1m_1 + n_2m_2 + b \equiv b \equiv 1 \,(\mathrm{mod}\ 2)$. Moreover, since $q(x') = 1(-q(x_0^{\perp})) = -q(x_0^{\perp})$, we have that $q(x) = q(x') + q(x_0^{\perp}) = -q(x_0^{\perp}) + q(x_0^{\perp}) = 0$. Thus $q_\theta(x) = \beta_q(x,\theta)^2 - 4q(x) = b^2 - 0 = b^2 \equiv 1 \,(\mathrm{mod}\ 8)$, and so $\theta \in \mathcal{P}(X,q)'$.

From the above two cases we see that $\mathcal{P}(X,q)^{odd} \subset \mathcal{P}(X,q)'$. Since the opposite inclusion is trivial, we thus have that $\mathcal{P}(X,q)^{odd} = \mathcal{P}(X,q)'$, and the theorem follows.

In view of what was proved above, the last part of Theorem 20 can also be stated in the following way.

Corollary 29 *If $q : X = \mathbb{Z}^r \to \mathbb{Z}$ is an integral quadratic form with $\Delta(q) \neq 0$, and if (X,q) contains a hyperbolic plane H, then $\Theta(X,q)^{odd} \subset \mathrm{gen}(1 \perp (4q'))$, where $q' = -q_{|H^{\perp}}$.*

Proof. Let x_1, x_2 be a hyperbolic basis of H and put $\theta_0 = x_1 + x_2$. Then $\theta_0 \in \mathcal{P}(X,q)$ and by Proposition 23 we know that $\bar{q}_{\theta_0} \sim 1 \perp (4q')$, and so the corollary follows from Theorem 20.

In the case that $r = 3$, a much stronger result than Corollary 29 was proved in [11], §5. Indeed, by using the composition theory of binary quadratic forms (and a precise classification of the binary quadratic forms $\bar{q}_\theta$), it was shown there that in fact equality holds in (20). While the argument there does not carry over to arbitrary r, it does yield the following useful general result (Proposition 30) which shows that equality holds in (20) in the case that $r = 2$.

In order to state this result, we first introduce the following (well-known) concept:

Definition. If (X, q) and (X', q') are two quadratic R-modules, then we say that (X, q) *represents* (X', q') if there exists an injective R-module homomorphism $\varphi : X' \hookrightarrow X$ such that $q' = q \circ \varphi$. If φ can be chosen such that in addition $X/\varphi(X')$ is R-torsionfree, then we say that (X, q) *primitively represents* (X', q') and write $(X, q) \to (X', q')$ or $q \to q'$.

Proposition 30 *Let $q : X = \mathbb{Z}^r \to \mathbb{Z}$ be an integral quadratic form with $q \to xy - dz^2$, where $d \geq 1$. If $q_0 \in \mathrm{gen}(x^2 + 4dy^2)$ or if $q_0 \in \mathrm{gen}(4x^2 + 4xy + (d-1)y^2)$ and $d \equiv 3 \pmod 4$, then there is a $\theta \in \mathcal{P}(X, q)$ such that $\bar{q}_\theta \to q_0$.*

Proof. Since $q \to xy - dz^2$, there is a submodule X' of X such that X/X' is torsionfree and such that $(X', q_{|X'}) \simeq (\mathbb{Z}^3, xy - dz^2)$. Thus, X' has a basis $\{x_1, x_2, x_3\}$ such that $H = \mathbb{Z}x_1 + \mathbb{Z}x_2$ is a hyperbolic plane and $x_3 \in H^\perp$ satisfies $q(x_3) = -d$.

By Proposition 15 of [11], there exists $s = (n_1, n_2, k) \in \mathbb{Z}^3$ with $n_1 n_2 - dk^2 = 1$ such that $q_0 \sim q_s := n_2^2 x^2 - 2k(t-d)xy + n_1^2 t y^2$, where $t = d(n_1 n_2 + 3)$. (Note that although the case that $q_0 \sim x^2 + 4y^2$ was excluded in that result, we can include it here by taking $s = (1, 1, 0)$.) Put $\theta = n_1 x_1 + n_2 x_2 + k x_3 \in X'$. Then $\theta \in \mathcal{P}(X', q') \subset \mathcal{P}(X, q)$, and the proof of Proposition 28 of [11] shows that $q_\theta \to q_s \sim q_0$.

For convenience of the reader, we recall the proof here. Put $y = kdx_2 + n_1 x_3$. Then $x_2 = n_1\theta - ky - n_1^2 x_1$ and $x_3 = n_2 y - kd\theta + n_1 k d x_1$, so $\{x_1, \theta, y\}$ is another basis of X'. Thus, if $\bar{x}_1 := \pi_\theta(x)$ and $\bar{y} := \pi_\theta(y)$, then $\{\bar{x}_1, \bar{y}\}$ is a basis of $\bar{X}' := \pi_\theta(X')$.

Next we observe that $\beta_q(mx_1 + ny, \theta) = n_2 m - n_1 k d n$ and $q(mx_1 + ny) = kdmn - n_1^2 d n^2$, and so $q_\theta(mx + ny) = \beta_q(mx + ny, \theta)^2 - 4q(mx + ny) = n_2^2 m^2 - 2kd(n_1 n_2 + 2)mn + n_1^2 d(k^2 d + 4)n^2 = q_s(m, n)$; here we used the fact that $k^2 d + 4 = n_1 n_2 + 3$ by equation (5) of [11]. From this we see that $(\bar{q}_\theta)_{|\bar{X}'} \sim q_s \sim q_0$, and so $\bar{q}_\theta \to q_0$ because $\bar{X}/\bar{X}' \simeq X/X'$ is torsionfree.

Remark 31 The above proof of Proposition 30 actually yields the following more precise statement: *if X' is a submodule of X such that X/X' is torsionfree and $q_{|X'} \sim xy - dz^2$, then $\exists \theta \in X' \cap \mathcal{P}(X, q)$ such that $(\mathbb{Z}^2, q_0) \simeq (\bar{X}', (\bar{q}_\theta)_{|\bar{X}'})$, where $\bar{X}' = \pi_\theta(X')$.*

In addition, we note that if we write $\theta = \theta_H + k x_3$ with $\theta_H \in H = \mathbb{Z}x_1 + \mathbb{Z}x_2$, then it follows from Lemma 16 of [11] that $q_0 \in \mathrm{gen}(x^2 + 4dy^2) \Leftrightarrow \theta_H \notin 2H$.

We will use the above result to show that (under suitable hypotheses) there exists a $\theta \in \mathcal{P}(X,q)$ such that $q_\theta \not\to 1$. We begin by characterizing the trivial case that $\theta \in \mathcal{P}(X,q)^{ev}$; recall that by Remark 11 we know that for such a θ we have $q_\theta \not\to 1$.

Proposition 32 *Let $q : X = \mathbb{Z}^r \to \mathbb{Z}$ be an integral quadratic form, and suppose that (X,q) contains a hyperbolic plane H with complement $X' = H^\perp$. Write $q' = -q_{|X'}$. Then $\mathcal{P}(X,q)^{ev} \neq \emptyset$ if and only if*

$$(29) \quad \exists x' \in X' \text{ with } q'(x') \equiv 3 \,(\mathrm{mod}\ 4) \text{ and } \beta_{q'}(x', x'') \equiv 0 \,(\mathrm{mod}\ 2), \forall x'' \in X'.$$

Proof. Let $\{x_1, x_2\}$ be a hyperbolic basis of H, and let $\theta \in \mathcal{P}(X,q)$. Then $\theta = n_1x_1 + n_2x_2 + x'$ with $n_1, n_2 \in \mathbb{Z}$ and $x' \in X' = H^\perp$. Moreover, by definition and (23) we have

$$(30) \quad \theta \in \mathcal{P}(X,q)^{ev} \quad \Leftrightarrow \quad n_1 \equiv n_2 \equiv 0 \,(\mathrm{mod}\ 2) \text{ and } \beta_{q'}(x', x'') \equiv 0 \,(\mathrm{mod}\ 2).$$

Thus, if $\theta \in \mathcal{P}(X,q)^{ev}$, then $n_1 \equiv n_2 \equiv 0 \,(\mathrm{mod}\ 2)$ and so $1 = q(\theta) = n_1n_2 - q'(x') \equiv -q'(x') \,(\mathrm{mod}\ 4)$, which shows that (29) holds.

Conversely, suppose that $x' \in X'$ satisfies condition (29). Then $-q'(x') = 1 + 4m$ with $m \in \mathbb{Z}$, and so $\theta := 2x_1 + 2mx_2 + x'$ satisfies $q(\theta) = 1$, and from (30) we see that $\theta \in \mathcal{P}(X,q)^{ev}$.

Remark 33 It is clear that if $q'(x) = mx^2$, then q' satisfies condition (29) if and only if $m \equiv 3 \,(\mathrm{mod}\ 4)$.

Similarly, if $q'(x,y) = ax^2 + bxy + cy^2$, then q' satisfies condition (29) if and only if $\Delta(q') = b^2 - 4ac \equiv 0 \,(\mathrm{mod}\ 4)$ and $q'(r,s) \equiv 3 \,(\mathrm{mod}\ 4)$ for some $r, s \in \mathbb{Z}$.

Indeed, if this latter condition holds, then $b \equiv 0 \,(\mathrm{mod}\ 2)$ and then (29) holds for $x' = (r,s) \in \mathbb{Z}^2 = X'$ because $\beta_{q'}((r,s),(m,n)) = 2arm + bsm + brn + 2csn \equiv 0 \,(\mathrm{mod}\ 2)$, for all $m, n \in \mathbb{Z}$. Conversely, suppose that (29) holds for $x' = (r,s) \in \mathbb{Z}^2 = X'$. Since $\beta_{q'}((r,s),(m,n)) = 2arm + bsm + brn + 2csn \equiv 0 \,(\mathrm{mod}\ 2)$, for all $m, n \in \mathbb{Z}$, we see that either $b \equiv 0 \,(\mathrm{mod}\ 2)$ or $r \equiv s \equiv 0 \,(\mathrm{mod}\ 2)$. However, in the latter case $q'(x') \equiv 0 \,(\mathrm{mod}\ 4)$, contradiction. Thus $b \equiv 0 \,(\mathrm{mod}\ 2)$ and hence $\Delta(q') \equiv 0 \,(\mathrm{mod}\ 4)$.

We now turn to investigate when $q_\theta \not\to 1$ in the case that $\theta \in \mathcal{P}(X,q)^{odd}$. The following result suffices for our purposes.

Proposition 34 *Let $q : X = \mathbb{Z}^r \to \mathbb{Z}$ be an integral quadratic form, and suppose that (X,q) contains a hyperbolic plane H with complement $X' = H^\perp$. Suppose that $q' := -q_{|X'}$ is a positive-definite binary quadratic form, and that $\theta \in \mathcal{P}(X,q)$ has the form $\theta = \theta_H + k\theta^\perp$, where $\theta_H \in H$, $k \in \mathbb{Z}$ and $\theta^\perp \in X'$ is primitive. If $a := q'(\theta^\perp) \leq |\Delta(q')|$, then*

$$(31) \qquad q_\theta \to 1 \quad \Leftrightarrow \quad q_\theta(y) = 1, \quad \text{for some } y \in H + \mathbb{Z}\theta^\perp,$$

except in the case that $a = |\Delta(q')| \equiv 3 \,(\mathrm{mod}\ 4)$, $\theta_H \in 2H$ and $q' \sim ax^2 \pm axy + \frac{a+1}{4}y^2$.

The proof of this will be based on the following elementary identity.

Lemma 35 *Suppose (X,q) contains a hyperbolic plane H. Let $\theta \in \mathcal{P}(X,q)$, and write $\theta = \theta_H + k\theta^\perp$ where $\theta_H \in H$, $\theta^\perp \in H^\perp$ and $k \in \mathbb{Z}$. If $a := q(\theta^\perp)$, then*

$$4a^2 q_\theta(x+y) = q_\theta(2ax + \beta_q(y,\theta^\perp)\theta^\perp) + 4ad(y), \tag{32}$$

for all $x \in H + \mathbb{Z}\theta^\perp$ and $y \in H^\perp$, where $d(y) = \beta_q(y,\theta^\perp)^2 - 4q(\theta^\perp)q(y)$.

Proof. Put $H_\theta = H + \mathbb{Z}\theta^\perp$. We first observe that

$$q_\theta(x+z) \ = q_\theta(x) - 4q(z), \quad \text{if } x \in H_\theta,\ z \in (H_\theta)^\perp \tag{33}$$

because $q_\theta(x+z) = \beta_q(x+z,\theta)^2 - 4q(x+z) = \beta_q(x,\theta)^2 - 4q(x) - 4q(z) = q_\theta(x) - 4q(z)$.

Now let $x \in H_\theta$ and $y \in H^\perp$, and put $z = 2ay - b\theta^\perp \in H^\perp$, where $b = \beta_q(y,\theta^\perp)$. Then $\beta_q(z,\theta^\perp) = 0$, and so $z \in (H_\theta)^\perp$. Moreover, $q(z) = -ad(y)$ because $4a^2q(y) = q(2ay) = q(z+b\theta^\perp) = q(z) + q(b\theta^\perp) = q(z) + ab^2$. Thus, if we put $\tilde{x} = 2ax + b\theta^\perp \in H_\theta$, then $\tilde{x} + z = 2a(x+y)$ and so by (33) we obtain $4a^2 q_\theta(x+y) = q_\theta(\tilde{x}+z) = q_\theta(\tilde{x}) - 4q(z) = q_\theta(\tilde{x}) + 4ad(y)$, which proves (32).

Proof of Proposition 34. Since $\theta^\perp$ is primitive in X', there exists $x' \in X'$ such that $\{\theta^\perp, x'\}$ is a basis of X'. Put $b = -\beta_{q'}(\theta^\perp, x') = \beta_q(\theta^\perp, x')$ and $c = q'(x')$; then $\Delta(q') = (-b)^2 - 4ac = d(x')$ (in the notation of Lemma 35). Note that we can assume without loss of generality that $|b| \le a$ by replacing x' by $x' + nx$, for a suitable $n \in \mathbb{Z}$ (because $\beta_{q'}(\theta^\perp, x' + nx) = 2na - b$).

Suppose $q_\theta(x) = 1$ for some $x \in X$. Write $x = x_H + m\theta^\perp + nx'$ with $m,n \in \mathbb{Z}$, and put $\tilde{x} = x_H + m\theta^\perp \in H_\theta = H + \mathbb{Z}\theta^\perp$. Since $d(nx') = n^2 d(x') = n^2\Delta(q') = -n^2|\Delta(q')|$, it follows from (32) (applied to $(\tilde{x}, nx', -a)$ in place of (x,y,a)) that

$$4a^2 \ = \ 4a^2 q_\theta(x) \ = \ q_\theta(-2a\tilde{x} + nb\theta^\perp) \ + \ 4an^2|\Delta(q')| \ \ge \ 4an^2|\Delta(q')|, \tag{34}$$

where the last inequality follows from fact that q_θ is positive definite (cf. Corollary 24). We thus see that if $a < |\Delta(q')|$, then $n^2 < 1$ and so $n = 0$ and $x = \tilde{x} \in H_\theta$. This proves (31) in this case.

If $a = |\Delta(q')|$ and $n \neq 0$, then (34) shows that $n = \pm 1$ and $q_\theta(-2a\tilde{x} + nb\theta^\perp) = 0$, so $-2a\tilde{x} + nb\theta^\perp = t\theta$, for some $t \in \mathbb{Z}$ because $\bar{q}_\theta$ is positive definite. To analyze this equation, let $\{x_1, x_2\}$ be a hyperbolic basis of H and write $x_H = m_1x_1 + m_2x_2$ and $\theta = n_1x_1 + n_2x_2 + k\theta^\perp$. Then the identity $-2a\tilde{x} + nb\theta^\perp = t\theta$ is equivalent to the three equations

$$-2am_1 \ = \ tn_1, \quad -2am_2 \ = \ tn_2, \quad -2am + nb \ = \ tk.$$

Since $q(\theta) = n_1n_2 - k^2a = 1$, we see from the first two equations that $n_i | 2m_i$, for $i = 1,2$, and so $a|t$. Thus, the third equation yields that $a|nb = \pm b$. Since $|b| \le a$, this is only possible if $b = 0$ or $b = \pm a$. Now $b \neq 0$ because otherwise $a = |\Delta(q')| = 4ac$,

contradiction. Thus $b = \pm a$, so $c = \frac{|\Delta(q')|+b^2}{4a} = \frac{a+a^2}{4a} = \frac{1+a}{4}$, and hence $a \equiv 3 \pmod 4$ and $q' \sim ax^2 \pm axy + \frac{1+a}{4}y^2$. Moreover, from the third equation we now see that tk and hence t is odd, so the first two equations show that n_1 and n_2 are even. This means that $\theta_H \in 2H$, and so we are in the exceptional case, contradiction. Thus $n = \pm 1$ is not possible, and hence $n = 0$. This proves (31).

Note that the above results yield the implication (iii) $\Rightarrow$ (iv) of Theorem 13:

Corollary 36 *Suppose $q = xy \perp (-q')$, where q' is a positive definite binary quadratic form. If q' is not a special idoneal-valued form, then there exists $\theta \in \mathcal{P}(\mathbb{Z}^4, q)$ such that $q_\theta \not\to 1$.*

Proof. By hypothesis, $X = \mathbb{Z}^4 = H \oplus X'$, where H is a hyperbolic plane, $X' = H^\perp$ and $q_{|X'} = -q'$. Since q' is not a special idoneal-valued form, we have the following three possibilities:

Case 1: $\Delta(q') \equiv 0 \pmod 4$ and $q' \to n \equiv 3 \pmod 4$.

From Proposition 32 together with Remark 33 it follows that in this case $\exists \theta \in \mathcal{P}(X, q)^{ev}$, and so $q_\theta \not\to 1$ by Remark 11.

Case 2: $q' \to n \equiv 3 \pmod 4$ and $n < |\Delta(q')|$.

Let $x' \in X'$ be such that $q'(x') = n$, and put $X'' = H + \mathbb{Z}x'$. Note that $X/X'' \simeq X'/\mathbb{Z}x'$ is torsionfree since x' is primitive (by hypothesis). Moreover, since $q_{|X''} \sim xy - nz^2$, we see that $q \to xy - nz^2$. Let $q_0 := 4x^2+4xy+(n+1)y^2$. Then by Proposition 30 and Remark 31 we have that $\exists \theta \in X'' \cap \mathcal{P}(X, q)$ such that $(\bar{X}'', (\bar{q}_\theta)_{X''}) \simeq (\mathbb{Z}^2, q_0)$, where $\bar{X}'' = \pi_\theta(X'')$. Since $q_0(x) \equiv 0 \pmod 4$ for all $x \in \mathbb{Z}^2$, we see that $q_\theta(x'') \neq 1$, for all $x'' \in X''$, and so by Proposition 34 it follows that $q_\theta \not\to 1$.

Case 3: $q \to n$, $n \leq |\Delta(q')|$ and $4n$ is not idoneal.

Since $4n$ is not idoneal, we have that $c(x^2 + 4ny^2) > 1$, so $\exists q_0 \in \mathrm{gen}(x^2 + 4ny^2)$ with $q_0 \not\to 1$. Then by the same argument (and notation) as in Case 2, there exists $\theta \in X'' \cap \mathcal{P}(X, q)$ such that $(\bar{X}'', (\bar{q}_\theta)_{X''}) \simeq (\mathbb{Z}^2, q_0)$. Thus, $q_\theta(x'') \neq 1, \forall x'' \in X''$. Since $\theta_H \notin 2H$ by Remark 31, it follows from Proposition 34 that $q_\theta \not\to 1$.

5 Idoneal-valued quadratic forms

By the previous Corollary 36 we see that the hypothesis of Problem 10 (for $r = 2$) naturally leads to the condition that q is a special idoneal-valued binary quadratic form, or, more briefly, a *special form*.

We shall now classify the special forms $q(x, y) = ax^2 + bxy + cy^2$ and begin by classifying those whose *content* $\mathrm{cont}(q) = \gcd(a, b, c)$ is odd.

Proposition 37 *Let q be a special form with* $\mathrm{cont}(q) \equiv 1 \pmod 2$. *Then q is equivalent to one of the following four forms $f(x,y) = ax^2 + bxy + cy$ whose coefficients (a,b,c) are in the list $\mathcal{L}_1 = \{(1,1,1),(1,0,1),(1,1,2),(1,1,3)\}$.*

Remark 38 The above Proposition 37 is all that is needed to deduce (a generalization of) of the existence theorem of Hayashida and Nishi[7]. Indeed, if we assume that $\mathrm{End}(E_i) \simeq \mathfrak{O}_F$ is a maximal order of an imaginary quadratic field F of discriminant $-d$, then by [13], Corollary 39, we know that $q = q_{E_1,E_2}$ is a form of discriminant $-d$ and content $\mathrm{cont}(q) = 1$. Thus, if $E_1 \times E_2$ does not contain a curve of genus 2, then by Corollary 8 and Corollary 36 we know that q is special, and so by Proposition 37 we have that $d = 3, 4, 7, 15$ and that $E_1 \simeq E_2$ (and that the same is result true if the conductors of E_i are odd). This, therefore, proves the existence part of the theorem in [7], p. 14.

Note that the above proof is quite different from that of [7] because here we consider the problem of whether the (positive definite) *ternary* forms Q_θ represent 1 whereas Hayashida and Nishi consider the problem of determining whether specific numbers are represented by certain (positive definite) *quaternary* forms; cf. [7], p. 10. Note that if $\mathrm{cont}(q_{E_1,E_2}) > 1$, then it is questionable whether their criterion (for the existence of genus 2 curves) still holds, and so their method cannot be adapted readily to the more general case.

In order to prove Proposition 37 and other related results, it is useful to introduce the following notation.

Notation. If $q(x,y) = ax^2 + bxy + cy^2$ is a positive definite binary quadratic form, then we write $q = [a,b,c]$. Moreover, we let $\mathcal{R}(q) = \{n \in \mathbb{Z} : q \to n\}$ denote the set of values which are primitively represented by q. Furthermore, we let

$$\mathcal{R}'(q) = \{n \in \mathcal{R}(q) : n < |\Delta(q)|\} \quad \text{and} \quad \mathcal{R}^*(q) = \{n \in \mathcal{R}(q) : n \leq |\Delta(q)|\}.$$

Lemma 39 *If $q = [a,b,c]$ is reduced, then $a, c \in \mathcal{R}'(q)$ and $a \pm b + c \in \mathcal{R}^*(q)$. Moreover, $a \pm b + c \in \mathcal{R}'(q)$ except when $a = b = c = 1$.*

Proof. Put $d = |\Delta(q)|$. Since q is reduced, we have $a \leq \sqrt{d/3} < d$ and $c \leq \frac{1}{4}(\sqrt{d/3} + d) \leq \frac{d}{2} < d$ (cf. e.g. [3], p. 184), so $a = q(1,0) \in \mathcal{R}'(q)$ and $c = q(0,1) \in \mathcal{R}'(q)$. Furthermore, $q(1,\pm 1) = a \pm b + c \leq 2a + c \leq 2\sqrt{d/3} + \frac{1}{4}\sqrt{d/3} + \frac{1}{4}d = \frac{9}{4}\sqrt{d/3} + \frac{1}{4}d \leq d$, and equality holds only if $\sqrt{d/3} = d/3$, i.e. $d = 3$. Thus, $a \pm b + c \in \mathcal{R}'(q)$ except when $d = 3$ (and then $q = [1,1,1]$ because this is the only reduced form with $\Delta(q) = -3$).

We next recall some elementary properties of idoneal numbers. For this, it is useful to introduce the following notation.

Notation. Let $I = \{n \geq 1 : c(x^2 + ny^2) = 1\}$ denote the set of idoneal numbers, and put

$$\tilde{S} = \{n : 4n \in I\} \quad \text{and} \quad S = \{n : 4n \in I, n \not\equiv 3 \,(\mathrm{mod}\, 4)\}.$$

We call S the set of *special* idoneal numbers.

Remark 40 If q is a positive definite binary quadratic form, then

(35) $\quad q$ is a special idoneal-valued form $\quad \Leftrightarrow \quad \mathcal{R}'(q) \subset S$ and $\mathcal{R}^*(q) \subset \tilde{S}$.

Indeed, if q is special, then the first condition of the definition is equivalent to the inclusion $\mathcal{R}^*(q) \subset \tilde{S}$. Moreover, since $q \not\to n \equiv 3 \,(\mathrm{mod}\, 4)$, if $n < |\Delta(q)|$, we also have $\mathcal{R}'(q) \subset S$. Conversely, if $\mathcal{R}'(q) \subset S$ and $\mathcal{R}^*(q) \subset \tilde{S}$, then it is clear that q is special if $\Delta(q) \equiv 1 \,(\mathrm{mod}\, 4)$. Thus, assume $\Delta(q) \equiv 0 \,(\mathrm{mod}\, 4)$, and (without loss of generality) that $q = [a, b, c]$ is reduced. Then $a, c, a \pm b + c \in \mathcal{R}'(q) \subset S$ (by Lemma 39) and $2|b$. Thus, either $2|\mathrm{cont}(q)$ or $(a, b, c) \equiv (0, 0, 1), (1, 0, 0), (1, 0, 1), (1, 2, 1), (1, 2, 2), (2, 2, 1) \,(\mathrm{mod}\, 4)$. In all these cases we see that q does not represent any number $n \equiv 3 \,(\mathrm{mod}\, 4)$, and so q is special.

The following properties of idoneal numbers are essentially due to Euler and Grube[5].

Lemma 41 (a) *If $n \in S$ and $n > 1$, then $n \equiv 2, 4, 6 \,(\mathrm{mod}\, 8)$. Moreover, if $S_{kn} := \{n \in S : n \leq 10^5\}$ denotes the set of "known" special idoneal numbers, then*

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

(b) *If $n \in I$ and $n \equiv 3 \,(\mathrm{mod}\, 4)$, then $n = 3, 7, 15$. In particular, $\tilde{S} = S \cup \{3, 7, 15\}$.*

(c) *If $n \in S$ and $n > 60$, then n is squarefree. Thus*

$$S_4 := \{n \in S : 4|n\} \;=\; \{4, 12, 28, 60\}.$$

Proof. (a) This follows immediately from Euler's results; cf. Theorem 1 and Corollary 10 of [12]. (See also [11].)

(b) The first assertion is due to Grube; cf. [12], Corollary 8. The second assertion follows from this and Euler's result ([12], Corollary 10(b)).

(c) Since $n \not\equiv 0 \,(\mathrm{mod}\, 8)$ by (a), it follows from Grube's Theorem ([12], Theorem 12) that n is squarefree when $n > 60$. If $n \in S_4$, then $n \equiv 4 \,(\mathrm{mod}\, 8)$ (because $n \not\equiv 0 \,(\mathrm{mod}\, 8)$), so $n \in S_4 \Leftrightarrow n \in \{4, 12, 28, 60\}$ by Grube (cf. [12], Theorem 12(c)).

Corollary 42 *The form q is not special if any one of the following conditions hold:*

(i) $\exists n \in \mathcal{R}'(q)$ *with* $n \equiv 1 \,(\mathrm{mod}\, 2)$ *and* $n > 1$;

(ii) $q = [a, b, c]$ *is reduced and one of a, b, c is an odd number $\neq 1$;*

(iii) $1 \in \mathcal{R}(q)$, $\Delta(q) \equiv 0 \,(\mathrm{mod}\, 4)$, *and* $\Delta(q) \neq -4$;

(iv) $1 \in \mathcal{R}(q)$, $\Delta(q) \equiv 1 \,(\mathrm{mod}\, 4)$ *but* $\Delta(q) \not\equiv 1 \,(\mathrm{mod}\, 8)$ *and* $\Delta(q) \neq -3$.

Proof. (i) Since $n \notin S$ by Lemma 41(a), we have $\mathcal{R}'(q) \not\subset S$, and hence q cannot be special (cf. (35)).

(ii) Since $a, c \in \mathcal{R}'(q)$ by Lemma 39, it follows from (i) that q cannot be special if $a \neq 1$ is odd or if $c \neq 1$ is odd. Now suppose that $b \neq 1$ is odd. Then $c \geq a \geq |b| \geq 3$, so if a or c are odd, then we are done. If not, then $a + |b| + c \in \mathcal{R}'(q)$ is odd, and so q is not special by (i).

(iii) If $1 \in \mathcal{R}(q)$ and $\Delta(q) = -4d$, then $q \sim q_1 := [1, 0, d]$. If $d > 1$ and odd, then q_1 and hence q are not special by (ii). If d is even, then $1 + 0 + d \in \mathcal{R}'(q)$ is odd, and so q_1 and q are not special by (i).

(iv) If $1 \in \mathcal{R}(q)$ and $\Delta(q) = -4d + 1$, then $q \sim q_1 := [1, 1, d]$. By hypothesis, $d > 1$ is odd, so q_1 and q are not special by (ii).

Proof of Proposition 37. Let $q \sim q_1 := [a, b, c]$, where q_1 is reduced. Since $\mathrm{cont}(q) = \mathrm{cont}(q_1)$ is odd, at least one of a, b, c must be odd. If $a > 1$ then q is not special because if a or $c \geq a$ is odd, then we are done by Corollary 42(ii), and if a and c are even, then $a + |b| + c \in \mathcal{R}'(q)$ is odd, so we are done by Corollary 42(i). Thus, assume that $a = 1$. If $\Delta(q) \equiv 0 \,(\mathrm{mod}\, 4)$, then $q \sim [1, 0, 1]$ by Corollary 42(iii), and if $\Delta(q) \equiv 1 \,(\mathrm{mod}\, 4)$ but $\Delta(q) \not\equiv 1 \,(\mathrm{mod}\, 8)$ then $q \sim [1, 1, 1]$ by Corollary 42(iv).

Thus, assume that $\Delta(q) \equiv 1 \,(\mathrm{mod}\, 8)$. Then $q \sim q_1 = [1, 1, d]$ with $d \equiv 0 \,(\mathrm{mod}\, 2)$. Thus $4d - 1 = q_1(1, -2) \in \mathcal{R}^*(q) \subset \tilde{S}$, and so $4d - 1 \in \{3, 7, 15\}$ by Lemma 41. Thus $d = 1, 2$, or 4, and the assertion follows.

In view of Proposition 37, this leaves us to classify the special forms whose content is even. If, in fact, $4|\mathrm{cont}(q)$, then the answer is simple.

Proposition 43 *If q is special and $4|\mathrm{cont}(q)$, then $q \sim [4, 4, 4]$.*

The proof of this is based on the following fact which gives a useful lower bound on the number of elements in $\mathcal{R}'(q)$.

Lemma 44 *Let $q = [a, b, c]$ be reduced and $b \geq 0$. If $n \geq 1$ satisfies the inequality*

$$n(n+1) \;<\; c(3 - 1/a) + c - b, \tag{36}$$

then $q(k, \pm 1) \in \mathcal{R}'(q)$, for $0 \leq k \leq n$. Thus

$$\#\mathcal{R}'(q) \;\geq\; n + 1 \quad \textit{and even} \quad \#\mathcal{R}'(q) \;\geq 2n + 1, \quad \textit{if } a > b > 0. \tag{37}$$

Proof. For $0 \leq k \leq n$ we have

$$q(k, \pm 1) = ak^2 \pm bk + c \leq an^2 + an + c = an(n+1) + c.$$

Combining this inequality with (36) yields

$$q(k, \pm 1) \leq an(n+1) + c < a(c(3 - 1/a) + c - b) + c = 4ac - ab \leq 4ac - b^2 = |\Delta(q)|,$$

and so $q(k, \pm 1) \in \mathcal{R}'(q)$, as claimed.

Since the $q(k,1)$'s are distinct for $0 \le k \le n$, the first inequality of (37) is clear. The second follows from the fact that the function $q(\pm k, 1) = q(k, \pm 1)$ takes on $2n+1$ distinct values for $0 \le k \le n$ because for $x, y \in \mathbb{Z}$ we have that

$$q(x,1) \;=\; q(y,1) \quad \Leftrightarrow \quad x \;=\; y, \quad \text{provided that } a > b > 0. \tag{38}$$

Indeed, suppose $ax^2 + bx + c = ay^2 + by + c$. Then $ax^2 - by^2 = by - bx$, so if $x \neq y$ then $-a(x+y) = b$. Thus $a|b$ which is impossible since $0 < b < a$.

Proof of Proposition 43. By reduction theory there exists a reduced form $q_1 := [a,b,c]$ with $b \ge 0$ such that $q \sim q_1$ ($\mathrm{GL}_2(\mathbb{Z})$-equivalence). Since $4|\mathrm{cont}(q_1)$, we have $c \ge 4$. If $c = 4$, then also $a = 4$ and $b = 0$ or 4. Thus $q_1 = [4,0,4]$ or $]4,4,4]$. However, since $4 + 0 + 4 = 8 \notin S_4$ by Lemma 41(c), the form $[4,0,4]$ is not special, so only $q_1 = [4,4,4]$ is possible if $c = 4$.

Now assume $c > 4$. Since $c \in S_4$, we have by Lemma 41(c) that $c \ge 12$. Since $4(4+1) = 20 < 12(\frac{11}{4}) \le c(3 - 1/a) + c - b$ (because $a \ge 4$ and $c \ge b$), it follows from Lemma 44 that $q(k,1) \in \mathcal{R}'(q_1)$ for $0 \le k \le 4$. If q_1 were special, then these would give 5 distinct numbers in S_4, which contradicts the fact that $\#S_4 = 4$ by Lemma 41(c). Thus q_1 is not special for $c > 4$.

The above results reduce the classification problem to the case that $\mathrm{cont}(q) \equiv 2 \pmod 4$. Here we first prove:

Proposition 45 *If $q = [a,b,c]$ is a reduced special form with $\mathrm{cont}(q) \equiv 2 \pmod 4$ and $4|c$, then $q = [2,0,4]$.*

Proof. As in the proof of Proposition 43, we may assume that $b \ge 0$.

Suppose first that $c = 4$. If $a = 2$, then $b = 0$ or 2. But $q = [2,2,4]$ is not special since $q(1,1) = 8 \notin S_4$, so we must have $q = [2,0,4]$. If $a > 2$, then $a = 4$ and $b = 2$. But $q = [4,2,4]$ is not special because $q(2,1) = 24 < |\Delta(q)| = 60$ but $24 \notin S_4$.

Thus, assume $c > 4$. Then $c \ge 12$ because $c \in S_4$. If $a = 2$, then $q = [2,0,c]$ or $q = [2,2,c]$. In the first case $q(2,1) = 8 + c < 8c = |\Delta(q)|$, but $8 + c \notin S_4$ (when $c \in S_4$ and $c \ge 12$), so $[2,0,4]$ is not special. Similarly, if $q = [2,2,c]$, then $q(2,-1) = c + 4 < 8c - 4 = |\Delta(q)|$, but $c + 4 \notin S_4$ (when $c \in S_4$ and $c \ge 12$), and so $[2,2,c]$ is not special.

We thus have that $a > 2$, so $a \ge 4$. Then, as in the proof of Proposition 43 we have that $q(k, \pm 1) \in \mathcal{R}'(q)$ for $0 \le k \le 4$. Thus, if q is special, then $q(4,1) \in S_4$ (because $4|q(4,1)$). But $q(4,1) \ge 4^2 a + 4b + c > 4^2 4 = 64 > 60$, so $q(4,1) \notin S_4$, contradiction. Thus q is not special, and so the only possible case is $q = [2,0,4]$.

Proposition 46 *If $q = [a,b,c]$ is a reduced special form with $\mathrm{cont}(q) \equiv 2 \pmod 4$ and $4|a$, then $q = [4,0,6]$.*

Here we shall use the following technical fact.

Lemma 47 *If $q = [a, b, c]$ is reduced, and if $a \geq 2$ and $b \geq 0$, then*

$$q(-1, 2) \in \mathcal{R}'(q), \quad \textit{and also} \quad q(1, 2) \in \mathcal{R}'(q), \quad \textit{if } c > b. \tag{39}$$

Proof. Since $a \geq 2$, it follows that we have

$$(b-1)^2 < (4a-5)c + 1, \quad \text{and even} \quad (b+1)^2 < (4a-5)c + 1, \quad \text{if } c > b. \tag{40}$$

Indeed, if $b = 0$, then this is clear, so assume that $b \geq 1$. Then $3a - 6 \geq 3 \cdot 2 - 6 = 0$, so $b + 1 \leq a + 1 \leq 4a - 5$. Thus $0 \leq b - 1 < b + 1 \leq 4a - 5$ and $0 \leq b - 1 < c$, so $(b-1)^2 < (4a-5)c < (4a-5)c + 1$, which proves the first part of (40). Note that if $c > b$, then $b + 1 \leq c$, so a similar argument shows that the second part of (40) holds.

From the first part of (40) we obtain that $q(-1, 2) = a - 2b + 4c = (b-1)^2 + 4c + a - b^2 + 1 < (4a-5)c + 1 + a - b^2 - 1 = 4ac - b^2 - (c - a) \leq 4ac - b^2$. Thus, $q(-1, 2) < 4ac - b^2 = |\Delta(q)|$, and so $q(-1, 2) \in \mathcal{R}'(q)$. Similarly, if $c > b$, then a similar argument (using the second part of (40)) shows that $q(1, 2) < |\Delta(q)|$, so (39) follows.

Proof of Proposition 46. Note first that $b < c$ for else $q = [a, a, a]$ and then $\text{cont}(q) = a \equiv 0 \pmod 4$, contradiction. Thus, since $a \geq 4$, we have by (39) that $q(1, \pm 2) = a \pm 2b + 4c \in S_4$ (and $a \in S_4$).

If $a \geq 12$, then $q(1, 2) = a + 2b + 4c \geq 5a \geq 60$, so $q(1, 2) \notin S_4$ unless $a = c = 12$ and $b = 0$. But $q = [12, 0, 12]$ is not special since $q(1, 1) = 24 \notin S_4$.

Thus, $a < 12$, and hence $a = 4$ because $a \in S_4$. Then $b = 0$, 2, or 4. Suppose first that $b = 4$. Since $q(\pm 1, 2) \in S_4$ and since $q(1, 2) - q(-1, 2) = 4b = 16$, it follows that $q(-1, 2) = 12$ because $(12, 28)$ is the only pair of numbers in S_4 whose difference is 16. Thus $c = 4$ and so $4 | \text{cont}(q)$, contradiction. Next, suppose $b = 2$. Here we have $q(-1, 2) = 4$ because $(4, 12)$ is the only pair of numbers in S_4 whose difference is $2b = 8$, and so $c = 1$, contradiction.

Thus, only $b = 0$ is possible. Then $q(1, 2) = 4 + 4c \in S_4$, so $4c \in \{8, 25, 56\}$ or $c \in \{2, 6, 14\}$. Now $c = 2 < a$ is impossible. Moreover, since $c = 14 \notin S$ (cf. Lemma 41(a)), we must have $c = 6$, so $q = [4, 0, 6]$, as claimed.

Proposition 48 *Let $q = [a, b, c]$ be a reduced special form with $\text{cont}(q) \equiv 2 \pmod 4$. If $q \not\equiv [2, 2, 2] \pmod 4$, then $q \in \mathcal{L}_0 := \{[2, 0, 2], [2, 0, 4], [4, 0, 6], [6, 0, 6], [2, 0, 10]\}$.*

Proof. If $4|c$ or $4|a$, then $q = [2, 0, 4] \in \mathcal{L}_0$ or $q = [4, 0, 6] \in \mathcal{L}_0$ by Propositions 45 and 46, respectively. Thus, assume $a \equiv c \equiv 2 \pmod 4$. Then $b \equiv 0 \pmod 4$, for otherwise $q \equiv [2, 2, 2] \pmod 4$. Thus, if k is odd, then $q(k, 1) \equiv a + c \equiv 0 \pmod 4$. As before, we may assume that $b \geq 0$.

Suppose first that $c < b + 4$. Then we must have that $a = c = b + 2$, so we can write $q = [4k + 2, 4k, 4k + 2]$, for some integer $k \geq 0$. Since $q(1, \pm 1) \in \mathcal{R}'(d)$ by Lemma 39, we have that $12k + 4 = q(1, 1) \in S_4$ and $4k + 4 = q(1, -1) \in S_4$. This

is only possible for $k = 0$ or $k = 2$. If $k = 2$, then we obtain $q = [10, 8, 10]$. But since $124 = q(3, 1) \in \mathcal{R}'(q)$ (because $124 < |\Delta(q)| = 336$) yet $124 \notin S_4$, we see that $[10, 8, 10]$ cannot be special, and so we must have $k = 0$, and hence $q = [2, 0, 2] \in \mathcal{L}_0$.

Now suppose that $c \geq b + 4$. Then in fact $c \geq b + 6$ because $c \not\equiv b \,(\mathrm{mod}\ 4)$. Since $3(3 + 1) = 12 < 6(\frac{5}{2}) \leq c(3 - \frac{1}{a}) + c - b$, we see from (36) that $q(k, \pm 1) \in \mathcal{R}'(q)$ for $0 \leq k \leq 3$. Now if $b \neq 0$, then $0 < b < a$ (because $b \not\equiv a \,(\mathrm{mod}\ 4)$), and so it follows from (38) that $q(1, \pm 1)$ and $q(3, \pm 1)$ are 4 distinct numbers S_4. But since they are $\geq c \geq 6$, this is impossible.

Thus, $b = 0$. Now $10a \leq 9a + c = q(3, 1) \in S_4$, so $10a \leq 60$ or $a \leq 6$. If $a = 6$, then the inequalities $60 = 10a \leq 9a + c \leq 60$ force that $c = a = 6$, and so $q = [6, 0, 6] \in \mathcal{L}_0$. Thus, assume that $a < 6$. Then $a = 2$ because $a \equiv 2 \,(\mathrm{mod}\ 4)$. Since $18 + c = q(3, 1) \in S_4$, only the cases $c = 28 - 18 = 10$ and $c = 60 - 18 = 42$ are possible. But since $2 + 42 = 44 \notin S_4$, it follows that $[2, 0, 42]$ is not special, and so only $q = [2, 0, 10] \in \mathcal{L}_0$ is possible. This proves the assertion.

By the above results, the only case left to investigate is the case that $q \equiv [2, 2, 2] \,(\mathrm{mod}\ 4)$. The analysis of this case, however, seems to require much deeper results about idoneal numbers than the previous cases. Indeed, we shall use here the following basic fact which will be deduced from the (unconditional!) results of Weinberger[22]:

Theorem 49 *If q is a special idoneal-valued form, then $|\Delta(q)| \leq 10^6$ and hence $\mathcal{R}'(q) \subset S_{kn}$.*

Proof. We first note that if there exists $d^* \in S \setminus S_{kn}$, then by Lemma 41(c) we know that d^* is squarefree and so $-4d^*$ is a fundamental discriminant. By Weinberger[22] we therefore know that d^* is unique and that $4d^* > 10^{11}$. We thus have that

$$\text{either } S = S_{kn} \quad \text{or} \quad S = S_{kn} \cup \{d^*\} \text{ with } d^* > 10^{10}.$$

Thus, if $q = [a, b, c]$ is reduced and special, then by Lemma 39 we have that $a, c, a + |b| + c \in S$. But if $c \in S \setminus S_{kn} = \{d^*\}$, then $a + |b| + c > c = d^*$, so $a + b + c \notin S$, contradiction. Thus, $c \in S_{kn}$, and hence $a \leq c \leq 462$. Thus $|\Delta(q)| \leq 4 \cdot 462^2 < 10^6 < d^*$, and hence $\mathcal{R}'(q) \subset S_{kn}$.

Using this result, we can now prove the following:

Proposition 50 *If $q = [a, 2, c]$ is a reduced special form with $a \equiv c \equiv 0 \,(\mathrm{mod}\ 2)$, then $q \in \mathcal{L}_2 := \{[2, 2, 2], [2, 2, 6], [2, 2, 18]\}$.*

Proof. By Lemma 39 and Theorem 49 we have that $a, c, a + c \pm 2 \in S_{kn}$, and so $a + c - 2 \in T_4 := \{n \in S_{kn} : n + 4 \in S_{kn}\}$. Since S_{kn} is known explicitly (cf. Lemma 41), one checks easily that

$$T_4 \stackrel{\text{def}}{=} \{n \in S_{kn} : n + 4 \in S_{kn}\} \;=\; \{2, 6, 18\}. \tag{41}$$

Thus, $a+c = 4, 8$ or 20. If $a+c=4$, then $2a \le a+c = 4$ and so $a \le 2$. Thus $a = c = 2$ and hence $q = [2,2,2] \in \mathcal{L}_2$.

Next, if $a+c = 8$, then $2a \le a+c = 8$, so $a \le 4$, i.e. $a = 2$ or 4. If $a = 4$, then $q = [4,2,4]$ which is not special by Proposition 45. Thus, $a = 2$ and $q = [2,2,6] \in \mathcal{L}_2$.

We are thus left with the case that $a+c = 20$, so $2a \le a+c = 20$ or $a \le 10$. The cases $a = 4$ and $a = 8$ are not possible by Proposition 46. Moreover, the case $a = 6$ is also not possible because then $c = 14$, but $c \notin S_{kn}$. In addition, $a = 10$ is out because for $q = [10,2,10]$ we have that $54 = q(1,2) \in \mathcal{R}'(q)$ by (39) but $54 \notin S_{kn}$. Thus, only $q = [2,2,18] \in \mathcal{L}_2$ is possible, and the assertion follows.

The last remaining case to be studied is the following.

Proposition 51 *If $q = [a,b,c]$ is a reduced special form with $\mathrm{cont}(q) \equiv 0 \pmod 2$ and $b > 2$, then $q \in \mathcal{L}_3 := \{[k,k,k] : k = 4, 6, 10\}$.*

Proof. First note that if $4|\mathrm{cont}(q)$, then $q = [4,4,4] \in \mathcal{L}_3$ by Proposition 43, so we can assume that $\mathrm{cont}(q) \equiv 2 \pmod 4$. It thus follows from Proposition 48 that $a \equiv b \equiv 2 \pmod 4$, and hence $b \ge 6$ because $b > 2$. Thus also $c \ge a \ge 6$. In addition, we know from Theorem 49 that $\mathcal{R}'(q) \subset S_{kn}$.

Suppose first that $c > 10$. Then $c \ge 18$ because $c \in S_{kn}$ and $c \equiv 2 \pmod 4$. Since $a \ge 6$ we have $42 < 51 = 18(3 - \frac{1}{6}) \le c(3 - \frac{1}{a}) + (c - b)$, so we see that (36) holds with $n = 6$ and hence $q(6,1) \in \mathcal{R}'(q)$ by Lemma 44. Then $a \le 10$, for otherwise $a \ge 18$ (because $a \in S_{kn}$ and $a \equiv 2 \pmod 4$) and then $q(6,1) \ge 36(18) + 6(6) + 18 = 702 > 462$, so $q(6,1) \notin S_{kn}$ and hence q is not special. If $a = 10$, then $b = 6$ or 10. In the first case $q(6,1) = 396 + c \in S_{kn}$. Since $q(6,1) > 330$, it follows that $q(6,1) = 462$, so $c = 462 - 396 = 66$. But then $c \notin S_{kn}$, contradiction. Similarly, for $b = 10$ we have $q(6,1) = 420 + c \in S_{kn}$, so $c = 462 - 420 = 42$ and hence $q = [10,10,42]$. But $q(1,1) = 62 \notin S_{kn}$, contradiction.

We thus have that $a < 10$. Then $a = b = 6$ and so $q(6,1) = 252 + c \ge 270$. Thus, only $q(6,1) = 330$ or 462 are possible. In the first case we get $c = 330 - 252 = 78$, but $q = [6,6,78]$ is not special since $q(1,1) = 90 \notin S_{kn}$. Similarly, $c = 462 - 252 = 210$ is impossible since then $q(1,1) = 222 \notin S_{kn}$.

We are thus left with the case that $c \le 10$. If $c = 6$, then $q = [6,6,6] \in \mathcal{L}_3$, so assume that $c = 10$. If $b \ge 10$, then $q = [10,10,10] \in \mathcal{L}_3$, so assume $b = 6$. Thus $a = 6$ or 10, so either $q = [6,6,10]$ or $q = [10,6,10]$. But neither of these is special because in the latter case $q(1,1) = 26 \notin S_{kn}$, and in the first case $q(3,1) = 82 \notin S_{kn}$ but $82 \in \mathcal{R}'(q)$ because $82 < 204 = |\Delta(q)|$. This proves the assertion.

Combining Propositions 37, 43, 48, 50 and 51, we obtain:

Theorem 52 *If q is a special idoneal-valued binary form, then $q \sim [a,b,c]$, where $[a,b,c] \in \mathcal{L} := \mathcal{L}_0 \cup \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$.*

Proof. As in the proof of Proposition 43, there is a reduced form $q_1 = [a, b, c]$ with $b \geq 0$ such that $q \sim q_1$. If $\mathrm{cont}(q_1)$ is odd, then $q_1 \in \mathcal{L}_1$ by Proposition 37. Thus, assume that $\mathrm{cont}(q_1)$ is even. If $b > 2$, then $q_1 \in \mathcal{L}_3$ by Proposition 51, and if $b = 2$, then $q_1 \in\in \mathcal{L}_2$ by Proposition 50. If $b = 0$, then by Proposition 43 we must have $\mathrm{cont}(q_1) \equiv 2 \pmod 4$, and so Proposition 48 shows that $q_1 \in \mathcal{L}_0$. Thus, in all cases $q_1 \in \mathcal{L}$, as claimed.

6 The mass formula for ternary forms

In the previous section we saw that if $q(x, y)$ is a special idoneal-valued binary quadratic form, then q is equivalent to one of the 15 forms in $\mathcal{L}$; cf. Theorem 52. This does not imply, however, that the forms in $\mathcal{L}$ are actually special idoneal-valued forms. In order to verify that this is indeed the case, we shall show first that the class number $c(f_q)$ of the ternary form $f_q(x, y, z) = x^2 + 4q(y, z)$ is equal to 1, and then use the theory developed in §4 to deduce from this that q is special; cf. Theorem 13, which is proved in the next section.

In order to show that $c(f_q) = 1$, we shall use the *mass formula* for positive definite ternary forms which is due to Eisenstein, Smith and Brandt; cf. Brandt[1]. This formula gives a simple expression for the *mass* $M(f)$ of a ternary form, which is defined as

$$M(f) \;=\; \sum_{f' \in \mathrm{gen}(f)} \frac{1}{w(f')}, \quad \text{where } w(f') = |\mathrm{Aut}^+(f')|;$$

cf. Smith[17], p. 483. In order to state the result, it is useful to introduce the abbreviation

$$\psi(n, \Delta) \;:=\; n \prod_{p \mid n} \left(1 + \left(\frac{\Delta}{p}\right) \frac{1}{p}\right);$$

here $\Delta \equiv 0$ or $1 \pmod 4$, and $(\frac{\Delta}{p})$ denotes the Kronecker-Legendre symbol. Note that this function generalizes the usual Dedekind function $\psi(n) = \psi(n, 1)$. If $\phi(n)$ denotes the Euler ϕ-function, then the mass formula of Eisenstein/Smith/Brandt for the form f_q is as follows.

Proposition 53 *Let q' be a primitive positive definite binary quadratic form of discriminant $\Delta' = -d'$, and let $t \geq 1$ be an integer. Put $q = tq'$ and $\delta = (d', 2t)$. Then the mass of $f_q(x, y, z) = x^2 + 4q(y, z)$ is given by*

$$M(f_q) \;=\; \frac{1}{24 g(-16t) g(\Delta') \delta^2} \phi(\delta) \psi(\delta) \psi(t, \Delta') \psi(d', -16tr'), \tag{42}$$

where $g(d)$ denotes the number of genera of binary quadratic forms of discriminant d, and $r' \in \mathcal{R}(q')$ is any number represented by q' with $(r', d') = 1$.

Proof. Let f be any primitive positive definite ternary form with primitive positive definite adjoint F, and let I_1 and I_2 be their invariants as defined on p. 316 of [1]. Let r_f (respectively, r_F) be a number represented by f with $(r_f, I_1) = 1$ (respectively, by F with $(r_F, I_2) = 1$). Then the mass formula on p. 316 of Brandt[1] is

$$M(f) = \frac{\varkappa I}{6 \cdot 2^{\nu}} \prod_{p|(I_1,I_2)} \left(1 - \frac{1}{p^2}\right) \prod_{p|I} \left(1 + \left(\frac{I_2 r_f}{p}\right)\frac{1}{p}\right)\left(1 + \left(\frac{I_1 r_F}{p}\right)\frac{1}{p}\right), \tag{43}$$

where $I = I_1 I_2/16$, $\varkappa \in \{1, \frac{1}{2}, \frac{1}{3}\}$ is as defined on p. 317 of [1] and 2^{ν} denotes the total number of characters attached to f and to F. Thus, $2^{\nu} = 2^{\nu_1}2^{\nu_2}$, where $2^{\nu_k} = [(\mathbb{Z}/I_k\mathbb{Z})^{\times} : ((\mathbb{Z}/I_k\mathbb{Z})^{\times})^2]$, for $k = 1, 2$. Note that 2^{ν_k} equals the total number of factorizations of I_k into prime discriminants, and so this definition of 2^{ν_k} agrees with that of Brandt[2], p. 339. In addition, we observe that by Gauss's genus theory we have $2^{\nu_k} = 2g(I_k)$.

We now apply this formula to $f = f_q$. For this, we need to determine F, I_1, I_2, etc. To calculate F, recall that if $A(f)$ is the symmetric matrix associated to f (so $f(\vec{x}) = \frac{1}{2}\vec{x}^t A(f)\vec{x}$ as on p. 2 of [18]), then by [18], p. 25, the *adjoint form* $\mathrm{adj}(f)$ of f is given by the formula

$$A(\mathrm{adj}(f)) \;=\; (-2)\mathrm{adj}(A(f)) \;=\; (-2)\det(A(f))A(f)^{-1},$$

and we have $\mathrm{adj}(f) = I_1 F$, where F is positive definite and primitive and $I_1 \in \mathbb{Z}$.

Applying this to $f = f_q$, and writing $q(x, y) = ax^2 + bxy + cy^2 = t(a'x^2 + b'xy + c'y^2) = tq'(x, y)$ and $d = -\Delta(q)$, we have

$$A(f) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 8a & 4b \\ 0 & 4b & 8c \end{pmatrix} \quad \text{and hence} \quad \mathrm{adj}(A(f)) = (-2)\begin{pmatrix} 16d & 0 & 0 \\ 0 & 8c & -4b \\ 0 & -4b & 8a \end{pmatrix}$$

because $\det(A(f)) = 32(4ac - b^2) = 32d$. Thus $\mathrm{adj}(f_q)(x, y, z) = (-2)2(8dx^2 + 4cy^2 - 4byz + 4az^2) = -16tF(x, y, z)$, where $F(x, y, z) := d'tx^2 + c'y^2 - b'yz + a'z^2$. Since F is clearly primitive and positive definite (because q' is), we see that the primitive adjoint of f_q is

$$F(x, y, z) \;=\; d'tx^2 + c'y^2 - b'yz + a'z^2 \;\sim\; d'tx^2 + q'(y, z). \tag{44}$$

In addition, we see that $I_1 = -16t$ (because $\mathrm{adj}(f_q) = -16tF = I_1 F$). Moreover, since f_q has discriminant $\Delta(f_q) = -\frac{1}{2}\det(A(f_q)) = -16d$, it follows from the last line of [1], §5, that $I_2 = 16\Delta(f_q)/I_1^2 = -16^2 d/(16t)^2 = -d/t^2 = \Delta'$, and so

$$I_1 \;=\; -16t \quad \text{and} \quad I_2 \;=\; \Delta'.$$

(Note that above we used a slightly different definition of F, I_1 and I_2 than that given in [1]. However, this gives the same form and invariants because one can check that

the above form $F(x,y,z)$ and invariants I_1 and I_2 do indeed satisfy the two formulae in the middle of p. 316 of [1].)

Since $16|I_1$ we have $\varkappa = 1$ by [1], p. 317. Moreover, since $f_q(1,0,0) = 1$ and $F(0,y,-x) = q'(x,y)$, we see that we can take $r_f = 1$ and $r_F = r'$, where $r' = r_{q'}$ is any number represented by q' with $(d',r') = 1$.

Since the prime divisors of $\delta = (d', 2t)$ are the same as those of $(I_1, I_2) = (16t, d')$, we thus see that the mass formula (43) for f_q becomes

$$\begin{aligned} M(f) &= \frac{td'}{6\cdot 2^\nu}\prod_{p|\delta}\left(1-\frac{1}{p^2}\right)\prod_{p|td'}\left(1+\left(\frac{\Delta'}{p}\right)\frac{1}{p}\right)\left(1+\left(\frac{-16tr'}{p}\right)\frac{1}{p}\right) \\ &= \frac{1}{6\delta^2\cdot 2^\nu}\phi(\delta)\psi(\delta)\psi(t,\Delta')\psi(d',-16tr'), \end{aligned}$$

where the latter equality uses the fact that $\left(1+\left(\frac{\Delta'}{p}\right)\frac{1}{p}\right) = \left(1+\left(\frac{-16tr'}{p}\right)\frac{1}{p}\right) = 1$ when $p|(t,d')$. From this, equation (42) follows immediately because $2^\nu = 4g(I_1)g(I_2) = 4g(-16t)g(\Delta')$, as was mentioned above.

We now want to analyze the *weight* (or mass) $w(f) = |\mathrm{Aut}^+(f)|$ of the form $f = f_q$. For this we shall prove the following general result.

Proposition 54 *If q_1 and q_2 are two positive definite binary quadratic forms, then we have a bijection*

$$\mathrm{Isom}(f_{q_1}, f_{q_2}) \simeq \{\pm 1\}\times \mathrm{Isom}(q_1,q_2), \tag{45}$$

where $\mathrm{Isom}(\cdot,\cdot)$ *denotes the set of isometries between two forms. In particular, for any positive binary form q we have $c(f_q) \geq c(q)$ and $wt(f_q) = |\mathrm{Aut}(q)|$.*

Proof. Let e_1, e_2, e_3 be the standard basis of $M := \mathbb{Z}^3$, and put $M_1 = \mathbb{Z}e_1$ and $M_2 = \mathbb{Z}e_2 + \mathbb{Z}e_3$. Then $f_{q_i}(xe_1+ye_3+ze_3) = x^2+4q_i(y,z)$, so $(M_1)^\perp_{q_i} = M_2$ and $(f_{q_i})_{|M_2} = 4q_i$, for $i = 1,2$. Thus, if $\varphi \in \mathrm{Isom}(q_1,q_2) = \{\varphi \in \mathrm{Aut}(M_2) = \mathrm{GL}_2(\mathbb{Z}) : q_1 = q_2\circ\varphi\}$, and if $\varepsilon = \pm 1$, then $\varepsilon id_{M_1}\oplus\varphi \in \mathrm{Isom}(f_{q_1}, f_{q_2}) = \{\varphi \in \mathrm{Aut}(M) : f_{q_1} = f_{q_2}\circ\varphi\}$, and so the rule $(\varepsilon,\varphi)\mapsto \varepsilon id_{M_1}\oplus\varphi$ defines an injection $\{\pm\}\times\mathrm{Isom}(q_1,q_2)\to\mathrm{Isom}(f_{q_1},f_{q_2})$.

To show that this map is also surjective, note first that for $m \in M$ we have that $f_{q_i}(m) = 1 \Leftrightarrow m = \pm e_1$ because $4q_i(y,z) \geq 4$ for $(y,z)\neq(0,0)$. Thus, if $\varphi \in \mathrm{Isom}(f_{q_1}, f_{q_2})$, then $f_{q_2}(\varphi(e_1)) = f_{q_1}(e_1) = 1$, and so $\varphi(e_1) = \pm e_1$. It thus follows that $\varphi(M_2) = \varphi((M_1)^\perp_{q_1}) = (M_1)^\perp_{q_2} = M_2$, so $\varphi_{|M_2} \in \mathrm{Isom}(q_1,q_2)$, and hence $\varphi = \pm id_{M_1}\oplus\varphi_{|M_2}$. Thus, the above map is surjective and hence bijective.

From (45) we see that the natural map $\mathrm{gen}(q)\to\mathrm{gen}(f_q)$ (given by $q_1\mapsto f_{q_1}$, for $q_1\in\mathrm{gen}(q)$) is injective, and so $c(q) = \#\mathrm{gen}(q) \leq \#\mathrm{gen}(f_q) = c(f_q)$.

To verify the last assertion, it is enough to show that $|\mathrm{Aut}^+(f_q)| = |\mathrm{Aut}(q)|$ (because $wt(f_q) = |\mathrm{Aut}^+(f_q)|$), and this follows immediately from (45) together with the observation that if $\alpha\in\mathrm{Aut}(q)$, then there is a unique choice of sign $\varepsilon\in\{\pm1\}$ such that $\det(\varepsilon id_{M_1}\oplus\alpha) = 1$, i.e. such that $\varepsilon id_{M_1}\oplus\alpha\in\mathrm{Aut}^+(f_q)$.

Corollary 55 *Let q' be a primitive positive definite binary quadratic form of discriminant Δ' and put $q = tq'$, where $t \geq 1$. Then*

$$wt(f_q) \;=\; \begin{cases} 12 & \text{if } \Delta' = -3, \\ 8 & \text{if } \Delta' = -4, \\ 4 & \text{if } \Delta' < -4 \text{ and } q' \text{ is ambiguous}, \\ 2 & \text{if } \Delta' < -4 \text{ and } q' \text{ is not ambiguous}. \end{cases} \tag{46}$$

Proof. By Proposition 54 we have $wt(f_q) = |\mathrm{Aut}(q)| = |\mathrm{Aut}(q')|$. Now it is well-known that $|\mathrm{Aut}(q')| = \varepsilon|\mathrm{Aut}^+(q')|$, where $\varepsilon = 2$ if q is ambiguous, and $\varepsilon = 1$ otherwise (cf. e.g. Jones[9], p. 147). Since $|\mathrm{Aut}^+(q')| = 6$ and 4 for $\Delta = -3$ and -4, respectively, and $|\mathrm{Aut}^+(q')| = 2$ for $\Delta < -4$, the formula (46) follows.

We are now ready to prove the main result of this section.

Proposition 56 *For every $q \in \mathcal{L}$ we have $M(f_q) = 1/wt(f_q)$, and so $c(f_q) = 1$.*

Proof. We shall apply the mass formula (42) to the form $q = tq' \in \mathcal{L}$. Since each form q' except $q' = [2, 0, 3]$ represents 1, we can take $r' = 1$ for all except for the last, where we can take $r' = 5$. To evaluate the right hand side of (42), note that for any discriminant Δ we have that

$$g(\Delta) \;=\; 2^{\omega(\Delta)-1+\varepsilon(\Delta)}, \tag{47}$$

where $\omega(\Delta)$ denotes the number of distinct prime divisors of Δ and $\varepsilon(\Delta) = 1$ if $\Delta \equiv 0 \,(\mathrm{mod}\, 32)$, $\varepsilon = -1$ if $\Delta \equiv 4 \,(\mathrm{mod}\, 16)$ and $\varepsilon(\Delta) = 0$ otherwise; cf. e.g. [12], §2.2.

Now if we let ν^* be defined by $2^{\nu^*} = g(-16t)g(\Delta')$ and put $\phi\psi = \phi(\delta)\psi(\delta)$, $\psi_1 = \psi(t, \Delta')$ and $\psi_2 = \psi(d', -16tr')$, then the quantities appearing on the right hand side of (42) for $q \in \mathcal{L}$ are given in the Table 1 below.

Since all the forms q' here are ambiguous, we see from Table 1 and (46) that $M(f_q) = 1/wt(f_q)$, for all $q \in \mathcal{L}$. Now it is clear from the definition that

$$M(f_q) \;\geq\; 1/wt(f_q) \quad \text{and} \quad M(f_q) \;=\; 1/wt(f_q) \;\Leftrightarrow\; \#\mathrm{gen}(f_q) = 1,$$

and so we obtain from this that $c(f_q) = \#\mathrm{gen}(f_q) = 1$, for all $q \in \mathcal{L}$.

Remark 57 It is perhaps worthwhile to mention that the forms q which are equivalent to those in $\mathcal{L}$ are not the only binary forms q for which $c(f_q) = 1$ (so the "converse" of Proposition 56 is false). Indeed, the forms $q \in \{[1, 0, 2], [1, 0, 3], [1, 0, 6], [3, 0, 3]\}$ also satisfy $c(f_q) = 1$. But each of these represents an integer $n \equiv 3 \,(\mathrm{mod}\, 4)$ (with $n < |\Delta(q)|$), so they cannot be special idoneal-valued forms. Note that such forms are excluded from consideration in the hypothesis of Theorem 13, and hence this shows that this extra hypothesis is necessary for the validity of Theorem 13.

q	d'	t	δ	ν^*	$\phi\psi$	ψ_1	ψ_2	$M(f_q)^{-1}$
$[1,1,1]$	3	1	1	0	1	1	2	12
$[2,2,2]$	3	2	1	1	1	1	4	12
$[4,4,4]$	3	4	1	1	1	2	2	12
$[6,6,6]$	3	6	3	2	8	3	3	12
$[10,10,10]$	3	10	1	2	1	4	2	12
$[1,0,1]$	4	1	2	0	3	1	4	8
$[2,0,2]$	4	2	4	1	12	2	4	8
$[6,0,6]$	4	6	4	2	12	4	4	8
$[1,1,2]$	7	1	1	0	1	1	6	4
$[1,1,4]$	15	1	1	1	1	1	12	4
$[2,2,6]$	11	2	1	1	1	1	12	4
$[2,2,18]$	35	2	1	2	1	1	24	4
$[2,0,4]$	8	2	4	1	12	2	8	4
$[2,0,10]$	20	2	4	2	12	2	16	4
$[4,0,6]$	12	2	4	1	12	2	8	4

Table 1: Evaluating the mass formula for $q \in \mathcal{L}$.

7 Proofs of the main results

We are now ready to put the above results together to prove the main theorems of this paper. We begin with the main theorem on quadratic forms.

Proof of Theorems 6 and 13. (i) $\Rightarrow$ (ii): Trivial, since $f_q \to 1$.

(ii) $\Rightarrow$ (iii): Here we use the hypothesis that $\mathcal{P}(Q) = \mathcal{P}(Q)^{odd}$. (Note that by Remark 33 this hypothesis is equivalent to the condition that either $\Delta \equiv 1 \pmod 4$ or that $q \not\to n$, for any $n \equiv 3 \pmod 4$). Thus, if $\theta \in \mathcal{P}(Q) = \mathcal{P}(Q)^{odd}$, then by Corollary 29 we have that $Q_\theta \in \mathrm{gen}(f_q)$ and so it follows from (ii) that $Q_\theta \to 1$.

(iii) $\Rightarrow$ (iv): Corollary 36.

(iv) $\Rightarrow$ (v): Theorem 52.

(v) $\Rightarrow$ (i): Proposition 56.

As was already explained after the statement of Theorem 13, this theorem, together with Corollary 8, immediately implies Theorem 2 of the introduction.

We next prove Corollary 3, which requires some results from [13].

Proof of Corollary 3. Suppose that A/K is a CM abelian product surface, i.e. suppose that $A \sim E \times E$, for some CM elliptic curve E/K. Then by [13], Theorem 2, we have that $A \simeq E_1 \times E_2$, for some elliptic curves E_i/K. Now by Theorem 2 we know

that $E_1 \times E_2$ does not contain a genus 2 curve if and only if $q_{E_1,E_2} \sim q$, with $q \in \mathcal{L}$. Then by (6) we have that $q_A \sim xy \perp (-q_{E_1,E_2}) \sim xy \perp (-q)$. Write $q = tq'$ with q' primitive and $t \geq 1$.

Now by [13], Theorem 69 (and its proof), there is a CM abelian product surface A/K with $q_A \sim xy \perp (-q)$ if and only if there is a CM elliptic curve E'/K with $\Delta_{E'} := \Delta(q_{E',E'}) = \Delta(q)$. If this is the case, then by [13], Corollary 68, the number N_q of isomorphism classes of abelian product surfaces A with $q_A \sim xy \perp (-q)$ is given by $N_q = h(\Delta')/g(\Delta')$, where $\Delta' = \Delta(q')$ and $h(\Delta')$ denotes the usual class number of forms of discriminant Δ' (and $g(\Delta')$ denotes, as in §6, the number of genera). Since for $q \in \mathcal{L}$ we have that $c(f_q) = 1$ by Proposition 56, it follows from Proposition 54 that also $c(q) = 1$ and hence that $h(\Delta')/g(\Delta') = 1$. Thus, for a given $q \in \mathcal{L}$, there is at most one isomorphism class of surfaces A/K such that $q_A \sim xy \perp (-q)$ and hence there are at most 15 such surfaces (up to isomorphism).

Note that if $\mathrm{char}(K) = 0$, then for each discriminant $\Delta < 0$ there is a CM elliptic curve E'/K with $\Delta_{E'} = \Delta$ (cf. [13], Proposition 33(a)), and so the above argument shows that there are precisely 15 such non-isomorphic surfaces.

Remark 58 It is not difficult to refine the above argument to determine how many exceptional surfaces exist when $\mathrm{char}(K) = p \neq 0$. Indeed, since a CM elliptic curve E/K with $\Delta_E = \Delta$ exists if and only if $(\frac{\Delta}{p}) = 1$ (cf. [13], Proposition 33(b)), it follows easily from the above proof that the number $Ex(K)$ of exceptional CM product surfaces over K is given by

$$Ex(K) = \#(\mathcal{L}_p), \quad \text{where } \mathcal{L}_p \ = \ \left\{ q \in \mathcal{L} : \left(\tfrac{\Delta(q)}{p}\right) = 1 \right\}.$$

From this we see that $Ex(K)$ determined by suitable congruence conditions on $p = \mathrm{char}(K)$. In particular, there are infinitely many characteristics p for which no exceptional surfaces exist, i.e. $Ex(K) = 0$ (the smallest is $p = 479$) and there are infintely many for which all 15 surfaces exist, i.e. $Ex(K) = 15$ (the smallest is $p = 2689$). Similarly, since $\#\mathcal{L}_2 = 2$, $\#\mathcal{L}_3 = 4$ and $\#\mathcal{L}_5 = 5$, we see that there are precisely $2, 4,$ and 5 exceptional surfaces when $\mathrm{char}(K) = 2, 3,$ and 5, respectively.

By using the theory of [13], the exceptional surfaces can be written down fairly explicitly. Here we use the method due to Deuring (see the reference in [13]) which associates to each ideal I of $\mathrm{End}(E)$ a finite subgroup scheme $H(I)$ of E.

Corollary 59 *Let $q \in \mathcal{L}$ and suppose that there exists an elliptic curve E/K with $\Delta_E = \Delta := \Delta(q)$. Fix an isomorphism $\mathrm{End}(E) \simeq R_\Delta := \mathbb{Z} + \mathbb{Z}\frac{\Delta+\sqrt{\Delta}}{2}$, and put $c = \mathrm{cont}(q)$. Then the unique exceptional surface A_q/K with $q_{A_q} \sim xy \perp (-q)$ is given by*

$$A_q \ = \ E \times E/H(I_q), \quad \textit{where } I_q = \begin{cases} cR_{\Delta/c^2} & \textit{if } \Delta \neq -96 \\ 4\mathbb{Z} + \sqrt{-24}\mathbb{Z} & \textit{if } \Delta = -96. \end{cases}$$

Proof. In view of the bijection of [13], Theorem 65 (see also [13], Remark 66), together with equations (103) and (83) of [13], it is enough to show that $q \sim [R(I) : R]q^+_{I_q}$, where $q^+_{I_q}$ denotes the equivalence class of (primitive) forms associated to the lattice (ideal) I_q of $R = R_\Delta$. Now if $\Delta(q) \neq -96$, then $q \sim c1_{\Delta'}$, where $\Delta' = \Delta/c^2$, and so the desired equivalence is clear in this case. If $\Delta(q) = -96$, then $q \sim [4, 0, 6]$, and it is easy to see that here $q^+_{I_q} \sim [2, 0, 3]$ and so the result is true here as well.

Remark 60 If $K = \mathbb{C}$, then it follows from Corollary 59 (and [13], Proposition 26) that the exceptional surfaces A_q with $q \in \mathcal{L}$ have a very simple analytic description:

$$A_q \simeq \mathbb{C}/R_\Delta \times \mathbb{C}/L_q, \quad \text{where } L_q = \begin{cases} R_{\Delta/c^2} & \text{if } \Delta \neq -96, \\ 2\mathbb{Z} + \sqrt{-6}\mathbb{Z} & \text{if } \Delta = -96. \end{cases}$$

Here, as before, $\Delta = \Delta(q)$, $c = \mathrm{cont}(q)$ and $R_\Delta = \mathbb{Z} + \mathbb{Z}\frac{\Delta+\sqrt{\Delta}}{2}$.

We now turn to the proof of Corollary 4. This will we be deduced from the following more precise statement.

Theorem 61 *Let A/K_0 be an abelian surface such that A is isogenous to $E \times E$, where E/K_0 is a CM elliptic curve with* $\mathrm{rank}(\mathrm{End}_{K_0}(E)) = 2$. *If $\Delta(A)|\Delta_E$, then there exist elliptic curves E_1 and E_2/K_0 such that $A \simeq E_1 \times E_2$, and the following conditions are equivalent:*

(i) *There is a curve C/K_0 such that $J_C \simeq A \simeq E_1 \times E_2$;*

(i′) *There is a genus 2 curve on $A \simeq E_1 \times E_2$;*

(ii) *q_A is not equivalent to $xy \perp (-q)$, for any $q \in \mathcal{L}$;*

(iii) *q_{E_1,E_2} is not equivalent to any $q \in \mathcal{L}$.*

Remark 62 If K is algebraically closed or if K is a finite field, then the condition that $\Delta(A)|\Delta_E$ is unncessary, for in those cases we can use Theorem 2 of [13] in place of Theorem 69 in the proof below to obtain the same conclusion.

Proof of Theorem 61. The existence of E_1 and E_2 with $A \simeq E_1 \times E_2$ follows directly from [13], Theorem 69. It thus remains to show that the conditions (i) – (iii) are equivalent.

(i) $\Rightarrow$ (iii): Let $K = \overline{K}_0$ be the algebraic closure of K_0 and write $\overline{E}_i = E_i \otimes K$. The hypothesis implies that $\mathrm{Hom}(E_1, E_2) = \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$, and so $q_{E_1,E_2} \sim q_{\overline{E}_1,\overline{E}_2}$. Since $\overline{C} = C \otimes K$ is a genus 2 curve on $J_{\overline{C}} \simeq \overline{E}_1 \times \overline{E}_2$, it follows from Theorem 2 that q_{E_1,E_2} cannot be equivalent to any $q \in \mathcal{L}$.

(iii) $\Rightarrow$ (ii): Put $\overline{A} = A \otimes K = \overline{E}_1 \times \overline{E}_2$. Then by (48) below we have $\mathrm{NS}(A) = \mathrm{NS}(\overline{A})$, and so by (6) (applied to $\overline{A}$) we have $q_A \sim q_{\overline{A}} \sim xy \perp (-q_{\overline{E}_1,\overline{E}_2}) \sim xy \perp$

$(-q_{E_1,E_2})$. Now suppose that (iii) is false, i.e. that $q_A \sim xy \perp (-q)$, for some $q \in \mathcal{L}$. Then by Corollary 26 we know that $q_{E_1,E_2} \in \mathrm{gen}(q)$. But for $q \in \mathcal{L}$ we have $c(q) = 1$ (cf. proof of Corollary 3), and so $q_{E_1,E_2} \sim q$, which is contrary to the hypothesis (ii).

(ii) $\Rightarrow$ (i′): If (ii) holds, then it is clear that also (iii) holds because if $q_{E_1,E_2} \sim q$, then $q_A \sim xy \perp (-q_{E_1,E_2}) \sim xy \perp (-q)$, contradiction. Thus, by Theorem 2 (applied to $\overline{A} \simeq \overline{E}_1 \times \overline{E}_2$), we see that there exists a genus 2 curve $\overline{C}$ on $\overline{A}$. By Lemma 63 below we then also have a genus 2 curve on A, and so (i′) holds.

(i′) $\Rightarrow$ (i): This follows from Weil[21], Satz 2.

In the above proof we used the following fact.

Lemma 63 *Let E_1 and E_2 be elliptic curves over a field K_0, and suppose that $\mathrm{Hom}(E_1, E_2) = \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$, where $\overline{E}_i = E_i \otimes K$ and K is the algebraic closure of K_0. If $\overline{C}$ is genus 2 curve on $\overline{A} := \overline{E}_1 \times \overline{E}_2$, then there exists a genus 2 curve C on $A = E_1 \times E_2$ such that $C \otimes K$ is a translate of $\overline{C}$.*

Proof. We first show that

$$\overline{D} \in \mathrm{Div}(\overline{A}) \quad \Rightarrow \quad \exists D \in \mathrm{Div}(A) \text{ such that } D \otimes K \equiv \overline{D}, \tag{48}$$

where $D \otimes K$ denotes the pullback of the divisor D under base change, and $\equiv$ denotes numerical equivalence (as in §2). Indeed, let $\theta_i = pr_i^*(0_{E_i}) \in \mathrm{Div}(A)$ and $\overline{\theta}_i = \theta_i \otimes K = pr_i^*(0_{\overline{E}_i}) \in \mathrm{Div}(\overline{A})$, for $i = 1, 2$. Then by the fundamental identification $\mathrm{NS}(\overline{A}) \simeq \mathbb{Z}^2 \oplus \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$ (cf. [11], Proposition 22), there exist integers $a, b \in \mathbb{Z}$ and $\overline{h} \in \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$ such that $\overline{D} \equiv a\overline{\theta}_1 + b\overline{\theta}_2 + \Gamma_{\overline{h}}$, where $\Gamma_{\overline{h}}$ denotes the graph of $\overline{h}$. By hypothesis, there is an $h \in \mathrm{Hom}(E_1, E_2)$ such that $h \otimes K = \overline{h}$. Thus, if we put $D = a\theta_1 + b\overline{\theta}_2 + \Gamma_h \in \mathrm{Div}(A)$, then $D \otimes K = a\overline{\theta}_1 + b\overline{\theta}_2 + \Gamma_{\overline{h}}$, and so (48) follows.

Applying this to $\overline{D} = \overline{C}$, we thus see that there exists $D \in \mathrm{Div}(A)$ such that $D \otimes K \equiv \overline{C}$. Since $\overline{C}^2 = 2$ by the adjunction formula, we conclude from the Riemann-Roch theorem on $\overline{A}$ (cf. Mumford[15], p. 150) that $\overline{C}$ defines a principal polarization and that hence $D \otimes K \sim \overline{C}_x$, for some $x \in \overline{A}(K)$. Thus $\dim_{K_0} H^0(A, \mathcal{O}(D)) = \dim_K H^0(\overline{A}, \mathcal{O}(D \otimes K)) = 1$ (the latter by Riemann-Roch and the Vanishing Theorem; cf. [15], p. 150), and hence $D \sim C$, for a unique effective divisor $C \geq 0$, $C \in \mathrm{Div}(A)$. By uniqueness we then have $C \otimes K = \overline{C}_x$, which proves the lemma.

Proof of Corollary 4. Since $q_A \sim xy \perp (-q_{E_1,E_2})$, it follows that $\Delta(q_A) = -\Delta(q_{E_1,E_2})$, and so it is clear that Corollary 4 follows from Theorem 61 because the discriminants of the forms in $\mathcal{L}$ are the negative of the numbers listed in (2).

Proof of Theorem 5. As is mentioned on p. 145 of [8], it follows from a result of Deligne that $E_1 \times E_2 \simeq E_0 \times E_0$, where E_0/K is a fixed supersingular curve, so all such product abelian surfaces are isomorphic. Thus, using Weil[21], Satz 2, again, there is a genus 2 curve C on $E_1 \times E_2$ if and only if there is a genus 2 curve C with

$J_C \simeq E_1' \times E_2'$, for some supersingular curves E_1' and E_2', and so the assertion follows immediately from the mass formula of [8], p. 149.

References

[1] H. Brandt, Über das Maß positiver ternärer quadratischer Formen. *Math. Nachr.* **6** (1952), 315–318.

[2] H. Brandt, Zur Zahlentheorie der ternären quadratischen Formen. *Math. Ann.* **124** (1952), 334–342.

[3] J. Buchmann, U. Vollmer, *Binary Quadratic Forms*. Springer, Berlin, 2007.

[4] J. Conway, N. Sloane, *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York, 1988.

[5] F. Grube, Ueber einige Euler'sche Sätze aus der Theorie der quadratischen Formen. *Zeitschrift Math. Physik* **19** (1874), 492–519.

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

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

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

[9] B. Jones, *The Arithmetic Theory of Quadratic Forms.* Carus Math. Monographs, MAA; Wiley, New York, 1950.

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

[11] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. Preprint, 39 pages.

[12] E. Kani, Idoneal numbers and some generalizations. Preprint, 32 pages.

[13] E. Kani, Products of CM-elliptic curves. *Inst. Exp. Math., Essen*, Universität Duisburg-Essen, IEM Preprint No. 2–2009, 54 pages.

[14] J. Milnor, D. Husemoller, *Symmetric Bilinear Forms*. Springer-Verlag, Berlin, 1973.

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

[16] O.T. O'Meara, *Introduction to Quadratic Forms*. Springer-Verlag, Berlin, 1973.

[17] H.J.S. Smith, On the orders and genera of ternary quadratic forms. *Philosoph. Transac.* **142** (1867) = *Collected Math. Papers I*, pp. 455–509.

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

[19] G.L. Watson, The equivalence of quadratic forms. *Can. J. Math.* **9** (1957), 526-548.

[20] G.L. Watson, One-class genera of positive quadratic forms in nine and ten variables. *Mathematika* **25** (1978), 57–67.

[21] A. Weil, Zum Beweis des Torellischen Satzes. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse* 1954, = Œuvres II, pp. 307–327.

[22] P. Weinberger, Exponents of the class groups of complex quadratic fields. *Acta Arith.* **22** (1973), 117–124.